PLEC DE PRESCRIPCIONS TÈCNIQUES REGULADORES DE LA CONTRACTACIÓ DEL PROJECTE PER A LA IMPLANTACIÓ D'UNA OFICINA TÈCNICA DE SEGURETAT I RENOVACIÓ D'ELECTRÒNICA DE XARXA, EN EL MARC DEL PLA DE RECUPERACIÓ, TRANSFORMACIÓ I RESILIÈNCIA –FINANÇAT PER LA UNIÓ EUROPEA – NEXTGENERATIONEU (CONEXP2023000036)

Plaça Major, 1, 5 i 6 08241 MANRESA (Bages) Tel. 93 878 23 00 – Fax 93 878 23 07 E-mail: ajt@ajmanresa.org NIF P-0811200-E

PRESCRIPCIÓ PRIMERA: INTRODUCCIÓ 3
PRESCRIPCIÓ SEGONA: ABAST DEL CONTRACTE....3
PRESCRIPCIÓ TERCERA: SITUACIÓ ACTUAL....4
3.1 Comunicacions perimetrals:....4
3.2 Seguretat perimetral: 4
3.3 Electrònica de xarxa perimetral: 5
3.4 Infraestructura de xarxa local de les seus:....5
3.5 Seguretat local a punt final (antivirus local): 5
3.6 Controladors de domini:....5
3.7 Documentació adjunta:....5
PRESCRIPCIÓ QUARTA: OBJECTE DEL CONTRACTE....6
4.1 Implantació d'una oficina tècnica de seguretat (OTS).....6
4.2 Renovació de l'electrònica de xarxa relacionada.....13
4.3 Llicències i programari 16
PRESCRIPCIÓ CINQUENA: MILLORES QUE ELS LICITADORS PODEN OFERIR ÚNICA I EXCLUSIVAMENT PER VALORAR ELS CRITERIS D'ADJUDICACIÓ QUANTIFICABLES AUTOMÀTICAMENT A INCLOURE EN EL SOBRE 3, AQUESTES MILLORES NO ES PODRAN INCLOURE A LA MEMÒRIA TÈCNICA QUE CONTINDRÀ EL SOBRE 2: 18
5.2 Doble autenticació.....18
5.3 Acompliment.....18
PRESCRIPCIÓ SISENA: GARANTIES PER PART DE L'ADJUDICATARI:....18
PRESCRIPCIÓ SETENA: CONDICIONS QUE ES REQUEREIXEN PER EXECUTAR EL PROJECTE. 20
PRESCRIPCIÓ VUITENA: DADES I SEGURETAT DEL SISTEMA D'INFORMACIÓ DE L'AJUNTAMENT DE MANRESA. 21

ANNEX1- SITUACIÓ ACTUAL ARQUITECTURA DEL SISTEMA DE SEGURETAT PERIMETRAL CENTRAL I SISTEMES DE CENTRES

ANNEX2- ESPECIFICACIONS TÈCNIQUES DE L'ACTUAL SISTEMA DE SEGURETAT PERIMETRAL.

ANNEX3- INFRAESTRUCTURA D'ELECTRÒNICA DE XARXA ACTUAL.

ANNEX4- CAPACITATS I SISTEMES DE LES COMUNICACIONS I SEUS.

ANNEX5- DESCRIPCIÓ DEL SISTEMA ANTIVIRUS LOCAL ACTUAL.

ANNEX6- PERFIL DE PROTECCIÓ COMMON CRITERIA.

ANNEX7- CCN-STIC-105 CATÀLEG PRODUCTES STIC

Plaça Major, 1, 5 i 6 08241 MANRESA (Bages) Tel. 93 878 23 00 – Fax 93 878 23 07 E-mail: ajt@ajmanresa.org NIF P-0811200-E

PLEC DE PRESCRIPCIONS TÈCNIQUES REGULADORES DE LA CONTRACTACIÓ DEL PROJECTE PER A LA IMPLANTACIÓ D'UNA OFICINA TÈCNICA DE SEGURETAT I RENOVACIÓ D'ELECTRÒNICA DE XARXA, EN EL MARC DEL PLA DE RECUPERACIÓ, TRANSFORMACIÓ I RESILIÈNCIA –FINANÇAT PER LA UNIÓ EUROPEA – NEXTGENERATIONEU (CON.EXP 2023000036)

PRESCRIPCIÓ PRIMERA: INTRODUCCIÓ

A l'Ajuntament de Manresa, es disposa d'un entorn tecnològic cada vegada més ampli i complex, tant per les noves aplicacions que ja estan en producció com per aquelles que s'estan desenvolupant i que seran implementades en breu.

Atesa la necessitat de protegir els sistemes informàtics de pèrdues o robatoris d'informació i d'atacs, així com garantir el rendiment del perímetre de la xarxa, es fa necessària la contractació del servei d'una oficina tècnica de seguretat (OTS), el manteniment de la infraestructura de seguretat perimetral i local i la renovació i manteniment de l'electrònica de xarxa relacionada.

Aquest projecte es basarà en els requeriments normatius de l'Esquema Nacional de Seguretat ENS. Aquesta normativa constitueix els principis bàsics i requisits mínims per a una adequada protecció de la informació. Són objectius d'aquesta normativa, assegurar l'accés, integritat, disponibilitat, autenticitat, confidencialitat, traçabilitat i conservació de les dades.

PRESCRIPCIÓ SEGONA: ABAST DEL CONTRACTE

El present plec de prescripcions tècniques, té com objectiu fixar les bases per a la contractació del servei d'una Oficina Tècnica de Seguretat (OTS), en temes relacionats amb la ciberseguretat, millora i eficiència dels sistemes d'informació. També, adjudicar el manteniment del sistema de seguretat perimetral i local i la renovació i manteniment de l'electrònica de xarxa relacionada amb aquest i les llicències associades.

Els principals eixos a implementar són:

a. Desenvolupar un projecte que enforteixi la ciberseguretat dels sistemes d'informació amb l'objectiu de millora.

b. Garantir la seguretat i estabilitat de les infraestructures, comunicacions i serveis digitals.

c. Millorar les capacitats de detecció, prevenció i resposta davant d'atacs i d'incidents de seguretat.

d. Millorar la seguretat i connectivitat de la plataforma d'accés als llocs de treball amb mobilitat i no presencial.

Plaça Major, 1, 5 i 6 08241 MANRESA (Bages) Tel. 93 878 23 00 – Fax 93 878 23 07 E-mail: ajt@ajmanresa.org NIF P-0811200-E

e. Renovar i mantenir la infraestructura d'electrònica de xarxa relacionada amb el perímetre. Millorar la connectivitat i disponibilitat dels sistemes per al correcte funcionament de noves aplicacions virtuals que actualment estan en procés d'implementació.

f. Garantir els serveis de manteniment de la infraestructura de seguretat del perímetre i les llicències associades.

PRESCRIPCIÓ TERCERA: SITUACIÓ ACTUAL

L'Ajuntament de Manresa té una xarxa de 780 usuaris distribuïts en 21 seus connectades amb fibra òptica a la seu central ubicada a Pl Major 5.

3.1 Comunicacions perimetrals:

L'arquitectura de comunicacions entre les diferents seus i la seu principal respon a una topologia en estrella, centralitzant tots els serveis d'intranet, internet i dades en la seu central ubicada al CPD a Pl. Major 5.

Les comunicacions entre els centres i l'ajuntament es fan amb fibra òptica, amb routers del fabricant Microtick mitjançant VPN. Aquestes comunicacions estan gestionades per l'operadora.

3.2 Seguretat perimetral:

El sistema de seguretat perimetral central es tracta mitjançant un cluster de 2 firewalls treballant amb redundància i alta disponibilitat mode Actiu-Passiu. El sistema actual és del fabricant FORTINET, model Fortigate 601E i Firmware v6.4.12 build 2060 (GA), inclou els serveis de seguretat UTM: control d'aplicacions, control de filtre web, control d'intrusions i antivirus perimetral. Treballa integrat amb els controladors de domini.

Les llicències de seguretat d'aquest equipament caduquen a finals del 2023.

El sistema es complementa amb la plataforma Fortianalyzer VM-64, amb firmware v6.2.9 basat en màquina virtual ubicada localment corrent sobre entorn VmWare Vsphere, per fer les funcions de gestió de logs i de reporting de seguretat.

Les llicències d'aquests equipaments caduquen a finals de 2023.

Una de les seus no connectades a l'ajuntament, concretament, el Casal de joves La Kampana, disposa d'un sistema de seguretat perimetral FortiGate 40F i un punt d'accés del mateix fabricant. FAP-231F-E
Aquest sistema està totalment desvinculat del sistema central.

Les llicències d'aquests equipaments caduquen a finals de 2024.

Plaça Major, 1, 5 i 6 08241 MANRESA (Bages) Tel. 93 878 23 00 – Fax 93 878 23 07 E-mail: ajt@ajmanresa.org NIF P-0811200-E

3.3 Electrònica de xarxa perimetral:

El sistema de seguretat perimetral actual es complementa amb un sistema de 3 conmutadors del fabricant Cisco, concretament 2 conmutadors del model C92001-48t-4g i 1 conmutador de CORE, concretament model cisco WS-C6506-E. La funció d'aquest sistema és connectar el perímetre amb la xarxa interna.
Aquesta infraestructura està en fase d'obsolescència i els ports de comunicació presenten limitació de capacitat de connexió que afecta al rendiment general de la transmissió de dades.

3.4 Infraestructura de xarxa local de les seus:

La infraestructura de la xarxa local de tots els edificis està formada per conmutadors del fabricant Cisco models Cataliyst S2960 i routers del fabricant Microtick.

3.5 Seguretat local a punt final (antivirus local):

El sistema de seguretat local és Trend Micro Cloud One i XDR Vision One amb llicència per a protegir totes les màquines.

Aquestes llicències caduquen a finals del 2023 i seran renovades amb posterioritat i no formen part de l'objecte d'aquest contracte.

3.6 Controladors de domini:

Actualment hi ha dos controladors de domini amb funcionalitats d'Active Directory i DNS amb sistemes operatius windows 2019

3.7 Documentació adjunta:

ANNEX1- Situació actual arquitectura del sistema de seguretat perimetral central i sistemes de centres

ANNEX2- Especificacions tècniques de l'actual sistema de seguretat perimetral.

ANNEX3- Infraestructura d'electrònica de xarxa actual.

ANNEX4- Capacitats i sistemes de les comunicacions i seus.

ANNEX5- Descripció del sistema antivirus local actual.

ANNEX6- Perfil de protecció common criteria.

ANNEX7- CCN-STIC-105 Catálogo Productos STIC

Plaça Major, 1, 5 i 6 08241 MANRESA (Bages) Tel. 93 878 23 00 – Fax 93 878 23 07 E-mail: ajt@ajmanresa.org NIF P-0811200-E

PRESCRIPCIÓ QUARTA: OBJECTE DEL CONTRACTE

Serà objecte del contracte:

4.1 Implantació d'una oficina tècnica de seguretat (OTS).

L'OTS ha de ser un instrument de prevenció i de detecció d'amenaces en la seguretat dels sistemes informàtics, ha de ser l'òrgan responsable de la definició i implementació de les polítiques de seguretat TIC que regiran a l'Ajuntament de Manresa.
Els requeriments hauran d'entendre's com a mínims i d'obligat acompliment. Els licitadors podran millorar-los en les seves propostes.
En qualsevol dels casos, les propostes hauran d'oferir informació detallada sobre les característiques particulars del servei projectat.
Els adjudicataris hauran d'aportar els coneixements, metodologies, recursos humans i tècnics necessaris per assegurar la prestació òptima del servei.

4.1.1 Requeriments dels serveis OTS

Aquests serveis requereixen de l'elaboració d'un pla director de seguretat que inclogui com a mínim els següents objectius:

Fase 1: Pla d'auditoria i consultoria inicial.

Fase 2: Aplicació de correccions bàsiques inicials.

Fase 3: Implantació d'una plataforma de gestió de les incidències dels sistemes i registres de seguretat.

Fase 4: Operació del servei.

Fase 1: Pla d'auditoria i consultoria inicial.

Aquest consistirà en reunir tota la informació necessària per a la correcta prestació del servei.
Aquest estudi tindrà com a màxim 1 mes de durada i s'iniciarà a partir de la data d'entrada en vigor del contracte. A partir d'aquest pla de treball s'iniciarà el servei d'Oficina Tècnica de Seguretat.

L'auditoria inicial ha d'incloure com a mínim les següents tasques:

a. Adquisició del coneixement ple de la infraestructura de xarxa de perímetre i xarxa local.

Plaça Major, 1, 5 i 6 08241 MANRESA (Bages) Tel. 93 878 23 00 – Fax 93 878 23 07 E-mail: ajt@ajmanresa.org NIF P-0811200-E

b. Revisió de la correcta configuració de les polítiques de firewall i de l'antivirus local que tenim en funcionament.

c. Revisió de la sincronització horària de tots els sistemes implicats en la seguretat perimetral.

d. Revisió de la correcta integració del firewall amb els dos controladors de domini.

e. Revisió de la correcta configuració dels agents FSSO i correcta integració amb el Firewall.

A partir de les revisions anterior, elaborar un resum de l'estat actual de seguretat i un pla director d'actuacions que es faran al llarg del període del contracte, definint cronologia d'actuació

Fase 2: Aplicació de correccions.

Dels resultats obtinguts de les revisions i valoracions anteriors es portaran a terme les següents tasques:

a. Aplicació de correccions bàsiques inicials.

b. Aportació de recomanacions per a correccions de nivell superior. (seguretat d'accés a bases de dades, seguretat d'accés a aplicacions i privilegis…)

Fase 3: Implantació d'una plataforma de gestió de les incidències dels sistemes i registres de seguretat.

Per tal de poder portar a terme la monitorització de forma contínua la postura de seguretat de l'organització, identificant, prevenint, detectant, analitzant i responent als incidents de seguretat, l'adjudicatari haurà de proposar un servei de seguretat gestionada SOC bàsic.
Els requeriments mínims per aquest servei són els següents:

a. Subministrament i implantació d'una plataforma de gestió de les incidències de seguretat SIEM. Per aquest punt caldrà definir, desplegar i parametritzar els casos d'ús que es creguin convenients i que com a mínim seran els controladors de domin, els firewalls, el sistema antivirus local/XDR i l'electrònica relacionada amb el perímetre.

b. Serveis d'instal·lació avançada associats als subministres a adquirir. Cal garantir el disseny de la solució amb una correcta instal·lació, funcionament i màxima disponibilitat així com la integració amb els sistemes de monitorització i detecció de seguretat de que disposa l'ajuntament, com per exemple fortianalyzer i plataforma antivirus local.

Plaça Major, 1, 5 i 6 08241 MANRESA (Bages) Tel. 93 878 23 00 – Fax 93 878 23 07 E-mail: ajt@ajmanresa.org NIF P-0811200-E

Per al control de l'electrònica de xarxa es disposa, en el moment de publicar la licitació, de l'eina Cisco Prime. Cal tenir en compte el correcte dimensionament de la capacitat de recollida de logs de la plataforma proposada.

c. La garantia del servei així com la vigència de la plataforma seran durant tota la vigència del contracte.

d. La solució proposada haurà de tenir capacitat per a integrar-se amb les eines del CCN.

e. Es podrà oferir en mode servei, local o cloud.

f. En quant al registre d' incidències de la plataforma de gestió es tindran les següents consideracions:

- Capacitat de guardar un registre d'auditoria per les incidències de seguretat rellevants. Per a cada incidència d'auditoria rellevant s'enregistrarà com a mínim:
  - Data i hora
  - Tipus d' incidència
  - Resultat de la incidència
  - Actuació

- Protecció d'accés no autoritzat dels registres d'auditoria guardats.

- Disposar de sistemes per a preveure possibles pèrdues de registres d'auditoria.

- L'accés a la plataforma de gestió haurà d'identificar de forma única els usuaris i autenticar-los abans de permetre-hi l'accés. Els tècnics de l'ajuntament implicats en aquest projecte tindran accessibilitat i hauran de rebre formació en la seva gestió.

Fase 4: Operació del servei

a. Servei de manteniment i monitoratge del sistema.

El servei de monitoratge i detecció avançada d'amenaces i incidències en temps real requereix la monitorització dels registres d'activitat per a detectar incidències de seguretat crítiques i poder donar una resposta ràpida.
Aquest servei de supervisió i monitorització 24x7 consistirà en portar a terme les activitats següents:

- Supervisió i monitorització en temps real de les incidències de seguretat com a mínim dels sistemes:

Plaça Major, 1, 5 i 6 08241 MANRESA (Bages) Tel. 93 878 23 00 – Fax 93 878 23 07 E-mail: ajt@ajmanresa.org NIF P-0811200-E

- 2 Controladors de Domini.
- 2 Firewalls-fortianalyzer
  - Antivirus
  - Control aplicacions
  - Contingut web
  - IPS
  - DMZ
  - Connexions ssl-VPN
- Antivirus local-XDR.

b. Serveis requerits deduïts de les activitats del monitoratge:

Es defineixen 3 categories de serveis: Serveis reactius, serveis preventius/proactius i serveis de gestió de la qualitat de la seguretat.

- **Serveis reactius.**

  Es tracta de serveis que són activats per un esdeveniment o sol·licitud, com un informe d'un sistema que ha estat compromès, programari maliciós de difusió àmplia, vulnerabilitats de programari o algun altre esdeveniment detectat per un sistema de detecció d'intrusos o d'auditoria.

  Llista de serveis reactius:

  - Generació d'alertes i advertències.
  - Gestió d'incidents i vulnerabilitats.
  - Tractament d'incidents.
  - Resposta a incidents *in situ,* si cal.
  - Suport en la resposta a incidents.
  - Coordinació de la resposta a incidents.

Es requereix per als serveis reactius:

Monitorització i suport les 24 hores del dia els 7 per a gestió d'alarmes crítiques.

- **Serveis preventius/proactius**.

  Es tracta de serveis que ofereixen informació i assistència per ajudar a preparar i protegir de forma anticipada atacs, problemes o

Plaça Major, 1, 5 i 6 08241 MANRESA (Bages) Tel. 93 878 23 00 – Fax 93 878 23 07 E-mail: ajt@ajmanresa.org NIF P-0811200-E

esdeveniments. Aquests serveis redueixen directament el nombre d'incidents futurs tant de seguretat com d'estabilitat dels sistemes.

Llista de serveis preventius:

- Observatori vigència de llicències objecte del contracte.
- Manteniment de la documentació tècnica.
- Avaluació del rendiment i les prestacions del sistema actual per a aconseguir la màxima productivitat i detectar requisits futurs.
- Revisió periòdica de la documentació relativa al servei per a mantenir-la actualitzada.
- Anàlisi i verificació de la correcta definició dels llindars en les alertes de monitoratge per a minimitzar els falsos positius.
- Revisió preventiva dels entorns de sistemes per a informar anticipadament de la necessitat d'aplicar pegats de seguretat o realitzar upgrades per a la resolució de possibles bretxes de seguretat.

Llista de serveis proactius:

- Comunicats.
- Gestió de logs.
- Detecció d'intrusions.
- Pla bàsic d'actuació per la recuperació de l'activitat després de desastres.
- Difusió d'informació relacionada amb la seguretat.
- Seguiment de feines i generació d'informes.

L'adjudicatari del servei proposarà de forma proactiva accions de millora, destinades a resoldre possibles deficiències detectades, que disminueixin les incidències produïdes i evitar que es converteixin en problemes.

Es requereix per als serveis proactius:

- Derivat del pla bàsic d'actuació després de desastre, es portarà a terme l'execució de proves de pla de recuperació de l'activitat. Com a mínim 1 cop durant la vigència del contracte.
- Es farà un comunicat mensual de l'estat general de la seguretat i disponibilitat dels sistemes.
- Es farà un informe mensual de l'activitat de logs obtinguts.
- Es farà una revisió anual de la vigència del firmware i llicències.
- Es farà una reunió semestral per a seguiment de feines i propostes d'evolució i millores.

Plaça Major, 1, 5 i 6 08241 MANRESA (Bages) Tel. 93 878 23 00 – Fax 93 878 23 07 E-mail: ajt@ajmanresa.org NIF P-0811200-E

- **Serveis de gestió de la qualitat de la seguretat.**

  Els serveis relacionats amb la gestió de la qualitat de la seguretat són els que donen suport a diferents serveis ja existents que són independents de la gestió d'incidents, i que tradicionalment estan executats per altres entitats, com per exemple auditories de seguretat de CESICAT.
  També s'inclou en aquests serveis, les possibles consultes en l'àmbit de configuracions de firewall o a nivell de xarxa relacionades amb seguretat.
  Es requereix suport des de l'experiència, per a incrementar la seguretat global de l'organització, identificant riscos, amenaces i debilitats del sistema.
  Aquests serveis podrien formar part de serveis proactius, perquè contribueixen indirectament a reduir el nombre d'incidents però es consideren complementaris.

  Llista de serveis de gestió de la qualitat de la seguretat:

  - Consultoria de dubtes sobre incidents de seguretat de tipus lleu.
  - Suport en configuració, de polítiques de seguretat en plataforma tallafocs de protecció perimetral.
  - Suport en projectes de sistemes on calgui aplicar polítiques de seguretat:

    - Infraestructura de xarxa.
    - Protecció de dades.
    - Seguretat aplicacions.
    - Control d'accessos als sistemes.

c. Tractament dels serveis de gestió i suport d'incidències de seguretat.

Els incidents de seguretat classificats segons el seu risc, es prioritzaran segons el seu nivell, crític, alt i lleu.

Atenció prioritària 24x7 incidències de seguretat:

Per a incidències considerades de nivell crític i alt:

- Aquestes incidències s'enregistraran i s'iniciarà un procés de gestió.
- El temps de resposta serà immediat. (temps de notificació de la incidència)
- La finestra d'actuació serà immediata.

Per a incidències considerades no crítiques:

Plaça Major, 1, 5 i 6 08241 MANRESA (Bages) Tel. 93 878 23 00 – Fax 93 878 23 07 E-mail: ajt@ajmanresa.org NIF P-0811200-E

- S'avaluaran i seran escalades.
- La finestra d'actuació es traslladarà al següent dia laborable.
- Els incidents s'enregistraran i s'iniciarà un procés de gestió.

Atenció a incidències i suport amb SLA de 8x5:

Per a les incidències considerades de nivell lleu:

- Aquestes incidències s'enregistraran i s'iniciarà un procés de gestió.
- El temps de resposta serà immediat. (temps de notificació de la incidència)
- La finestra d'actuació serà al següent dia laborable.

- Es requereixen un mínim de 36 h anuals per donar cobertura a les necessitats del servei 8x5 en format remot.

4.1.2 Tasques de configuració i instal·lació de l'oficina de seguretat OTS

La solució proposada SIEM podrà tenir opció de ser implementada en local, al núvol o com a servei. En qualsevol dels casos, es garantirà la correcta configuració de la plataforma per tal d'ajustar-se als requeriments de capacitat i rendiment sense penalitzar la resta de serveis.
Els serveis relacionats amb la instal·lació, configuració i posterior funcionament de la solució inclouran:

a. Tasques de disseny, desplegament i integració de la solució contractada, tasques que requereixin una configuració personalitzada.

b. Configuració i proves de l'adequada informació dels esdeveniments rellevants als sistemes de monitorització.

c. Transferència de coneixements relacionats amb el procés d'instal·lació i configuració als tècnics de l'ajuntament participants del projecte.

d. Revisió periòdica de les eines instal·lades per a la seva correcta adaptació al cicle actualitzat de l'estat de seguretat.

4.1.3 Actualització i manteniment del programari:

L'empresa adjudicatària haurà d'informar a l'ajuntament de Manresa de les actualitzacions necessàries de firmware dels equips tallafocs i equips complementaris com la còmsola de logs Fortianalyzer, agents FSSO ,

Plaça Major, 1, 5 i 6 08241 MANRESA (Bages) Tel. 93 878 23 00 – Fax 93 878 23 07 E-mail: ajt@ajmanresa.org NIF P-0811200-E

així com del firmware de l'electrònica de xarxa (inclosa en aquest plec) relacionada amb el sistema de seguretat o altres programaris requerits per aquest projecte.
Les actualitzacions d'aquests programaris seran revisades com a mínim anualment i sempre que sigui necessari.
En el cas de coneixement de possibles actualitzacions dels sistemes, aquestes estaran sempre correctament justificades tant si es porten a terme com si no.

4.2 Renovació de l'electrònica de xarxa relacionada.

La renovació de la infraestructura d'electrònica de xarxa relacionada amb el perímetre pretén millorar la connectivitat i disponibilitat dels sistemes per al correcte funcionament de noves aplicacions virtuals que actualment estan en procés d'implementació.

La funció d'aquests equips complementaris és interconnectar el sistema perimetral i la xarxa local.

Caldrà fer un estudi de la infraestructura de xarxa perimetral i proposar una nova arquitectura i uns nous commutadors per tal d'optimitzar al màxim aquest sistema. Caldrà tenir en compte tota la infraestructura connectada a aquest sistema. (Firewalls, sistemes de servidors i electrònica de xarxa d'usuaris)

Es poden fer propostes d'unificació de commutadors tenint en compte la redundància i alta disponibilitat dels sistemes perimetrals.

No és requeriment que els ports d'aquest equip disposin de PoE.

4.2.1 Requeriments de l'electrònica de xarxa relacionada.

Els Requeriments tècnics de la infraestructura complementaria d'electrònica de xarxa- commutadors seran:

a. El sistema proposat haurà de connectar amb tots els equips actualment en producció: perímetre (2 firewall), sistema de servidors i xarxa LAN d'usuaris).

b. El número de ports amb transceptors requerits seran com a mínim els que hi ha actualment descrits a l'ANNEX 3 a més dels següents:

Plaça Major, 1, 5 i 6 08241 MANRESA (Bages) Tel. 93 878 23 00 – Fax 93 878 23 07 E-mail: ajt@ajmanresa.org NIF P-0811200-E

Núm ports+transceptors	connectivitat	Funcionalitat
6 2	10GBSFP+ 1GBaseT	Projecte futur Connexió a sistema d'escriptoris virtuals
4	10GBSFP+	Connexió amb cluster de Firewall (2 per cada firewall)

c. Escalabilitat. Es requereix que el sistema proposat ofereixi escalabilitat per tal de permetre afegir nous equips a la infraestructura preveient un creixement futur.

d. Disposar de redundància/alta disponibilitat de tots els elements: electrònica de xarxa, mòdul de gestió, fonts d'alimentació, mòduls de ventilació.

e. Disposar de fonts d'alimentació d'intercanvi en calent i mòduls de ventilació amb capacitat de distribució de càrrega.

f. Disposar de plataforma de gestió i administració.

g. Es requereix que l'electrònica de xarxa compleix amb els requeriments mínims estipulats de protecció common criteria de CCN-CERT. ANNEX 6.

h. Es requereix que l'electrònica de xarxa compleix amb el catàleg de productes i serveis de seguretat de les TIC considerats per CCN-CERT ANNEX 7.

i. L'equipament proposat estarà vigent, paràmetre (EOL), durant tota la durada del contracte.

j. La vigència del programari relacionat i les llicències associades serà durant tot el període del contracte.

k. Es requeriran tots els cables ethernet necessaris per a connectar els equips actuals diferenciats per colors segons el tipus de sistema o equip connectat, així com els de FO per a connectar el switch amb els 2 firewalls i amb el sistema de'escriptoris virtuals.

4.2.2 Requeriments d'implantació de l'electrònica de xarxa.

Plaça Major, 1, 5 i 6 08241 MANRESA (Bages) Tel. 93 878 23 00 – Fax 93 878 23 07 E-mail: ajt@ajmanresa.org NIF P-0811200-E

Els requeriments per a la implantació dels sistemes de xarxa després la revisió de la infraestructura actual i nova proposta, serà:

a. Anàlisi de la Infraestructura actual i validació del disseny proposat:
    - Revisió de les configuracions actuals i neteja de configuracions obsoletes que no estiguin en funcionament.
    - Inventari de ports utilitzats. Estudi de connexió amb els diferents equips (firewall, commutadors, sistemes de servidors i BD)
    - Verificació de la disponibilitat de tots els transceptors i cables necessaris per a fer les connexions.

b. Subministrament, de tot el maquinari requerit i proposat: commutadors +transceptors , cables de connexió i etiquetatge.

c. Configuració d'accés segur a la plataforma de gestió.

d. El firmware dels equips al final de la implantació serà la última versió estable.

e. Muntatge de maquinari i cablejat al rack ubicat al CPD de PL Major 5.

f. Instal·lació i configuració de tots els elements físics objecte del contracte.

g. Connectivitat i etiquetatge.

h. Verificació del funcionament correcte de l'entorn.

i. Retirada dels commutadors substituïts i cables actuals.

j. Totes les configuracions necessàries per a integrar el sistema a la xarxa. En cap cas es traspassarà la configuració actual, caldrà fer la configuració partint de zero.

k. Configuració de la redundància i alta disponibilitat amb els diferents sistemes: firewall, electrònica de xarxa d'usuaris i de servidors.

l. Revisió de la correcta configuració i connexió amb el sistema de seguretat perimetral firewall, amb els sistemes de servidors i amb l'electrònica de xarxa d'usuaris.

m. Banc de proves de rendiment, alta disponibilitat i redundància.

n. Inventari final, documentació final del projecte.

Plaça Major, 1, 5 i 6 08241 MANRESA (Bages) Tel. 93 878 23 00 – Fax 93 878 23 07 E-mail: ajt@ajmanresa.org NIF P-0811200-E

o. Compromís d'hores de traspàs de coneixement, informació, documentació, etc… a l'equip tècnic de l'ajuntament i a l'empresa amb qui l'ajuntament té contractats els serveis gestionats de suport i monitorització dels servidors.

p. En el cas de ser necessari, realitzar la implantació en horari fora d'hores de treball, s'indicarà dia i hora per tal de no penalitzar la continuïtat del servei.

q. El temps d'inici d'implantació no serà superior als 15 dies a partir del compromís de rebuda del material.

4.3 Llicències i programari

Tots els equips que formen la seguretat perimetral i electrònica de xarxa relacionada porten llicències de programari. Caldrà adquirir/renovar totes les llicències associades així com mantenir la seva vigència al llarg de la durada del contracte. Concretament: per als dos sistemes de seguretat perimetral (Pl Major 5 i casal de joves la kampana)

La gestió de les llicències seran propietat de l'ajuntament de Manresa, garantint un total accés a aquestes per a la seva gestió i administració. El licitador també podrà ser gestor d'aquestes.

4.3.1 Per a la seu central Pl Major 5 (anys 2024, 2025 i 2026)**:**

a. Renovació llicència Programari de seguretat perimetral UTM per a 2 firewalls:
   - FortiGate 601E. Unified Threat Protection (UTP) (IPS,Advanced Malware Protection, Application Control, Web & Video Filtering, Antispam Service, and 24x7 FortiCare).

b. Renovació llicència Programari de supervisió de logs de firewall Fortianalyzer. Aquest estarà dimensionat per a obtenir la recollida de logs de les funcionalitat instal·lades al Firewall Fortigate 601E.
   Upgrade de FortiAnalyzer fins 5 GB/dia i 3 TB. 24x7 FortiCare de FortiAnalyzer (fins 6 GB)

c. Adquisició de llicències de sistema doble autenticació per a 100 usuaris totalment compatible amb el sistema principal de seguretat perimetral central.:
   - Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 100 users. Electronic license certificate.
   - VM Base License supports 100 users. Expand user support to 1 million plus users by using FortiAuthenticator VM Upgrade

Plaça Major, 1, 5 i 6 08241 MANRESA (Bages) Tel. 93 878 23 00 – Fax 93 878 23 07 E-mail: ajt@ajmanresa.org NIF P-0811200-E

License. Unlimited vCPU. Supporting VMware ESXi / ESX, Microsoft Hyper-V, Linux Kernel-based Virtual Machine (KVM) on Virtual Machine Manager and QEMU 2.5.0, and Xen Virtual Machine platforms.
- FortiCare Premium Support (1 - 500 USERS)

4.3.2 Per a la seu Casal de joves la Kampana (anys 2025 i 2026)**:**

- Renovació llicència Programari de seguretat perimetral UTM per a 1 firewalls + 1 AP wifi
  a. FortiGate 40F. Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, Web & Video Filtering, Antispam Service, and 24x7 FortiCare).
  b. FAP-231F-E- FortiCare Premium Support.

L'adjudicatari estarà obligat a lliurar a l'Ajuntament de Manresa la següent documentació a la finalització de la implantació de cada part del projecte:

1. Documentació final de la implantació de l'oficina tècnica de seguretat.

   a. Documentació final de tot el projecte.
   b. Document de protocol a seguir en cas de riscos de ciberseguretat greu, detallant les actuacions per a portar-los a terme.

2. Documentació final de la implantació de l'electrònica de xarxa.

   a. Parametrització, Instal·lació i configuració.
   b. Esquemes definitius de l'arquitectura lògica i física.
   c. Plans de proves realitzades i resultats.
   d. Document de protocol a seguir en cas de fallada dels equips i com es portaria a terme.

3. Manuals i altres materials relacionats amb la transferència de coneixement.

4. Documentació de les llicències objecte del contracte.

PRESCRIPCIÓ CINQUENA: MILLORES QUE ELS LICITADORS PODEN OFERIR ÚNICA I EXCLUSIVAMENT PER VALORAR ELS CRITERIS D'ADJUDICACIÓ QUANTIFICABLES AUTOMÀTICAMENT A INCLOURE EN EL SOBRE 3, AQUESTES MILLORES NO ES PODRAN INCLOURE A LA MEMÒRIA TÈCNICA QUE CONTINDRÀ EL SOBRE 2:

Plaça Major, 1, 5 i 6 08241 MANRESA (Bages) Tel. 93 878 23 00 – Fax 93 878 23 07 E-mail: ajt@ajmanresa.org NIF P-0811200-E

Per tal de contribuir a la millora de la seguretat general de la infraestructura de xarxa de dades de l'Ajuntament els licitadors podran proposar millores que afavoreixin al conjunt del projecte.
Es valoraran altres serveis de valor afegit en el servei de SOC com pot ser servei de Pentesting (conjunt d'atacs simulats permesos i acordats, dirigits als sistemes informàtics) o qualsevol altre que pugui aportar valor al servei.

5.1 Doble autenticació.

Per a complimentar el requeriment de doble autenticació d'accés a la xarxa, es poden oferir sistemes d'autenticació físics amb la possibilitat de treballar amb Fortigate i Fortiautenticator.

5.2 Acompliment.

El maquinari i programari que formin part del projecte ha de complir amb el catàleg de productes i serveis de seguretat de les TIC considerats pel CCN-CERT. Adjunt ANNEX 7 i amb les certificacions dels perfils de common criteria. Adjunt ANNEX 6
Tots els productes o serveis inclosos en el catàleg de productes acrediten que han superat un procés d'avaluació/certificació en el qual s'ha comprovat que implementen, amb cert nivell de garantia, les funcionalitats de seguretat requerides pels requeriments fonamentals de seguretat definits per l'entitat CCN.

Es recorda als licitadors que, en cap cas, podran incloure en el sobre número 1 i 2, cap dada o referència a aquells criteris o aspectes que són objecte de valoració en el sobre número 3; i que d'alguna manera poguessin desvirtuar el secret de les propostes de valoració automàtica (*doctrina de la contaminació documental*).

En cas contrari, la proposta en qüestió serà exclosa de la present licitació.

Els licitadors a l'hora de redactar la proposta tècnica (sobre número 2) han de tenir en compte que no poden i no han d'incloure cap element que es valori o s'ofereixi com a millora dins dels criteris quantificables automàticament (sobre número 3).

PRESCRIPCIÓ SISENA: GARANTIES PER PART DE L'ADJUDICATARI:

L'adjudicatari amb la signatura del contracte garanteix, per a tots els elements objecte del contracte i durant tota la vigència del contracte, el següent:

6.1 El servei de garantia acreditada del fabricant de la vigència al mercat de maquinari i programari relacionat ofert per cobrir com a mínim tota la durada del contracte.

6.2 Per a l'electrònica de xarxa ha de garantir i garanteix l'acreditació per part del fabricant que l'atenció sigui en català/castellà com a mínim al nivell1 de suport.

Plaça Major, 1, 5 i 6 08241 MANRESA (Bages) Tel. 93 878 23 00 – Fax 93 878 23 07 E-mail: ajt@ajmanresa.org NIF P-0811200-E

6.3 L'adjudicatari garanteix i ha de garantir que els inicis de les instal·lacions i configuracions de maquinari es faran tan bon punt es tinguin en disponibilitat i com a màxim en 15 dies a partir de la rebuda del material.

6.4 L'adjudicatari ha de ser partner oficial de tots els productes oferts d'electrònica de xarxa i dels productes de seguretat perimetral objecte del contracte. L'adjudicatari haurà d'acreditar aquest extrem mitjançant l'aportació del corresponent certificat oficial.

6.5 L'adjudicatari, proporcionarà serveis d'instal·lació avançada a través d'experts en ciberseguretat i networking en la solució oferta per aquest.

6.6 L'adjudicatari garanteix i ha de garantir que els tècnics que formin part del projecte tindran experiència com a mínim d'un any en la implantació i gestió de les solucions ofertes, tres anys en implantació i gestió de plataformes de gestió de logs i estar certificats al màxim nivell en aquests tipus de plataformes.

6.7 L'adjudicatari garanteix i ha de garantir que el servei de manteniment de tots els elements objecte del contracte inclourà la possibilitat de fer petits canvis en configuracions. Aquests canvis seran valorats en el moment que sigui necessari.

6.8 L'adjudicatari donarà garantia i suport en relació a tots els serveis instal·lats i reconfigurats durant un any a partir de la data de tancament del projecte. Això és vàlid per als serveis de reconfiguració / adaptació de l'electrònica de xarxa.

6.9 L'adjudicatari garanteix i ha de de garantir un servei de disponibilitat en horari 24 hores al dia durant els 7 dies de la setmana de la plataforma de gestió de la seguretat així com el seu correcte funcionament.

6.10 L'adjudicatari garanteix i ha de garantir que el projecte proposat tindrà les capacitats de poder ser integrat amb les eines del CCN-CERT.

6.11 L'adjudicatari previ a la signatura del contracte ha d'aportar totes les acreditacions de certificacions tant a nivell de plataformes com de tècnics implicats. Les certificacions hauran d'estar vigents durant tota la durada del contracte. En el cas de que algun dels tècnics que formin part de l'equip deixin de prestar serveis o deixi de formar part de l'empresa, el tècnic substitut comptarà com a mínim amb el mateix grau de certificació.

6.12 Els licitadors i els adjudicataris han d'acreditar la seva categoria en certificació ENS. Hauran de disposar, com a mínim, de la categoria de certificació de nivell MITJÀ.

6.13 L'adjudicatari haurà de fer el traspàs del coneixement al personal tècnic municipal assignat a la gestió de la seguretat a més de l'empresa contractada per als serveis gestionats de l'ajuntament.

Plaça Major, 1, 5 i 6 08241 MANRESA (Bages) Tel. 93 878 23 00 – Fax 93 878 23 07 E-mail: ajt@ajmanresa.org NIF P-0811200-E

PRESCRIPCIÓ SETENA: CONDICIONS QUE ES REQUEREIXEN PER EXECUTAR EL PROJECTE.

7.1 Si la naturalesa de les feines ho requereix, aquestes seran realitzades a les instal·lacions de l'ajuntament.

7.2 Les actuacions realitzades han d'assegurar la no interrupció del servei operatiu, per tant, es faran en dates i horaris convinguts i autoritzats. Podria incloure caps de setmana.

7.3 Equip tècnic: L'equip tècnic que portarà a terme el projecte estarà format per perfils multidisciplinaris, essent el detall de cada perfil:

- Coordinador del projecte: L'adjudicatari nomenarà a un gestor tècnic que serà l'interlocutor amb els equips de treball. Serà un consultor amb experiència amb seguretat i capacitació per portar a terme les necessitats particulars el projecte.
- Els membres de l'equip tècnic encarregat de definir l'arquitectura i configuració de la plataforma de seguretat seran experts en seguretat. Es requereix que tinguin al menys una experiència de dos anys en disseny, desplegament i configuració de les eines a desplegar.
- Els membres de l'equip tècnic encarregat de la renovació de l'electrònica de xarxa seran experts en sistemes de xarxes. Es requereix que tinguin al menys una experiència de dos anys en disseny, desplegament i configuració del sistema proposat.
- L'Ajuntament de Manresa assignarà un o més tècnics per a portar a terme aquest projecte així com efectuar tasques de seguiment i cooperació durant la durada del contracte.

7.4 Sistema de seguiment i control del projecte: El model de seguiment i control del projecte permet garantir la comunicació i interlocució amb les diferents parts. L'empresa adjudicatària definirà aquest model de seguiment i control. Inclourà la definició d'un calendari i els indicadors per fer el seguiment.

PRESCRIPCIÓ VUITENA: DADES I SEGURETAT DEL SISTEMA D'INFORMACIÓ DE L'AJUNTAMENT DE MANRESA.

Les dades analitzades pels licitadors i per l'empresa adjudicatària no contenen ni contindran informació de caràcter personal ni afecta ni afectarà a la seguretat dels Sistemes d'Informació de l'Ajuntament de Manresa.

Montserrat Clotet Masana
Regidora de Recursos Humans i Govern Obert

Plaça Major, 1, 5 i 6 08241 MANRESA (Bages) Tel. 93 878 23 00 – Fax 93 878 23 07 E-mail: ajt@ajmanresa.org NIF P-0811200-E

ANNEX1: Situació actual arquitectura del sistema de seguretat perimetral central i sistemes de centres.

1-Arquitectura General

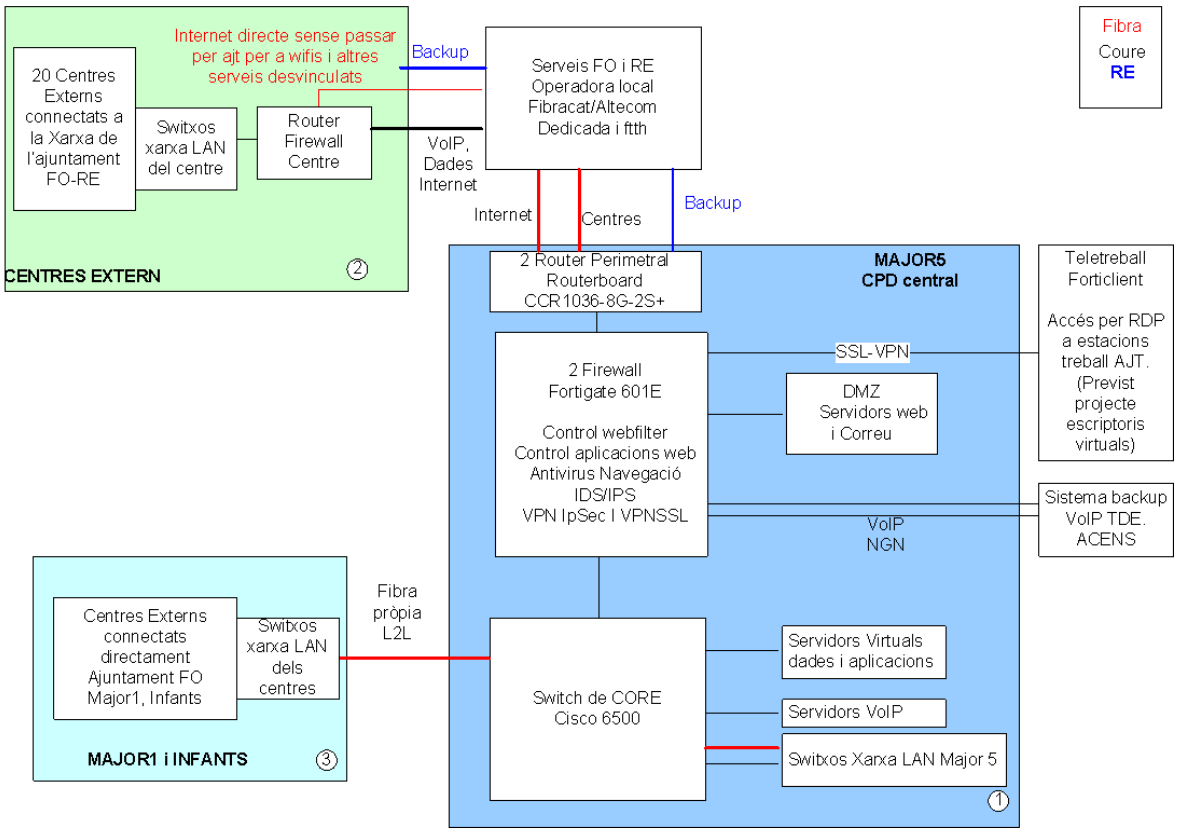
2-Arquitectura actual del sistema de seguretat perimetral Central.

3-Arquitectura actual de xarxa de les seus.

3.1-Seus connectades a l'ajuntament.

3.2-Seus no connectades a l'ajuntament.

1-Arquitectura General



Zona 1:
Aquesta infraestructura es troba ubicada al CPD a l'edifici Pl Major 5. És el nucli dels serveis i comunicacions.

Zona 2:
La zona 2 defineix els centres externs.

Zona 3:

La zona 3 defineix els centres connectats amb fibra dedicada propietat de l'ajuntament. Concretament existeix per als edificis Infants i Pl Major 1

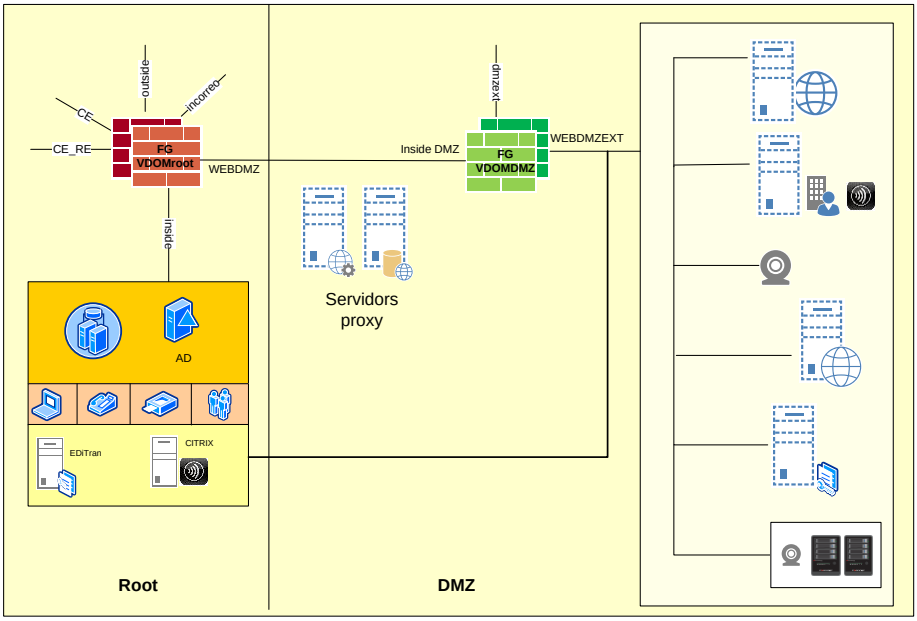
2-Arquitectura del sistema de seguretat perimetral Central.

El sistema actual és un equipament del fabricant Fortinet, en concret, 2 apliance Fortigate 601E amb Firmware v6.4.12 treballant en alta disponibilitat Actiu-Passiu i amb les funcionalitats activades: IPS, control d'aplicacions, antivirus perimetral, web filtering, forticlient VPN SSL, VPN IPSec, DMZ i complementat amb la Solució de FortiAnalyzer VM-64, amb firmware v6.2.9 basat en màquina virtual ubicada localment que corre sobre entorn VmWare Vsphere, per fer les funcions de gestió de logs i de reporting de seguretat. Integrat amb els controladors de domini.

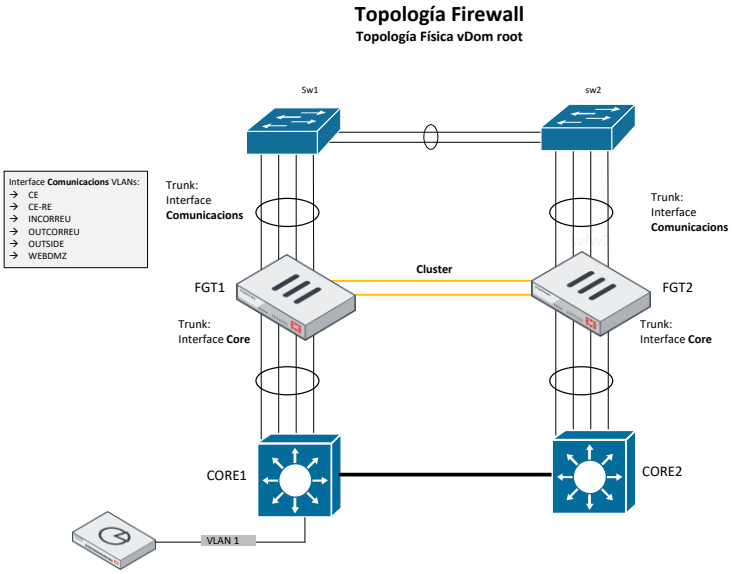
La topologia de xarxa de tots els edificis connectats a l'ajuntament és en estrella i tots els serveis estan centralitzats a la seu principal ubicada al CPD de Pl major 5
Totes les seus estan connectades a la seu central a través de fibra òptica (alguns, directes i propietat de l'ajuntament (Infants i major 1), altres amb fibra dedicada de l'operadora i altres ftth de l'operadora i tots ells amb redundància de Ràdio-enllaç.

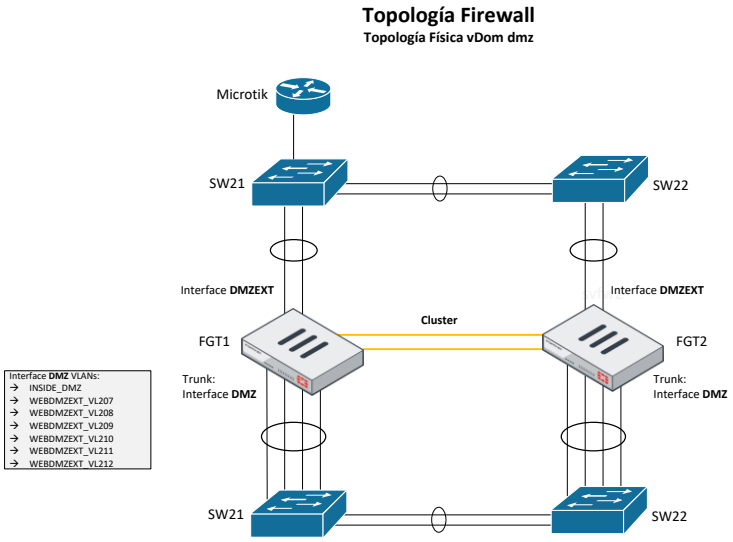
La xarxa corporativa consta de diferents xarxes controlades per 3 VDOMs configurades en el clúster de Fortigate. Cadascún d'aquests dominis virtuals funcionen com un Firewall independent. VDOM root (intern), VDOM Dmz (extern), VDOM_VPN (connexió remota administració i clients VPN SSL per a teletreball)

Esquema lògic:



Esquema físic: Dominis Virtuals i interfaces:





Polítiques de seguretat configurades als diferents dominis virtuals:

- **Control de Navegació Webfilter**. El filtrat web es fa mitjançant perfils aplicats a grups d'usuaris. El Firewall està integrat amb Active Directory. Aquesta integració es fa mitjançant agent FSSO instal·lat als controladors de domini.
- **Antivirus perimetral i control d'aplicacions**. S'aplica a les polítiques de navegació internet.
- **NAT**. A qualsevol política, des de qualsevol dels interfaces interns cap a internet, està habilitat NAT. A la resta de polítiques, està deshabilitat.
- **IPS**. S'aplica a la VDOM DMZ a les polítiques que permeten el tràfic d'extern a intern.
- **Geolocalització.** Polítiques aplicades per a denegació d'accés per regions.
- **VPN IPsec i VPN SSL.** Configurat per accés remot d'administració i teletreball.En aquests moments hi ha uns 200 usuaris que connecten amb client VPN i 2 serveis de VPN IPsec per a empresa de serveis gestionats i per còpies al cloud. No es disposa de doble autenticació.

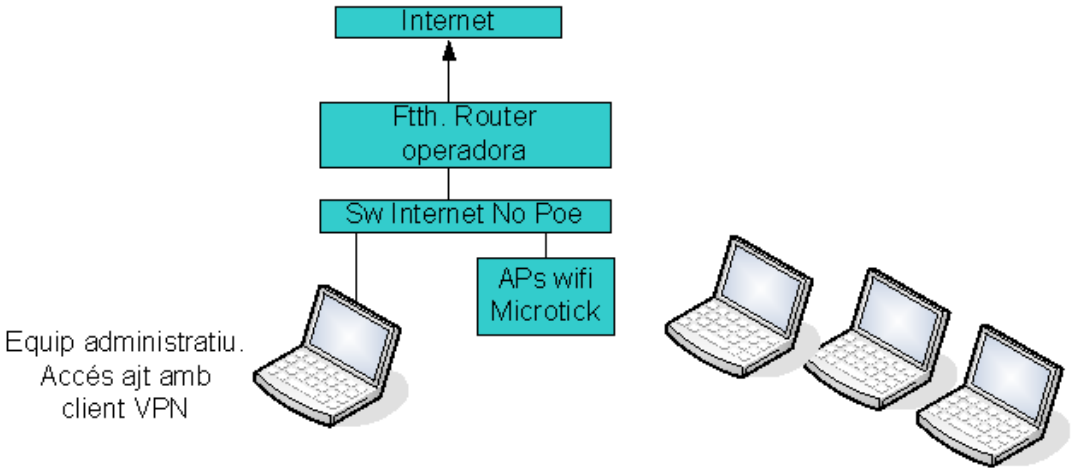
3-Arquitectura actual de xarxa de les seus.

A les seus connectades a l'ajuntament, per la seva topologia en estrella per accés a tots els recursos (internet, intranet, servidors de fitxers, telefonia IP i seguretat), no disposen d'equipament de seguretat perimetral específic. La seguretat la proporciona la connexió al sistema central amb enllaços vpn.
A tots els centres connectats es disposa d'un accés a internet descentralitzat, separat de la xarxa corporativa, per al sistema de wifi.
Els accesos a internet wifi descentralitzat dels edificis Conservatori municipal de música i Centre Cultural Casino, disposen de control de continguts de navegació. La resta, no.

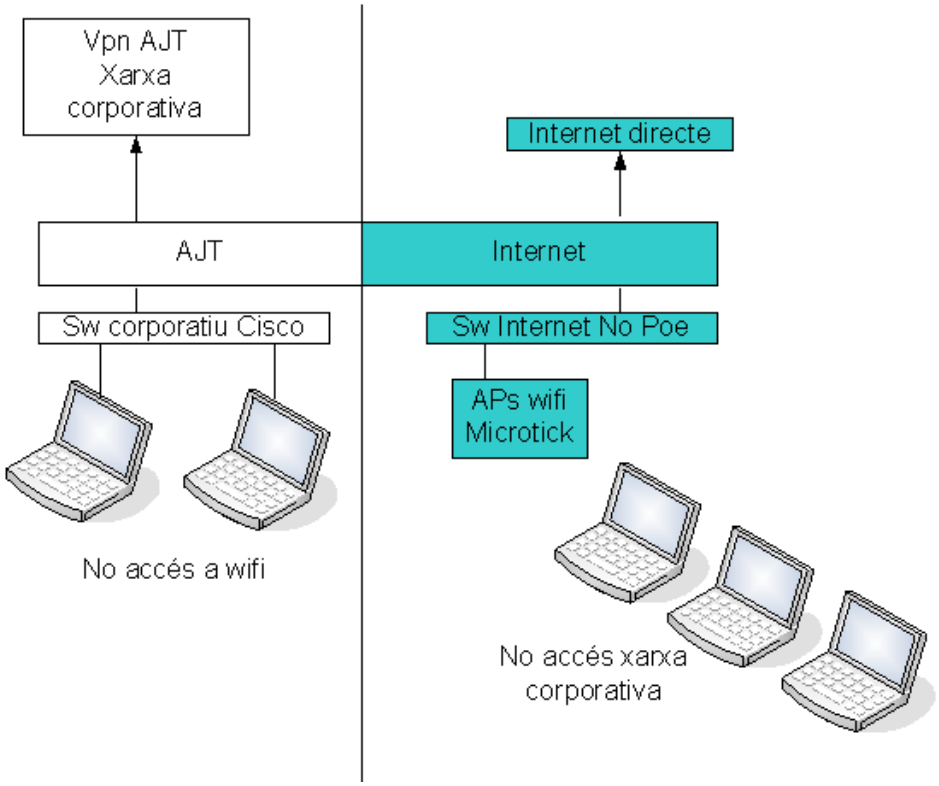
Els centres no connectats a l'ajuntament i on hi ha serveis d'accés internet tampoc disposen d'equipament de seguretat perimetral específic amb l'excepció d'un dels centres on hi ha un sistema de Fw Fortinet. El centre és el Casal de Joves la Kampana.

3.1 i 3.2 Esquemes dels sistemes dels centres:

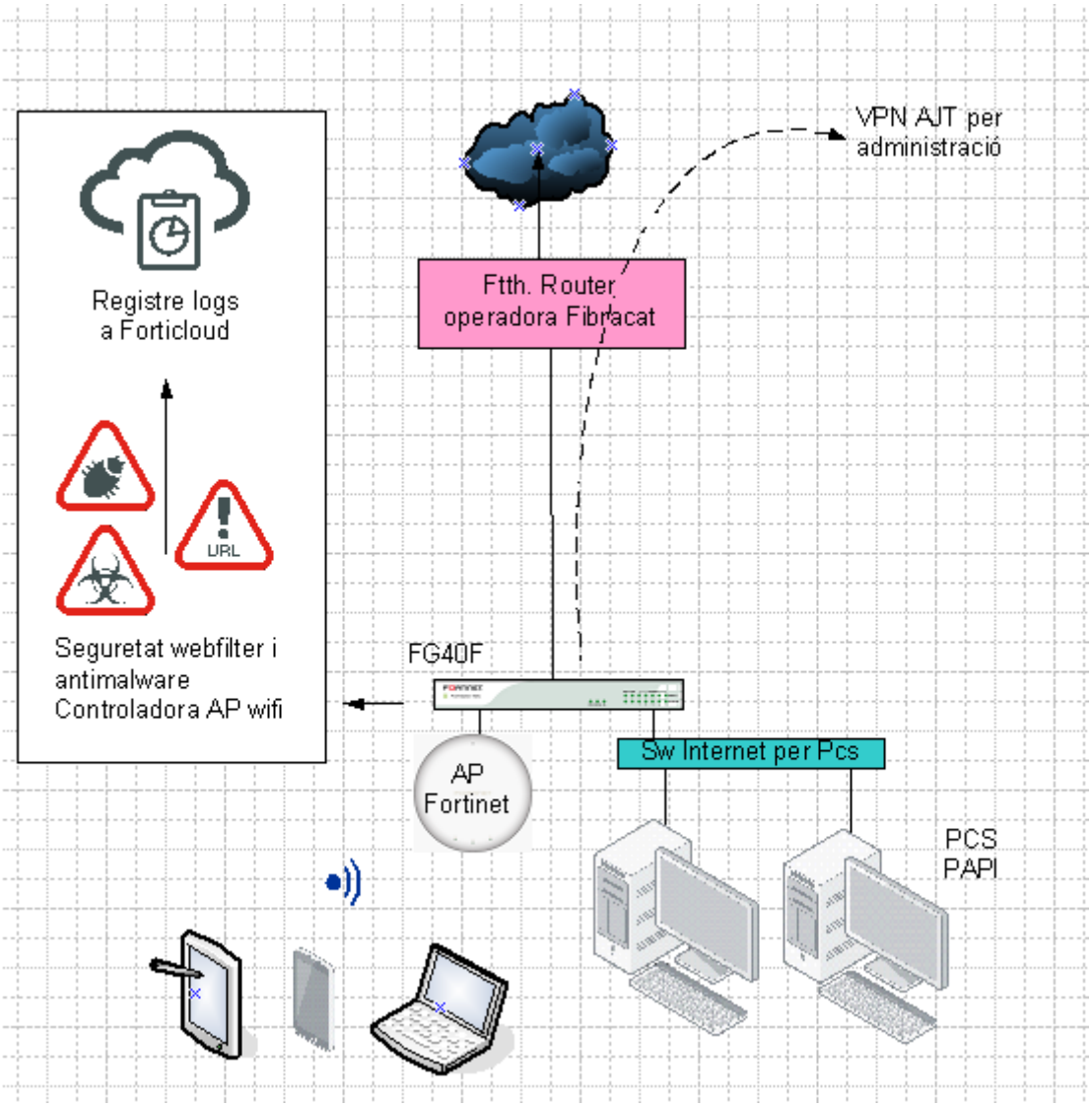
Centres no connectats a Ajt: (Aules, punts públics accés internet)
Escola D'Art (aules) Ludoteca Ludugurus, Centre obert La font, centre obert la xalesta



Centres connectats a Ajt amb aules, punts públics accés internet i activitat administració.



Seu no connectada a l'ajuntament: Casal de Joves la Kampana i Espai Jove del centre Joan amades. Securització Fortinet.



DATA SHEET

FortiGate® 600E Series

FortiGate 600E and 601E

Next Generation Firewall
Secure SD-WAN



The FortiGate 600E series delivers next generation firewall capabilities for mid-sized to large enterprises, with the flexibility to be deployed at the campus or enterprise branch. Protect against cyber threats with security processor powered high performance, security efficacy and deep visibility.

Security
- Identifies thousands of applications inside network traffic for deep inspection and granular policy enforcement
- Protects against malware, exploits, and malicious websites in both encrypted and non-encrypted traffic
- Prevent and detect against known and unknown attacks using continuous threat intelligence from AI powered FortiGuard Labs security services

Performance
- Delivers industry's best threat protection performance and ultra-low latency using purpose built-security processor (SPU) technology
- Provides industry-leading performance and protection for SSL encrypted traffic

Certification
- Independently tested and validated best security effectiveness and performance
- Received unparalleled third-party certifications from NSS Labs, ICSA, Virus Bulletin and AV Comparatives

Networking
- Best of Breed SD-WAN capabilities to enable application steering using WAN path control for high quality of experience
- Delivers extensive routing, switching, wireless controller, high-performance, and scalable IPsec VPN capabilities to consolidate networking and security

Management
- Includes management console that's effective, simple to use, and provides comprehensive network automation & visibility.
- Provides Zero Touch Integration with Security Fabric's Single Pane of Glass Management
- Predefined compliance checklist analyzes the deployment and highlights best practices to improve overall security posture

Security Fabric
- Enables Fortinet and Fabric-ready partners' products to provide broader visibility, integrated end-to-end detection, threat intelligence sharing and automated remediation
- Automatically builds Network Topology visualizations which discover IoT devices and provide complete visibility into Fortinet and Fabric-ready partner products

Firewall	IPS	NGFW	Threat Protection	Interfaces
36 Gbps	**10 Gbps**	**9.5 Gbps**	**7 Gbps**	Multiple GE RJ45, GE SFP and 10 GE SFP+ Slots

Refer to specification table for details

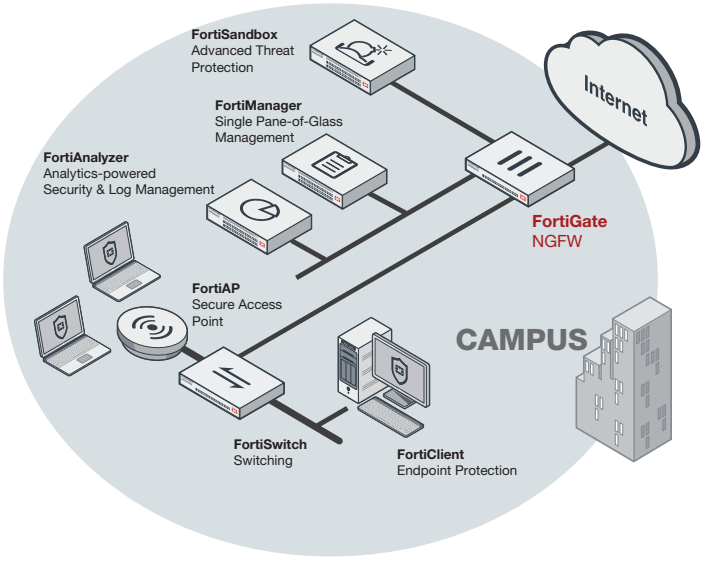
Deployment

Next Generation Firewall (NGFW)

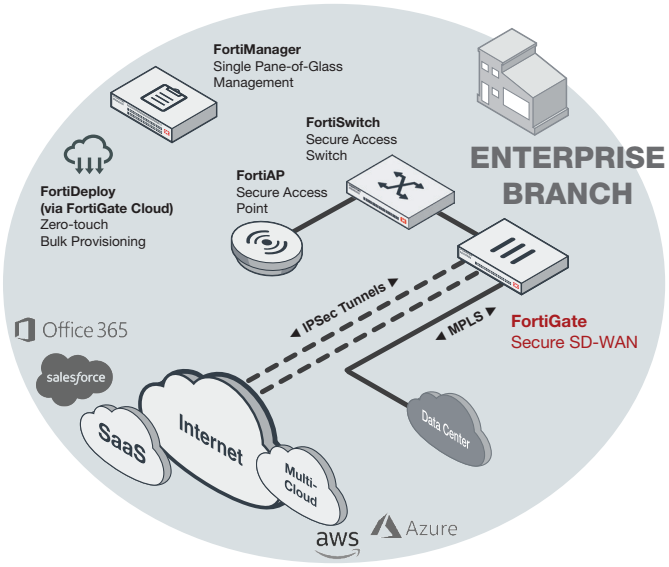
- Reduce complexity by combining threat protection security capabilities into single high-performance network security appliance
- Identify and stop threats with powerful intrusion prevention beyond port and protocol that examines the actual applications in your network traffic
- Delivers industry's highest SSL inspection performance using industry-mandated ciphers while maximizing ROI
- Proactively blocks newly discovered sophisticated attacks in real-time with advanced threat protection

Secure SD-WAN

- Secure direct Internet access for Cloud applications for improved latency and reduce WAN cost spending
- High-performance and cost-effective threat protection capabilities
- WAN Path Controller and Link Health Monitoring for better application performance
- Security Processor powered industry's best IPsec VPN and SSL Inspection performance
- Simplified Management and Zero-Touch deployment



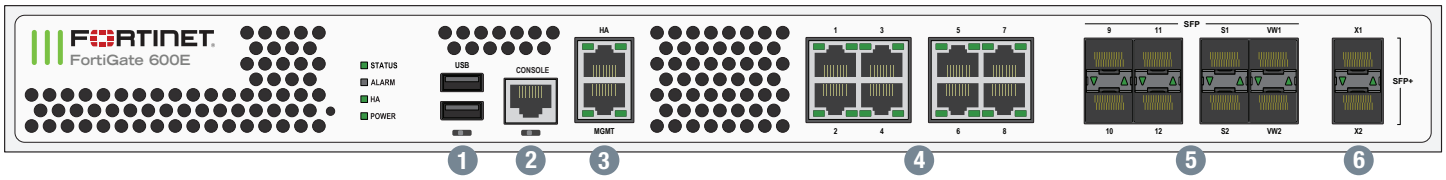
FortiGate 600E/601E deployment in Campus (NGFW)

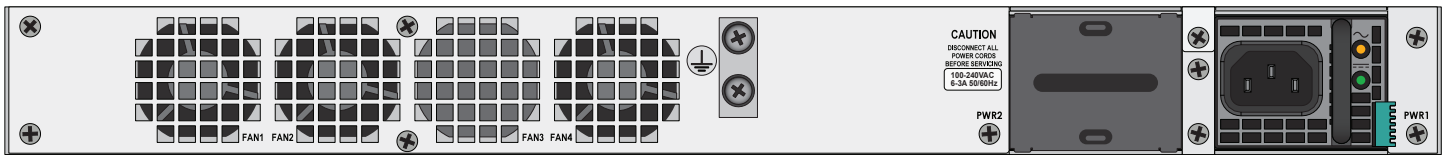


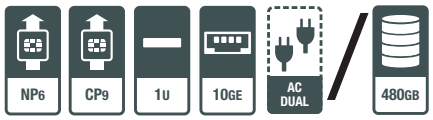
FortiGate 600E/601E deployment in Enterprise Branch (Secure SD-WAN)

Hardware

FortiGate 600E/601E







Interfaces

1. USB Port
2. Console Port
3. 2x GE RJ45 MGMT/HA Ports
4. 8x GE RJ45 Ports
5. 8x GE SFP Slots
6. 2x 10 GE SFP+ Slots

Powered by SPU



- Custom SPU processors deliver the power you need to detect malicious content at multi-Gigabit speeds
- Other security technologies cannot protect against today's wide range of content- and connection-based threats because they rely on general-purpose CPUs, causing a dangerous performance gap
- SPU processors provide the performance needed to block emerging threats, meet rigorous third-party certifications, and ensure that your network security solution does not become a network bottleneck

Network Processor

Fortinet's new, breakthrough SPU NP6 network processor works inline with FortiOS functions delivering:

- Superior firewall performance for IPv4/IPv6, SCTP and multicast traffic with ultra-low latency down to 2 microseconds
- VPN, CAPWAP and IP tunnel acceleration
- Anomaly-based intrusion prevention, checksum offload and packet defragmentation
- Traffic shaping and priority queuing

Content Processor

Fortinet's new, breakthrough SPU CP9 content processor works outside of the direct flow of traffic and accelerates the inspection of computationally intensive security features:

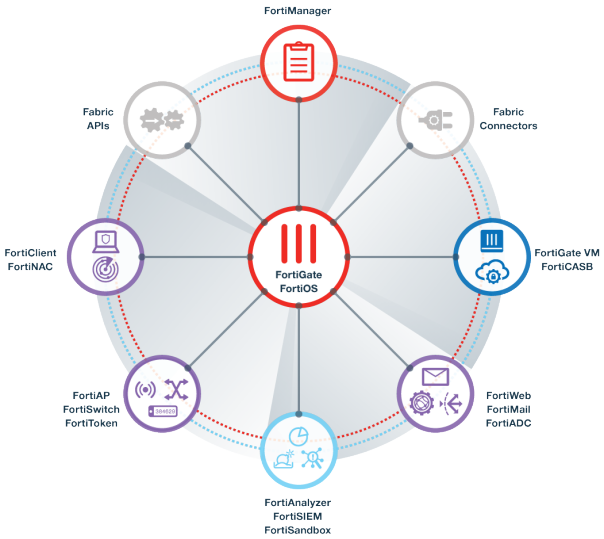
- Enhanced IPS performance with unique capability of full signature matching at ASIC
- SSL Inspection capabilities based on the latest industry mandated cipher suites
- Encryption and decryption offloading

Fortinet Security Fabric

Security Fabric

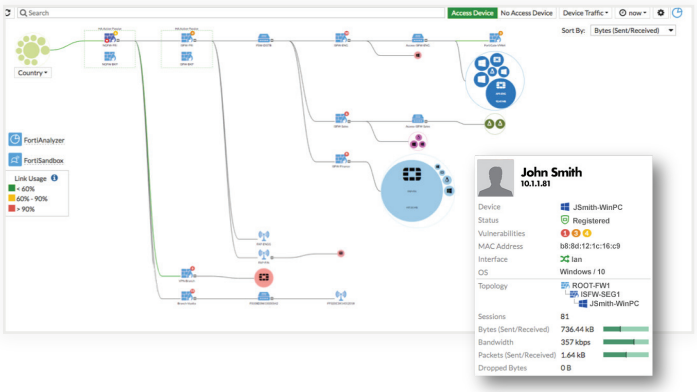
The Security Fabric delivers broad visibility, integrated AI-driven breach prevention, and automated operations, orchestration, and response across all Fortinet and its ecosystem deployments. It allows security to dynamically expand and adapt as more and more workloads and data are added. Security seamlessly follows and protects data, users, and applications as they move between IoT, devices, and cloud environments throughout the network. All this is ties together under a single pane of glass management for significantly thereby delivering leading security capabilities across your entire environment while also significantly reducing complexity.

FortiGates are the foundation of Security Fabric, expanding security via visibility and control by tightly integrating with other Fortinet security products and Fabric-Ready Partner solutions.



FortiOS

Control all security and networking capabilities across the entire FortiGate platform with one intuitive operating system. Reduce complexity, costs, and response time with a truly consolidated next- generation security platform.



- A truly consolidated platform with a single OS and pane-of-glass for all security and networking services across all FortiGate platforms.
- Industry-leading protection: NSS Labs Recommended, VB100, AV Comparatives, and ICSA validated security and performance. Ability to leverage latest technologies such as deception-based security.
- Control thousands of applications, block the latest exploits, and filter web traffic based on millions of real-time URL ratings in addition to true TLS 1.3 support.
- Prevent, detect, and mitigate advanced attacks automatically in minutes with integrated AI-driven breach prevention and advanced threat protection.
- Fulfil your networking needs with extensive routing, switching, and SD-WAN capabilities along with intent-based segmentation.
- Utilize SPU hardware acceleration to boost security capability performance.

Services

FortiGuard™ Security Services

FortiGuard Labs offers real-time intelligence on the threat landscape, delivering comprehensive security updates across the full range of Fortinet's solutions. Comprised of security threat researchers, engineers, and forensic specialists, the team collaborates with the world's leading threat monitoring organizations and other network and security vendors, as well as law enforcement agencies.

FortiCare™ Support Services

Our FortiCare customer support team provides global technical support for all Fortinet products. With support staff in the Americas, Europe, Middle East, and Asia, FortiCare offers services to meet the needs of enterprises of all sizes.

For more information, please refer to forti.net/fortiguard and forti.net/forticare

Specifications

	FORTIGATE 600E	FORTIGATE 601E
Interfaces and Modules		
10 GE SFP+ Slots	2	
GE RJ45 Interfaces	8	
GE SFP Slots	8	
GE RJ45 Management Ports	2	
USB Ports	2	
RJ45 Console Port	1	
Local Storage	NIL	2x 240 GB SSD
Included Transceivers	2x SFP (SX 1 GE)	
System Performance — Enterprise Traffic Mix		
IPS Throughput [2]	10 Gbps	
NGFW Throughput [2, 4]	9.5 Gbps	
Threat Protection Throughput [2, 5]	7 Gbps	
System Performance and Capacity		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	36 / 36 / 27 Gbps	
IPv6 Firewall Throughput (1518 / 512 / 64 byte, UDP)	36 / 36 / 27 Gbps	
Firewall Latency (64 byte, UDP)	2 µs	
Firewall Throughput (Packet per Second)	40.5 Mpps	
Concurrent Sessions (TCP)	8 Million	
New Sessions/Second (TCP)	450,000	
Firewall Policies	10,000	
IPsec VPN Throughput (512 byte) [1]	20 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	2,000	
Client-to-Gateway IPsec VPN Tunnels	50,000	
SSL-VPN Throughput	7 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	10,000	
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	8 Gbps	
SSL Inspection CPS (IPS, avg. HTTPS) [3]	5,500	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	800,000	
Application Control Throughput (HTTP 64K) [2]	15 Gbps	
CAPWAP Throughput (HTTP 64K)	18 Gbps	
Virtual Domains (Default / Maximum)	10 / 10	
Maximum Number of FortiSwitches Supported	64	
Maximum Number of FortiAPs (Total / Tunnel)	1,024 / 512	
Maximum Number of FortiTokens	5,000	
Maximum Number of Registered FortiClients	2,000	
High Availability Configurations	Active-Active, Active-Passive, Clustering	

	FORTIGATE 600E	FORTIGATE 601E
Dimensions and Power		
Height x Width x Length (inches)	1.75 x 17.0 x 15.0	
Height x Width x Length (mm)	44.45 x 432 x 380	
Weight	16.1 lbs (7.3 kg)	16.6 lbs (7.5 kg)
Form Factor	1 RU	
Power Consumption (Average / Maximum)	129 W / 244 W	
Power Source	100–240V 60–50Hz	
Current (Maximum)	6A @ 100V	
Heat Dissipation	832 BTU/h	
Redundant Power Supplies (Hot Swappable)	optional	
Operating Environment and Certifications		
Operating Temperature	32–104°F (0–40°C)	
Storage Temperature	-31–158°F (-35–70°C)	
Humidity	10–90% non-condensing	
Noise Level	59 dBA	
Operating Altitude	Up to 7,400 ft (2,250 m)	
Compliance	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB	
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN; USGv6/IPv6	

Note: All performance values are "up to" and vary depending on system configuration.

1. IPsec VPN performance test uses AES256-SHA256.
2. IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.
3. SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.
4. NGFW performance is measured with Firewall, IPS and Application Control enabled.
5. Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.

Order Information

Product	SKU	Description
FortiGate 600E	FG-600E	2x 10 GE SFP+ slots, 10x GE RJ45 ports (including 1x MGMT port, 1x HA port, 8x switch ports), 8x GE SFP slots, SPU NP6 and CP9 hardware accelerated.
FortiGate 601E	FG-601E	2x 10 GE SFP+ slots, 10x GE RJ45 ports (including 1x MGMT port, 1x HA port, 8x switch ports), 8x GE SFP slots, SPU NP6 and CP9 hardware accelerated, 2x 240 GB onboard SSD storage.
Optional Accessories		
1 GE SFP LX Transceiver Module	FG-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP RJ45 Transceiver Module	FG-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+slots.
1 GE SFP SX Transceiver Module	FG-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Short Range	FG-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots
10 GE SFP+ Transceiver Module, Long Range	FG-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots
10 GE Copper SFP+ Transceiver Module, up to 30m	FS-TRAN-SFP+GC	10 GE copper SFP+ RJ45 transceiver. For FortiSwitch only, up to 30m.
10 GE SFP+ Active Direct Attach Cable, 10m / 32.8 ft	SP-CABLE-ADASFP+	10 GE SFP+ active direct attach cable, 10m / 32.8 ft for all systems with SFP+ and SFP/SFP+ slots
Optional Power Supply	SP-FG300E-PS	AC power supply for FG-300/301E, FG-400/401E, FG-500/501E, FG-600/601E, FAZ-200F/300F/800F and FMG-200F/300F.

Bundles



FortiGuard Bundle

FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with one of these FortiGuard Bundles.

Bundles	360 Protection	Enterprise Protection	UTM	Threat Protection
FortiCare	ASE [1]	24x7	24x7	24x7
FortiGuard App Control Service	•	•	•	•
FortiGuard IPS Service	•	•	•	•
FortiGuard Advanced Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
FortiGuard Web Filtering Service	•	•	•	
FortiGuard Antispam Service	•	•	•	
FortiGuard Security Rating Service	•	•		
FortiGuard Industrial Service	•	•		
FortiCASB SaaS-only Service	•	•		
FortiConverter Service	•			
SD-WAN Cloud Assisted Monitoring [2]	•			
SD-WAN Overlay Controller VPN Service [2]	•			
FortiAnalyzer Cloud [2]	•			
FortiManager Cloud [2]	•			

1. 24x7 plus Advanced Services Ticket Handling 2. Available when running FortiOS 6.2

FORTINET®

www.fortinet.com

Copyright © 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

ANNEX 3: Infraestructura actual de xarxa central. Sistema ubicat a CPD Edifici Pl Major 5

1-Esquema infraestructura actual xarxa central.

2-Proposta nova connexió.

Algunes consideracions actuals de la infraestructura de xarxa perimetral:

- El switch de Core actual no està redundat.
- El switch de Core actual no te ports PoE i no es requereix en aquest plec.
- El sistema de Base de Dades Oracle, format per 1 cluster de 2 equips, actualment està connectat al switch de Core amb trunks 1000BaseT.
- El sistema virtual de servidors està connectat actualment al Core amb trunks 1000BaseT.
- Els firewalls estan preparats amb 2 ports cadascun a 10GB SFP+ , ara estan connectats al core amb un trk de 4 GB ethernet cada Firewall. Per a connectar aquest sistema es requerirà 4 ports 10GB SFP+ incloent els cables.
- Es pretén eliminar els SW21 i SW22 i passar les connexions d'aquests switxos al sw del nou core.
- Per a projecte de virtualització d'escriptoris futur, es requereix 6 ports 10GB SFP+ mínim i 2 ports 1GBBase T
- El swich de core i els firewalls estan ubicats en diferents racks de comunicacions separats 2 m dins del mateix CPD. La idea és mantenir aquestes ubicacions, per tant, s'haurà de tenir en compte el plantejament de la correcta connexió entre aquests dos racks.

1-Esquema infraestructura actual xarxa central.

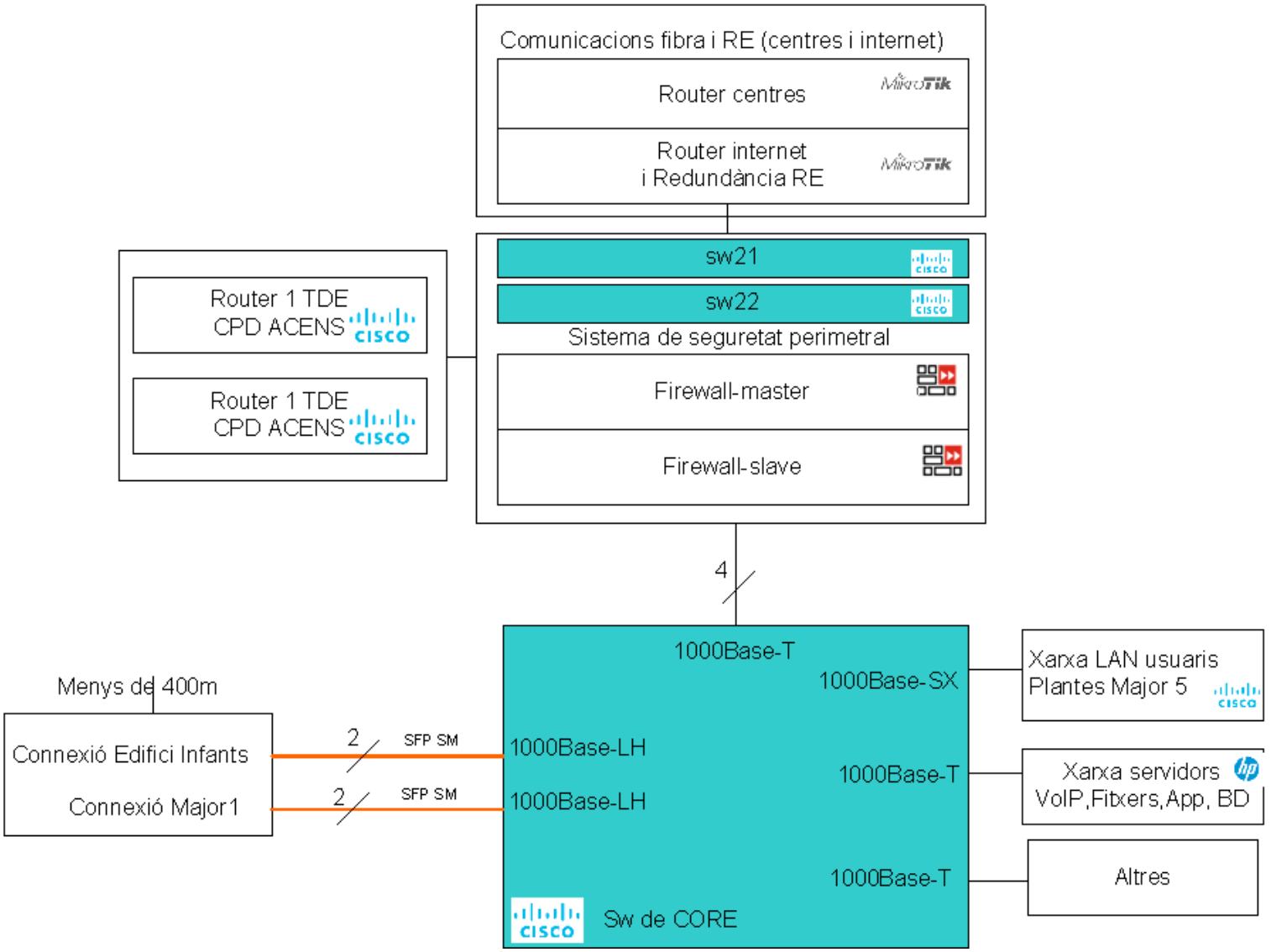
En aquest esquema es resumeix la infraestructura actual de xarxa de perímetre i s'adjunta una taula amb la disponibilitat de pots actuals.

2-Proposta nova connexió.

En aquest punt es proposa la nova infraestructura que es voldria tenir. Es poden fer altres propostes.

1-Esquema infraestructura actual xarxa central.

Esquema Infraestructura actual xarxa central
Sistema ubicat a CPD edifici Major 5

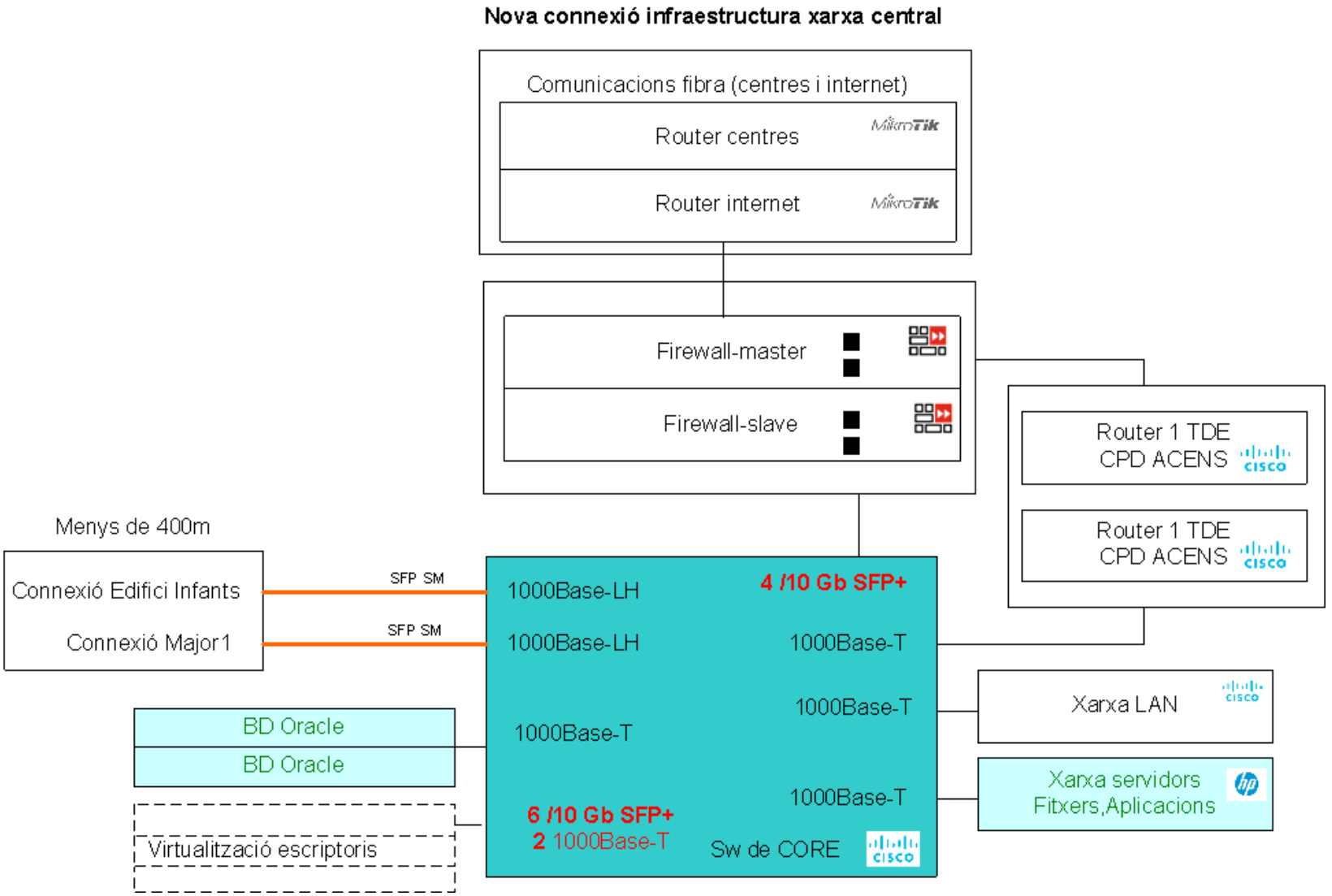


Relació de ports del sistemes actuals d'electrònica de xarxa central i perímetre:

Equip	Tipus port/Connector	Ports actius connectats	Ports lliures
CORE: cisco WS-C6506-E	10/100/1000BaseT	34 ports connectats	63 ports no connectats
	1000 1000BaseLH (connector SC duplex)	4 ports connectats (Major 1 i Edifici Infants)	4 ports no connectats
	1000 1000Base SX	4 ports connectats -1 sw P1 -1 sw P2 -1 sw P3 -1 sw P4	0 no connectats
SW1: C9200L-48T-4G	10/100/1000 baseTx	20 ports connectats -10 a Firewall -5 a RB Router -1 a Router VoIP TDE -4 varis	26 ports no connectats
SW2: C9200L-48T-4G	10/100/1000 baseTx	20 ports connectats -10 a Firewall -5 a RB Router -1 a Router VoIP TDE -4 varis	26 ports no connectats
Firewall 1	10GB SFP+	pendents de connectar a CORE	2 ports no connectats
	1000 baseTx	16 ports connectats -4 a core -4 a sw1 comunicacions -4 a sw1 DMZ -2 a sw1 DMZext -1 a sw vpn teletreball -1 a Routers VoIP TDE	0 no connectats

Firewall 2	10GB SFP+	pendents de connectar a CORE	2 ports no connectats
	1000 baseTx	16 ports connectats -4 a core -4 a sw1 comunicacions -4 a sw1 DMZ -2 a sw1 DMZext -1 a sw vpn teletreball -1 a Routers VoIP TDE	0 no connectats

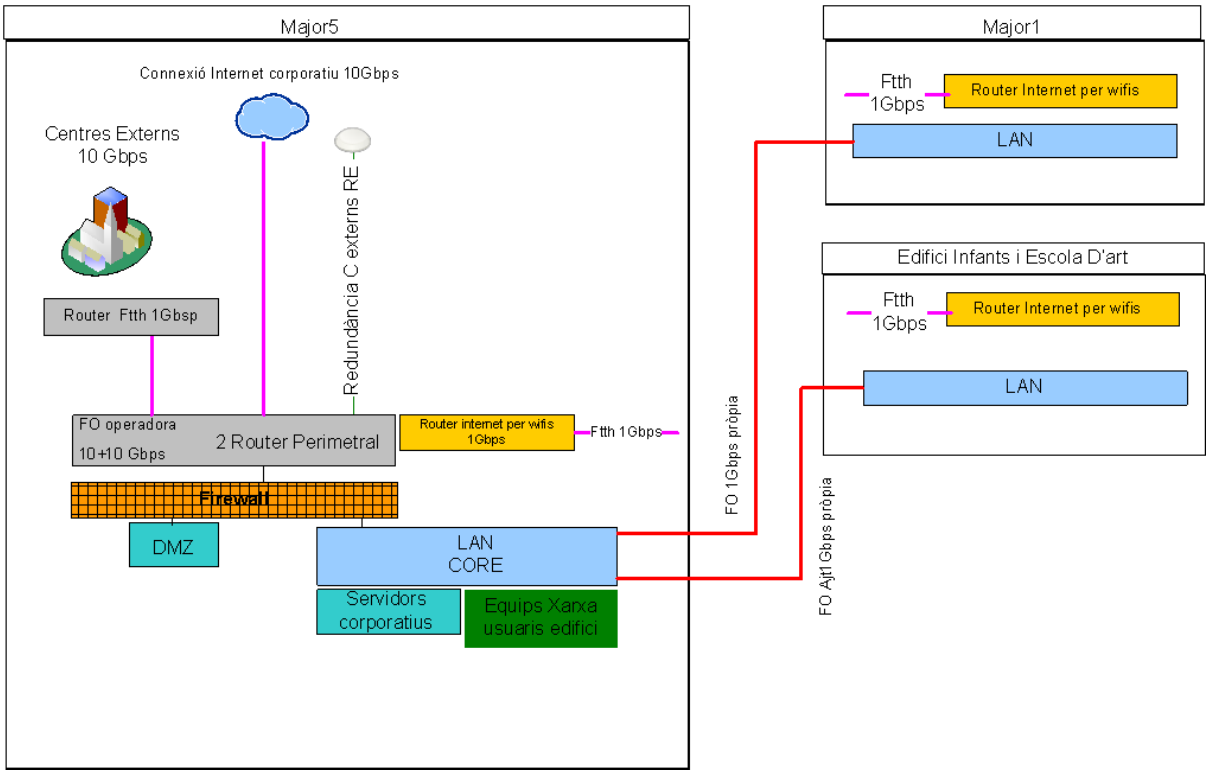
2-Proposta disponibilitat per futures noves connexions.



ANNEX4-Capacitats i sistemes de les comunicacions i seus.

Capacitat i sistemes de les comunicacions

L'arquitectura de comunicacions entre les diferents seus i la seu principal és en estrella i tota la relació entre elles es fa a través de la seu central ubicada al CPD a Pl. Major 5. Tots els serveis com accés a la intranet, a internet , correu i dades estan ubicats a la seu central.
Les comunicacions entre centres es fan amb routers Microtick a través de VPN.
Com a enllaços principals hi ha 2 fibres de 10Gbps cadascuna connectades a cadascun dels routers principals.
Els dos routers perimetral són del fabricant Microtik i el model és CCR1036 -8G2S+
Un dels routers connecta amb els centres externs i l'altre dona servei a internet i a la redundància de les comunicacions amb els centres a través de ràdio-enllaç.
La connexió amb els centres Edifici Infants i Edifici Pl Major1 (casa consistorial) és a través d'una fibra dedicada per a cadascun dels centres de 1 Gbps i és propietat de l'ajuntament.
L'edifici la Forinda (Policia Local) i Centre Cultural Casino, tenen una fibra dedicada de l'operadora Fibracat i la resta d'edificis tenen fibra Ftth també de la mateixa operadora.
Aquestes fibres són d'1Gbps. L'enllaç entre aquests edificis i el CPD s'estableix amb VPNs i la gestió dels routers de tots els centres és a càrrec de l'operadora Fibracat/Altecom.



Centres connectats i número d'usuaris:

Edifici	núm usuaris	capacitat comunicacions
1-Edifici principal (CPD): PLMAJOR5	202	Fibra punt a punt 1G
2-Edifici Pl Major 1 (Casa consistorial)	100	Fibra punt a punt 1G
3-Edifici Infants-Escola Art	94+ 6 aules	Fibra punt a punt 1G
4-Edifici CIO	60+ 4 aules	Fibra punt a punt 1G
5-Edifici Centre Cultural casino	14	Fibra punt a punt 1G
6-Edifici Habitatge	10	FTTH Gpon 1G
7-Edifici Florinda(Plocal)	65	Fibra punt a punt 1G
8-Edicici EBAS Centre-Mercat	23	FTTH Gpon 1G
9-Edifici EBAS Ponent	10+ 2 aules	Fibra punt a punt 1G
10-Edifici EBAS LLevant	12+ 2 aules	FTTH Gpon 1G
11-Edifici Escodines	9	FTTH Gpon 1G
12-Edifici Centre Històric	2	FTTH Gpon 1G
13-Edifici Acollida	10	FTTH Gpon 1G
14-Edifici Magatzem	12	FTTH Gpon 1G
15-Edifici Museu	8	FTTH Gpon 1G
16-Edifici Cementiri	1	FTTH Gpon 1G
17-Edifici Complex Congost	4	FTTH Gpon 1G
18-Edifici Pavelló nou Congost	1	FTTH Gpon 1G
19-Edifici Conservatori Música	8	FTTH Gpon 1G
20-Edifici Saleses	2	FTTH Gpon 1G
21-Ebas Nord	12	Fibra punt a punt 1G
22-Edifici OAE-serveis funeraris	10	FTTH Gpon 1G

ANNEX-5 Sistema de seguretat local antivirus.

El sistema antivirus end point actual és Trend Micro Cloud One - Endpoint Security i Vision One.XDR, New, Government, 501-1000
Núm Llicències: 737
Llicència: 01/01/202-31/12/2023 Es farà una renovació per a 3 anys més en una altra licitació.

Els sistemes operatius que hi ha en el moment de la publicació del plec són:

Windows Xp: 6
Windows Vista: 1
Windows 7: 575
Windows 10: 153
Windows 2003 server : 6
Windows 2012 server: 6
Windows 2016 server: 7
Windows 2019 server: 14

ANNEX 6- PERFIL DE PROTECCIÓN COMMON CRITERIA:

- **REQ.1** Los productos deberán estar certificados con uno de los siguientes perfiles de protección certificados de acuerdo a la norma Common Criteria:

PERFILES DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Collaborative Protection Profile for Network Devices[1]	2.2e	27/03/2020	CCDB
Collaborative Protection Profile for Network Devices[2]	2.1	24/09/2018	CCDB
Collaborative Protection Profile for Network Devices[3]	2.0 + Errata 20180314	14/03/2018	CCDB
Collaborative Protection Profile for Network Devices.4	1.0	27/02/2015	CCDB

Perfiles de protección Common Criteria – CCN STIC-140 Anexo B.6 pt.4.1

- **REQ.2**. En caso de que el producto no esté certificado contra ninguno de los perfiles anteriores, debe disponer de una declaración de seguridad (Security Target) certificada con un nivel de confianza EAL (Evaluation Assurance Level) EAL2 o superior. La declaración de seguridad debe implementar los SFR (Security Functional Requirements) apropiados para satisfacer, al menos, los Objetivos de Seguridad que se recogen en la siguiente tabla:

OBJETIVO	DESCRIPCIÓN
[AUDITORÍA] REGISTRO DE EVENTOS I	El producto deberá guardar un registro de auditoría para los eventos de seguridad relevantes que ocurran en el sistema.
[AUDITORÍA] REGISTRO DE EVENTOS II	Para cada evento de auditoría se registrará, al menos, la siguiente información: fecha/hora del evento, tipo de evento, sujeto identificado (si aplica) y resultado del evento (éxito o fracaso).
[AUDITORÍA] LECTURA DE REGISTROS	El producto deberá proteger los registros de auditoría almacenados de accesos de lectura no autorizados.
[AUDITORÍA] MODIFICACIÓN DE REGISTROS	El producto deberá proteger los registros de auditoría almacenados de modificaciones y borrados no autorizados.
[AUDITORÍA] PREVENCIÓN DE PÉRDIDA DE DATOS	El producto deberá disponer de mecanismos apropiados para prevenir la pérdida de registros de auditoría, en el caso de que el espacio para almacenamiento de los registros alcance su límite.
[AUDITORÍA] TRANSMISIÓN SEGURA DE REGISTROS	En caso de que el produzco tenga la capacidad de transmitir los registros de auditoría a otro dispositivo o servidor externo, deberá emplear un protocolo seguro para la transmisión (por ejemplo, TLS 1.2 o superior o IPsec).
[CONTROL DE ACCESO] IDENTIFICACIÓN Y AUTENTICACIÓN	El producto debe identificar de forma única a los usuarios, y autenticarlos antes de permitirles acceso las funciones y datos del producto.
[GESTIÓN DE LA SEGURIDAD] FUNCIONES	El producto debe proporcionar un conjunto de funciones de gestión que permitan el control adecuado de sus características y datos.
[GESTIÓN DE LA SEGURIDAD] PERMISOS	El producto debe garantizar que solo los usuarios con los privilegios adecuados puedan ejercer el control de sus funciones y datos.
[SELLADO DE TIEMPO]	El producto debe proporcionar una fuente de tiempo fiable para los registros de auditoría.

Objetivos de Seguridad – CCN STIC-140 Anexo B.6 pt.4.1

SOPORTE CRIPTOGRÁFICO:

- **REQ.3** El producto no almacenará ninguna credencial en claro en memoria no volátil.
- **REQ.4** El producto deberá impedir el acceso en claro a los parámetros de seguridad críticos del sistema (claves simétricas y claves privadas).
- **REQ.5** En caso de que el producto utilice algoritmos y funciones criptográficas, debe soportar el uso de aquellas aceptadas para nivel Alto del ENS según la guía CCN-STIC-807 con las longitudes de clave requeridas, así como proporcionar capacidades de configuración que permitan obligar al uso de estos algoritmos exclusivamente.

CANALES CONFIABLES:

- **REQ.6** El producto utilizará protocolos seguros (IPSec, TLS 1.2 o superior, etc.) para el establecimiento de canales confiables para el intercambio de información con otras entidades TI autorizadas, la administración remota o los usuarios remotos.

SIEM:

- **REQ.7** El producto deberá ser capaz de recibir, identificar e interpretar eventos procedentes de múltiples fuentes. Debe soportar, al menos, los protocolos: Syslog y SNMP (Simple Network Management Protocol). También debe ser suficientemente

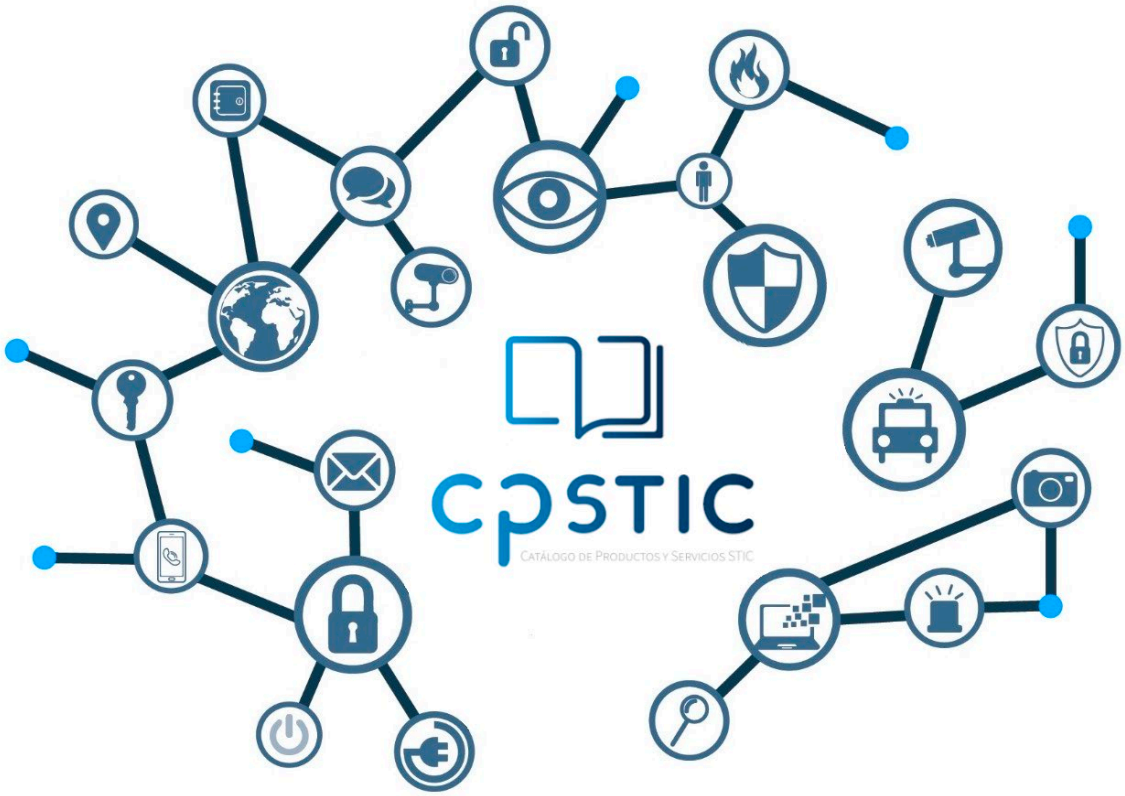
configurable para interpretar y normalizar información procedente de aplicaciones o herramientas propietarias.

- **REQ. 8** Para la funcionalidad de análisis y correlación de eventos, el producto facilitará la creación de alarmas o notificaciones en el caso de detectar potenciales riesgos para la seguridad.
- **REQ. 9** Para la funcionalidad de análisis de eventos, el producto deberá ser capaz de analizar los datos recolectados en función de reglas definidas, para identificar usos indebidos o actividades maliciosas, registrando el resultado de los análisis.
- **REQ.10** Para la funcionalidad de análisis de eventos y correlación, el producto debe proteger los eventos almacenados de accesos, modificaciones y borrados no autorizados, así como prevenir la pérdida de eventos por el llenado del espacio de almacenamiento.
- **REQ.11 Para su integración en la Red Nacional de SOC, solución dispondrá de una API para la federación con el CCN, con el fin de poder monitorizar las alertas de seguridad de peligrosidad Alta, Muy Alta y Crítica, según la norma CCN-STIC 817 de Gestión de Incidentes.**

centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 105

Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación



Abril de 2022

MINISTERIO DE DEFENSA

cpage.mpr.gob.es

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2022
NIPO: 083-22-047-8

Fecha de Edición: abril de 2022

LIMITACIÓN DE RESPONSABILIDAD
El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL
Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Abril de 2022



Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

ÍNDICE 4
1. INTRODUCCIÓN 7
2. OBJETIVO 8
3. ALCANCE 8
4. INCLUSIÓN DE UN PRODUCTO DEL CPSTIC 9
5. REVISIÓN DE VALIDEZ DE PRODUCTOS STIC 10
6. EXCLUSIÓN DE UN PRODUCTO O SERVICIO DEL CPSTIC 11
7. PRODUCTOS CUALIFICADOS 12
7.1 CATEGORÍA: CONTROL DE ACCESO 14
7.1.1 FAMILIA: CONTROL DE ACCESO A RED (NAC) 14
7.1.2 FAMILIA: DISPOSITIVOS BIOMÉTRICOS 17
7.1.3 FAMILIA: DISPOSITIVOS SINGLE SIGN-ON 17
7.1.4 FAMILIA: SERVIDORES DE AUTENTICACIÓN 18
7.1.5 FAMILIA: DISPOSITIVOS ONE-TIME PASSWORD 19
7.1.6 FAMILIA: GESTIÓN DE ACCESO PRIVILEGIADO (PAM) 19
7.1.7 FAMILIA: GESTIÓN DE IDENTIDADES (IM) 23
7.2 CATEGORÍA: EXPLOTACIÓN DE LA SEGURIDAD 24
7.2.1 FAMILIA: ANTI-VIRUS/EPP (ENDPOINT PROTECTION PLATFORM) 24
7.2.2 FAMILIA: EDR (ENDPOINT DETECTION AND RESPONSE) 29
7.2.3 FAMILIA: HERRAMIENTAS DE GESTIÓN DE RED 34
7.2.4 FAMILIA: ACTUALIZACIÓN DE SISTEMAS 35
7.2.5 FAMILIA: FILTRADO DE NAVEGACIÓN 35
7.2.6 FAMILIA: SISTEMAS DE GESTIÓN DE EVENTOS DE SEGURIDAD 35
7.2.7 FAMILIA: DISPOSITIVOS PARA GESTIÓN DE CLAVES CRIPTOGRÁFICAS 37
7.2.8 HERRAMIENTAS DE GESTIÓN DE DISPOSITIVOS MÓVILES (MDM) 39
7.3 CATEGORÍA: MONITORIZACIÓN DE LA SEGURIDAD 39
7.3.1 FAMILIA: DISPOSITIVOS DE PREVENCIÓN DE INTRUSIONES 39
7.3.2 FAMILIA: SISTEMAS HONEYPOT / HONEYNET 46
7.3.3 FAMILIA: CAPTURA, MONITORIZACIÓN Y ANÁLISIS DE TRÁFICO 47
7.3.4 FAMILIA: HERRAMIENTAS DE SANDBOX 49
7.4 CATEGORÍA: PROTECCIÓN DE LAS COMUNICACIONES 50
7.4.1 FAMILIA: ENRUTADORES 50
7.4.2 FAMILIA: SWITCHES 62
7.4.3 FAMILIA: CORTAFUEGOS 91
7.4.4 FAMILIA: PROXIES 113
7.4.5 FAMILIA: DISPOSITIVOS DE RED INALÁMBRICOS 115
7.4.6 PASARELAS SEGURAS DE INTERCAMBIO DE DATOS 120
7.4.7 FAMILIA: DIODOS DE DATOS 121
7.4.8 FAMILIA: REDES PRIVADAS VIRTUALES: IPSEC 121
7.4.9 FAMILIA: REDES PRIVADAS VIRTUALES: SSL 138
7.4.10 FAMILIA: HERRAMIENTAS PARA COMUNICACIONES MÓVILES SEGURAS 139

7.4.11 FAMILIA: CIFRADORES IP 139
7.4.12 FAMILIA: WEB APPLICATION FIREWALL (WAF) 142
7.5 CATEGORÍA: PROTECCIÓN DE LA INFORMACIÓN Y SOPORTES DE INFORMACIÓN 142
7.5.1 FAMILIA: ALMACENAMIENTO CIFRADO DE DATOS 142
7.5.2 FAMILIA. CIFRADO OFFLINE 143
7.5.3 FAMILIA: BORRADO SEGURO 145
7.5.4 FAMILIA: PREVENCIÓN DE FUGAS DE DATOS 147
7.5.5 FAMILIA. HERRAMIENTAS PARA FIRMA ELECTRÓNICA 148
7.5.6 FAMILIA. HARDWARE SECURITY MODULE (HSM) 149
7.6 CATEGORÍA: PROTECCIÓN DE EQUIPOS Y SERVICIOS 151
7.6.1 FAMILIA: DISPOSITIVOS MÓVILES 151
7.6.2 FAMILIA: SISTEMAS OPERATIVOS 158
7.6.3 FAMILIA: PROTECCIÓN DE CORREO ELECTRÓNICO 160
7.6.4 FAMILIA: TARJETAS INTELIGENTES 160
7.6.5 FAMILIA: COPIAS DE SEGURIDAD 160
7.6.6 FAMILIA: PLATAFORMAS CONFIABLES 160
7.6.7 FAMILIA: VIRTUALIZACIÓN 160
7.6.8 FAMILIA: BALANCEADORES DE CARGA 161
7.6.9 FAMILIA: HERRAMIENTAS CASB 161
7.6.10 FAMILIA: HIPERCONVERGENCIA 162
7.6.11 FAMILIA: HERRAMIENTAS DE VIDEOCONFERENCIA 163
7.7 CATEGORÍA: HERRAMIENTAS PARA EL DESARROLLO DE PRODUCTOS DE SEGURIDAD 164
7.8 CATEGORÍA: OTRAS HERRAMIENTAS 165
7.9 CATEGORÍA: SEGURIDAD OT 166
8. PRODUCTOS APROBADOS 167
8.1 CATEGORÍA: CONTROL DE ACCESO 168
8.1.1 FAMILIA: CONTROL DE ACCESO A RED (NAC) 168
8.1.2 FAMILIA: SERVIDORES DE AUTENTICACIÓN 170
8.1.3 FAMILIA: GESTIÓN DE ACCESO PRIVILEGIADO (PAM) 171
8.1.4 FAMILIA: GESTIÓN DE IDENTIDADES (IM) 172
8.2 CATEGORÍA: SEGURIDAD EN LA EXPLOTACIÓN 175
8.2.1 FAMILIA: ANTI-VIRUS/EPP (ENDPOINT PROTECTION PLATFORM) 175
8.2.2 FAMILIA: EDR (ENDPOINT DETECTION AND RESPONSE) 178
8.2.3 FAMILIA: SISTEMAS DE GESTIÓN DE EVENTOS DE SEGURIDAD 181
8.2.4 FAMILIA: DISPOSITIVOS PARA GESTIÓN DE CLAVES CRIPTOGRÁFICAS 182
8.2.5 FAMILIA: CAPTURA, MONITORIZACIÓN Y ANÁLISIS DE TRÁFICO 183
8.3 CATEGORÍA: MONITORIZACIÓN DE LA SEGURIDAD 185
8.3.1 FAMILIA: DISPOSITIVOS DE PREVENCIÓN DE INTRUSIONES 185
8.4 CATEGORÍA: PROTECCIÓN DE LAS COMUNICACIONES 186
8.4.1 FAMILIA: ENRUTADORES 186
8.4.2 FAMILIA: SWITCHES 189
8.4.3 FAMILIA: CORTAFUEGOS 202
8.4.4 FAMILIA: PROXIES 203

8.4.5 FAMILIA: PASARELAS DE INTERCAMBIO DE DATOS....203
8.4.6 FAMILIA: DIODOS DE DATOS....204
8.4.7 FAMILIA: REDES PRIVADAS VIRTUALES: IPSEC....205
8.4.8 FAMILIA: HERRAMIENTAS PARA COMUNICACIONES MÓVILES SEGURAS....206
8.4.9 FAMILIA: CIFRADORES IP....206
8.5 CATEGORÍA: PROTECCIÓN DE LA INFORMACIÓN Y SOPORTES DE INFORMACIÓN....209
8.5.1 FAMILIA: CIFRADO OFFLINE....209
8.5.2 FAMILIA: SISTEMAS PARA PREVENCIÓN DE FUGAS DE DATOS....211
8.5.3 FAMILIA: HERRAMIENTAS PARA FIRMA ELECTRÓNICA....211
8.6 CATEGORÍA: PROTECCIÓN DE EQUIPOS Y SERVICIOS....212
8.6.1 FAMILIA: DISPOSITIVOS MÓVILES....212
8.6.2 FAMILIA: SISTEMAS OPERATIVOS....212
8.6.3 FAMILIA: PROTECCIÓN DE CORREO ELECTRÓNICO....214
8.6.4 FAMILIA: HIPERCONVERGENCIA....215
8.7 CATEGORÍA: COMUNICACIONES TÁCTICAS SEGURAS....216
8.7.1 FAMILIA: PLATAFORMAS Y DISPOSITIVOS TÁCTICOS CONFIABLES....216
8.7.2 FAMILIA: SOLUCIONES PARA PROTECCIÓN DE LAS COMUNICACIONES TÁCTICAS....218
8.8 CATEGORÍA: OTRAS HERRAMIENTAS....221
8.8.1 FAMILIA: OTRAS HERRAMIENTAS....221
8.9 CATEGORÍA: TEMPEST....222
8.9.1 FAMILIA: ARMARIOS APANTALLADOS....222
8.9.2 FAMILIA: MONITORES....225
8.9.3 FAMILIA: PERIFÉRICOS....225
8.9.4 FAMILIA: CPU....227
8.9.5 FAMILIA: IMPRESORAS....228
9. PRODUCTOS Y SERVICIOS DE CONFORMIDAD Y GOBERNANZA DE LA SEGURIDAD....229
9.1 FAMILIA: GOBERNANZA Y PLANIFICACIÓN DE LA SEGURIDAD....230
9.2 FAMILIA: NORMATIVA DE SEGURIDAD Y CONFORMIDAD....230
9.3 FAMILIA: NOTIFICACIÓN Y GESTIÓN DE CIBERINCIDENTES....231
9.4 FAMILIA: FORMACIÓN Y CONCIENCIACIÓN EN CIBERSEGURIDAD....232
10. REFERENCIAS....233
11. ABREVIATURAS....234

1. INTRODUCCIÓN

1. La adquisición de un producto o la contratación de un servicio de seguridad TIC que va a manejar información nacional clasificada o información sensible debe estar precedida de un proceso de comprobación de que los mecanismos de seguridad implementados en el producto o servicio son adecuados para proteger dicha información.
2. La evaluación y certificación de un producto o servicio de seguridad TIC es el único medio objetivo que permite valorar y acreditar su capacidad para manejar información de forma segura. En España, esta responsabilidad está asignada al Centro Criptológico Nacional (CCN) a través del RD 421/2004 de 12 de marzo en su Artículo 1 y en su Artículo 2.1, el cual establece que el Director del CCN es la autoridad de certificación de la seguridad de las tecnologías de la información y la comunicación y autoridad de certificación criptológica.
3. Así mismo, dentro del RD 3/2010 de 8 de enero, modificado por el RD 951/2015, de 23 de octubre, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración electrónica, se indica que el Organismo de Certificación del CCN será el responsable de determinar los requisitos exigibles a cada producto o servicio de Seguridad TIC en materia de certificaciones y/o evaluaciones adicionales.
4. En base a estas competencias, el CCN publica la guía **CCN-STIC 105 Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC)**. Este catálogo tiene como finalidad ofrecer a los organismos de la Administración un conjunto de productos o servicios STIC de referencia cuyas funcionalidades de seguridad relacionadas con el objeto de su adquisición han sido certificadas.
5. De esta forma, el CPSTIC permite proporcionar un nivel mínimo de confianza al usuario final en los productos o servicios adquiridos, en base a las mejoras de seguridad derivadas del proceso de evaluación y certificación y a un procedimiento de empleo seguro.
6. El CPSTIC consta de dos (2) partes: **Productos Aprobados** y **Productos y Servicios Cualificados**. En el apartado de **Productos Aprobados** se recogen aquellos productos que se consideran adecuados para el manejo de información clasificada, mientras que en el apartado de **Productos y Servicios Cualificados** se incluyen aquellos que cumplen los requisitos de seguridad exigidos para el manejo de información sensible en el ENS, en cualquiera de sus categorías (ALTA, MEDIA y BÁSICA).

TIPO DE PRODUCTO O SERVICIO	INFORMACIÓN QUE MANEJA
APROBADO	CLASIFICADA
CUALIFICADO	SENSIBLE (ENS)

Tabla 1. Tipos de productos o servicios incluidos en el CPSTIC

2. OBJETIVO

7. El objeto de este documento es el de presentar el Catálogo de Productos de Seguridad de las Tecnologías de la Información y Comunicación que recoge un listado de productos aprobados para el manejo de información clasificada y de productos y servicios cualificados para el manejo de información sensible, de forma que pueda servir de referencia a la Administración Pública.

3. ALCANCE

8. En el apartado de Productos Cualificados de este documento se incluyen todos aquellos que han superado con éxito el proceso de inclusión en el CPSTIC descrito en la guía CCN-STIC 106 Procedimiento de inclusión de productos de seguridad TIC cualificados en el CPSTIC [1] y que por lo tanto se consideran cualificados para ser utilizados en sistemas de Categoría Alta en el ENS.
9. Este hecho implica que todos ellos poseen una certificación funcional Common Criteria en la que se incluyen los Requisitos Fundamentales de Seguridad (RFS) descritos en la guía CCN-STIC 140 Taxonomías de referencia para productos de seguridad TIC [2] para la familia en la que se consideran o que, en ausencia de productos que posean la certificación requerida, se han añadido de acuerdo al supuesto de excepcionalidad tras haber superado una evaluación STIC complementaria.
10. En el caso de productos multipropósito, éstos pueden aparecer en una o varias familias, siempre y cuando se haya certificado que cumplen con los RFS correspondientes a cada una de ellas. En estos casos, que un producto se considere cualificado para una determinada familia de productos no implica que lo esté para el resto de las familias en las que pueda encuadrarse, al margen de que implemente la funcionalidad asociada.
11. En el apartado de Productos Aprobados se incluyen todos aquellos que han superado con éxito el proceso de inclusión en el CPSTIC descrito en la guía CCN-STIC 102 Procedimiento para la Aprobación de Productos de seguridad TIC para manejar información Nacional clasificada [3] y que por lo tanto se consideran aprobados para manejar información clasificada. El nivel máximo de clasificación de la información para la que se aprueba su uso vendrá especificado en cada producto de manera individual.

4. INCLUSIÓN DE UN PRODUCTO DEL CPSTIC

12. Para la inclusión de un producto o servicio en el catálogo, el CCN tendrá en cuenta los siguientes criterios:

    a) En el caso de **Productos Aprobados** para el manejo de información clasificada, el máximo nivel de clasificación de la información que puede manejar (DIFUSIÓN LIMITADA, CONFIDENCIAL, RESERVADO, SECRETO).

    b) En el caso de **Productos y Servicios Cualificados**, la máxima categoría del sistema de información en el que puede emplearse (ALTA, MEDIA, BÁSICA[1]).

    c) Las funcionalidades de seguridad que implementa el producto o servicio y las certificaciones aportadas.

    d) Otros aspectos como el análisis de riesgos del producto o servicio, la necesidad operativa dentro de la Administración, la disponibilidad o no de otros productos o servicios certificados que satisfagan la misma funcionalidad, etc.

    En función de esta información, se determinarán las pruebas o evaluaciones que deberá superar el producto o servicio de seguridad TIC correspondiente.

13. El procedimiento para la inclusión de un producto STIC aprobado en el CPSTIC para manejar información nacional clasificada se describe en la guía **CCN-STIC 102 Procedimiento para la Aprobación de Productos de seguridad TIC para manejar información Nacional clasificada** [3]. Los requisitos exigidos, la relación de la documentación y el equipamiento a aportar para realizar la evaluación criptológica se describe en la **CCN-STIC 130 Requisitos de Aprobación de Productos de Cifra para Manejar Información Nacional Clasificada** [4] y para realizar la evaluación TEMPEST se describe en la guía **CCN-STIC 151 Evaluación y Clasificación TEMPEST de equipos** [5]**.** Ver **Figura 1.**

14. El producto o servicio STIC cualificado por el CCN hará referencia a una versión concreta y con una configuración determinada, de acuerdo a unas normas de utilización que serán descritas en un procedimiento de empleo seguro. Dicho procedimiento será distribuido por la empresa fabricante junto con el producto y además se publicará como una guía CCN-STIC de la serie 1000.

1 Clasificación por categorías definida en el ENS.

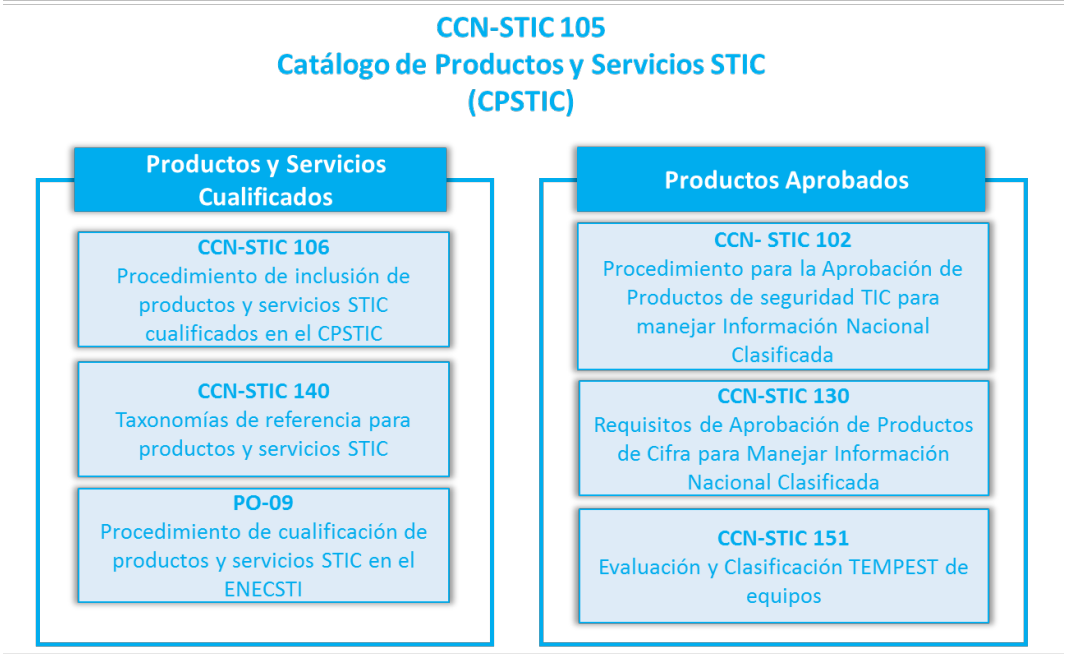


Figura 1. Inclusión de productos y servicios de seguridad en el CPSTIC

5. REVISIÓN DE VALIDEZ DE PRODUCTOS STIC

15. Periódicamente se realizará una revisión de validez de los productos y servicios incluidos en el catálogo con el fin de garantizar que siguen cumpliendo con los requisitos exigidos para formar parte de él. La fecha de revisión de validez se indica en la ficha correspondiente a cada producto.

16. Por esta razón, tras una revisión de validez, un producto o servicio incluido en el catálogo puede bajar el máximo nivel de clasificación que está autorizado a procesar en el caso de los productos aprobados e incluso puede ser excluido cuando se dejen de cumplir los requisitos exigidos para su inclusión.

6. EXCLUSIÓN DE UN PRODUCTO O SERVICIO DEL CPSTIC

17. Un producto o servicio podrá ser excluido del CPSTIC por cualquiera de los siguientes motivos:

    a) Caducidad del certificado de Producto o Servicio Cualificado STIC. Todos los certificados serán emitidos con una fecha de revisión de validez (que dependerá de la familia considerada), a partir de la cual el solicitante deberá remitir una nueva solicitud de inclusión siguiendo el procedimiento descrito anteriormente. En el caso de que esta solicitud no se lleve a cabo, el CCN podrá excluir el producto o servicio del CPSTIC.

    b) Revocación o caducidad de alguna de las certificaciones requeridas al producto o servicio para acceder al catálogo: *Common Criteria*, LINCE, conformidad con el ENS, según el caso.

    c) Pérdida de las condiciones de excepcionalidad. En el caso de que el producto o servicio haya sido incluido en el catálogo por alguno de los supuestos de excepcionalidad, podrá ser excluido una vez deje de cumplirse alguno de ellos: aparición de productos o servicios sustitutivos con la certificación adecuada, pérdida de la consideración de producto o servicio estratégico para la Administración, etc.

    d) Que no cumpla con los RFS vigentes en el momento de la revisión de validez. Los avances tecnológicos pueden dejar obsoleta la tecnología empleada en unos casos y en otros hacer que se reduzca de forma considerable la seguridad del mismo, lo que implicará una evolución de los RFS.

    e) Que presente vulnerabilidades críticas no corregidas. En este caso, podrá solicitarse al fabricante un informe de impacto de dichas vulnerabilidades. Si este informe determinase que la vulnerabilidad es explotable siguiendo el PES, este será excluido del catálogo.

7. PRODUCTOS CUALIFICADOS

PRODUCTOS CUALIFICADOS







INFORMACIÓN IMPORTANTE

Todos los productos o servicios incluidos en este apartado han superado un proceso de evaluación/certificación en el que se ha comprobado que implementan, con cierto nivel de garantía, las funcionalidades de seguridad requeridas por los Requisitos Fundamentales de Seguridad definidos en la CCN-STIC-140 para la familia o familias a las que pertenecen.

Esta garantía avala su robustez frente a atacantes con un potencial determinado por el tipo de certificación que presentan, que en ningún caso alcanza el potencial que suelen presentar aquellos ataques motivados por estados.

Asimismo, el proceso de Cualificación no supone, en ningún caso, un posicionamiento del CCN sobre la fiabilidad del fabricante o proveedor de servicio. Esto tendría impacto en aquellos productos o servicios que, por su arquitectura, envían información de usuario a servidores externos a la organización controlados por el fabricante o proveedor de servicio, cuyas malas prácticas podrían derivar en divulgación no autorizada de datos de usuario o en su utilización con fines no declarados.

Estos aspectos son riesgos inherentes al producto o servicio que el Responsable de Seguridad del Sistema deberá valorar y, en caso de que resulten inasumibles, mitigar.

INFORMACIÓN IMPORTANTE

7.1 CATEGORÍA: CONTROL DE ACCESO

7.1.1 FAMILIA: CONTROL DE ACCESO A RED (NAC)

ClearPass Policy Manager (C1000, C2000, C3000)

Versión	6.9
Fabricante	Aruba
Familia	Control de acceso a red (NAC)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2019
Revisión de Validez	31/08/2022

Descripción

La familia de productos ClearPass de seguridad para el control de acceso a la red ofrece elaboración de perfiles, autenticación y autorización para usuarios, sistemas y dispositivos que intentan acceder a los recursos de TI. ClearPass se ha diseñado paraabordar los retos de seguridad asociados con una organización TI: Acceso seguro a la red (802.1X y Radius), funciones de NAC, Implementación de portal de Invitados e interno, soporte de funcionalidades BYOD, integración con Firewalls (PaloAlto, CheckPoint, Forninet y mas) todo ello mediante la integración múltiples fuentes de autenticación (Directorios activos, LDAP, BBDD y provedores externos de identidad)

Observaciones

CCN-STIC-1103 Procedimiento de empleo seguro ClearPass 6.9

Pulse Policy Secure (PSA-300, PSA-3000, PSA-5000, PSA-7000c/f y appliance virtual)

Versión	9.1R1
Fabricante	Pulse Secure
Familia	Control de Acceso a Red (NAC)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2020
Revisión de Validez	30/11/2022



Descripción

La solución de control de acceso corporativo Pulse Policy Secure (PPS) incorpora tanto elementos de perfilado de elementos de red como de cumplimiento de políticas de seguridad corporativa (NAC). Permite autenticar tanto usuarios (RBAC), sistemas u otrosdispositivos (802.1x, Radius, TACACS+) dentro del entorno corporativo, como el posterior enforcement (802.1x, SNMP).
Se integra de forma nativa con diferentes elementos corporativos como pueden ser MDMs, Firewalls o Switches dentro del entorno, para así hacer cumplir las normativas de seguridad y el control de acceso.
Incorpora la capacidad de federación de perfiles de usuarios con terceros como pueden ser la solución de VPN (PCS) de Pulse Secure o diferentes Firewalls a través de diferentes tecnologías (syslog, IF-MAP, API) permitiendo así elevar la seguridad y el manejo del control de acceso a niveles corporativos.
La solución incluye también funcionalidades de detección especificas para entornos IoT, así como capacidades de análisis de comportamiento (Behaviour Analytics) como una integración avanzada para el análisis de Host (Hostchecker; con o sin Agente), elevando de esta manera el grado de seguridad en las redes corporativas y protegiéndolas contra elementos no autorizados & autenticados.

Observaciones

CCN-STIC 1109 Procedimiento de Empleo Seguro Pulse Policy Secure v9.1R1

INFORMACIÓN IMPORTANTE

Forescout 8.1 (CT-R, CT-100, CT-1000, CT-2000, CT-4000, CT-10000, CEM-5, CEM-10, CEM-25, CEM-50, CEM-100, CEM-150, and CEM-200, 5110, 5120, 5140, 5160)	
Versión	8.1
Fabricante	Forescout
Familia	Control de Acceso a Red (NAC)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2020
Revisión de Validez	30/09/2022

Descripción

La plataforma Forescout es una plataforma unificada de seguridad que permite a las empresas y organismos oficiales obtener información completa sobre el estado de sus entornos empresariales ampliados y orquestar medidas destinadas a reducir el riesgo operativo y de ciberseguridad. Se despliega de forma rápida y segura en entornos de campus, centros de datos, la nube y redes de OT. Ofrece descubrimiento, clasificación en tiempo real y evaluación continua de estado, sin necesidad de agentes.
Para más información, véase: https://forescouttechnologies.es

Observaciones

CCN-STIC-1106 Procedimiento de empleo seguro Forescout v8.1

Citrix ADC (formerly NetScaler) MPX 14030 FIPS, MPX 14060 FIPS y MPX 14080 FIPS	
Versión	Platinum Edition Version 11.1
Fabricante	Citrix Systems
Familia	Control de Acceso a Red (NAC)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2020
Revisión de Validez	30/09/2022



Descripción

Citrix ADC (antes NetScaler) es un Application Delivery Controller con funciones específicas de seguridad para el control de acceso a la red corporativa de usuarios y dispositivos, permitiendo discriminar en el acceso no solo por usuario sino también porel estado de la seguridad en el momento de la conexión y durante la misma. Tanto en accesos SSL VPN como mediante un portal completo de aplicaciones servido al usuario -donde están sus aplicaciones internas, SaaS y aplicaciones y desktops virtuales-, se autenticará al usuario (con opción de múltiples factores, incluso con OTP Nativo sin necesidad de otro OTP adicional) contra un sistema corporativo o mediante federación de identidades, se tendrá en cuenta su perfil (usuario, grupos, atributos en el Directorio), y se comprobará la seguridad del dispositivo (antivirus, firewall, dominio, procesos activos, etc.) y la de la conexión (punto de acceso, ubicación desde la que se accede, etc.), para aplicar según el resultado unas políticas de acceso granulares,ya sea en el propio appliance o en un dispositivo de red posterior como un firewall. De esta forma se garantiza el acceso a cada recurso interno únicamente de aquellas combinaciones aprobadas de usuario/dispositivo/conexión.

Observaciones

Procedimiento de empleo pendiente de publicación.

INFORMACIÓN IMPORTANTE

OpenNAC Enterprise	
Versión	V1.2
Fabricante	OpenCloud Factory
Familia	Control de Acceso a Red (NAC)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2018
Revisión de Validez	30/06/2022

Descripción

OpenNAC Enterprise , Network Access Control de nueva generación con capacidad para poder gestionar de manera segura el acceso a las redes corporativas y así poder obtener el control total sobre la red. Disponible como Virtual Appliance, permite su puestaen marcha en grandes redes corporativas con diversos centros de datos y oficinas remotas. OpenNAC Enterprise utiliza múltiple métodos de descubrimiento de dispositivos (802.1x, Traps, Agente..); el Sensor (sonda) admite la visibilidad de activos sin 802.1X y logra una inspección profunda de paquetes fuera de banda. La solución proporciona soporte multi-vendor para infraestructura de red, basado en múltiples métodos de autenticación y enforcement a través de la segmentación (VLAN), microsegmentación etc. Puede integrarse con múltiples LDAPs y Directorios Activos. Es una solución completamente modular en función de la necesidad de las organizaciones. www.opencloudfactory.com https://www.opencloudfactory.com/solucion-opennac/

Observaciones

Procedimiento de empleo pendiente de publicación.

EMMA	
Versión	-
Fabricante	OpenCloud Factory / CCN
Familia	Control de Acceso a Red (NAC)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2020
Revisión de Validez	31/10/2022

Descripción

EMMA es una solución de Visualización de activos en una red, su autenticación y segregación, así como la automatización de auditorías de seguridad de la infraestructura. El alcance de la cualificación abarca los siguiente módulos de EMMA:
Visibilidad, Control / Respuesta, Segmentación, Cumplimiento, BYOD y Gestión de invitados.
Se recoge el inventario y perfilado del equipo que se podrá utilizar en las políticas de acceso a la conexión remota. Adicionalmente, permite definir y aplicar políticas de acceso en función de una postura de seguridad basada en el nivel de bastionado, además de otros factores (horario de la conexión, características del equipo, role de usuario etc.). EMMA se integrará con soluciones del ecosistema CCN-CERT: ROCIO y ANA.
https://www.ccn-cert.cni.es/pdf/documentos-publicos/4153-datasheet-emma/file.html

Observaciones

CCN-STIC-1105 Procedimiento de empleo seguro EMMA

INFORMACIÓN IMPORTANTE

Cisco Identity Services Engine (ISE)	
Versión	2.6
Fabricante	Cisco Systems
Familia	Control de Acceso a Red (NAC)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2020
Revisión de Validez	31/12/2022

Descripción

Cisco ISE es una plataforma de control de acceso que combina la autenticación, autorización y trazabilidad (AAA), así como la gestión de usuarios, en un appliance. ISE permite control de acceso seguro en las conexiones cableadas, inalámbricas y VPN. Permite realizar búsquedas en la red para dar visibilidad sobre quién o qué accede a los distintos recursos.
Productos cualificados:
- Cisco Identity Services Engine Appliance 3515, 3595, 3615, 3655, 3695
- Cisco Identity Services Engine Virtual Machine (ISE-VM) en ESXi 6.7 ejecutado sobre UCSC-C220-M5SX
- Cisco Identity Services Engine ejecutado sobre Cisco Application Deployment Engine (ADE) Release 3.0 operating system (ADE-OS)

Observaciones

CCN-STIC-1104 Procedimiento de Empleo CISCO ISE 2.6

7.1.2 FAMILIA: DISPOSITIVOS BIOMÉTRICOS

Pendiente de recepción de solicitudes de productos que cumplan con Requisitos Fundamentales de Seguridad (RFS) correspondientes a esta familia.

7.1.3 FAMILIA: DISPOSITIVOS SINGLE SIGN-ON

Pendiente de recepción de solicitudes de productos que cumplan con Requisitos Fundamentales de Seguridad (RFS) correspondientes a esta familia.

INFORMACIÓN IMPORTANTE

7.1.4 FAMILIA: SERVIDORES DE AUTENTICACIÓN

ClearPass Policy Manager (C1000, C2000, C3000)

Versión	6.9
Fabricante	Aruba
Familia	Servidores de Autenticación
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2019
Revisión de Validez	31/08/2022

Descripción

La familia de productos ClearPass de seguridad para el control de acceso a la red ofrece elaboración de perfiles, autenticación y autorización para usuarios, sistemas y dispositivos que intentan acceder a los recursos de TI. ClearPass se ha diseñado paraabordar los retos de seguridad asociados con una organización TI: Acceso seguro a la red (802.1X y Radius), funciones de NAC, Implementación de portal de Invitados e interno, soporte de funcionalidades BYOD, integración con Firewalls (PaloAlto, CheckPoint, Forninet y mas) todo ello mediante la integración múltiples fuentes de autenticación (Directorios activos, LDAP, BBDD y provedores externos de identidad)

Observaciones

CCN-STIC-1103 Procedimiento de empleo seguro ClearPass 6.9

Pulse Policy Secure (PSA-300, PSA-3000, PSA-5000, PSA-7000c/f y appliance virtual)

Versión	9.1R1
Fabricante	Pulse Secure
Familia	Servidores de Autenticación
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2020
Revisión de Validez	30/11/2022



Descripción

La solución de control de acceso corporativo Pulse Policy Secure (PPS) incorpora tanto elementos de perfilado de elementos de red como de cumplimiento de políticas de seguridad corporativa (NAC). Permite autenticar tanto usuarios (RBAC), sistemas u otrosdispositivos (802.1x, Radius, TACACS+) dentro del entorno corporativo, como el posterior enforcement (802.1x, SNMP).
Se integra de forma nativa con diferentes elementos corporativos como pueden ser MDMs, Firewalls o Switches dentro del entorno, para así hacer cumplir las normativas de seguridad y el control de acceso.
Incorpora la capacidad de federación de perfiles de usuarios con terceros como pueden ser la solución de VPN (PCS) de Pulse Secure o diferentes Firewalls a través de diferentes tecnologías (syslog, IF-MAP, API) permitiendo así elevar la seguridad y el manejo del control de acceso a niveles corporativos.
La solución incluye también funcionalidades de detección especificas para entornos IoT, así como capacidades de análisis de comportamiento (Behaviour Analytics) como una integración avanzada para el análisis de Host (Hostchecker; con o sin Agente), elevando de esta manera el grado de seguridad en las redes corporativas y protegiéndolas contra elementos no autorizados & autenticados (RADIUS, A

Observaciones

CCN-STIC 1109 Procedimiento de Empleo Seguro Pulse Policy Secure v9.1R1

INFORMACIÓN IMPORTANTE

7.1.5 FAMILIA: DISPOSITIVOS ONE-TIME PASSWORD

Pendiente de publicación los Requisitos Fundamentales de Seguridad (RFS) de esta familia.

7.1.6 FAMILIA: GESTIÓN DE ACCESO PRIVILEGIADO (PAM)

IBM Secret Server Government Edition	
Versión	10.7
Fabricante	IBM
Familia	Gestión de acceso privilegiado (PAM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2020
Revisión de Validez	30/11/2022

Descripción

IBM Secret Server es una solución de gestión de cuentas privilegiadas que permite descubrir, securizar, administrar y auditar contraseñas, credenciales así como monitorizar y grabar las sesiones privilegiadas. Permite gestionar el acceso a cada cuenta privilegiada y activo crítico, automatizar las mejores prácticas de seguridad y cumplir las regulaciones normativas.

Las capacidades de PAM de Secret Server para la administración de las cuentas privilegiadas incluyen:

- Gestión del Ciclo de Vida de las credenciales con privilegios:
  - Descubrimiento Automatizado de cuentas privilegiadas y “onboarding” de las mismas en un Repositorio central seguro
  - Rotado automático de las credenciales y Gestión, control y auditoria de las sesiones privilegiadas
- Análisis del comportamiento del usuario privilegiado
- Gestión de cuentas de servicio
- Políticas de acceso basadas en RBAC y Gestión de políticas de seguridad.
- Arquitectura escalable. Alta Disponibilidad y DR. Integración con múltiples plataformas Out-Of-The-Box
- Módulo de Reporting capaz de generar informes totalmente a medida
- Securización de los procesos de DevOps.

Observaciones

CCN-STIC-1101 Procedimiento de Empleo Seguro SECRET SERVER de THYCOTIC

INFORMACIÓN IMPORTANTE

Thycotic Secret Server Government Edition	
Versión	10.1
Fabricante	Thycotic
Familia	Gestión de acceso privilegiado (PAM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2019
Revisión de Validez	30/11/2022

Descripción

Thycotic Secret Server es una solución de gestión de cuentas privilegiadas que permite descubrir, securizar, administrar y auditar contraseñas, credenciales así como monitorizar y grabar las sesiones privilegiadas. Permite gestionar el acceso a cada cuenta privilegiada y activo crítico, automatizar las mejores prácticas de seguridad y cumplir las regulaciones normativas.

Las capacidades de PAM de Secret Server para la administración de las cuentas privilegiadas incluyen:

- Gestión del Ciclo de Vidade las credenciales con privilegios:
  - Descubrimiento Automatizado de cuentas privilegiadas y “onboarding” de las mismas en un Repositorio central seguro
  - Rotado automático de las credenciales y Gestión, control y auditoria de las sesiones privilegiadas
- Análisis del comportamiento del usuario privilegiado
- Gestión de cuentas de servicio
- Políticas de acceso basadas en RBAC y Gestión de políticas de seguridad.
- Arquitectura escalable. Alta Disponibilidad y DR. Integración con múltiples plataformas Out-Of-The-Box
- Módulo de Reporting capaz de generar informes totalmente a medida
- Securización de los procesos de DevOps.

Observaciones

CCN-STIC-1101 Procedimiento de Empleo Seguro SECRET SERVER de THYCOTIC

INFORMACIÓN IMPORTANTE

CyberArk Privileged Account Security Solution	
Versión	10.4
Fabricante	CyberArk
Familia	Gestión de acceso privilegiado (PAM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2020
Revisión de Validez	31/12/2022

Descripción

CyberArk Core PAS es una solución de seguridad que permite proteger, controlar y monitorizar el acceso privilegiado a infraestructura locales, en la nube e híbridas. Permite a las organizaciones administrar y proteger las credenciales de las cuentas privilegiadas y los derechos de acceso, monitorizar y controlar la actividad de las cuentas privilegiadas, identificar las actividades sospechosas y responder a las amenazas.

• Asegurar y controlar centralmente el acceso a las credenciales privilegiadas basadas en políticas de seguridad definidas administrativamente.

• Aislar y asegurar sesiones de usuarios privilegiados. Las capacidades de monitorización y grabación permiten a los equipos de seguridad ver sesiones privilegiadas en tiempo real, suspender automáticamente y terminar remotamente las sesiones sospechosas.

• Detectar, alertar y responder a actividades privilegiadas anómalas.

• Controlar el acceso de privilegios mínimos para * NIX y Windows. La solución permite a los usuarios con privilegios ejecutar comandos administrativos autorizados desde sus sesiones nativas de Unix o Linux, a la vez que se eliminan los privilegios de raíz innecesarios.

• Proteger los controladores de dominio de Windows.

Observaciones

CCN-STIC-1108 Procedimiento de empleo seguro CyberArk Privileged Account Security Solution 10.4

INFORMACIÓN IMPORTANTE

Safeguard for Privileged Passwords	
Versión	6.0 LTS
Fabricante	One Identity
Familia	Gestión de acceso privilegiado (PAM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2021
Revisión de Validez	30/04/2022

Descripción

Safeguard for Privileged Passwords (SPP) es una solución de seguridad de gestión de cuentas privilegiadas cuya función principal es prevenir el mal uso potencial de las cuentas privilegiadas en los sistemas IT locales, híbridos o en la nube así como las aplicaciones de las organizaciones, permitiendo almacenar, gestionar y monitorizar el uso de estas cuentas por parte de los usuarios. SPP automatiza, controla y asegura la gestión de credenciales privilegiadas con un acceso basado en roles y flujos automatizados.

• Arquitectura escalable basada en dispositivos físicos o virtuales en alta disponibilidad escalable en modelo Activo-Activo-Activo.
• Gestión del acceso basado en un motor de políticas, flujos de aprobación y revisión, etc.
• Informes de auditoría de la actividad registrada en los dispositivos.
• Importar, descubrir y rotado automático de cuentas privilegiadas y contraseñas de los sistemas y aplicaciones.
• Gestión de cuentas de servicio, IIS, tareas programadas y COM+ en entornos Microsoft.
• Integración con Safeguard for Sessions para extender las capacidades del SPP para la grabación de sesiones, análisis de comportamiento y detección.
• Gestión de secretos en entornos DevOps y RPA.
• Integración con sistemas externos mediante RestAPI

Observaciones

Procedimiento de empleo seguro pendiente de publicación

INFORMACIÓN IMPORTANTE

7.1.7 FAMILIA: GESTIÓN DE IDENTIDADES (IM)

One Identity Manager	
Versión	v8.1
Fabricante	One Identity
Familia	Gestión de identidades (IM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2020
Revisión de Validez	30/04/2023

Descripción

One Identity Manager es una solución de gobierno y gestión de identidades (IAM) que permite automatizar la gestión de los accesos de los usuarios, permitiendo que accedan a las aplicaciones y a los datos estrictamente necesarios para desempeñar su trabajo. La solucion permite que la administración de los usuarios, sus identidades digitales y sus accesos puedan ser impulsadas por otros departamentos como RRHH.

• Gestione el acceso a recursos en las instalaciones, en la nube e híbridos desde cualquier departamento de la organización

• Reduzca el riesgo al asegurarse de que los usuarios tengan solo los accesos que necesitan

• Satisfaga auditorías e iniciativas de cumplimiento con políticas de confirmación/recertificación

Otorgue derechos de acceso en función de roles, reglas y políticas definidas. Establezca procesos estándares de aprovisionamiento y desaprovisionamiento para sus empleados y proveedores. Administre de forma rápida y fácil el acceso a recursos a medida que las responsabilidades del usuario evolucionen con la empresa.

Observaciones

CCN-STIC-1107 Procedimiento de Empleo Seguro One Identity Manager 8.1

INFORMACIÓN IMPORTANTE

7.2 CATEGORÍA: EXPLOTACIÓN DE LA SEGURIDAD

7.2.1 FAMILIA: ANTI-VIRUS/EPP (ENDPOINT PROTECTION PLATFORM)

Intercept X Advanced with EDR	
Versión	2.5.4 BETA/ 10.8.6/2.0.16 BETA
Fabricante	Sophos
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/03/2020
Revisión de Validez	31/08/2022

Descripción

Sophos Intercept X Advanced con EDR es una solución que ofrece protección avanzada de puesto trabajo y servidores. Está especialmente diseñada para detener la gran mayoría de ataques y hacer frente a nuevas amenazas como ransomware, fileless, o ataques zero-day. Con diferentes capas de protección, las primeras están diseñadas para reducir la superficie de ataque a través del control de USBs, control de aplicaciones, control de navegación y DLP. Posteriormente tiene capas que detectan, primero lo malo conocido a través de las firmas que desarrollan los Sophos LABS y, segundo, lo malo desconocido, como el ransomware, gracias a la monitorización de procesos, el control de comportamiento, utilizando la tecnología única de Deep Learning que permite detectar malware no identificado previamente, y la detección de técnicas de explotación/ataque y de post compromiso. Además, la solución cuenta con capacidades avanzadas de detección y respuesta inteligentes (EDR) que permiten a la organización hacer investigaciones y threat hunting para ser proactivo a la hora de identificar amenazas e investigar posibles eventos maliciosos, así como comprender el alcance y el impacto o buscar los indicadores de amenazas en toda la red. Todo ello desde una única consola de gestión

Observaciones

CCN-STIC 1207 Procedimiento de Empleo Seguro Sophos Central Intercept X

INFORMACIÓN IMPORTANTE

ESET Endpoint Security	
Versión	7.2.2055.3
Fabricante	ESET SPOL S.R.O
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/04/2020
Revisión de Validez	30/07/2022

Descripción

ESET Endpoint Security es una solución fácil de implementar y utilizar, administrable de forma centralizada, con protección multicapa que se basa en tres pilares básicos: primar el rendimiento del sistema, una detección eficaz y no importunar al usuario con falsos positivos. Este enfoque de protección multicapa permite a ESET detectar y/o bloquear diferentes tipos de amenazas, como ransomware, ataques sin archivos, botnets, ataques de red o exploits.
Los componentes de protección que han sido analizados en el proceso de cualificación son:
1) Antivirus y antiespía: Elimina todo tipo de amenazas tales como virus, rootkits, gusanos y software espía.
2) Sistema avanzado de prevención de intrusiones (HIPS): Permite controlar los procesos, archivos y claves deregistro a través de reglas. Protege frente a modificaciones no autorizadas y detecta las amenazas basándose en su comportamiento en el sistema.
3) Análisis avanzado de memoria: Monitoriza el comportamiento de todos los procesos y los analiza cuando seejecutan en memoria. Esto permite una prevención más efectiva contra las infecciones, incluso en el caso de que estén especialmente diseñadas para evitar su detección.
4) Protección contra botnets: Evita que los equipos de tu empresa formen parte de una

Observaciones

CCN-STIC 1204 Procedimiento de empleo seguro ESET Endpoint Security 7

Cytomic EDR/EPDR	
Versión	3.71 (Protection Agent v8.0)
Fabricante	Panda Security
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2020
Revisión de Validez	28/03/2023

Descripción

Cytomic EPDR integra en una única solución un conjunto completo de tecnologías preventivas en el endpoint, con capacidades EDR y el Servicio Zero-Trust Application. Extiende las capacidades de prevención, detección y respuesta con una gama completa de capacidades de protección del endpoint necesarias para evitar que las amenazas lleguen a los dispositivos y servidores y reducir la superficie de ataque.
Sus capacidades de protección avanzada cubren todas fases de la Seguridad Adaptativa: Prevención, Detección, Respuesta y Remediación, gracias a los servicios gestionados: servicio de clasificación del 100% de los programas, procesos y ejecutables en los endpoints y el servicios de Threat Hunting y Análisis Forense, que permite una enforzamiento de la seguridad corporativa continua.

Observaciones

CCN-STIC-1211 Procedimiento de empleo seguro Cytomic EPDR

INFORMACIÓN IMPORTANTE

Panda Adaptive Defense 360

Versión	3.71 (Protection Agent v8.0)
Fabricante	Panda Security
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2020
Revisión de Validez	28/02/2023

Descripción

Panda Adaptive Defense 360 es una solución de seguridad completa para los puestos de trabajo, portátiles y servidores que además de proteger contra amenazas conocidas, avanzadas y zero-day, ransomware y ataques de seguridad fileless (en memoria) y malwareless, incluye firewall personal, IPS/IDS, anti-spam, anti-spam en correo, filtrado y categorización en navegación web y control de dispositivos, entre otras técnicas de seguridad y control de productividad.
Sus capacidades de protección avanzada cubrentodas fases de la Seguridad Adaptativa: Prevención, Detección, Respuesta y Remediación, gracias a los servicios gestionados: servicio de clasificación del 100% de los programas, procesos y ejecutables en los endpoints y el servicios de Threat Hunting y Análisis Forense, que permite una enforzamiento de la seguridad corporativa continua.

Observaciones

CCN-STIC-1213 PES Panda Adaptive Defense 360

Checkpoint Endpoint Security (Sandblast Agent)

Versión	E82.40 (82.40.1159)
Fabricante	Check Point Software Technologies
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/05/2020
Revisión de Validez	31/10/2022

Descripción

Check Point SandBlast Agent es una solución de protección avanzada para endpoints y navegadores de Internet, garantiza protección completa contra los diferentes vectores de amenazas con capacidades de prevención, detección y respuesta. Incorpora una gestión integrada disponible en nube o instalación local. Prestaciones:
• Emulación de amenazas (Sandbox) y Extracción (Entrega archivos limpios a usuarios en tiempo real)
• Anti-Ransomware (prevención y reparación) y defensa contra ciberextorsión
• Anti-Bot,
• Anti-Exploit
• Anti-Malware.
• Análisis de comportamientos (detección y bloqueo)

Observaciones

CCN-STIC-1214 Procedimiento de Empleo Seguro Checkpoint Endpoint Security (SBA)

INFORMACIÓN IMPORTANTE

Kaspersky Endpoint Security for Windows	
Versión	11.0.0.6499 AES256
Fabricante	Kaspersky Labs
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2020
Revisión de Validez	31/05/2023

Descripción

Kaspersky Endpoint Security es una solución de protección avanzada que proporciona una protección integral mediante componentes de control (Control de dispositivos, Control Web, Control de anomalías adaptable) y de protección (Detección de comportamiento, Prevención de vulnerabilidades, Prevención de intrusiones en el host, Motor de reparación, Protección frente a amenazas en archivos, Protección frente a amenazas web, Protección frente a amenazas en el correo, Protección frente a amenazas en la red, Firewall, Prevención de ataques de BadUSB, Proveedor de protección AMSI). Este enfoque de protección multicapa permite detectar y bloquear amenazas como Ransomware, ataques sin archivos (Fileless), ataques de día cero, ataques de red o ataques mediante el uso de Exploits o técnicas Phishing. Sus capacidades de protección avanzada cubren las fases de Seguridad Adaptativa de Prevención, Detección y Respuesta (Remediación). Cuenta con capacidades avanzadas de detección y respuesta inteligentes que permiten hacer investigaciones, análisis forense y Threat Hunting para ser proactivo a la hora de identificar amenazas e investigar eventos maliciosos, así como buscar los indicadores de amenazas en toda la red. Todo ello desde una única consola de gestión.

Observaciones

CCN-STIC-1209 Procedimiento de Empleo Seguro Kaspersky Endpoint Security 11 for Windows

McAfee Endpoint Security	
Versión	10.6 with ePolicy Orchestrator 5.3.3
Fabricante	McAfee
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2020
Revisión de Validez	31/01/2023

Descripción

El endpoint de McAfee integra capacidades de antivirus, aprendizaje automático, prevención de exploits, firewall y control web. Proporciona una gestión centralizada y una visualización integral de las amenazas para reforzar las defensas y realizar cambiosen las políticas globales de protección. Las actividades de escaneo en tiempo real, análisis en la nube, contención de aplicaciones y la corrección de reversión trabajan juntas para limitar el impacto de los archivos sospechosos y el malware de día cero.Las detecciones y remediaciones manuales se reemplazan por análisis, contención y remediación automáticos para detener las amenazas antes de que se propaguen y devuelvan los endpoints a un estado saludable. Dispone de una tecnología sencilla, integrada,automatizada y adaptable de detección y respuesta de terminales (EDR). Las investigaciones guiadas por IA facilitan las tareas a los analistas con cualquier nivel de experiencia.

Observaciones

CCN-STIC-1208 Procedimiento de Empleo Seguro Mcafee Endpoint

INFORMACIÓN IMPORTANTE

Mobileiron Mobile Threat Defense – MTD	
Versión	11.1
Fabricante	Mobileiron
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2021
Revisión de Validez	30/04/2022

Descripción

MobileIron Threat Defense permite supervisar, administrar y securizar los dispositivos móviles frente a ciberataques en dispositivos, redes y aplicaciones. Detecta las amenazas, tanto conocidas, como zero-day, incluso sin conectividad en red. Los cuatro pilares que definen esta funcionalidad de seguridad son la detección proactiva de amenazas y ataques, la corrección puntual, una mayor visibilidad de los dispositivos y de la red y una fácil administración.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Falcon Sensor	
Versión	6.27.14102
Fabricante	CrowdStrike
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/11/2021
Revisión de Validez	30/04/2022

Descripción

La plataforma CrowdStrike Falcon®, construida sobre conocimiento de adversarios (Inteligencia de amenazas) ofrece y unifica la higiene de TI, el antivirus de nueva generación, la detección y respuesta de puntos finales (EDR), threat hunting y la inteligencia de amenazas, todo ello a través de un único agente ligero de despliegue rápido y sencillo sin requerir reinicio ni impacto significativo en el rendimiento de los sistemas protegidos.

El agente de Falcon registra todas las actividades de interés en un punto final (puestos de trabajo, servidores, movilidad y cloud) para una inspección más profunda, incluso aquellas que evaden las medidas de prevención estándar, aplicando técnicas de Deep Machine Learning e IA, Protección basada en el comportamiento del Indicador de Ataque (IOA), protección antiexploit y gestión de IOCs.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Deep Security (Manager y Agente/Relay Linux/Windows)	
Versión	11
Fabricante	Trend Micro
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2021
Revisión de Validez	31/05/2024

Descripción

Deep Security es la respuesta de Trend Micro para proteger el cloud híbrido ya sean servidores físicos o virtuales. Gracias a su agente ligero, el cual incorpora funcionalidades: EDR (con respuesta frente a amenazas conocidas, zero-day), reputación web, control de aplicaciones, supervisión de logs, Supervisión de Integridad (FIM), Firewall de Host y Host IPS (que incorpora la tecnología de parcheado virtual), ayuda a mejorar la postura de seguridad proporcionando seguridad, visibilidad y control. La cualificación abarca los siguientes componentes: Manager, Agente/Relay Linux y el Agente/Relay Windows. El *Virtual Appliance* no está cualificado.

Observaciones

CCN-STIC-1216 PES Trendmicro Deep Security

7.2.2 FAMILIA: EDR (ENDPOINT DETECTION AND RESPONSE)

Intercept X Advanced with EDR	
Versión	2.5.4 BETA/ 10.8.6/2.0.16 BETA
Fabricante	Sophos
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/03/2020
Revisión de Validez	31/08/2022

Descripción

Sophos Intercept X Advanced con EDR es una solución que ofrece protección avanzada de puesto trabajo y servidores. Está especialmente diseñada para detener la gran mayoría de ataques y hacer frente a nuevas amenazas como ransomware, fileless, o ataques zero-day. Con diferentes capas de protección, las primeras están diseñadas para reducir la superficie de ataque a través del control de USBs, control de aplicaciones, control de navegación y DLP. Posteriormente tiene capas que detectan, primero lo malo conocido a través de las firmas que desarrollan los Sophos LABS y, segundo, lo malo desconocido, como el ransomware, gracias a la monitorización de procesos, el control de comportamiento, utilizando la tecnología única de Deep Learning que permite detectar malware no identificado previamente, y la detección de técnicas de explotación/ataque y de post compromiso. Además, la solución cuenta con capacidades avanzadas de detección y respuesta inteligentes (EDR) que permiten a la organización hacer investigaciones y threat hunting para ser proactivo a la hora de identificar amenazas e investigar posibles eventos maliciosos, así como comprender el alcance y el impacto o buscar los indicadores de amenazas en toda la red. Todo ello desde una única consola de gestión

Observaciones

CCN-STIC 1207 Procedimiento de Empleo Seguro Sophos Central Intercept X

INFORMACIÓN IMPORTANTE

McAfee Endpoint Security	
Versión	10.6 with ePolicy Orchestrator 5.3.3
Fabricante	McAfee
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2020
Revisión de Validez	31/01/2023

Descripción

El endpoint de McAfee integra capacidades de antivirus, aprendizaje automático, prevención de exploits, firewall y control web. Proporciona una gestión centralizada y una visualización integral de las amenazas para reforzar las defensas y realizar cambiosen las políticas globales de protección. Las actividades de escaneo en tiempo real, análisis en la nube, contención de aplicaciones y la corrección de reversión trabajan juntas para limitar el impacto de los archivos sospechosos y el malware de día cero.Las detecciones y remediaciones manuales se reemplazan por análisis, contención y remediación automáticos para detener las amenazas antes de que se propaguen y devuelvan los endpoints a un estado saludable. Dispone de una tecnología sencilla, integrada,automatizada y adaptable de detección y respuesta de terminales (EDR). Las investigaciones guiadas por IA facilitan las tareas a los analistas con cualquier nivel de experiencia.

Observaciones

CCN-STIC-1208 Procedimiento de Empleo Seguro Mcafee Endpoint

Cytomic EDR/EPDR	
Versión	3.71 (Protection Agent v8.0)
Fabricante	Panda Security
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2020
Revisión de Validez	28/03/2023

Descripción

Cytomic EPDR integra en una única solución un conjunto completo de tecnologías preventivas en el endpoint, con capacidades EDR y el Servicio Zero-Trust Application. Extiende las capacidades de prevención, detección y respuesta con una gama completa de capacidades de protección del endpoint necesarias para evitar que las amenazas lleguen a los dispositivos y servidores y reducir la superficie de ataque.

Sus capacidades de protección avanzada cubren todas fases de la Seguridad Adaptativa: Prevención, Detección, Respuesta y Remediación, gracias a los servicios gestionados: servicio de clasificación del 100% de los programas, procesos y ejecutables en los endpoints y el servicios de Threat Hunting y Análisis Forense, que permite una enforzamiento de la seguridad corporativa continua.

Observaciones

CCN-STIC-1211 Procedimiento de empleo seguro Cytomic EPDR

INFORMACIÓN IMPORTANTE

Panda Adaptive Defense 360

Versión	3.71 (Protection Agent v8.0)
Fabricante	Panda Security
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2020
Revisión de Validez	28/02/2023

Descripción

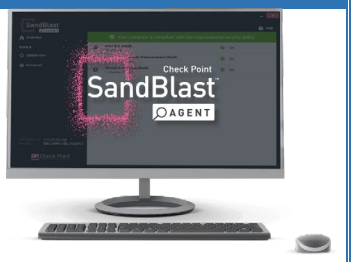
Panda Adaptive Defense 360 es una solución de seguridad completa para los puestos de trabajo, portátiles y servidores que además de proteger contra amenazas conocidas, avanzadas y zero-day, ransomware y ataques de seguridad fileless (en memoria) y malwareless, incluye firewall personal, IPS/IDS, anti-spam, anti-spam en correo, filtrado y categorización en navegación web y control de dispositivos, entre otras técnicas de seguridad y control de productividad.
Sus capacidades de protección avanzada cubren todas fases de la Seguridad Adaptativa: Prevención, Detección, Respuesta y Remediación, gracias a los servicios gestionados: servicio de clasificación del 100% de los programas, procesos y ejecutables en los endpoints y el servicios de Threat Hunting y Análisis Forense, que permite una enforzamiento de la seguridad corporativa continua.

Observaciones

CCN-STIC-1213 PES Panda Adaptive Defense 360

Checkpoint Endpoint Security (Sandblast Agent)

Versión	E82.40 (82.40.1159)
Fabricante	Check Point Software Technologies
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/05/2020
Revisión de Validez	31/10/2022



Descripción

Check Point SandBlast Agent es una solución de protección avanzada para endpoints y navegadores de Internet, garantiza protección completa contra los diferentes vectores de amenazas con capacidades de prevención, detección y respuesta. Incorpora una gestión integrada disponible en nube o instalación local. Prestaciones:
• Emulación de amenazas (Sandbox) y Extracción (Entrega archivos limpios a usuarios en tiempo real)
• Anti-Ransomware (prevención y reparación) y defensa contra ciberextorsión
• Anti-Bot,
• Anti-Exploit
• Anti-Malware.
• Análisis de comportamientos (detección y bloqueo)

Observaciones

CCN-STIC-1214 Procedimiento de Empleo Seguro Checkpoint Endpoint Security (SBA)

INFORMACIÓN IMPORTANTE

Kaspersky Endpoint Security for Windows	
Versión	11.0.0.6499 AES256
Fabricante	Kaspersky Labs
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2020
Revisión de Validez	31/05/2023

Descripción

Kaspersky Endpoint Security es una solución de protección avanzada que proporciona una protección integral mediante componentes de control (Control de dispositivos, Control Web, Control de anomalías adaptable) y de protección (Detección de comportamiento, Prevención de vulnerabilidades, Prevención de intrusiones en el host, Motor de reparación, Protección frente a amenazas en archivos, Protección frente a amenazas web, Protección frente a amenazas en el correo, Protección frente a amenazas en la red, Firewall, Prevención de ataques de BadUSB, Proveedor de protección AMSI). Este enfoque de protección multicapa permite detectar y bloquear amenazas como Ransomware, ataques sin archivos (Fileless), ataques de día cero, ataques de red o ataques mediante el uso de Exploits o técnicas Phishing. Sus capacidades de protección avanzada cubren las fases de Seguridad Adaptativa de Prevención, Detección y Respuesta (Remediación). Cuenta con capacidades avanzadas de detección y respuesta inteligentes que permiten hacer investigaciones, análisis forense y Threat Hunting para ser proactivo a la hora de identificar amenazas e investigar eventos maliciosos, así como buscar los indicadores de amenazas en toda la red. Todo ello desde una única consola de gestión.

Observaciones

CCN-STIC-1209 Procedimiento de Empleo Seguro Kaspersky Endpoint Security 11 for Windows

Harmony SandBlast Mobile (Android)	
Versión	3.8.2.3023
Fabricante	Check Point Software Technologies
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/04/2021
Revisión de Validez	30/09/2023

Descripción

Harmony Mobile es una completa solución de defensa contra amenazas móviles. Mantiene sus datos corporativos seguros porque protege los dispositivos móviles de los empleados de todos los vectores de ataque: aplicaciones, red y sistema operativo. Diseñada para reducir los gastos generales de los administradores y aumentar la adopción del usuario, se adapta perfectamente a su entorno móvil existente, se implementa y escala rápidamente, y protege los dispositivos sin afectar la experiencia ni la privacidad del usuario.

Observaciones

CCN-STIC-1212 Procedimiento de empleo seguro Harmony Sandblast Mobile

INFORMACIÓN IMPORTANTE

Harmony SandBlast Mobile (iOS)	
Versión	3.8.2.5594
Fabricante	Check Point Software Technologies
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/04/2021
Revisión de Validez	30/09/2023





Descripción

Harmony Mobile es una completa solución de defensa contra amenazas móviles. Mantiene sus datos corporativos seguros porque protege los dispositivos móviles de los empleados de todos los vectores de ataque: aplicaciones, red y sistema operativo. Diseñada para reducir los gastos generales de los administradores y aumentar la adopción del usuario, se adapta perfectamente a su entorno móvil existente, se implementa y escala rápidamente, y protege los dispositivos sin afectar la experiencia ni la privacidad del usuario.

Observaciones

CCN-STIC-1212 Procedimiento de empleo seguro Harmony Sandblast Mobile

Mobileiron Mobile Threat Defense – MTD	
Versión	11.1
Fabricante	Mobileiron
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2021
Revisión de Validez	30/04/2022





Descripción

MobileIron Threat Defense permite supervisar, administrar y securizar los dispositivos móviles frente a ciberataques en dispositivos, redes y aplicaciones. Detecta las amenazas, tanto conocidas, como zero-day, incluso sin conectividad en red. Los cuatro pilares que definen esta funcionalidad de seguridad son la detección proactiva de amenazas y ataques, la corrección puntual, una mayor visibilidad de los dispositivos y de la red y una fácil administración.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Falcon Sensor	
Versión	6.27.14102
Fabricante	CrowdStrike
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/11/2021
Revisión de Validez	30/04/2022

Descripción

La plataforma CrowdStrike Falcon®, construida sobre conocimiento de adversarios (Inteligencia de amenazas) ofrece y unifica la higiene de TI, el antivirus de nueva generación, la detección y respuesta de puntos finales (EDR), threat hunting y la inteligencia de amenazas, todo ello a través de un único agente ligero de despliegue rápido y sencillo sin requerir reinicio ni impacto significativo en el rendimiento de los sistemas protegidos.

El agente de Falcon registra todas las actividades de interés en un punto final (puestos de trabajo, servidores, movilidad y cloud) para una inspección más profunda, incluso aquellas que evaden las medidas de prevención estándar, aplicando técnicas de Deep Machine Learning e IA, Protección basada en el comportamiento del Indicador de Ataque (IOA), protección antiexploit y gestión de IOCs.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Deep Security (Manager y Agente/Relay Linux/Windows)	
Versión	11
Fabricante	Trend Micro
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2021
Revisión de Validez	31/05/2024

Descripción

Deep Security es la respuesta de Trend Micro para proteger el cloud híbrido ya sean servidores físicos o virtuales. Gracias a su agente ligero, el cual incorpora funcio
alidades: EDR (con respuesta frente a amenazas conocidas, zero-day), reputación web, control de aplicaciones, supervisión de logs, Supervisión de Integridad (FIM), Firewall de Host y Host IPS (que incorpora la tecnología de parcheado virtual), ayuda a mejorar la postura de seguridad proporcionando seguridad, visibilidad y control. La cualificación abarca los siguientes componentes: Manager, Agente/Relay Linux y el Agente/Relay Windows. El *Virtual Appliance* no está cualificado.

Observaciones

CCN-STIC-1216 PES Trendmicro Deep Security

7.2.3 FAMILIA: HERRAMIENTAS DE GESTIÓN DE RED

Pendiente de recepción de solicitudes de productos que cumplan con Requisitos Fundamentales de Seguridad (RFS) correspondientes a esta familia.

INFORMACIÓN IMPORTANTE

7.2.4 FAMILIA: ACTUALIZACIÓN DE SISTEMAS

Pendiente de recepción de solicitudes de productos que cumplan con Requisitos Fundamentales de Seguridad (RFS) correspondientes a esta familia.

7.2.5 FAMILIA: FILTRADO DE NAVEGACIÓN

Pendiente de recepción de solicitudes de productos que cumplan con Requisitos Fundamentales de Seguridad (RFS) correspondientes a esta familia.

7.2.6 FAMILIA: SISTEMAS DE GESTIÓN DE EVENTOS DE SEGURIDAD

IBM Qradar	
Versión	v7.3.2
Fabricante	IBM
Familia	Sistemas de gestión de eventos de seguridad
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2019
Revisión de Validez	30/04/2022

Descripción

La familia de productos QRadar, plataforma de seguridad inteligente líder en el mercado SIEM, ofrece una visibilidad absoluta y unificada de la seguridad en tiempo real, aplicando tanto en entornos IT como OT.
QRadar recolecta, consolida y correlaciona información de todos los endpoints, dispositivos de red, entornos de las nubes, aplicaciones e incluso de diferentes data-lakes.
Aplica análisis avanzado para priorizar las amenazas y clasificarlas con mayor precisión. Adicionalmente, nuestra tecnología ofrece facilidades de búsquedas profundas para ayudar a encontrar nuevas amenazas de forma proactiva.
QRadar proporciona todas las funcionalidades que una organización necesita para abordar los desafíos de seguridad más importantes, ya sean amenazas avanzadas, amenazas internas, riesgos en la nube u otras vulnerabilidades.
https://www.ibm.com/support/knowledgecenter/es/SS42VS_7.3.2/com.ibm.qradar.doc/qradar_IC_welcome.html

Observaciones

CCN-STIC-1203 Procedimiento de empleo seguro IBM QRadar Security Intelligence Platform

INFORMACIÓN IMPORTANTE

GLORIA	
Versión	V5.6.0
Fabricante	S2Grupo / CCN
Familia	Sistemas de gestión de eventos de seguridad
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2021
Revisión de Validez	30/04/2022

Descripción

Gloria es una plataforma para la gestión de incidentes y amenazas de ciberseguridad a través de técnicas de correlación compleja de eventos. Badado en los sistemas SIEM, va un paso más allá de las capacidades de monitorización, almacenamiento e interpretación de los datos relevantes.Así, mediante técnicas de correlación compleja de varias fuentes de eventos o análisis de patrones para la identificación de anomalías, permite una orientación muy flexible hacia la vigilancia del mundo IP.
La plataforma permite las siguientes funcionalidades a través de distintos módulos:
- Monitorización de entornos tecnológicos (IT/OT).
- Inteligencia.
- Gestión del servicio.
- Automatización, orquestación y reducción de tiempos de respuesta.

Para más información, (https://ccn-cert.cni.es/soluciones-seguridad/gloria.html)

Observaciones

Procedimiento de empleo seguro pendiente de publicación

LogICA5 Next Generation SIEM	
Versión	v7.1
Fabricante	Grupo ICA Sistemas y Seguridad
Familia	Sistemas de gestión de eventos de seguridad
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2020
Revisión de Validez	30/06/2023

Descripción

La plataforma española Next Generation SIEM LogICA permite a los analistas de ciberseguridad recopilar logs e información ilimitada de seguridad, detectar ataques basados en anomalías y comportamientos desconocidos así como automatizar la respuesta anteincidentes en entornos IT, OT e IoT.
LogICA NG SIEM recopila información de cualquier fuente interna y externa a la empresa (comercial, propietaria, aplicaciones, cloud), correlando y analizando en tiempo real esa información, permitiendo contextualizary priorizar los incidentes de seguridad tanto internos como externos. Combina los casos de uso de detección más sofisticados con la información más precisa de amenazas y vulnerabilidades zero day gracias a la información de fuentes externas de inteligencia, threat hunting y anomalías de red/usuario. Incorpora, además, un cuadro de mando de gestión del servicio, centralizando la información y facilitando su consumo por parte de la organización.
LogICA permite adaptarse a las necesidades de despliegue de las organizaciones, en modo on-premise, virtual o entorno cloud.

Observaciones

CCN-STIC-1206 PES NGSIEM LogICA

INFORMACIÓN IMPORTANTE

NetWitness	
Versión	v.11
Fabricante	RSA
Familia	Sistemas de gestión de eventos de seguridad
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2019
Revisión de Validez	31/05/2022

Descripción

La plataforma RSA Netwitness es la solución de SIEM evolucionado, con capacidades de visibilidad completa gracias a su modelo de datos unificado pudiendo capturar logs, netflow, tráfico de red y end point de forma integrada, bajo un único motor de análisis y correlación avanzada. Además, incluye funcionalidades necesarias por un SOC para hacer frente a amenazas complejas. RSA Netwitness Platform cuenta además con componentes adicionales como UEBA y SOAR. La solución permite capturar todo tipo de información, permitiendo el análisis avanzado de amenazas, priorización en base al contexto de negocio y haciendo más eficiente el trabajo del analista. Es una plataforma que, gracias su capacidad de análisis, muestra el alcance completo de un ataque a los analistas. Además, gracias a su estrategia Run Anywhere, la plataforma se puede desplegar en cualquier entorno (virtual, cloud, físico, híbrido), así como hacer frente a arquitecturas altamente distribuidas. RSA Netwitness incluye en todos sus clientes +50 feeds de inteligencia, agente para endpoints ilimitados así como el despliegue ilimitado de dispositivos para cubrir cualquier forma de despliegue. https://www.rsa.com/en-us/products/threat-detection-response.

Observaciones

CCN-STIC-1210 Procedimiento de Empleo Seguro RSA Netwitness Platform

7.2.7 FAMILIA: DISPOSITIVOS PARA GESTIÓN DE CLAVES CRIPTOGRÁFICAS

EP543N	
Versión	V.1.7
Fabricante	Epicom
Familia	Dispositivos para gestión de claves criptográficas
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	27/12/2021
Revisión de Validez	31/12/2024



Descripción

Centro de Gestión de cifradores IP EP430GN sobre ordenador seguro EP1140.

Observaciones

INFORMACIÓN IMPORTANTE

EP543X	
Versión	SW v 4.15
Fabricante	Epicom
Familia	Dispositivos para gestión de claves criptográficas
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2022



Descripción

Centro de Gestión sobre la plataforma EP1140, que da soporte a los cifradores de la familia EP430, incluidos los modelos EP430TX y EP430GX.

Observaciones

Utilización según PE-2012-49 Procedimiento de Empleo EP430GX v2

AWS Key Management Service (KMS)	
Versión	
Fabricante	AWS
Familia	Dispositivos para gestión de claves criptográficas
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2022

Descripción

AWS Key Management Service (KMS) facilita la creación y la administración de claves criptográficas y el control de su uso en una amplia gama de servicios de AWS y en sus aplicaciones. Utiliza módulos de seguridad de hardware que se han validado según FIPS140-2 para proteger sus claves.
AWS KMS le proporciona un control centralizado sobre las claves criptográficas que se utilizan para proteger sus datos. El servicio está integrado con otros servicios de AWS, lo que facilita el cifrado de los datos que almacena en estos servicios y el control del acceso a las claves que los descifran. Los servicios integrados con KMS se pueden encontrar en https://aws.amazon.com/kms/

Observaciones

Procedimiento de empleo pendiente de publicación.

INFORMACIÓN IMPORTANTE

7.2.8 HERRAMIENTAS DE GESTIÓN DE DISPOSITIVOS MÓVILES (MDM)

Mobileiron Core – Plataforma de Seguridad	
Versión	10.0.1
Fabricante	Mobileiron
Familia	Herramientas de Gestión de dispositivos móviles (MDM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2019
Revisión de Validez	30/04/2022

Descripción

La administración Unificada de Puntos de Conexión (UEM) de MobileIron permite a los usuarios de una organización disfrutar de un acceso fluido a aplicaciones y datos corporativos a través de dispositivos móviles, tabletas y equipos, a la vez que mantieneun total control de su privacidad. Permite además optimizar al máximo y de forma segura el potencial de los dispositivos, las aplicaciones y la movilidad en general, posibilitando así la transformación digital y la innovación corporativa.
Vídeo descriptivo del producto: https://youtu.be/I1N7uqKfMLk

Observaciones

CCN-STIC-1202 Procedimiento de empleo seguro UEM Mobileiron Core

7.3 CATEGORÍA: MONITORIZACIÓN DE LA SEGURIDAD

7.3.1 FAMILIA: DISPOSITIVOS DE PREVENCIÓN DE INTRUSIONES

Cisco Firepower Threat Defense (FTD) en Firepower 1000 Series (FP1010, FP1120 y FP1140) con FMC y FMCv	
Versión	FTD 6.4 y FMC/FCMv 6.4
Fabricante	Cisco Systems
Familia	Dispositivos de prevención y detección de intrusiones
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2022

Descripción

Cisco Firepower Threat Defense (FTD) tiene capacidades de firewall, VPN e IPS. Esta plataforma ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).
Compatible con:
-Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)
-FMCv running on ESXi 6.0 or 6.5 on the Unified Computing System (UCS) UCSB-B200-M4, UCSC-C220-M4S, UCSC-C240-M4SX, UCSC-C240-M4L, UCSB-B200-M5, UCSC-C220-M5, UCSC-C240-M5, UCS-E160S-M3 and UCS-E180D-M3

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Cisco Firepower Threat Defense (FTD) en Firepower 2000 Series FP2110, FP2120, FP2130 y FP2140) con FMC y FMCv	
Versión	FTD 6.4 y FMC/FCMv 6.4
Fabricante	Cisco Systems
Familia	Dispositivos de prevención y detección de intrusiones
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2022

Descripción

Cisco Firepower Threat Defense (FTD) tiene capacidades de firewall, VPN e IPS. Esta plataforma ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).
Compatible con:
-Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)
-FMCv running on ESXi 6.0 or 6.5 on the Unified Computing System (UCS) UCSB-B200-M4, UCSC-C220-M4S, UCSC-C240-M4SX, UCSC-C240-M4L, UCSB-B200-M5, UCSC-C220-M5, UCSC-C240-M5, UCS-E160S-M3 and UCS-E180D-M3

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Fortigate FG-30E, FWF-30E, FG-40F, FG-40F-3G4G, FG-50E, FWF-50E, FG-51E, FWF-51E, FG-52E, FG-60E, FG-60E-DSL, FG-60E-PoE, FWF-60E, FWF-60E-DSL, FG-60F, FG-60F-3G4G, FWF-60F, FG-61E, FG-61F, FWF-61E, FWF-61F, FG-80E, FG-80E-PoE, FG-81E y FG-81E-PoE	
Versión	FortiOS 6.2.7
Fabricante	Fortinet
Familia	Dispositivos de prevención y detección de intrusiones
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2022

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos para entornos pequeños y sedes remotas de pocos usuarios. Las funcionalidades de seguridad son similares a las del resto de modelos más grandes (reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf).

Observaciones

CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.

INFORMACIÓN IMPORTANTE

Fortigate FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140E, FG-140E-PoE, FG-200E, FG-201E, FG-300D, FG-300E, FG-301E, FG-400D, FG-400E, FG-401E, FG-500D, FG-500E, FG-501E, FG-600D, FG-601E y FG-900D.	
Versión	FortiOS 6.2.7
Fabricante	Fortinet
Familia	Dispositivos de prevención y detección de intrusiones
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2022

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos para entornos pequeños y sedes remotas de pocos usuarios. Las funcionalidades de seguridad son similares a las del resto de modelos más grandes (reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf).

Observaciones

CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.

Fortigate FG-1000D, FG-1100E, FG-1100E-DC, FG-1101E, FG-1200D, FG-1500D, FG-1500DT, FG-1500D-DC, FG-2000E, FG-2201E y FG-2500E	
Versión	FortiOS 6.2.7
Fabricante	Fortinet
Familia	Dispositivos de prevención y detección de intrusiones
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2022

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos para entornos pequeños y sedes remotas de pocos usuarios. Las funcionalidades de seguridad son similares a las del resto de modelos más grandes (reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf).

Observaciones

CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.

INFORMACIÓN IMPORTANTE

Fortigate FG-3000D, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3600E, FG-3601E, FG-3700D, FG-3800D, FG-3801D, FG-3815D, FG-3960E, FG-3980E, FG-5001E, FG-5001E1, FG-6301F, FG-6501F, FGR-30D, FGR-60F y FGR-60F-3G4G	
Versión	FortiOS 6.2.7
Fabricante	Fortinet
Familia	Dispositivos de prevención y detección de intrusiones
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2022
Descripción	
Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos para entornos pequeños y sedes remotas de pocos usuarios. Las funcionalidades de seguridad son similares a las del resto de modelos más grandes (reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf).	
Observaciones	
CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.	

Fortigate-VM00, Fortigate-VM01, Fortigate-VM02, Fortigate-VM04, Fortigate-VM08, Fortigate-VM16, Fortigate-VM32 y Fortigate-VMUL	
Versión	FortiOS 6.2.7
Fabricante	Fortinet
Familia	Dispositivos de prevención y detección de intrusiones
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2022
Descripción	
Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos para entornos pequeños y sedes remotas de pocos usuarios. Las funcionalidades de seguridad son similares a las del resto de modelos más grandes (reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf).	
Observaciones	
CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.	

INFORMACIÓN IMPORTANTE

Junos 15.1X49-D60 for SRX platforms
SRX300, SRX320, SRX340, SRX345, SRX550M, SRX5400E, SRX5400X, SRX5600E, SRX5600X, SRX5800E and SRX 5800X

Versión	SW: Junos 15.1X49-D60
Fabricante	Juniper Networks
Familia	Dispositivos de prevención y detección de intrusiones
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2021
Revisión de Validez	31/10/2023

Descripción

La gama de productos SRX de Juniper Networks ofrece, en un solo dispositivo, capacidades de conectividad, conmutación y seguridad que le permiten dar funciones simultaneas de enrutador, switch y cortafuegos de nivel 7, así como dispositivo de detección yprevención de intrusiones. Su sistema operativo Junos, provee de un lenguaje universal con el resto de soluciones de Juniper que facilitan la operación y las tareas de automatización e integración con otras soluciones.

Observaciones

CCN-STIC-1404 “Procedimiento de Empleo Seguro Plataformas SRX Juniper”

McAfee Network Security Platform (IPS-NS9100, IPS-NS9200, IPS-NS9300 P, IPS-NS9300 S, PS-NS7150, IPS-NS7250, IPS-NS7350, IPS-NS7100, IPS-NS7200, IPS-NS7300, PS-NS5200, IPS-NS5100, IPS-NS3200, IPS-NS3100 y NSM-MAPL-NG)

Versión	NS Sensor v 9.1.17.100 and NSM v9.1.21.20
Fabricante	McAfee
Familia	Dispositivos de prevención y detección de intrusiones
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2020
Revisión de Validez	31/10/2022

Descripción

McAfee® Network Security Platform (NSP) es un sistema de detección y prevención de intrusiones (IDPS) de próxima generación que descubre y bloquea amenazas de malware sofisticadas en la red. Emplea técnicas avanzadas de detección y emulación, y va más allá de la comparación con patrones para ofrecer protección contra los ataques ocultos con un alto grado de precisión. Para satisfacer las necesidades de las redes más exigentes, la plataforma puede adaptarse hasta 40 Gbit/s con un solo dispositivo y hasta 100 Gbit/s con dispositivos apilados. La integración de la solución de IPS simplifica las operaciones de seguridad mediante la combinación de la información en tiempo real de McAfee Global Threat Intelligence y los datos contextuales completos sobre usuarios, dispositivos y aplicaciones, con el fin de responder de manera rápida y precisa a los ataques que se propagan por la red.
Otras funciones: Administración centralizada, cifrado SSL, y alta disponibilidad y protección de recuperación ante desastre.

Observaciones

CCN-STIC 1302 Procedimiento de Empleo Seguro de McAfee Network Security Platform (NSP)

INFORMACIÓN IMPORTANTE

Serie SOHO (SOHOW)	
Versión	SonicOS 6.5.2
Fabricante	SonicWall
Familia	Dispositivos de prevención y detección de intrusiones
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2019
Revisión de Validez	30/04/2022

Descripción

Los cortafuegos de la serie TZ SOHO de Sonicwall son una solución adecuada para oficinas pequeñas y domésticas, así como para entornos distribuidos en ubicaciones remotas. Despliegan funcionalidades para construir Secure SD-WAN y conectividad WIFI (opcional). El SOHO 250 proporciona un 50% más de rendimiento sobre su antecesor SOHO, así como acceso a los sandboxes avanzados Capture ATP, con lo que se mejora la seguridad en prevención y detección de malware desconocido en un entorno remoto.

Observaciones

CCN-STIC-1420 Procedimiento de Empleo Seguro Sonicwall SonicOS

SonicWall NSA Serie (2650, 3600, 3650, 4600, 4650, 5600, 5650, 6600, 6650, 9250, 9450, 9650)	
Versión	SonicOS 6.5.2
Fabricante	SonicWall
Familia	Dispositivos de prevención y detección de intrusiones
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2019
Revisión de Validez	30/04/2022

Descripción

Los firewall de la serie NSa de SonicWall están indicados para compañías medianas / grandes (de entre 50 y 3000 usuarios aprox), empresas deslocalizadas geográficamente y datacenters, consolidando tecnologías automatizadas de prevención y detección de amenazas como la inspección de memoria profunda en tiempo real (RTDMI). Desarrollados sobre una arquitectura de hardware de múltiples núcleos con interfaces 10-GbE y 2.5-GbE, la serie NSa cuenta con capacidades basadas en la nube y en el equipo, como descifrado e inspección TLS/SSL, application intelligence y control, SD-WAN segura, visualización en tiempo real y administración de WLAN. Más info en: https://www.sonicwall.com/es-mx/products/firewalls/mid-range

Observaciones

CCN-STIC-1420 Procedimiento de Empleo Seguro Sonicwall SonicOS

INFORMACIÓN IMPORTANTE

SonicWall SM Serie (9200, 9400, 9600, 9800)	
Versión	SonicOS 6.5.2
Fabricante	SonicWall
Familia	Dispositivos de prevención y detección de intrusiones
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2019
Revisión de Validez	30/04/2022

Descripción

Diseñado para grandes empresas, centros de datos, carriers y proveedores de servicios con necesidades multi-gigabit. Dirigido a compañías de entre 1000 y más de 50.000 usuarios (aprox.), realiza detección y prevención de amenazas mediante la combinación de la protección basada en appliances con la inteligencia de la nube en una plataforma de alto desempeño y consolida tecnologías de seguridad que brindan protección contra amenazas a millones de conexiones sin ralentizar el desempeño. Más info en: https://www.sonicwall.com/es-mx/products/firewalls/high-end

Observaciones

CCN-STIC-1420 Procedimiento de Empleo Seguro Sonicwall SonicOS

SonicWall TZ Serie (300/W, 400/W, 500/W, 600)	
Versión	SonicOS 6.5.2
Fabricante	SonicWall
Familia	Dispositivos de prevención y detección de intrusiones
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2019
Revisión de Validez	30/04/2022

Descripción

La serie TZ de SonicWall ofrece seguridad y rendimiento de entorno Enterprise orientado a pequeñas compañías. Enfocado a entornos departamentales o PYMES de entre 5 y 100 usuarios (aprox), incorpora funciones de prevención de intrusiones, antimalware, filtrado de contenidos/URL y control de aplicaciones a través de redes y entornos inalámbricos. Proporciona inspección profunda de paquetes (DPI), SD-WAN y despliegue zero-touch. Opciones de puertos PoE y wifi 802.11ac. Más info en: https://www.sonicwall.com/es-mx/products/firewalls/entry-level

Observaciones

CCN-STIC-1420 Procedimiento de Empleo Seguro Sonicwall SonicOS

INFORMACIÓN IMPORTANTE

SonicWall TZ Serie (300P, 350, 350W, 600P)	
Versión	6.5.4.4-44n-federal-12n
Fabricante	SonicWall
Familia	Dispositivos de prevención y detección de intrusiones
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2021
Revisión de Validez	31/01/2024

Descripción

La serie TZ de SonicWall ofrece seguridad y rendimiento de entorno Enterprise orientado a pequeñas compañías. Enfocado a entornos departamentales o PYMES de entre 5 y 100 usuarios (aprox), incorpora funciones de prevención de intrusiones, antimalware, filtrado de contenidos/URL y control de aplicaciones a través de redes y entornos inalámbricos. Proporciona inspección profunda de paquetes (DPI), SD-WAN y despliegue zero-touch. Opciones de puertos PoE y wifi 802.11ac.
Más info en: https://www.sonicwall.com/es-mx/products/firewalls/entry-level.

Observaciones

CCN-STIC-1420 Procedimiento de Empleo Seguro Sonicwall SonicOS

SonicWall SOHO Serie (250, 250W)	
Versión	6.5.4.4-44n-federal-12n
Fabricante	SonicWall
Familia	Dispositivos de prevención y detección de intrusiones
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2021
Revisión de Validez	31/01/2024

Descripción

Los cortafuegos de la serie TZ SOHO de Sonicwall son una solución adecuada para oficinas pequeñas y domésticas, así como para entornos distribuidos en ubicaciones remotas. Despliegan funcionalidades para construir Secure SD-WAN y conectividad WIFI (opcional). El SOHO 250 proporciona un 50% más de rendimiento sobre su antecesor SOHO, así como acceso a los sandboxes avanzados Capture ATP, con lo que se mejora la seguridad en prevención y detección de malware desconocido en un entorno remoto.

Observaciones

CCN-STIC-1420 Procedimiento de Empleo Seguro Sonicwall SonicOS

7.3.2 FAMILIA: SISTEMAS HONEYPOT / HONEYNET

Pendiente de publicación los Requisitos Fundamentales de Seguridad (RFS) de esta familia.

INFORMACIÓN IMPORTANTE

7.3.3 FAMILIA: CAPTURA, MONITORIZACIÓN Y ANÁLISIS DE TRÁFICO

GigaVUE (HD8, HD4, HC3, HC2, HC1)

Versión	version 5.1.01
Fabricante	Gigamon
Familia	Captura, Monitorización y Análisis de Tráfico
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2019
Revisión de Validez	30/04/2022

Descripción

Network Packet Brokers HC/HD Series. Network Packet Brokers de alto rendimiento con soporte de puertos 1g/10g/25g/40g/100g en fibra multimodo o/y monomodo y 100m/1000m/10g en cobre y funcionalidades de filtrado de trafico L2-3-4-7 con motor de DPI, generación de Netflow/IPFix/Metadatos, Cifrado/Descifrado de SSL/TLS (incluyendo protocolos RSA, DHE, ECC, y PFS), Terminación de túneles (GRE, VXLAN, ERSPAN, GMIP), Truncado de paquetes, Eliminación de cabeceras, Enmascarado, De-Duplicación, Clustering, Balanceo, Captura de tráfico para entornos virtuales (VMWare ESX/NSX, Openstack, Kubernetes, AWS, GCP, Azure, Nutanix), simetrización de tráfico para arquitectura HA, Inline Bypass con Heartbeat positivo y negativo, Cambio de medio y velocidad, Bypass HW, TAPsintegrados.

Observaciones

CCN-STIC-1301-Procedimiento de Empleo Seguro Giga VUE-OS 5.1.01 Gigamon

GigaVUE (TA10, TA40, TA100)

Versión	version 5.1.01
Fabricante	Gigamon
Familia	Captura, Monitorización y Análisis de Tráfico
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2019
Revisión de Validez	30/11/2020

Descripción

Agregadores TA Series (TA10/TA40/TA100)
Agregadores de alto rendimiento con soporte de puertos 1g/10g/25g/40g/100g en fibra multimodo o/y monomodo y 100m/1000m/10g en cobre y funcionalidades de filtrado de trafico L2-3-4, Terminación de túneles (GRE, VXLAN, ERSPAN, GMIP), Clustering, Balanceo, Cambio de medio y velocidad

Observaciones

CCN-STIC-1301-Procedimiento de Empleo Seguro Giga VUE-OS 5.1.01 Gigamon

INFORMACIÓN IMPORTANTE

GigaVUE (GVS-HC101, GVS-HC102, GVS-HC301, GVS-HC302, GVS-HC2A1 y GVS-HC2A2)	
Versión	version 5.9
Fabricante	Gigamon
Familia	Captura, Monitorización y Análisis de Tráfico
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2022
Revisión de Validez	31/08/2024

Descripción

Network Packet Brokers HC Series. Network Packet Brokers de alto rendimiento con soporte de puertos 1g/10g/25g/40g/100g en fibra multimodo o/y monomodo y 100m/1g/10g en cobre y funcionalidades de filtrado de trafico L2-3-4-7 con motor de DPI, generación de Netflow/IPFix/Metadatos, Cifrado/Descifrado de SSL/TLS (incluyendo protocolos RSA, DHE, ECC, y PFS), Terminación de túneles (GRE, VXLAN, ERSPAN, GMIP), Truncado de paquetes, Eliminación de cabeceras, Enmascarado, De-Duplicación, Clustering, Balanceo, Captura de tráfico para entornos virtuales (VMWare ESX/NSX, Openstack, Kubernetes, AWS, GCP, Azure, Nutanix), simetrización de tráfico para arquitectura HA, Inline Bypass con Heartbeat positivo y negativo, Cambio de medio y velocidad, Bypass HW, TAPs integrados.

Observaciones

CCN-STIC-1301 Procedimiento de Empleo Seguro GigaVUE-OS 5.1.01

GigaVUE (GVS-TAC21 y GVS-TAC22)	
Versión	version 5.9
Fabricante	Gigamon
Familia	Captura, Monitorización y Análisis de Tráfico
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2022
Revisión de Validez	31/08/2024

Descripción

Agregadores TA Series. Agregadores de alto rendimiento con soporte de puertos 1g/10g/25g/40g/100g en fibra multimodo o/y monomodo y 100m/1g/10g en cobre y funcionalidades de filtrado de trafico L2-3-4, Terminación de túneles (GRE, VXLAN, ERSPAN, GMIP), Clustering, Balanceo, Cambio de medio y velocidad y Timestamping

Observaciones

CCN-STIC-1301 Procedimiento de Empleo Seguro GigaVUE-OS 5.1.01

INFORMACIÓN IMPORTANTE

CARMEN	
Versión	Versión 7.2.4
Fabricante	S2 GRUPO / CCN
Familia	Captura, Monitorización y Análisis de Tráfico
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2021
Revisión de Validez	30/09/2023

Descripción

CARMEN (Centro de Análisis de Registros y Minería de EveNtos) es una solución software de adquisición, procesamiento y análisis de información para soportar el proceso de identificación de Amenazas Persistentes Avanzadas (APT) a partir del tráfico de redinterno y saliente de una forma eficiente, apoyando la toma de decisiones a partir de la información generada y procesada. Se compone de agentes que recopilan los flujos de tráfico, un motor de almacenamiento en el que se inserta la información, un sistema de detección de anomalías que se encarga de procesar la información almacenada y una aplicación web que permite la representación y consulta tanto de la información obtenida como de la procesada. Para más información, se puede consultar la web del CCN-CERT (https://ccn-cert.cni.es/soluciones-seguridad/carmen.html)

Observaciones

CCN-STIC-1304 Procedimiento de empleo seguro CARMEN 7.2.4

7.3.4 FAMILIA: HERRAMIENTAS DE SANDBOX

McAfee Advanced Threat Defense (ATD)	
Versión	Version 4.0.2
Fabricante	McAfee
Familia	Herramientas de Sandbox
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2020
Revisión de Validez	30/04/2023

Descripción

McAfee® Advanced Threat Defense permite detectar ataques avanzados y el malware evasivo, y transformar la información de amenazas en medidas y protección inmediatas. A diferencia de los entornos aislados tradicionales, incluye nuevas funciones de inspección que mejoran la detección y revelan las amenazas evasivas. La firme integración entre las soluciones de seguridad —desde la red y los endpoints hasta la investigación— permite compartir al instante la información sobre las amenazas con todo el entorno,lo que redunda en beneficio de la protección y la investigación.
Proporciona opciones de despliegue flexibles para todas las redes.
Es integrable con soluciones de terceros compatibles con estándares abiertos.
Combina análisis en profundidad de código estático, análisis dinámicos y aprendizaje automático para garantizar una detección más precisa con datos de análisis inigualables.

Observaciones

CCN-STIC-1303 Procedimiento de Empleo Seguro Mcafee ATD

INFORMACIÓN IMPORTANTE

7.4 CATEGORÍA: PROTECCIÓN DE LAS COMUNICACIONES

7.4.1 FAMILIA: ENRUTADORES

Aruba 8320 Switch Series



Versión	Aruba OS-CX version 10.03
Fabricante	Aruba
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2019
Revisión de Validez	30/04/2022



Descripción

Equipos orientados a ser equipos de núcleo de red (CORE) de Campus como de Centros de Datos. Es un equipo con categoría de operador. Dispone de una arquitectura interna de Sistema Operativo que proporciona una forma de trabajar con el completamente programable. Su motor de analíticas (NAE) permite la inserción de scripts de para la ejecución de tareas avanzadas de monitorización y respuestas a eventos.
Ofrecen interfaces a alta velocidad así como una tecnología de chasis virtual.

Observaciones

Procedimiento de empleo pendiente de publicación.

Aruba 8325 Switch Series



Versión	Aruba OS-CX version 10.03
Fabricante	Aruba
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2019
Revisión de Validez	30/04/2022



Descripción

Equipos orientados a ser equipos de núcleo de red (CORE) de Campus como de Centros de Datos. Es un equipo con categoría de operador. Dispone de una arquitectura interna de Sistema Operativo que proporciona una forma de trabajar con el completamente programable. Su motor de analíticas (NAE) permite la inserción de scripts de para la ejecución de tareas avanzadas de monitorización y respuestas a eventos.
Ofrecen interfaces a alta velocidad así como una tecnología de chasis virtual.

Observaciones

Procedimiento de empleo pendiente de publicación.

INFORMACIÓN IMPORTANTE

Aruba 8400 Switch Series	
Versión	Aruba OS-CX version 10.03
Fabricante	Aruba
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2019
Revisión de Validez	30/04/2022



Descripción

Equipos orientados a ser equipos de núcleo de red (CORE) de Campus como de Centros de Datos. Es un equipo con categoría de operador. Dispone de una arquitectura interna de Sistema Operativo que proporciona una forma de trabajar con el completamente programable. Su motor de analíticas (NAE) permite la inserción de scripts de para la ejecución de tareas avanzadas de monitorización y respuestas a eventos.
Ofrecen interfaces a alta velocidad así como una tecnología de chasis virtual.

Observaciones

Procedimiento de empleo pendiente de publicación.

Junos 15.1X49-D60 for SRX platforms SRX300, SRX320, SRX340, SRX345, SRX550M, SRX5400E, SRX5400X, SRX5600E, SRX5600X, SRX5800E and SRX 5800X	
Versión	SW: Junos 15.1X49-D60
Fabricante	Juniper Networks
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2021
Revisión de Validez	31/10/2023

Descripción

La gama de productos SRX de Juniper Networks ofrece, en un solo dispositivo, capacidades de conectividad, conmutación y seguridad que le permiten dar funciones simultaneas de enrutador, switch y cortafuegos de nivel 7, así como dispositivo de detección yprevención de intrusiones. Su sistema operativo Junos, provee de un lenguaje universal con el resto de soluciones de Juniper que facilitan la operación y las tareas de automatización e integración con otras soluciones.

Observaciones

CCN-STIC-1404 “Procedimiento de Empleo Seguro Plataformas SRX Juniper”

INFORMACIÓN IMPORTANTE

Cisco Catalyst 9200 Series	
Versión	IOS 16.12
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2022
Revisión de Validez	30/06/2022

Descripción

9200: C9200-24T, C9200-48T, C9200-24P, C9200-48P. C9200-24PB, C9200-48PB, C9200-24PXG, C9200-48PXG con C9200-NM-4G, C9200-NM-4X, C9200-NM2Y, C9200-NM-2Q
9200L: C9200L-24P-4G, C9200L-24P-4X, C9200L-24T-4G, C9200L-24P-4X, C9200L-48P-4G, C9200L-48P-4X,C9200L-48T-4G, C9200L-248T-4X, C9200L-24PXG-2Y, C9200L-48PXG-2Y, C9200L-24PXG-4X, C9200L-48PXG-4X

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Cisco Catalyst 9300 Series	
Versión	IOS 16.12
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2022
Revisión de Validez	30/06/2022

Descripción

C9300-24T, C9300-48S, C9300-48U, C9300D-24UB, C9300D-48UB, C9300D-48UXB, C9300L-24T-4G, C9300L-24P-4G, C9300L-48T-4G, C9300L-48P-4G, C9300L-24T-4X, C9300L-24P-4X, C9300L-48T-4X, C9300L-48P-4X, C9300L-24UXG-4X, C9300-24UXG-2Q, C9300L-48UXG-2Q, C9300L-48PF-4G, C9300L-48PF-4X, C9300L-48UXG-4X

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Cisco Catalyst 9400 Series	
Versión	IOS 16.12
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2022
Revisión de Validez	30/06/2022

Descripción

Chasis: C9404R, C9407R, C9410R.
Supervisoras: C9400-SUP-1, C9400-SUP-1XL, C9400-SUP-1XL-Y.
Tarjetas: C9400-LC-48U, C9400-LC-48T, C9400-LC-48P, C9400-LC-24XS, C9400-LC-48UX, C9400-LC-24S, C9400-LC-48S, C9400-LC-48H

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Cisco Catalyst 9600 Series	
Versión	IOS 16.12
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2022
Revisión de Validez	30/06/2022

Descripción

Series Cisco Catalyst 9600 con Cisco Catalyst 9600 series Supervisor Engine y una o más tarjetas de línea: C9600-LC-48YL, C9600-LC-24C

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Cisco Network Convergence System 5500 Series: NCS5504, NCS5508, NCS5516, NCS-55A1-36H-S y NCS-55A1-36H-SE-S.	
Versión	Universal Cisco Internet Operating System (IOS-XR), Release 6.3.2.
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2020
Revisión de Validez	31/01/2022

Descripción

Cisco Network Convergence System 5500 Series es un producto de routing, usado principalmente para agregar tráfico en redes WAN (Wide Area Network). Proporciona funcionalidades de redundancia, enrutamiento de segmentos de red y gestión de redes programables.
El producto ejecuta el sistema operativo IOS-XR, diseñado para procesar el tráfico de red sin sufrir retrasos de buffering.

Observaciones

Procedimiento de empleo pendiente de publicación.

Cisco Nexus 3100, 3100V, 3100Z Series Switches (3172PQ/PQ-XL, 3172TQ, 31128PQ, 31108PC-V, 31108TC-V, Nexus 3132Q-V, 3132C-Z)	
Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2022

Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Cisco Nexus 3200 Series Switches (3232C, 3264C-E)	
Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2022

Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Cisco Nexus 3400 Series Switches (34180-YC, 3464C, 3432D-S, 3408-S)	
Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2022

Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Cisco Nexus 3500 Series Switches (3524-X/XL, 3548-X/XL)	
Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2022

Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Cisco Nexus 3600 Series Switches (36180YC-R, 3636C-R)	
Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2022

Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

IE2000 Series, IE4000 Series, IE5000 Series y 2500 Series CGS	
Versión	IOS 15.2
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2019
Revisión de Validez	31/01/2022

Descripción

Los Cisco IoT son switches, que incluyen servicios de routing, usados para construir redes IP conectando pequeñas redes y segmentos de red.
Estos equipos Cisco están especialmente desarrollados para soportar entornos industriales complejos. Ofrecen configuraciones flexibles con administración simple y ejecución de aplicaciones avanzadas en un único dispositivo.
Por otro lado, Cisco IOS es un sistema operativo propietario y altamente configurable desarrollado por Cisco que provee servicios de routing y switching.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Dell EMC Networking SmartFabric (Modelos: S3048-ON, S4048-ON, S4048T-ON, S4112F-ON, S4112T-ON, S4128F-ON, S4128T-ON, S4148F-ON, S4148T-ON, S4148U-ON, MX5108n, S4248FB-ON, S4248FBL-ON, S6010-ON, Z9100-ON, MX9116n, S5212F-ON, S5224F-ON, S5232F-ON, S5248F-ON

Versión	OS 10 Build: 10.5.1.3.
Fabricante	Dell Computer
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2020
Revisión de Validez	31/05/2022

Descripción

Dell EMC Smart Fabric OS10 es el sistema operativo de red (NOS) que se utiliza en las familias de enrutadores y conmutadores de las serie N (algunos modelos), serie S, serie Z y serie MX de Dell EMC Networking (las plataformas HW que actualmente soportanOS10 son N3200, S3048-ON, S4048-ON, S4048T-ON, S4112F-ON, S4112T-ON, S4128F-ON, S4128T-ON, S4148F-ON, S4148T-ON, S4148U-ON, S4248FB-ON, S4248FBL-ON, S6010-ON, S5212F-ON, S5224F-ON, S5232F-ON, S5248F-ON, S5296F-ON, Z9100-ON, Z9264F-ON, Z9332F-ON, MX5108n yMX9116n). Dell EMC SmartFabric OS10 es un sistema operativo de red (NOS) que admite múltiples arquitecturas y entornos. La solución SmartFabric OS10 permite la desagregación en varias capas de la funcionalidad de red. SmartFabric OS10 comprende la administración, monitorización y funcionalidad completa y estándar de la industria de redes de nivel 2 y nivel 3 a través de interfaces CLI, SNMP y REST. Los usuarios pueden elegir sus propias aplicaciones de organización, gestión, supervisión y redes de terceros. Para desarrollar redes escalables L2 y L3, SmartFabric OS10 ofrece una solución modular y desagregada en una única imagen binaria.

Observaciones

CCN-STIC-1429 PES DELL EMC Networking

SLX Product Series (SLX9150, SLX9250 y SLX9640)

Versión	20.1.1aa
Fabricante	Extreme Networks
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2021
Revisión de Validez	31/07/2023



Descripción

Familia de switches y routers para Centros de Datos y Border Routing enfocada a operadores, proveedores de servicios y empresas. Se soportan tecnologías tales como MPLS/VPLS, Carrier Ethernet y EVPN, con equipos dotados de buffer ultra-profundos. Los equipos son compactos y proporcionan gran densidad de puertos a velocidades 1/10/25/40/50/100 Gbps en una unidad de rack.

El despliegue de soluciones IP Fabric para datacenter puede automatizarse desde una máquina virtual residente en el propio switch. Se soportan arquitecturas Clos (Leaf and Spine) sin necesidad de controlador externo. También se soporta la interconexión de Datacenters mediante Leaf especializados.

Observaciones

CCN-STIC-1430 PES Switches Extreme Networks SLXOS

INFORMACIÓN IMPORTANTE

Huawei AR6000&AR600 Series Routers (NetEngine AR6120, NetEngine AR6121,NetEngine AR6140-9G-2AC, NetEngine AR6140-16G-4XG. NetEngine AR6280, NetEngine AR6300, NetEngine AR651, NetEngine AR651C, NetEngine AR651W, NetEngine AR657W, NetEngine AR611W y NetEng	
Versión	V300R019C11SPC200 + Patch V300R019C11HP0095T
Fabricante	Huawei Technologies España
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2022
Revisión de Validez	30/06/2022

Descripción

Las plataformas de enrutamiento Huawei AR son los primeros diseñados para la era de la cloud, presenta enlaces ascendente de banda ultra ancha 4G/5G y cuenta con un rendimiento de reenvío que es tres veces el promedio de la industria. Ofreciendo además diversas características. Compatible con la red definida por software (SD-WAN), la gestión de la nube, la red privada virtual (VPN), la conmutación de etiquetas (MPLS), la seguridad y la voz.

Observaciones

Procedimiento de empleo pendiente de publicación.

Huawei NE40E Series running on Hardware Models NE40E-X3A and NE40E-X16A	
Versión	Version: V800R010C00SPC200 Patch: V800R010SPH220T
Fabricante	Huawei Technologies España
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2021
Revisión de Validez	31/08/2023

Descripción

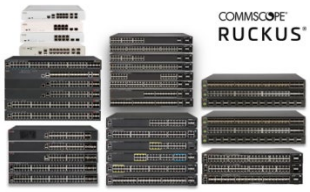
Enrutadores de servicio completo diseñados para servir como nodos centrales en redes WAN empresariales, nodos de acceso en grandes redes empresariales, nodos de interconexión y agregación en redes de campus y nodos de borde en grandes redes IDC.

Observaciones

CCN-STIC-1419 Procedimiento de empleo seguro Routers Huawei NE40E Series

INFORMACIÓN IMPORTANTE

Ruckus FastIron ICX Series Switch/Router (ICX 7150-24, ICX 7150-24P, ICX 7150-48, ICX 7150-48P, ICX 7150-48PF, ICX 7150-48F, ICX 7150-C10ZP, ICX 7150-C12P, ICX 7150-C08P, ICX 7150-C08PT, ICX 7150-48ZP,ICX 7250-24, ICX 7250-24P, ICX 7250-48, ICX 7250-48P, ICX 7450-24, ICX 7450-24P, ICX 7450-48, ICX 7450-48P, ICX 7450-48F, ICX 7650-48P, ICX 7650-48ZP, ICX 7650-48F, ICX 7750-48F, ICX 7750-48C, ICX 7750-26Q, ICX 7850-32Q, ICX 7850-48FS y ICX 7850-48F)	
Versión	8.0.90 y 8.0.95.
Fabricante	Ruckus Wireless
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2021
Revisión de Validez	30/01/2022





Descripción

La familia RUCKUS ICX de conmutadores de nivel 2 y 3 está diseñada para simplificar la configuración y la gestión de la red, mejorar la seguridad, minimizar la resolución de problemas y facilitar las actualizaciones. Su arquitectura de baja latencia sin bloqueo garantiza una capacidad y un rendimiento excelentes para las aplicaciones más exigentes.

La familia de conmutadores RUCKUS ICX dispone de una gama completa de modelo, tanto para campus y redes empresariales de 2 y 3 niveles (acceso, agregación y Core) como para Data Center, con tecnologías avanzadas como Stacking a corta y larga distancia, PoE+ y PoE++, MultiGigabit, todo el rango de velocidades de puerto desde 1G hasta 100G, fuentes de alimentación modulares y reemplazables en caliente, nivel 2 y nivel 3 avanzado, MultiChassis Trunking, Campus Fabric, automatización, etc.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Aruba 6200F, 6300M, 6300F, 6405, 8320, 8325, 8360, and 8400	
Versión	Aruba OS-CX version 10.06
Fabricante	Aruba
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2021
Revisión de Validez	30/04/2022





Descripción

La familia Aruba CX implementan soluciones de switching y routing para redes de sucursales, campus y datacenter. Los equipos 8320, 8325, 8360, y 8400 son idóneos para Datacenter y equipos nucleo (core) de la red de campus. Los equipos 6400 se posicionan como equipos nucleo (core) de la red de campus, mientras los 6300 y 6200 están orientados para redes de acceso.
Implementan funcionalidades multicapa, implementan múltiples mecanismos de seguridad en el acceso y administración. Orientado a la segmentación dinámica y a implementar entornos Zero Trust. Permite el despliegue automático desasistido (ZTP).
Aruba CX dispone de una arquitectura interna de Sistema Operativo que proporciona una forma de trabajar con el completamente programable. Su motor de analíticas (NAE) permite la inserción de scripts de para la ejecución de tareas avanzadas de monitorización y respuestas a eventos.

Observaciones

Procedimiento de empleo pendiente de publicación.

INFORMACIÓN IMPORTANTE

SLX Product Series (SLX 9740 y SLX 9540)	
Versión	20.2.1aa
Fabricante	Extreme Networks
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2021
Revisión de Validez	31/07/2023



Descripción

Familia de switches y routers para Centros de Datos y Border Routing enfocada a operadores, proveedores de servicios y empresas. Se soportan tecnologías tales como MPLS/VPLS, Carrier Ethernet y EVPN, con equipos dotados de buffer ultra-profundos. Los equipos son compactos y proporcionan gran densidad de puertos a velocidades 1/10/25/40/50/100 Gbps en una unidad de rack.

El despliegue de soluciones IP Fabric para datacenter puede automatizarse desde una máquina virtual residente en el propio switch. Se soportan arquitecturas Clos (Leaf and Spine) sin necesidad de controlador externo. También se soporta la interconexión de Datacenters mediante Leaf especializados

Observaciones

CCN-STIC-1430 PES Switches Extreme Networks SLXOS

Aruba 2930F y 2930M Switch Series	
Versión	Aruba OS version 16.04
Fabricante	Aruba
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2022



Descripción

Familia de switches y routers para Centros de Datos y Border Routing enfocada a operadores, proveedores de servicios y empresas. Se soportan tecnologías tales como MPLS/VPLS, Carrier Ethernet y EVPN, con equipos dotados de buffer ultra-profundos. Los equipos son compactos y proporcionan gran densidad de puertos a velocidades 1/10/25/40/50/100 Gbps en una unidad de rack.

El despliegue de soluciones IP Fabric para datacenter puede automatizarse desde una máquina virtual residente en el propio switch. Se soportan arquitecturas Clos (Leaf and Spine) sin necesidad de controlador externo. También se soporta la interconexión de Datacenters mediante Leaf especializados

Observaciones

CCN-STIC-647C Seguridad en conmutadores HPE Aruba

INFORMACIÓN IMPORTANTE

Aruba 3810M Switch Series	
Versión	Aruba OS version 16.04
Fabricante	Aruba
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2022





Descripción

Familia de switches y routers para Centros de Datos y Border Routing enfocada a operadores, proveedores de servicios y empresas. Se soportan tecnologías tales como MPLS/VPLS, Carrier Ethernet y EVPN, con equipos dotados de buffer ultra-profundos. Los equipos son compactos y proporcionan gran densidad de puertos a velocidades 1/10/25/40/50/100 Gbps en una unidad de rack.

El despliegue de soluciones IP Fabric para datacenter puede automatizarse desde una máquina virtual residente en el propio switch. Se soportan arquitecturas Clos (Leaf and Spine) sin necesidad de controlador externo. También se soporta la interconexión de Datacenters mediante Leaf especializados

Observaciones

CCN-STIC-647C Seguridad en conmutadores HPE Aruba

Aruba 5400R Switch Series	
Versión	Aruba OS version 16.04
Fabricante	Aruba
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2022





Descripción

Familia de switches y routers para Centros de Datos y Border Routing enfocada a operadores, proveedores de servicios y empresas. Se soportan tecnologías tales como MPLS/VPLS, Carrier Ethernet y EVPN, con equipos dotados de buffer ultra-profundos. Los equipos son compactos y proporcionan gran densidad de puertos a velocidades 1/10/25/40/50/100 Gbps en una unidad de rack.

El despliegue de soluciones IP Fabric para datacenter puede automatizarse desde una máquina virtual residente en el propio switch. Se soportan arquitecturas Clos (Leaf and Spine) sin necesidad de controlador externo. También se soporta la interconexión de Datacenters mediante Leaf especializados

Observaciones

CCN-STIC-647C Seguridad en conmutadores HPE Aruba

INFORMACIÓN IMPORTANTE

Aruba Switch 2930F, 2930M, 3810M y 5400R	
Versión	ArubaOS version 16.08
Fabricante	Aruba
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2021
Revisión de Validez	31/05/2022





Descripción

Equipos diseñados para utilizarse en labores de acceso y agregación, o nucleo de red de acceso. Son equipos que proporcionan conexiones de todas las velocidades y tipos de medios. Equipos con capacidad de conmutación sin bloqueo (non-blocking). Según la familia, ofrecen soluciones escalables mediante constitución de stacks via puerto de red, puerto dedicado así como exiten modelos de chasis. Todas las funciones del sistema operativo se ofrecen con el equipo. Ofrecen diversos tipos de interfaces y velocidades. Ofrecen PoE en algunos modelos, a diferentes potencias. Pueden son gestionables, tanto localmente (gestión on-premise) como pueden llegar a administrarse en modalidad Software-as-a-Service

Observaciones

Procedimiento de empleo pendiente de publicación.

7.4.2 FAMILIA: SWITCHES

Aruba 8320 Switch Series	
Versión	Aruba OS-CX version 10.03
Fabricante	Aruba
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2019
Revisión de Validez	30/04/2022





Descripción

Equipos orientados a ser equipos de núcleo de red (CORE) de Campus como de Centros de Datos. Es un equipo con categoría de operador. Dispone de una arquitectura interna de Sistema Operativo que proporciona una forma de trabajar con el completamente programable. Su motor de analíticas (NAE) permite la inserción de scripts de para la ejecución de tareas avanzadas de monitorización y respuestas a eventos.
Ofrecen interfaces a alta velocidad así como una tecnología de chasis virtual.

Observaciones

Procedimiento de empleo pendiente de publicación.

INFORMACIÓN IMPORTANTE

Aruba 8325 Switch Series	
Versión	Aruba OS-CX version 10.03
Fabricante	Aruba
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2019
Revisión de Validez	30/04/2022





Descripción

Equipos orientados a ser equipos de núcleo de red (CORE) de Campus como de Centros de Datos. Es un equipo con categoría de operador. Dispone de una arquitectura interna de Sistema Operativo que proporciona una forma de trabajar con el completamente programable. Su motor de analíticas (NAE) permite la inserción de scripts de para la ejecución de tareas avanzadas de monitorización y respuestas a eventos.
Ofrecen interfaces a alta velocidad así como una tecnología de chasis virtual.

Observaciones

Procedimiento de empleo pendiente de publicación.

Aruba 8400 Switch Series	
Versión	Aruba OS-CX version 10.03
Fabricante	Aruba
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2019
Revisión de Validez	30/04/2022





Descripción

Equipos orientados a ser equipos de núcleo de red (CORE) de Campus como de Centros de Datos. Es un equipo con categoría de operador. Dispone de una arquitectura interna de Sistema Operativo que proporciona una forma de trabajar con el completamente programable. Su motor de analíticas (NAE) permite la inserción de scripts de para la ejecución de tareas avanzadas de monitorización y respuestas a eventos.
Ofrecen interfaces a alta velocidad así como una tecnología de chasis virtual.

Observaciones

Procedimiento de empleo pendiente de publicación.

INFORMACIÓN IMPORTANTE

Cisco Catalyst 9200 Series	
Versión	IOS 16.12
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2022
Revisión de Validez	30/06/2022

Descripción

9200: C9200-24T, C9200-48T, C9200-24P, C9200-48P. C9200-24PB, C9200-48PB, C9200-24PXG, C9200-48PXG con C9200-NM-4G, C9200-NM-4X, C9200-NM2Y, C9200-NM-2Q
9200L: C9200L-24P-4G, C9200L-24P-4X, C9200L-24T-4G, C9200L-24P-4X, C9200L-48P-4G, C9200L-48P-4X,C9200L-48T-4G, C9200L-248T-4X, C9200L-24PXG-2Y, C9200L-48PXG-2Y, C9200L-24PXG-4X, C9200L-48PXG-4X

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Cisco Catalyst 9300 Series	
Versión	IOS 16.12
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2022
Revisión de Validez	30/06/2022

Descripción

C9300-24T, C9300-48S, C9300-48U, C9300D-24UB, C9300D-48UB, C9300D-48UXB, C9300L-24T-4G, C9300L-24P-4G, C9300L-48T-4G, C9300L-48P-4G, C9300L-24T-4X, C9300L-24P-4X, C9300L-48T-4X, C9300L-48P-4X, C9300L-24UXG-4X, C9300-24UXG-2Q, C9300L-48UXG-2Q, C9300L-48PF-4G, C9300L-48PF-4X, C9300L-48UXG-4X

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Cisco Catalyst 9400 Series	
Versión	IOS 16.12
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2022
Revisión de Validez	30/06/2022

Descripción

Chasis: C9404R, C9407R, C9410R.
Supervisoras: C9400-SUP-1, C9400-SUP-1XL, C9400-SUP-1XL-Y.
Tarjetas: C9400-LC-48U, C9400-LC-48T, C9400-LC-48P, C9400-LC-24XS, C9400-LC-48UX, C9400-LC-24S, C9400-LC-48S, C9400-LC-48H

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Cisco Catalyst 9600 Series	
Versión	IOS 16.12
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2022
Revisión de Validez	30/06/2022

Descripción

Series Cisco Catalyst 9600 con Cisco Catalyst 9600 series Supervisor Engine y una o más tarjetas de línea: C9600-LC-48YL, C9600-LC-24C

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Cisco Nexus 3100, 3100V , 3100Z Series Switches (3172PQ/PQ-XL, 3172TQ, 31128PQ, 31108PC-V, 31108TC-V, Nexus 3132Q-V, 3132C-Z)

Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2022

Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Cisco Nexus 3200 Series Switches (3232C, 3264C-E)

Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2022

Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Cisco Nexus 3400 Series Switches (34180-YC, 3464C, 3432D-S, 3408-S)

Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2022

Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Cisco Nexus 3500 Series Switches (3524-X/XL, 3548-X/XL)	
Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2022

Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Cisco Nexus 3600 Series Switches (36180YC-R, 3636C-R)	
Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2022

Descripción

Estos switches proporcionan a las organizaciones arquitecturas flexibles, avanzada programabilidad, visibilidad y telemetría en tiempo real, alta escalabilidad y excepcional disponibilidad

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Cisco Nexus 9000 Series Switches	
Versión	NX-OS 9.3
Fabricante	Cisco Systems
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2022

Descripción

- Cisco Nexus 9200 Series Switches: 92348GC-X, 92160YC-X, 92300YC, 9272Q
- Cisco Nexus 9300 Series Switches: 93108TC-EX, 93108TC-FX, 9348GC-FXP, 93216TC-FX2, 93180LC-EX, 93180YC-EX, 93180YC-FX, 93240YC-FX2, 93360YC-FX2, 9364C, 9332C, 9336C-FX2, 9364C-GX,9316D-GX, 93600CD-GX
- Cisco 9500 Series Switches: 9504, 9508, 9516, Supervisor 9500-Sup-A , Supervisor 9500-Sup-A +, Supervisor 9500-Sup-B , Supervisor 9500-Sup-B, System Controller N9k-SC-A

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Dell Networking C-Series (C9010 y C1048P)	
Versión	V9.14
Fabricante	Dell Computer
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2020
Revisión de Validez	30/11/2022

Descripción

Este switch ofrece una plataforma de conmutación modular, de varias velocidades. Puede admitir redes de grandes empresas, medianas empresas y campus. Su plataforma de 8U cuenta con ranuras para hasta 10 módulos de tarjetas de línea, 2 módulos de procesadores de ruta, 3 módulos de ventiladores y 4 módulos de fuente de alimentación. El chasis viene equipado con un plano posterior integrado y compatible con varias velocidades 100GbE. El C1048 incluye 48 puertos 10/100/1000Base-T POE+ para el acceso de usuario y 2 puertos uplink SFP+ para la conectividad con el C9010

Observaciones

CCN-STIC-1402 Procedimiento de empleo seguro DELL EMC OS 9.14

INFORMACIÓN IMPORTANTE

Dell Networking S-Series 10GbE (S5048F, S4048-ON, S4048T-ON)	
Versión	V9.14
Fabricante	Dell Computer
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2020
Revisión de Validez	30/11/2022

Descripción

Estos switches 10GbE flexibles ofrecen las siguientes prestaciones:
- S4048-ON es un switch de baja latencia y alta densidad para la parte superior del rack con 48 puertos 10GbE SFP+ y 6 puertos 40 GbE (o 72 puertos 10 GbE en modo de transición), así comoun rendimiento de 720 Gb/s máscimo. Es compatible con el entorno Open Network Install Environment (ONIE).
- S5000 ofrece un diseño modular que permite añadir módulos Ethernet y Fibre Channel. El módulo Fibre Channel es compatible con el modo NPG los servicios completos de estructura Fibre Channel. Admite 4 módulos.

Observaciones

CCN-STIC-1402 Procedimiento de empleo seguro DELL EMC OS 9.14

Dell Networking S-Series 1GbE (S3124, S3124P, S3124F, S3148, S3148P, S3048-ON)	
Versión	V9.14
Fabricante	Dell Computer
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2020
Revisión de Validez	30/11/2022

Descripción

Estos switches 1GbE ofrecen las siguientes prestaciones:
- Proporcionan baja latencia y alta densidad con redundancia de hardware y software..
- Ofrecen diseños de Active Fabric con el uso de switches principales de la serie S o Z para crear una arquitectura de red de centro de datos 1/10/40GbE de dos niveles.

Observaciones

CCN-STIC-1402 Procedimiento de empleo seguro DELL EMC OS 9.14

INFORMACIÓN IMPORTANTE

Dell Networking S-Series 25/40/50/100GbE (S6010-ON, S6100-ON)	
Versión	V9.14
Fabricante	Dell Computer
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2020
Revisión de Validez	30/11/2022

Descripción

Los Swtiches Serie S ofrecen una solución preparada para redes definidas por software, con las siguientes pestaciones:
- Alta densidad para las implementaciones basadas en 25/40/50/100GbE para la parte superior del rack, en medio de la fila o al final dela fila.
- Selección de switches 40GbE S5048F-ON, S6000-ON y S6010-ON, además del switch modular 10/25/40/50/100GbE S6100-ON.
- Módulos S6100-ON que incluyen: 16 puertos 14GbE, 8 puertos 100GbE, módulo combinado de 4 puertos 100GbE CXP y 4 puertos 100GbE

Observaciones

CCN-STIC-1402 Procedimiento de empleo seguro DELL EMC OS 9.14

Dell Networking Z-Series (Z9100-ON)	
Versión	V9.14
Fabricante	Dell Computer
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2020
Revisión de Validez	30/11/2022

Descripción

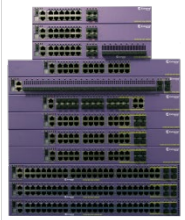
Este switch Open Networking de formato fijo y preparado para redes definidas por software (SDN) se ha diseñado para centros de datos y ofrece las siguientes prestaciones:
- Switch multivelocidad con opciones 10/25/40/50/100GbE.
- Alta densidad con hasta32 puertos 100GbE en 1U.
- Selección de los principales sistemas operativos de red.
- Vía de acceso fácil a las SDN para una parte o la totalidad de su entorno de producción.

Observaciones

CCN-STIC-1402 Procedimiento de empleo seguro DELL EMC OS 9.14

INFORMACIÓN IMPORTANTE

Summit X440-G2 Series:
X440-G2-12t-10GE4, X440-G2-12p-10GE4, X440-G2-24t-10GE4
X440-G2-24p-10GE4, X440-G2-48t-10GE4, X440-G2-48p-10GE4, X440-G2-24t-10GE4-DC, X440-G2-48t-10GE4-DC, X440-G2-24x-10GE4, X440-G2-24fx-GE4, X440-G2-12t8fx-GE4, X440-G2-24t-GE4



Versión	EXOS v22.3.1.4-patch1CC-2
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2022

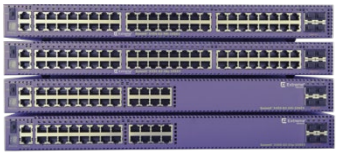
Descripción

Conmutador apilable de alto rendimiento, posicionado como equipo de acceso. Proporciona conmutación inteligente de Nivel 2 y routing básico de Nivel 3, con interfaces 10/100/1000 Mbps así como 10 Gb. Existen versiones PoE y no PoE y de puertos de fibra óptica y puede apilarse también con otras familias de switches Extreme Networks

Observaciones

CCN-STIC-642B Seguridad en Extreme Networks EXOS

Summit x450-G2 Series:
X450-G2-24t-GE4, X450-G2-24p-GE4, X450-G2-48t-GE4, X450-G2-48p-GE4, X450-G2-24t-10GE4, X450-G2-24p-10GE4, X450-G2-48t-10GE4, X450-G2-48p-10GE4, X450-G2-24p-10GE4-FB-715-TAA, X450-G2-48p-10GE4-FB-1100-TAA,X450-G2-24t-GE4-FB-TAA, X450



Versión	EXOS v22.3.1.4-patch1CC-2
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2022

Descripción

Conmutador apilable de alto rendimiento, posicionado como equipo de acceso de altas prestaciones. Proporciona conmutación avanzada de Nivel 2 y routing de Nivel 3, con interfaces 10/100/1000 Mbps, así como 10Gb. Existen versiones PoE y no PoE, y puede apilarse con otras familias de switches Extreme Networks.

Observaciones

CCN-STIC-642B Seguridad en Extreme Networks EXOS

INFORMACIÓN IMPORTANTE

Summit X460-G2 Series:
X460-G2-24t-10GE4, X460-G2-48t-10GE4, X460-G2-24p-10GE4, X460-G2-48p-10GE4, X460-G2-24x-10GE4, X460-G2-48x-10GE4, X460-G2-24t-GE4, X460-G2-48t-GE4, X460-G2-24p-GE4, X460-G2-48p-GE4

Versión	EXOS v22.3.1.4-patch1CC-2
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2022





Descripción

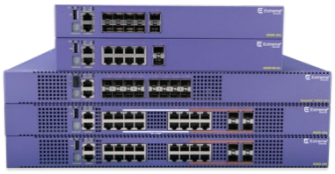
Conmutador apilable de alta rendimiento, posicionado como equipo de acceso de altas prestaciones y backbone de redes medias. Proporciona conmutación avanzada de Nivel 2 y de Nivel 3, con soporte de protocolos de alta complejidad (BGP, MPLS, etc). con interfaces 10/100/1000 Mbps, así como 10Gb y 40 Gb. Existen versiones PoE y no PoE, y puede apilarse con otras familias de switches Extreme Networks.

Observaciones

CCN-STIC-642B Seguridad en Extreme Networks EXOS

Summit X620 Series:
X620–16x, X620–16t, X620–10x, X620–8t-2x

Versión	EXOS v22.3.1.4-patch1CC-2
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2022





Descripción

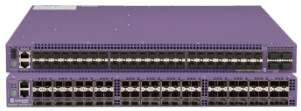
Conmutador apilable de alto rendimiento, proporcionando servicios avanzados de switching y enrutamiento básico. Destinado como concentrador de redes pequeñas y también para conexión de servidores. Soporta interfaces 100Mb, 1Gb y 10Gb. Asimismo puede proporcionar PoE. El equipo es apilable también con otras familias de switches Extreme Networks.

Observaciones

CCN-STIC-642B Seguridad en Extreme Networks EXOS

INFORMACIÓN IMPORTANTE

Summit x670-G2 Series: X670-G2-72x, X670-G2-48x-4q, X670-G2-48x-4q-FB-AC-TAA	
Versión	EXOS v22.3.1.4-patch1CC-2
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2022



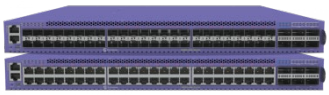
Descripción

La familia de productos x670-G2 proporciona servicios avanzados de switching y routing, pudiendo utilizarse como equipo concentrador o bien como una solución Top of Rack para una granja de servidores, gracias a su baja latencia y capacidades avanzadas. Se soportan interfaces 10Gb y 40Gb. El equipo es apilable también con otras familias de switches Extreme Networks.

Observaciones

CCN-STIC-642B Seguridad en Extreme Networks EXOS

Summit X690 Series: (X690-48x-2q-4c, X690-48t-2q-4c)	
Versión	EXOS v22.3.1.4-patch1CC-2
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2022



Descripción

La familia de productos x690 proporciona servicios avanzados de switching y routing, pudiendo utilizarse como equipo concentrador o bien como una solución Top of Rack para una granja de servidores, gracias a su baja latencia y capacidades avanzadas. Se soportan interfaces 10Gb, 25Gb, 40Gb, 50 Gb y 100Gb. El equipo es apilable también con otras familias de switches Extreme Networks.

Observaciones

CCN-STIC-642B Seguridad en Extreme Networks EXOS

INFORMACIÓN IMPORTANTE

Summit X870 Series: (X870-32c, X870-96x-8c)

Versión	EXOS v22.3.1.4-patch1CC-2
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2022



Descripción

La familia de productos x870 proporciona servicios de switching y de routing. Soporta velocidades de 10 Gb, 25Gb, 40GB, 50Gby 100GB en un formato compacto de 1U. La conmutación directa de baja latencia y un conjunto de características avanzadas lo hacenideal para centros de datos de alto rendimiento. El equipo es apilable también con otras familias de switches Extreme Networks.

Observaciones

CCN-STIC-642B Seguridad en Extreme Networks EXOS

Series AlliedWare Plus x930 (x930-28GTX, x930-28GPX, x930-28GSTX, x930-52GTX, x930-52GPX) y x950 (x950-28XSQ y x950-28XTQm)

Versión	Software Version 5.5.0-0.6
Fabricante	Allied Telesys
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2019
Revisión de Validez	30/04/2022



Descripción

Switches apilables Layer 3 con puertos Gigabit. Ofrecen flexibilidad, fiabilidad y alto rendimiento al estar orientados a soluciones de core y distribución de redes. Vienen con opciones de 24 y 48 puertos con uplinks de 10G y 40G. Son apilables hasta 8 unidades gracias a la tecnología Virtual Chassis Stacking (VCStack™) que permite crear pilas con equipos separados hasta 40 km.Están equipados con el sistema operativo AlliedWare Plus. Entre sus características más reseñables, destacan:

- Soporte de AMF para gestión avanzada de redes convergentes
- Protocolos para redes flexibles como EPSR, G.8032 o UDLD
- Monitorización activa de fibra (AFM)
- Análisis de tráfico sFlow
- POE continuo
- Layer 3: RIP, OSPF, BGP, VRF
- Controlador wireless

Observaciones

CCN-STIC-1422 Procedimiento de empleo Seguro AlliedWare Plus (AW+) versión 5.5.0-0.6

INFORMACIÓN IMPORTANTE

Series AlliedWare Plus x550 (X550-18XTQ, X550-18XSQ, X550-18XSPQm) y x530-x530L (X530-28GPXm, X530-28GPXm, X530-52GTXm, X530-52GPXm, X530L-28GTX, X530L-28GPX, X530L-52GTX, X530L-52GPX)

Versión	Software Version 5.5.0-0.6
Fabricante	Allied Telesys
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2019
Revisión de Validez	30/04/2022





Descripción

Switches apilables Layer 3 con puertos Gigabit. Ofrecen flexibilidad, fiabilidad y alto rendimiento al estar orientados a soluciones de core y distribución de redes. Vienen con opciones de 24 y 48 puertos con uplinks de 10G y 40G. Son apilables hasta 8 unidades gracias a la tecnología Virtual Chassis Stacking (VCStack™) que permite crear pilas con equipos separados hasta 40 km.Están equipados con el sistema operativo AlliedWare Plus. Entre sus características más reseñables, destacan:

- Soporte de AMF para gestión avanzada de redes convergentes
- Protocolos para redes flexibles como EPSR, G.8032 o UDLD
- Monitorización activa de fibra (AFM)
- Análisis de tráfico sFlow
- POE continuo
- Layer 3: RIP, OSPF, BGP, VRF
- Controlador wireless

Observaciones

CCN-STIC-1422 Procedimiento de empleo Seguro AlliedWare Plus (AW+) versión 5.5.0-0.6

Series AlliedWare Plus x230 (X230-10GP, X230-10GT, X230-18GP, X230-18GT, X230-28GP, X230-28GT, X230L-17GT, X230L-26GT) y x200 (X220-28GS, X220-52GP, X220-52GT)

Versión	Software Version 5.5.0-0.6
Fabricante	Allied Telesys
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2019
Revisión de Validez	30/04/2022





Descripción

Switches apilables Layer 3 con puertos Gigabit. Ofrecen flexibilidad, fiabilidad y alto rendimiento al estar orientados a soluciones de core y distribución de redes. Vienen con opciones de 24 y 48 puertos con uplinks de 10G y 40G. Son apilables hasta 8 unidades gracias a la tecnología Virtual Chassis Stacking (VCStack™) que permite crear pilas con equipos separados hasta 40 km.Están equipados con el sistema operativo AlliedWare Plus. Entre sus características más reseñables, destacan:

- Soporte de AMF para gestión avanzada de redes convergentes
- Protocolos para redes flexibles como EPSR, G.8032 o UDLD
- Monitorización activa de fibra (AFM)
- Análisis de tráfico sFlow
- POE continuo
- Layer 3: RIP, OSPF, BGP, VRF
- Controlador wireless

Observaciones

CCN-STIC-1422 Procedimiento de empleo Seguro AlliedWare Plus (AW+) versión 5.5.0-0.6

INFORMACIÓN IMPORTANTE

Series AlliedWare Plus SBX81CFC960 (SBx81CFC960, SBx81GP24, SBx81GT24, SBx81GS24a, SBx81GC40, SBx81XLEM) y SBX908 GEN2 (XEM2-8XSTm, XEM2-12XTm, XEM2-12XT, XEM2-12XS, XEM2-4QS, XEM2-1CQ)	
Versión	Software Version 5.5.0-0.6
Fabricante	Allied Telesys
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2019
Revisión de Validez	30/04/2022





Descripción

Switches apilables Layer 3 con puertos Gigabit. Ofrecen flexibilidad, fiabilidad y alto rendimiento al estar orientados a soluciones de core y distribución de redes. Vienen con opciones de 24 y 48 puertos con uplinks de 10G y 40G. Son apilables hasta 8 unidades gracias a la tecnología Virtual Chassis Stacking (VCStack™) que permite crear pilas con equipos separados hasta 40 km.Están equipados con el sistema operativo AlliedWare Plus. Entre sus características más reseñables, destacan:

- Soporte de AMF para gestión avanzada de redes convergentes
- Protocolos para redes flexibles como EPSR, G.8032 o UDLD
- Monitorización activa de fibra (AFM)
- Análisis de tráfico sFlow
- POE continuo
- Layer 3: RIP, OSPF, BGP, VRF
- Controlador wireless

Observaciones

CCN-STIC-1422 Procedimiento de empleo Seguro AlliedWare Plus (AW+) versión 5.5.0-0.6

Series AlliedWare Plus x510 (X510-28GSX)	
Versión	Software Version 5.5.0-0.6
Fabricante	Allied Telesys
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2019
Revisión de Validez	30/04/2022





Descripción

Switches apilables Layer 3 con puertos Gigabit. Ofrecen flexibilidad, fiabilidad y alto rendimiento al estar orientados a soluciones de core y distribución de redes. Vienen con opciones de 24 y 48 puertos con uplinks de 10G y 40G. Son apilables hasta 8 unidades gracias a la tecnología Virtual Chassis Stacking (VCStack™) que permite crear pilas con equipos separados hasta 40 km.Están equipados con el sistema operativo AlliedWare Plus. Entre sus características más reseñables, destacan:

- Soporte de AMF para gestión avanzada de redes convergentes
- Protocolos para redes flexibles como EPSR, G.8032 o UDLD
- Monitorización activa de fibra (AFM)
- Análisis de tráfico sFlow
- POE continuo
- Layer 3: RIP, OSPF, BGP, VRF
- Controlador wireless

Observaciones

CCN-STIC-1422 Procedimiento de empleo Seguro AlliedWare Plus (AW+) versión 5.5.0-0.6

INFORMACIÓN IMPORTANTE

Huawei Cloud Engine 6800 (6881-48T6CQ)	
Versión	V200R020C00SPC600 Patch V200R020SPH100T
Fabricante	Huawei Technologies España
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/12/2023

Descripción

Es un switch que proporciona servicios estables, fiables y de alto rendimiento en capa 2 y capa 3. Estos switches están diseñados para centros de datos y redes de campus de alta gama. Proporcionan alto rendimiento, interfaces de alta densidad y baja latencia. Tienen un diseño hardware avanzado que suministra puertos de alta densidad mientras usa la misma plataforma software Huawei VRP.

Observaciones

CCN-STIC 1424 Procedimiento de Empleo Seguro Huawei CE Series Switches

EX2300 Series (EX2300-48P/48T y EX2300-C-12T/12T)	
Versión	Junos OS 19.1R2
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2020
Revisión de Validez	31/12/2022

Descripción

Los switches EX son dispositivos de red que soportan la definición, y cumplimiento, de las políticas de flujo de información entre los nodos de la red. Junto a funciones de seguridad del tránsito de información, el producto registra todas las actividadesrelevantes, y cuenta con herramientas de seguridad para la gestión de las funcionalidades de seguridad.

Como switch de nivel 2 en la capa OSI, realiza un análisis de los paquetes entrantes, reenviando dichos paquetes en función de la información que contienen, haciéndolos llegar así a su destinatario.

Como switch de nivel 3 en la capa OSI, admite el enrutamiento del trafico basado en tablas identificando las rutas disponibles, las condiciones, la distancia y los costes para así determinar la ruta más adecuada para cada paquete.

Observaciones

CCN-STIC-1427 Procedimiento de Empleo Seguro Switches Jniper EX2300-EX3400, JunOS 19.1

INFORMACIÓN IMPORTANTE

EX3400 Series (EX3400-24P/24T y EX3400-48P/48T)	
Versión	Junos OS 19.1R2
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2020
Revisión de Validez	31/12/2022

Descripción

Los switches EX son dispositivos de red que soportan la definición, y cumplimiento, de las políticas de flujo de información entre los nodos de la red. Junto a funciones de seguridad del tránsito de información, el producto registra todas las actividadesrelevantes, y cuenta con herramientas de seguridad para la gestión de las funcionalidades de seguridad.
Como switch de nivel 2 en la capa OSI, realiza un análisis de los paquetes entrantes, reenviando dichos paquetes en función de la información que contienen, haciéndolos llegar así a su destinatario.
Como switch de nivel 3 en la capa OSI, admite el enrutamiento del trafico basado en tablas identificando las rutas disponibles, las condiciones, la distancia y los costes para así determinar la ruta más adecuada para cada paquete.

Observaciones

CCN-STIC-1427 Procedimiento de Empleo Seguro Switches Jniper EX2300-EX3400, JunOS 19.1

EX4600 Series (EX4600-40F-AFO, EX4600-40F-AFI, EX4600-40F-DC-AFO y EX4600-40F-DC-AFI)	
Versión	Junos OS 18.1R1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2020
Revisión de Validez	31/12/2022

Descripción

Los switches EX son dispositivos de red que soportan la definición, y cumplimiento, de las políticas de flujo de información entre los nodos de la red. Junto a funciones de seguridad del tránsito de información, el producto registra todas las actividadesrelevantes, y cuenta con herramientas de seguridad para la gestión de las funcionalidades de seguridad.
Como switch de nivel 2 en la capa OSI, realiza un análisis de los paquetes entrantes, reenviando dichos paquetes en función de la información que contienen, haciéndolos llegar así a su destinatario.
Como switch de nivel 3 en la capa OSI, admite el enrutamiento del trafico basado en tablas identificando las rutas disponibles, las condiciones, la distancia y los costes para así determinar la ruta más adecuada para cada paquete.

Observaciones

CCN-STIC-1428 Procedimiento de Empleo Seguro Switches Jniper QFX5100-EX4600, JunOS 19.1

INFORMACIÓN IMPORTANTE

QFX5100 Series (QFX5100-48S-AFO/AFI, QFX5100-48T-AFO/AFI, QFX5100-24Q-AFO/AFI, QFX5100-24Q-AA-AFO/AFI y QFX5100-96S-AFO/AFI)	
Versión	Junos OS 18.1R1
Fabricante	Juniper Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2020
Revisión de Validez	31/12/2022

Descripción

Los switches QFX son dispositivos de red que soportan la definición, y cumplimiento, de las políticas de flujo de información entre los nodos de la red. Junto a funciones de seguridad del tránsito de información, el producto registra todas las actividadesrelevantes, y cuenta con herramientas de seguridad para la gestión de las funcionalidades de seguridad.
Como switch de nivel 2 en la capa OSI, realiza un análisis de los paquetes entrantes, reenviando dichos paquetes en función de la información que contienen, haciéndolos llegar así a su destinatario.
Como switch de nivel 3 en la capa OSI, admite el enrutamiento del trafico basado en tablas identificando las rutas disponibles, las condiciones, la distancia y los costes para así determinar la ruta más adecuada para cada paquete.

Observaciones

CCN-STIC-1428 Procedimiento de Empleo Seguro Switches Jniper QFX5100-EX4600, JunOS 19.1

SLX Product Series (SLX9150, SLX9250 y SLX9640)	
Versión	20.1.1aa
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2021
Revisión de Validez	31/07/2023



Descripción

Familia de switches y routers para Centros de Datos y Border Routing enfocada a operadores, proveedores de servicios y empresas. Se soportan tecnologías tales como MPLS/VPLS, Carrier Ethernet y EVPN, con equipos dotados de buffer ultra-profundos. Los equipos son compactos y proporcionan gran densidad de puertos a velocidades 1/10/25/40/50/100 Gbps en una unidad de rack.

El despliegue de soluciones IP Fabric para datacenter puede automatizarse desde una máquina virtual residente en el propio switch. Se soportan arquitecturas Clos (Leaf and Spine) sin necesidad de controlador externo. También se soporta la interconexión de Datacenters mediante Leaf especializados.

Observaciones

CCN-STIC-1430 PES Switches Extreme Networks SLXOS.

INFORMACIÓN IMPORTANTE

Dell EMC Networking SmartFabric (Modelos: S3048-ON, S4048-ON, S4048T-ON, S4112F-ON, S4112T-ON, S4128F-ON, S4128T-ON, S4148F-ON, S4148T-ON, S4148U-ON, MX5108n, S4248FB-ON, S4248FBL-ON, S6010-ON, Z9100-ON, MX9116n, S5212F-ON, S5224F-ON, S5232F-ON, S5248F-ON

Versión	OS 10 Build: 10.5.1.3.
Fabricante	Dell Computer
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2020
Revisión de Validez	30/04/2022

Descripción

Dell EMC Smart Fabric OS10 es el sistema operativo de red (NOS) que se utiliza en las familias de enrutadores y conmutadores de las serie N (algunos modelos), serie S, serie Z y serie MX de Dell EMC Networking (las plataformas HW que actualmente soportanOS10 son N3200, S3048-ON, S4048-ON, S4048T-ON, S4112F-ON, S4112T-ON, S4128F-ON, S4128T-ON, S4148F-ON, S4148T-ON, S4148U-ON, S4248FB-ON, S4248FBL-ON, S6010-ON, S5212F-ON, S5224F-ON, S5232F-ON, S5248F-ON, S5296F-ON, Z9100-ON, Z9264F-ON, Z9332F-ON, MX5108n yMX9116n). Dell EMC SmartFabric OS10 es un sistema operativo de red (NOS) que admite múltiples arquitecturas y entornos. La solución SmartFabric OS10 permite la desagregación en varias capas de la funcionalidad de red. SmartFabric OS10 comprende la administración, monitorización y funcionalidad completa y estándar de la industria de redes de nivel 2 y nivel 3 a través de interfaces CLI, SNMP y REST. Los usuarios pueden elegir sus propias aplicaciones de organización, gestión, supervisión y redes de terceros. Para desarrollar redes escalables L2 y L3, SmartFabric OS10 ofrece una solución modular y desagregada en una única imagen binaria.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Huawei S Series Ethernet Switches S1730 (S1730S-S24T4S-A, S1730S-S24P4S-A, S1730S-S48T4S-A, S1730S-H24T4S-A, S1730S-S24T4X-A, S1730S-S48P4S-A y S1730S-H48T4S-A)

Versión	V200R020C00SPC300 y V200R021C00SPC100
Fabricante	Huawei Technologies España
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2021
Revisión de Validez	31/08/2023

Descripción

Los switches de la Serie-S de Huawei están diseñados para cubrir las necesidades de evolución de la red de campus. Entre sus capacidades destacan la gestión simplificada y el alto rendimiento. Pueden ser utilizados en cualquier tipo de sector: empresarial, gubernamental, educativo, financiero o industrial.

Observaciones

CCN-STIC-1418 Procedimiento de empleo seguro Switches Huawei Serie S Ethernet

INFORMACIÓN IMPORTANTE

Huawei S Series Ethernet Switches S5720 (S5720-28X-PWR-LI-AC, S5720-52X-PWR-LI-AC, S5720-52P-LI-AC y S5720-52P-PWR-LI-AC)	
Versión	V200R020C00SPC300 y V200R021C00SPC100
Fabricante	Huawei Technologies España
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2021
Revisión de Validez	31/08/2023

Descripción

Los switches de la Serie-S de Huawei están diseñados para cubrir las necesidades de evolución de la red de campus. Entre sus capacidades destacan la gestión simplificada y el alto rendimiento. Pueden ser utilizados en cualquier tipo de sector: empresarial, gubernamental, educativo, financiero o industrial.

Observaciones

CCN-STIC-1418 Procedimiento de empleo seguro Switches Huawei Serie S Ethernet

Huawei S Series Ethernet Switches S5731 (S5731-H24T4XC, S5731-H48T4XC, S5731-H24P4XC, S5731-H48P4XC, S5731-S24T4X, S5731-S24P4X, S5731-S48T4X y S5731-S48P4X)	
Versión	V200R020C00SPC300 y V200R021C00SPC100
Fabricante	Huawei Technologies España
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2021
Revisión de Validez	31/08/2023

Descripción

Los switches de la Serie-S de Huawei están diseñados para cubrir las necesidades de evolución de la red de campus. Entre sus capacidades destacan la gestión simplificada y el alto rendimiento. Pueden ser utilizados en cualquier tipo de sector: empresarial, gubernamental, educativo, financiero o industrial.

Observaciones

CCN-STIC-1418 Procedimiento de empleo seguro Switches Huawei Serie S Ethernet

INFORMACIÓN IMPORTANTE

Huawei S Series Ethernet Switches S5732 (S5732-H24S6Q, S5732-H48S6Q, S5732-H48XUM2CC, S5732-H48UM2CC y S5732-H24UM2CC)	
Versión	V200R020C00SPC300 y V200R021C00SPC100
Fabricante	Huawei Technologies España
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2021
Revisión de Validez	31/08/2023

Descripción

Los switches de la Serie-S de Huawei están diseñados para cubrir las necesidades de evolución de la red de campus. Entre sus capacidades destacan la gestión simplificada y el alto rendimiento. Pueden ser utilizados en cualquier tipo de sector: empresarial, gubernamental, educativo, financiero o industrial.

Observaciones

CCN-STIC-1418 Procedimiento de empleo seguro Switches Huawei Serie S Ethernet

Huawei S Series Ethernet Switches S5735 y S5736	
Versión	V200R020C00SPC300 y V200R021C00SPC100
Fabricante	Huawei Technologies España
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2021
Revisión de Validez	31/08/2023

Descripción

Modelos: S5735-L24T4S-A, S5735-L12T4S-A, S5735-L24T4X-A, S5735-L12P4S-A, S5735-L24P4S-A, S5735-L24P4X-A, S5735-L32ST4X-A, S5735-S32ST4X, S5735-L48T4S-A, S5735-L48T4X-A, S5735-S24T4X, S5735-S24P4X S5735-S48T4X, S5735-S48P4X, S5735-L48P4X-A, S5735-S48S4X,S5735-S24T4X-I, S5735-L8T4X-A1, S5735-L8T4S-A1, S5735-L8P4X-A1, S5735-L8P4S-A1, S5735-L48T4X-A1, S5735-L48T4S-A1, S5735-L48P4X-A1, S5735-L48P4S-A1, S5735-L24T4X-A1, S5735-L24T4S-A1, S5735-L24P4X-A1, S5735-L24P4S-A1, S5735-L32ST4X-A1, S5735-L8T4S-QA1, S5735-L8P4S-QA1, S5735-L24T4S-QA1, S5735-L24T4X-QA1, S5736-S24UM4XC, S5736-S48S4X-A, S5736-S48S4X-D3.
Los switches de la Serie-S de Huawei están diseñados para cubrir las necesidades de evolución de la red de campus. Entre sus capacidades destacan la gestión simplificada y el alto rendimiento. Pueden ser utilizados en cualquier tipo de sector: empresarial, gubernamental, educativo, financiero o industrial.

Observaciones

CCN-STIC-1418 Procedimiento de empleo seguro Switches Huawei Serie S Ethernet

INFORMACIÓN IMPORTANTE

Huawei S Series Ethernet Switches S6730 (S6730-H48X6C, S6730-H24X6C, S6730-S24X6Q, S6730-H48X6C y S6730-H24X6C)	
Versión	V200R020C00SPC300 y V200R021C00SPC100
Fabricante	Huawei Technologies España
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2021
Revisión de Validez	31/08/2023

Descripción

Los switches de la Serie-S de Huawei están diseñados para cubrir las necesidades de evolución de la red de campus. Entre sus capacidades destacan la gestión simplificada y el alto rendimiento. Pueden ser utilizados en cualquier tipo de sector: empresarial, gubernamental, educativo, financiero o industrial.

Observaciones

CCN-STIC-1418 Procedimiento de empleo seguro Switches Huawei Serie S Ethernet

Huawei S Series Ethernet Switches S5770 (S7703, S7706 y S7712)	
Versión	V200R020C00SPC300 y V200R021C00SPC100
Fabricante	Huawei Technologies España
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2021
Revisión de Validez	31/08/2023

Descripción

Los switches de la Serie-S de Huawei están diseñados para cubrir las necesidades de evolución de la red de campus. Entre sus capacidades destacan la gestión simplificada y el alto rendimiento. Pueden ser utilizados en cualquier tipo de sector: empresarial, gubernamental, educativo, financiero o industrial.

Observaciones

CCN-STIC-1418 Procedimiento de empleo seguro Switches Huawei Serie S Ethernet

INFORMACIÓN IMPORTANTE

Huawei S Series Ethernet Switches S12700 (SS12700E-4, S12700E-8 y S12700E-12)	
Versión	V200R020C00SPC300 y V200R021C00SPC100
Fabricante	Huawei Technologies España
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2021
Revisión de Validez	31/08/2023

Descripción

Los switches de la Serie-S de Huawei están diseñados para cubrir las necesidades de evolución de la red de campus. Entre sus capacidades destacan la gestión simplificada y el alto rendimiento. Pueden ser utilizados en cualquier tipo de sector: empresarial, gubernamental, educativo, financiero o industrial.

Observaciones

CCN-STIC-1418 Procedimiento de empleo seguro Switches Huawei Serie S Ethernet

Ruckus FastIron ICX Series Switch/Router (ICX 7150-24, ICX 7150-24P, ICX 7150-48, ICX 7150-48P, ICX 7150-48PF, ICX 7150-48F, ICX 7150-C10ZP, ICX 7150-C12P, ICX 7150-C08P, ICX 7150-C08PT, ICX 7150-48ZP,ICX 7250-24, ICX 7250-24P, ICX 7250-48, ICX 7250-48P, ICX 7450-24, ICX 7450-24P, ICX 7450-48, ICX 7450-48P, ICX 7450-48F, ICX 7650-48P, ICX 7650-48ZP, ICX 7650-48F, ICX 7750-48F, ICX 7750-48C, ICX 7750-26Q, ICX 7850-32Q, ICX 7850-48FS y ICX 7850-48F)	
Versión	8.0.90 y 8.0.95.
Fabricante	Ruckus Wireless
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2021
Revisión de Validez	30/11/2021

Descripción

La familia RUCKUS ICX de conmutadores de nivel 2 y 3 está diseñada para simplificar la configuración y la gestión de la red, mejorar la seguridad, minimizar la resolución de problemas y facilitar las actualizaciones. Su arquitectura de baja latencia sin bloqueo garantiza una capacidad y un rendimiento excelentes para las aplicaciones más exigentes.

La familia de conmutadores RUCKUS ICX dispone de una gama completa de modelo, tanto para campus y redes empresariales de 2 y 3 niveles (acceso, agregación y Core) como para Data Center, con tecnologías avanzadas como Stacking a corta y larga distancia, PoE+ y PoE++, MultiGigabit, todo el rango de velocidades de puerto desde 1G hasta 100G, fuentes de alimentación modulares y reemplazables en caliente, nivel 2 y nivel 3 avanzado, MultiChassis Trunking, Campus Fabric, automatización, etc.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Alcatel-Lucent Enterprise OmniSwitch Serie 6465 (OS6465-P6, OS6465-P12, OS6465-P28, OS6465T-P12 y OS6465T-12)	
Versión	AOS 8.6.R11.
Fabricante	Alcatel-Lucent Enterprise
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2021
Revisión de Validez	30/09/2023





Descripción

Familia de conmutadores L2+ con puertos 1G y 10G, preparados para entorno industrial, con amplio rango de temperaturas de funcionamiento (-40ºC a +75ºC). Diseñados como equipos de acceso en redes de tipo industrial, transportes o utilities.
https://www.al-enterprise.com/es-es/productos/conmutadores

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS

Alcatel-Lucent Enterprise OmniSwitch Serie 6560 (OS6560-P24Z8, OS6560-P24Z24, OS6560-P48Z16, OS6560-24Z8, OS6560-24Z24, OS6560-24X4, OS6560-P24X4, OS6560-48X4, OS6560-P48X4 y OS6560-X10)	
Versión	AOS 8.6.R11.
Fabricante	Alcatel-Lucent Enterprise
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2021
Revisión de Validez	30/09/2023





Descripción

Familia de conmutadores L3 compactos apilables con alta densidad de puertos 1GE, Multigigabit ethernet 1/2.5 GigE y enlaces 10GE, diseñados como equipos de acceso en redes convergentes de alta capacidad.
https://www.al-enterprise.com/es-es/productos/conmutadores

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS

INFORMACIÓN IMPORTANTE

Alcatel-Lucent Enterprise OmniSwitch Serie 6860 (OS6860-24, OS6860-P24, OS6860-48, OS6860-P48, OS6860E-24, OS6860E-P24, OS6860E-48, OS6860E-P48, OS6860E-U28 y OS6860E-P24Z8)	
Versión	AOS 8.6.R11.
Fabricante	Alcatel-Lucent Enterprise
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2021
Revisión de Validez	30/09/2023





Descripción

OS6860: Familia de conmutadores L3+ compactos apilables con alta densidad de puertos 1GE, Multigigabit ethernet 1/2.5/5/10 GigE y enlaces 10GE, 25GE y 100GE, diseñadas para redes convergentes. Con funciones de Acceso unificado avanzadas que permiten la creación de redes orientadas a las aplicaciones. Puede supervisar y controlar las aplicaciones de la red mediante capacidades de Deep Packet Inspection (DPI).
https://www.al-enterprise.com/es-es/productos/conmutadores

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS

Alcatel-Lucent Enterprise OmniSwitch Serie 6865 (OS6865-P16X, OS6865-U12X y OS6865-U28X)	
Versión	AOS 8.6.R11.
Fabricante	Alcatel-Lucent Enterprise
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2021
Revisión de Validez	30/09/2023





Descripción

Familia de conmutadores L3+ con puertos 1G y 10G, preparados para entorno industrial o redes de misión crítica como transportes y utilities, con amplio rango de temperaturas de funcionamiento (-40ºC a +75ºC).
https://www.al-enterprise.com/es-es/productos/conmutadores

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS

INFORMACIÓN IMPORTANTE

Alcatel-Lucent Enterprise OmniSwitch Serie 6900 (OS6900-X20, OS6900-X40, OS6900-T20, OS6900-T40, OS6900-X72, OS6900-Q32, OS6900-V72 y OS6900-C32)	
Versión	AOS 8.6.R11.
Fabricante	Alcatel-Lucent Enterprise
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2021
Revisión de Validez	30/09/2023





Descripción

Familia de conmutadores L3+ compactos apilables de alta densidad 10GE, 25GE, 40GE y 100GE. Diseñadas para que sean flexibles. Pueden instalarse como conmutadores convergentes situados en la parte superior del bastidor (TOR) o tipo spine para entornos de Data Centers y también como dispositivos de agregación y de núcleo en una red de campus.
https://www.al-enterprise.com/es-es/productos/conmutadores

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS

Alcatel-Lucent Enterprise OmniSwitch Serie 9900 (OmniSwitch 9907 Chassis, OS9907-CFM, OS99-CMM, OS99-XNI-48, OS99-XNI-U48, OS99-GNI-48, OS99-GNI-P48, OS99-CNI-U8, OS99-XNI-P24Z8, OS99-XNI-P48Z16, OS99-XNI-U12Q, OS99-XNI-U24, OS99-XNI-U48 y OS99-XNI-UP24Q2)	
Versión	AOS 8.6.R11.
Fabricante	Alcatel-Lucent Enterprise
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2021
Revisión de Validez	30/09/2023





Descripción

Conmutador LAN L3+ con chasis modular de alta capacidad de interfaces 1GE, 10GE y 100GE para conmutación segura y con alta disponibilidad en el núcleo de las redes empresariales, campus y redes Metro Ethernet.
https://www.al-enterprise.com/es-es/productos/conmutadores

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS

INFORMACIÓN IMPORTANTE

Huawei CloudEngine 16800 (CE16804, CE16808 y CE16816), Huawei CloudEngine 12800 (CE12804, CE12808 y CE12816), Huawei CloudEngine 8800 (CE8861-4C-EI y CE8850-64CQ-EI) y Huawei CloudEngine 6800 (CE6863-48S6CQ, CE6881-48S6CQ y CE6820-48S6CQ)

Versión	V200R019C10SPC800 Patch V200R019SPH008T
Fabricante	Huawei Technologies España
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2021
Revisión de Validez	31/12/2023

Descripción

Huawei CloudEngine 16800, Huawei CloudEngine 12800, Huawei CloudEngine 8800 and Huawei CloudEngine 6800 son switches que proporcionan servicios estables, fiables y de alto rendimiento en capa 2 y capa 3. Estos switches están diseñados para centros de datos y redes de campus de alta gama. Proporcionan alto rendimiento, interfaces de alta densidad y baja latencia. Los switches CloudEngine Series tienen un diseño hardware avanzado que suministra puertos de alta densidad mientras usa la misma plataforma software Huawei VRP.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Aruba 6200F, 6300M, 6300F, 6405, 8320, 8325, 8360, and 8400

Versión	Aruba OS-CX version 10.06
Fabricante	Aruba
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2021
Revisión de Validez	30/04/2022



Descripción

La familia Aruba CX implementan soluciones de switching y routing para redes de sucursales, campus y datacenter. Los equipos 8320, 8325, 8360, y 8400 son idóneos para Datacenter y equipos nucleo (core) de la red de campus. Los equipos 6400 se posicionan como equipos nucleo (core) de la red de campus, mientras los 6300 y 6200 están orientados para redes de acceso.

Implementan funcionalidades multicapa, implementan múltiples mecanismos de seguridad en el acceso y administración. Orientado a la segmentación dinámica y a implementar entornos Zero Trust. Permite el despliegue automático desasistido (ZTP)

Aruba CX dispone de una arquitectura interna de Sistema Operativo que proporciona una forma de trabajar con el completamente programable. Su motor de analíticas (NAE) permite la inserción de scripts de para la ejecución de tareas avanzadas de monitorización y respuestas a eventos.

Observaciones

Procedimiento de empleo pendiente de publicación.

INFORMACIÓN IMPORTANTE

Aruba 2930F y 2930M Switch Series

Versión	Aruba OS version 16.04
Fabricante	Aruba
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2022





Descripción

Familia de switches y routers para Centros de Datos y Border Routing enfocada a operadores, proveedores de servicios y empresas. Se soportan tecnologías tales como MPLS/VPLS, Carrier Ethernet y EVPN, con equipos dotados de buffer ultra-profundos. Los equipos son compactos y proporcionan gran densidad de puertos a velocidades 1/10/25/40/50/100 Gbps en una unidad de rack.

El despliegue de soluciones IP Fabric para datacenter puede automatizarse desde una máquina virtual residente en el propio switch. Se soportan arquitecturas Clos (Leaf and Spine) sin necesidad de controlador externo. También se soporta la interconexión de Datacenters mediante Leaf especializados

Observaciones

CCN-STIC-647C Seguridad en conmutadores HPE Aruba

Aruba 3810M Switch Series

Versión	Aruba OS version 16.04
Fabricante	Aruba
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2022





Descripción

Familia de switches y routers para Centros de Datos y Border Routing enfocada a operadores, proveedores de servicios y empresas. Se soportan tecnologías tales como MPLS/VPLS, Carrier Ethernet y EVPN, con equipos dotados de buffer ultra-profundos. Los equipos son compactos y proporcionan gran densidad de puertos a velocidades 1/10/25/40/50/100 Gbps en una unidad de rack.

El despliegue de soluciones IP Fabric para datacenter puede automatizarse desde una máquina virtual residente en el propio switch. Se soportan arquitecturas Clos (Leaf and Spine) sin necesidad de controlador externo. También se soporta la interconexión de Datacenters mediante Leaf especializados

Observaciones

CCN-STIC-647C Seguridad en conmutadores HPE Aruba

INFORMACIÓN IMPORTANTE

Aruba 5400R Switch Series	
Versión	Aruba OS version 16.04
Fabricante	Aruba
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2022





Descripción

Familia de switches y routers para Centros de Datos y Border Routing enfocada a operadores, proveedores de servicios y empresas. Se soportan tecnologías tales como MPLS/VPLS, Carrier Ethernet y EVPN, con equipos dotados de buffer ultra-profundos. Los equipos son compactos y proporcionan gran densidad de puertos a velocidades 1/10/25/40/50/100 Gbps en una unidad de rack.

El despliegue de soluciones IP Fabric para datacenter puede automatizarse desde una máquina virtual residente en el propio switch. Se soportan arquitecturas Clos (Leaf and Spine) sin necesidad de controlador externo. También se soporta la interconexión de Datacenters mediante Leaf especializados

Observaciones

CCN-STIC-647C Seguridad en conmutadores HPE Aruba

Aruba Switch 2930F, 2930M, 3810M y 5400R	
Versión	ArubaOS version 16.08
Fabricante	Aruba
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2021
Revisión de Validez	31/05/2022





Descripción

Equipos diseñados para utilizarse en labores de acceso y agregación, o nucleo de red de acceso. Son equipos que proporcionan conexiones de todas las velocidades y tipos de medios. Equipos con capacidad de conmutación sin bloqueo (non-blocking). Según la familia, ofrecen soluciones escalables mediante constitución de stacks via puerto de red, puerto dedicado así como exiten modelos de chasis. Todas las funciones del sistema operativo se ofrecen con el equipo. Ofrecen diversos tipos de interfaces y velocidades. Ofrecen PoE en algunos modelos, a diferentes potencias. Pueden son gestionables, tanto localmente (gestión on-premise) como pueden llegar a administrarse en modalidad Software-as-a-Service

Observaciones

Procedimiento de empleo pendiente de publicación.

INFORMACIÓN IMPORTANTE

Nokia 1830 Photonic Service Switch (PSS)	
Versión	9.1.0
Fabricante	NOKIA
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2022
Revisión de Validez	31/08/2022

Descripción

El conmutador de servicio fotónico Nokia 1830PSS es una plataforma que ofrece conectividad multiservicio de multiplexación óptica por división de longitud de onda densa de gran capacidad. Incluye cifrado, baja latencia y detección de intrusiones ópticas, lo que garantiza la confidencialidad e integridad de los datos, así como el soporte de comunicaciones.
La familia 1830PSS consta de diferentes plataformas que se han optimizado para su aplicabilidad en diversos entornos de despliegue de redes ópticas, desde la interconexión de CPD hasta el escalado de grandes redes ópticas multiservicio, multicapa, regionales y de larga distancia. Estos equipos aprovechan el software, el hardware, la gestión y el control comunes, para ofrecer operaciones fluidas en toda la cartera de posibilidades que ofrece la familia 1830PSS.
Son compatibles con múltiples aplicaciones de red de transporte, que incluyen: transporte y agregación metro multiservicio, implementaciones de larga distancia/núcleo óptico, configuraciones de conmutación fotónica con enrutamiento colorless, directionless y contentionless con Flexgrid, agregación/conmutación en capa L1, medidas reflextométricas OTDR de las fibras ópticas, y otros mecanismos de protección.

Observaciones

Procedimiento de empleo pendiente de publicación.

7.4.3 FAMILIA: CORTAFUEGOS

Cisco Firepower Threat Defense (FTD) en Firepower 1000 Series (FP1010, FP1120 y FP1140) con FMC y FMCv	
Versión	FTD 6.4 y FMC/FCMv 6.4
Fabricante	Cisco Systems
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2022

Descripción

Cisco Firepower Threat Defense (FTD) tiene capacidades de firewall, VPN e IPS. Esta plataforma ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).
Compatible con:
-Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)
-FMCv running on ESXi 6.0 or 6.5 on the Unified Computing System (UCS) UCSB-B200-M4, UCSC-C220-M4S, UCSC-C240-M4SX, UCSC-C240-M4L, UCSB-B200-M5, UCSC-C220-M5, UCSC-C240-M5, UCS-E160S-M3 and UCS-E180D-M3

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Cisco Firepower Threat Defense (FTD) en Firepower 2000 Series FP2110, FP2120, FP2130 y FP2140) con FMC y FMCv	
Versión	FTD 6.4 y FMC/FCMv 6.4
Fabricante	Cisco Systems
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2022

Descripción

Cisco Firepower Threat Defense (FTD) tiene capacidades de firewall, VPN e IPS. Esta plataforma ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).
Compatible con:
-Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)
-FMCv running on ESXi 6.0 or 6.5 on the Unified Computing System (UCS) UCSB-B200-M4, UCSC-C220-M4S, UCSC-C240-M4SX, UCSC-C240-M4L, UCSB-B200-M5, UCSC-C220-M5, UCSC-C240-M5, UCS-E160S-M3 and UCS-E180D-M3

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Fortigate FG-30E, FWF-30E, FG-40F, FG-40F-3G4G, FG-50E, FWF-50E, FG-51E, FWF-51E, FG-52E, FG-60E, FG-60E-DSL, FG-60E-PoE, FWF-60E, FWF-60E-DSL, FG-60F, FG-60F-3G4G, FWF-60F, FG-61E, FG-61F, FWF-61E, FWF-61F, FG-80E, FG-80E-PoE, FG-81E y FG-81E-PoE	
Versión	FortiOS 6.2.7
Fabricante	Fortinet
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2022

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos para entornos pequeños y sedes remotas de pocos usuarios. Las funcionalidades de seguridad son similares a las del resto de modelos más grandes (reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf).

Observaciones

CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.

INFORMACIÓN IMPORTANTE

Fortigate FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140E, FG-140E-PoE, FG-200E, FG-201E, FG-300D, FG-300E, FG-301E, FG-400D, FG-400E, FG-401E, FG-500D, FG-500E, FG-501E, FG-600D, FG-601E y FG-900D.	
Versión	FortiOS 6.2.7
Fabricante	Fortinet
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2022

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos para entornos pequeños y sedes remotas de pocos usuarios. Las funcionalidades de seguridad son similares a las del resto de modelos más grandes (reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf).

Observaciones

CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.

Fortigate FG-1000D, FG-1100E, FG-1100E-DC, FG-1101E, FG-1200D, FG-1500D, FG-1500DT, FG-1500D-DC, FG-2000E, FG-2201E y FG-2500E	
Versión	FortiOS 6.2.7
Fabricante	Fortinet
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2022

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos para entornos pequeños y sedes remotas de pocos usuarios. Las funcionalidades de seguridad son similares a las del resto de modelos más grandes (reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf).

Observaciones

CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.

INFORMACIÓN IMPORTANTE

Fortigate FG-3000D, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3600E, FG-3601E, FG-3700D, FG-3800D, FG-3801D, FG-3815D, FG-3960E, FG-3980E, FG-5001E, FG-5001E1, FG-6301F, FG-6501F, FGR-30D, FGR-60F y FGR-60F-3G4G

Versión	FortiOS 6.2.7
Fabricante	Fortinet
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2022

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos para entornos pequeños y sedes remotas de pocos usuarios. Las funcionalidades de seguridad son similares a las del resto de modelos más grandes (reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf).

Observaciones

CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.

Fortigate-VM00, Fortigate-VM01, Fortigate-VM02, Fortigate-VM04, Fortigate-VM08, Fortigate-VM16, Fortigate-VM32 y Fortigate-VMUL

Versión	FortiOS 6.2.7
Fabricante	Fortinet
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2022

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos para entornos pequeños y sedes remotas de pocos usuarios. Las funcionalidades de seguridad son similares a las del resto de modelos más grandes (reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf).

Observaciones

CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.

INFORMACIÓN IMPORTANTE

WatchGuard Fireware on Firebox NGFWs (T35, T40, T80, T55, M270, M370, M470, M570, M670, M4600 y M5600)	
Versión	FirewareOS 12.6.2 Linux Kernel 4.14.83.
Fabricante	WatchGuard Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2021
Revisión de Validez	30/09/2023

Descripción

Los equipos UTM de WatchGuard están enfocados en ofrecer la mejor seguridad para cualquier empresa y entorno corporativo distribuido. Nuestros dispositivos de seguridad de red están diseñados, desde el inicio, para enfocarse en facilitar el despliegue, el uso y la administración continua.

Proporcionan protección contra ataques de malware avanzado y phishing, así como las protecciones de seguridad tradicionales: prevención de intrusiones (IPS), filtrado de URL, control de aplicaciones, antispam y antivirus, … ofreciendo en todo momento visibilidad del entorno (productividad y seguridad)

Cuentan con capacidades SD-WAN, y VPN.

Están disponibles tanto en equipos físicos como virtuales.
https://www.watchguard.com/es/wgrd-products/network-security

Observaciones

CCN-STIC-1421 Procedimiento de empleo seguro WatchGuard Fireware OS v12.6.2

Forcepoint NGFW 1100 Series y 2100 Series (NGFW 1101, NGFW 1105, NGFW 2101 y NGFW 2105)	
Versión	SW: 6.3.1
Fabricante	Forcepoint
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2018
Revisión de Validez	30/04/2022

Descripción

Firewalls de Nueva Generación orientados a compañías u organismos de tamaño medio, de tipo appliance físico de 1RU, con capacidades IPS, SD-WAN, URL Filtering y Detección Avanzada de Malware. Dependiendo del modelo concreto de dispositivo se puede disponer de hasta un rendimiento de 3 Gbps de Throughput NGFW/NGIPS, 20 millones de conexiones concurrentes y 100 contextos virtuales. Más información en:
https://www.forcepoint.com/environments/forcepoint-ngfw-appliances

Observaciones

CCN-STIC-1409 Procedimiento de empleo seguro cortafuegos Forcepoint NGFW

INFORMACIÓN IMPORTANTE

Forcepoint NGFW 3300 Series (NGFW 3301 y NGFW 3305)	
Versión	SW: 6.3.1
Fabricante	Forcepoint
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2018
Revisión de Validez	30/04/2022

Descripción

Firewalls de Nueva Generación orientados a grandes redes Campus y Datacenters, de tipo appliance físico de 2RU, IPS, SD-WAN, URL Filtering y Detección Avanzada de Malware. Dependiendo del modelo concreto de dispositivo se puede disponer de hasta un rendimiento de 15 Gbps de Throughput NGFW/NGIPS, 50 millones de conexiones concurrentes y 250 contextos virtuales. Más información en:
https://www.forcepoint.com/environments/forcepoint-ngfw-appliances

Observaciones

CCN-STIC-1409 Procedimiento de empleo seguro cortafuegos Forcepoint NGFW

Forcepoint NGFW 6200 Series (NGFW 6205)	
Versión	SW: 6.3.1
Fabricante	Forcepoint
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2018
Revisión de Validez	30/04/2022

Descripción

Firewall de Nueva Generación orientado a Grandes Empresas y Datacenters, de tipo appliance físico en formato chasis de 4RU, IPS, SD-WAN, URL Filtering y Detección Avanzada de Malware. Proporciona un rendimiento de hasta de 22 Gpbs de Throughput NGFW/NGIPS, 60 millones de conexiones concurrentes y 250 contextos virtuales. Más información en:
https://www.forcepoint.com/environments/forcepoint-ngfw-appliances

Observaciones

CCN-STIC-1409 Procedimiento de empleo seguro cortafuegos Forcepoint NGFW

INFORMACIÓN IMPORTANTE

Stormshield Network Security UTM/NG-Firewall (Appliances desde SN200 a SN6100 en 4 compilaciones distintas: S, M, L y XL).	
Versión	3.10.1
Fabricante	Stormshield SAS
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2020
Revisión de Validez	30/09/2022

Descripción

Firewalls de nueva generación de capa 7, IPS y concentrador de túneles VPN. Con capacidades de bloqueo de amenazas avanzadas, ataques de día cero, filtrado de navegación web o gestión de vulnerabilidades.
El mismo equipamiento realiza inspección profundade protocolos OT, además de IT.

Observaciones

CCN-STIC-1415 Procedimiento de Empleo Seguro Cortafuegos UTMNG Stormshield

Junos 15.1X49-D60 for SRX platforms SRX300, SRX320, SRX340, SRX345, SRX550M, SRX5400E, SRX5400X, SRX5600E, SRX5600X, SRX5800E and SRX 5800X	
Versión	SW: Junos 15.1X49-D60
Fabricante	Juniper Networks
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2021
Revisión de Validez	31/10/2023

Descripción

La gama de productos SRX de Juniper Networks ofrece, en un solo dispositivo, capacidades de conectividad, conmutación y seguridad que le permiten dar funciones simultaneas de enrutador, switch y cortafuegos de nivel 7, así como dispositivo de detección yprevención de intrusiones. Su sistema operativo Junos, provee de un lenguaje universal con el resto de soluciones de Juniper que facilitan la operación y las tareas de automatización e integración con otras soluciones.

Observaciones

CCN-STIC-1404 “Procedimiento de Empleo Seguro Plataformas SRX Juniper”

INFORMACIÓN IMPORTANTE

Serie SOHO (SOHOW)	
Versión	SonicOS 6.5.2
Fabricante	SonicWall
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2019
Revisión de Validez	30/04/2022

Descripción

Los cortafuegos de la serie TZ SOHO de Sonicwall son la solución perfecta para oficinas pequeñas y domésticas, así como para entornos distribuidos en ubicaciones remotas. Ambos despliegan funcionalidades para construir Secure SD-WAN y conectividad WIFI (opcional). El SOHO 250 proporciona un 50% más de rendimiento sobre su antecesor SOHO, así como acceso a los sandboxes avanzados Capture ATP, con lo que se consigue la máxima seguridad en prevención y detección de malware desconocido en un entorno remoto.

Observaciones

CCN-STIC-1420 Procedimiento de Empleo Seguro Sonicwall SonicOS

Aruba Mobility Controller Series (7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM y 7280)	
Versión	ArubaOS 8.5.
Fabricante	Aruba
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2020
Revisión de Validez	31/12/2021

Descripción

Aruba Mobility Controller Series funcionan como gateway entre redes cableadas e inalámbricas y proveen funciones de comando y control sobre los puntos de acceso de Aruba (APs) dentro de una red inalámbrica Aruba. Los Mobility Controllers (MC) y Virtual Mobility Controllers (VMC) de Aruba, son switches inalámbricos (Appliance físicos o virtuales) que proporcionan una amplia gama de servicios y características de seguridad que incluyen la movilidad de red inalámbrica y cableada, seguridad, administración centralizada, auditoría, autenticación, acceso remoto seguro, auto-chequeos de integridad y operación, filtrado de tráfico y funcionalidad de Gateway VPN.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

SonicWall NSA Serie (2650, 3600, 3650, 4600, 4650, 5600, 5650, 6600, 6650, 9250, 9450, 9650)	
Versión	SonicOS 6.5.2
Fabricante	SonicWall
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2019
Revisión de Validez	30/04/2022

Descripción

Los firewall de la serie NSa de SonicWall están indicados para compañías medianas / grandes (de entre 50 y 3000 usuarios aprox), empresas deslocalizadas geográficamente y datacenters, consolidando tecnologías automatizadas de prevención y detección de amenazas como la inspección de memoria profunda en tiempo real (RTDMI). Desarrollados sobre una arquitectura de hardware de múltiples núcleos con interfaces 10-GbE y 2.5-GbE, la serie NSa cuenta con capacidades basadas en la nube y en el equipo, como descifrado e inspección TLS/SSL, application intelligence y control, SD-WAN segura, visualización en tiempo real y administración de WLAN. Más info en: https://www.sonicwall.com/es-mx/products/firewalls/mid-range

Observaciones

CCN-STIC-1420 Procedimiento de Empleo Seguro Sonicwall SonicOS

SonicWall SM Serie (9200, 9400, 9600, 9800)	
Versión	SonicOS 6.5.2
Fabricante	SonicWall
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2019
Revisión de Validez	30/04/2022

Descripción

Diseñado para grandes empresas, centros de datos, carriers y proveedores de servicios con necesidades multi-gigabit. Dirigido a compañías de entre 1000 y más de 50.000 usuarios (aprox.), realiza detección y prevención de amenazas mediante la combinación de la protección basada en appliances con la inteligencia de la nube en una plataforma de alto desempeño y consolida tecnologías de seguridad que brindan protección contra amenazas a millones de conexiones sin ralentizar el desempeño. Más info en: https://www.sonicwall.com/es-mx/products/firewalls/high-end

Observaciones

CCN-STIC-1420 Procedimiento de Empleo Seguro Sonicwall SonicOS

INFORMACIÓN IMPORTANTE

SonicWall TZ Serie (300/W, 400/W, 500/W, 600)	
Versión	SonicOS 6.5.2
Fabricante	SonicWall
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2019
Revisión de Validez	30/04/2022

Descripción

La serie TZ de SonicWall ofrece seguridad y rendimiento de entorno Enterprise orientado a pequeñas compañías. Enfocado a entornos departamentales o PYMES de entre 5 y 100 usuarios (aprox), incorpora funciones de prevención de intrusiones, antimalware, filtrado de contenidos/URL y control de aplicaciones a través de redes y entornos inalámbricos. Proporciona inspección profunda de paquetes (DPI), SD-WAN y despliegue zero-touch. Opciones de puertos PoE y wifi 802.11ac. Más info en: https://www.sonicwall.com/es-mx/products/firewalls/entry-level

Observaciones

CCN-STIC-1420 Procedimiento de Empleo Seguro Sonicwall SonicOS

Check Point Security Gateway Serie 15000 (CPAP-SG15400-NGTX, CPAP-SG15600-NGTX)	
Versión	R80.30
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2020
Revisión de Validez	31/12/2022

Descripción

Son dispositivos dedicados y que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 76Gbps de inspección Firewall, 13,5Gbps de IPS y 10.1 Gbps para protección ante amenazas avanzadas. Un máximo de 25.6 millones de conexiones concurrentes y 300.000 nuevas por segundo.
https://www.checkpoint.com/downloads/products/15400-security-gateway-datasheet.pdf
https://www.checkpoint.com/downloads/products/15600-security-gateway-datasheet.pdf

Observaciones

CCN-STIC 653 Seguridad en Check Point

INFORMACIÓN IMPORTANTE

Check Point Security Gateway Serie 23000, 26000/26000T, 16000/16000T (16200/16600HS), 3000 (3600/3800), 6000 (6200/6400/6600/6700/6900), 7000, 28000 (28000/28600HS)	
Versión	R80.30 GA 3.10 (take 300)
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2020
Revisión de Validez	31/12/2022

Descripción

Son dispositivos dedicados y que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 128Gbps de inspección Firewall, 26Gbps de IPS y 20 Gbps para protección ante amenazas avanzadas. Un máximo de 51,2 millones de conexiones concurrentes y 400.000 nuevas por segundo.
https://www.checkpoint.com/downloads/products/23500-security-gateway-datasheet.pdf
https://www.checkpoint.com/downloads/products/23800-security-gateway-datasheet.pdf
https://www.checkpoint.com/downloads/product-related/datasheets/ds-23900-appliance.pdf

Observaciones

CCN-STIC 653 Seguridad en Check Point

Check Point Security Gateway Serie 3000 (CPAP-SG3100-NGTX, CPAP-SG3200-NGTX)	
Versión	R80.30
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2020
Revisión de Validez	31/12/2022

Descripción

Son dispositivos dedicados y que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 4 Gbps de inspección Firewall, 1.1 Gbps de IPS y 510 Mbps para protección ante amenazas avanzadas. Un máximo de 3.2 millones de conexiones concurrentes y 40.000 nuevas por segundo.
https://www.checkpoint.com/downloads/products/3100-security-gateway-datasheet.pdf
https://www.checkpoint.com/downloads/products/3200-security-gateway-datasheet.pdf

Observaciones

CCN-STIC 653 Seguridad en Check Point

INFORMACIÓN IMPORTANTE

Check Point Security Gateway Serie 5000 (CPAP-SG5100-NGTX, CPAP-SG5200-NGTX, CPAP-SG5400-NGTX, CPAP-SG5600-NGTX, CPAP-SG5800-NGTX, CPAP-SG5900-NGTX)

Versión	R80.30
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2020
Revisión de Validez	31/12/2022

Descripción

Son dispositivos dedicados y que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 52 Gbps de inspección Firewall, 7.6 Gbps de IPS y 6.1 Gbps para protección ante amenazas avanzadas. Un máximo de 12.8 millones de conexiones concurrentes y 210.000 nuevas por segundo.
https://www.checkpoint.com/downloads/products/5100-security-gateway-datasheet.pdf
https://www.checkpoint.com/downloads/products/5200-security-gateway-datasheet.pdf
https://www.checkpoint.com/downloads/products/5400-security-gateway-datasheet.pdf
https://www.checkpoint.com/downloads/products/5600-security-gateway-datasheet.pdf
https://www.checkpoint.com/downloads/products/5800-security-gateway-datasheet.pdf
https://www.checkpoint.com/downloads/products/5900-security-gateway-datasheet.pdf

Observaciones

CCN-STIC 653 Seguridad en Check Point

Check Point Security Threat Emulation/Extraction (CPAP-SBTE100X-4VM, CPAP-SBTE250X-8VM, CPAP-SBTE1000X-A-28VM, CPAP-SBTE2000X-40VM , CPAP-SBTE2000X-56VM-HPP)

Versión	R80.30
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2020
Revisión de Validez	31/12/2022

Descripción

Equipos dedicados a emulación de ficheros para la detección y prevención de Malware de día Zero, tanto en Navegación (HTTP), como en Correo (SMTP). Permiten la integración con terceros tanto vía API como por protocolo ICAP. Estos equipos según el modelo,son capaces de analizar entre 450 ficheros y 5000 ficheros únicos la hora, soportando desde 450Mbps a más de 4Gbps, permitiendo ampliación hasta 14 puertos 1GbE RJ45, 8 puertos 10GbE de Fibra SFP+. Todos los modelos se pueden configurar con tarjetas de Bypass de 4 puertos 1GbE RJ45 o 2 puertos 10GbE de fibra.

Observaciones

CCN-STIC 653 Seguridad en Check Point

INFORMACIÓN IMPORTANTE

Smart1 Appliances
(CPAP-NGSM-405, CPAP-NGSM-410, CPAP-NGSM-625, CPAP-NGSM-5050, CPAP-NGSM-5150)

Versión	R80.30
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2020
Revisión de Validez	31/12/2022

Descripción

Smart-1 es la solución hardware para el servidor que gestiona los Gateways de Check Point.
Se trata de un hardware que combina la definición de políticas, logs, monitorización y aplicación de normativas (GDPR, 27001,..), y la correlación de eventos, en un solo punto.
Sus principales características, entre otras son; gestión por varios administradores de forma concurrente, gestión delegada total o parcial tanto de políticas como objetos a un usuario o grupo de usuarios, API Rest-Full con fines de automatización y orquestación, y versión Multi-Tenant.
Dependiendo del modelo, puede gestionar desde 5 Gateways o 500 puestos trabajo, a más de 150 Gateways o 15.000 por gestora.
Dependiendo del modelo disponen desde 16GB RAM hasta los 256 GB y entre 1TB y 48TB de almacenamiento, lo que les permite indexar entre 40.000 y 100.000 registros de log por segundo. Todos los modelos disponen de interfaces GBE, puerto consola y USB y en algunas versiones ofrecen la posibilidad de puertos de 10GbE y SAN fiber channel.
https://www.checkpoint.com/downloads/products/smart-1-security-management-platform-datasheet.pdf

Observaciones

CCN-STIC 653 Seguridad en Check Point

Smart1 Licencias Open Server
(CPSG-2C-NGTX, CPSG-4C-NGTX, CPSG-8C-NGTX, CPSG-16C-NGTX, CPSG-24C-NGTX, CPSG-32CNGTX)

Versión	R80.30
Fabricante	Check Point Software Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2020
Revisión de Validez	31/12/2022

Descripción

Las licencias de Open Server ofrecen la posibilidad de instalar el software de Check Point en un appliance no propietario en base una lista certificada y probada por Check Point. Las funcionalidades serán las mismas que si de un hardware dedicado se tratase. Dependiendo del número de cores del Gateway software, ofrece capacidades que van de 22Gbps a 128 Gbps de inspección Firewall, de 3,9 a 30 Gbps de IPS.

Observaciones

CCN-STIC 653 Seguridad en Check Point

INFORMACIÓN IMPORTANTE

Fortigate FG-30E, FG-50E, FG-51E, FG-52E, FG-60E, FG-60E-DSL, FG-60E-PoE, FG-61E, FG-80E, FG-80E- PoE, FG-81E, FG-81E-PoE	
Versión	FortiOS 6.0
Fabricante	Fortinet
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2021
Revisión de Validez	29/09/2022

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos para entornos pequeños y sedes remotas de pocos usuarios. Las funcionalidades de seguridad son similares a las del resto de modelos más grandes (reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf).
AP Wifi integrado en el dispositivo, para proporcionar cobertura inalámbrica a las oficinas.
Más información en: https://www.fortinet.com/products/next-generation-firewall.htm

Observaciones

CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.

FortiWifi FWF-30E, FWF-50E,FWF-51E, FWF-60E, FWF-60EDSL, FWF-61E	
Versión	FortiOS 6.0
Fabricante	Fortinet
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2021
Revisión de Validez	29/09/2022

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos para entornos pequeños y sedes remotas de pocos usuarios. Las funcionalidades de seguridad son similares a las del resto de modelos más grandes (reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf).
AP Wifi integrado en el dispositivo, para proporcionar cobertura inalámbrica a las oficinas.
Más información en: https://www.fortinet.com/products/next-generation-firewall.htm

Observaciones

CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.

INFORMACIÓN IMPORTANTE

Fortigate FG-100E, FG-100EF, FG-101E, FG-140E, FG-140EPoE, FG-200E, FG-201E, FG-300D, FG-300E, FG-301E, FG-400D, FG-400E, FG-401E,FG-500D, FG-500E, FG- 501E, FG-600D, FG-600E, FG-601E,FG-900D	
Versión	FortiOS 6.0
Fabricante	Fortinet
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2021
Revisión de Validez	29/09/2022

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos para entornos pequeños y sedes remotas de pocos usuarios. Las funcionalidades de seguridad son similares a las del resto de modelos más grandes (reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf).
AP Wifi integrado en el dispositivo, para proporcionar cobertura inalámbrica a las oficinas.
Más información en: https://www.fortinet.com/products/next-generation-firewall.htm

Observaciones

CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate

Fortigate FG-1000D, FG-1100E, FG-1101E,FG-1200D, FG-1500D, FG-2000E, FG-2200E, FG-2201E, FG-2500E	
Versión	FortiOS 6.0
Fabricante	Fortinet
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2021
Revisión de Validez	29/09/2022

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos para entornos pequeños y sedes remotas de pocos usuarios. Las funcionalidades de seguridad son similares a las del resto de modelos más grandes (reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf).
AP Wifi integrado en el dispositivo, para proporcionar cobertura inalámbrica a las oficinas.
Más información en: https://www.fortinet.com/products/next-generation-firewall.htm

Observaciones

CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate

INFORMACIÓN IMPORTANTE

Fortigate FG-3000D, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3600E, FG-3601E,FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG- 3960E, FG-3980E	
Versión	FortiOS 6.0
Fabricante	Fortinet
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2021
Revisión de Validez	29/09/2022

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos para entornos pequeños y sedes remotas de pocos usuarios. Las funcionalidades de seguridad son similares a las del resto de modelos más grandes (reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf).
AP Wifi integrado en el dispositivo, para proporcionar cobertura inalámbrica a las oficinas.
Más información en: https://www.fortinet.com/products/next-generation-firewall.htm

Observaciones

CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.

Fortigate FG-5001D, FG-5001E,FG-5001E1	
Versión	FortiOS 6.0
Fabricante	Fortinet
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2021
Revisión de Validez	29/09/2022

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos para entornos pequeños y sedes remotas de pocos usuarios. Las funcionalidades de seguridad son similares a las del resto de modelos más grandes (reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf).
AP Wifi integrado en el dispositivo, para proporcionar cobertura inalámbrica a las oficinas.
Más información en: https://www.fortinet.com/products/next-generation-firewall.htm

Observaciones

CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.

INFORMACIÓN IMPORTANTE

LTM+AFM (Bourne 1035v-F, Shuttle i5000 (i5600, i5800, i5820-DF), Shuttle i7000 (i7600, i7800, i7820-DF), Shuttle i10000 (i10600, i10800), Shuttle i11000 (i11600-DS, i11800-DS), Shuttle i15000 (i15800, i15600-DS), VIPRION B2250 y VIPRION B4450)	
Versión	14.1.0.3 BUILD bigip-14.1.0.3.75.6-ENG with Hotfix-BIGIP-14.1.0.3.0.75.6-ENG
Fabricante	F5 Networks Iberia,S.L.
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2021
Revisión de Validez	30/04/2022

Descripción

F5 BIG-IP, en su configuración de firewall, es una solución de seguridad perimetral de red para los centros de datos. Dota de mecanismos de seguridad de las capas 3 y 4 basados en políticas y una protección frente a ataques de denegación de servicio distribuidos. Con BIG-IP los ataques serán mitigados antes de llegar a los recursos críticos del centro de datos. Mediante una interfaz de gestión de políticas intuitiva, la generación de reportes y analíticas, BIG-IP proporciona una visión completa del estado de seguridad del perímetro de la red.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Aruba Mobility Controller (9004, 7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM, 7280) y puntos de acceso.	
Versión	ArubaOS 8.6
Fabricante	Aruba
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2021
Revisión de Validez	30/04/2022

Descripción

Las familias Aruba Mobility Controllers 7000´s, 7200´s, 9000s y las Virtual Mobility Controller (appliance virtual) junto con los puntos de acceso de las familias 500s, 300s y 200s permiten desplegar redes inalámbricas de máxima seguridad y rendimiento.
Con esta versión se soporta también WPA3 y Wifi-6/802.11ax (con las familias 500s) así como WiFi-5/802.1ac y Wifi-4/802.11n.
Se implementan avanzadas características de seguridad, en el control de acceso a la red así como en la asignación de políticas de seguridad. También se soportan mecanismos de monitorización de espectro. Los Puntos de Acceso en modo pueden trabajar en modo Campus (CAP) y modo Remoto (RAP,lo que permite conectar de forma segura puntos de acceso que cruzan redes ajenas como internet).
Se implementan mejoras en actualizaciones de software sin perdida de servicio. Aruba Multizona permite a un Punto de Acceso dar servicio a varias Mobility Controllers de diferentes dominios o entornos de seguridad. Los Mobility Controllers puede actuar como servidores de túneles IPSEC/SSL para el cliente Aruba VIA.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

SonicWall TZ Serie (300P, 350, 350W, 600P)	
Versión	6.5.4.4-44n-federal-12n
Fabricante	SonicWall
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2021
Revisión de Validez	31/01/2024

Descripción

La serie TZ de SonicWall ofrece seguridad y rendimiento de entorno Enterprise orientado a pequeñas compañías. Enfocado a entornos departamentales o PYMES de entre 5 y 100 usuarios (aprox), incorpora funciones de prevención de intrusiones, antimalware, filtrado de contenidos/URL y control de aplicaciones a través de redes y entornos inalámbricos. Proporciona inspección profunda de paquetes (DPI), SD-WAN y despliegue zero-touch. Opciones de puertos PoE y wifi 802.11ac.
Más info en: https://www.sonicwall.com/es-mx/products/firewalls/entry-level.

Observaciones

CCN-STIC-1420 Procedimiento de Empleo Seguro Sonicwall SonicOS

SonicWall SOHO Serie (250, 250W)	
Versión	6.5.4.4-44n-federal-12n
Fabricante	SonicWall
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2021
Revisión de Validez	31/01/2024

Descripción

Los cortafuegos de la serie TZ SOHO de Sonicwall son una solución adecuada para oficinas pequeñas y domésticas, así como para entornos distribuidos en ubicaciones remotas. Despliegan funcionalidades para construir Secure SD-WAN y conectividad WIFI (opcional). El SOHO 250 proporciona un 50% más de rendimiento sobre su antecesor SOHO, así como acceso a los sandboxes avanzados Capture ATP, con lo que se mejora la seguridad en prevención y detección de malware desconocido en un entorno remoto.

Observaciones

CCN-STIC-1420 Procedimiento de Empleo Seguro Sonicwall SonicOS

INFORMACIÓN IMPORTANTE

Palo Alto NGFW (PA-220, PA-220R, PA-820, PA-850, PA-3220, PA-3250, PA-3260, PA-5220, PA-5250, PA-5260, PA-5280, PA-7050, PA-7080, VM-50, VM-100, VM-200, VM-300, VM-500, VM-700 y VM-1000-HV)	
Versión	PAN-OS 10.0.5
Fabricante	Palo Alto
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2021
Revisión de Validez	31/05/2024

Descripción

Firewalls de Nueva Generación orientado a grandes empresas y datacenters, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP. Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido. Soportan hipervisores: vmware ESXi, Citrix SDX, Microsoft Hyper-V, KVM, vmware vCloud Air, Microsoft Azure y Amazon AWS.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

Palo Alto NGFW (VM-50, VM-100, VM-200, VM-300, VM-500, VM-700 y VM-1000-HV)	
Versión	PAN-OS 10.0.5
Fabricante	Palo Alto
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2021
Revisión de Validez	31/05/2024

Descripción

Firewalls de Nueva Generación orientado a grandes empresas y datacenters, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP. Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido. Soportan hipervisores: vmware ESXi, Citrix SDX, Microsoft Hyper-V, KVM, vmware vCloud Air, Microsoft Azure y Amazon AWS.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

INFORMACIÓN IMPORTANTE

Eudemon1000EN USG6510E, USG6530E, USG6525E, USG555E, USG6565E, USG6575E-B, USG6610E, USG6620E, USG6650E, USG6605E-B, USG6712E y USG6716E.	
Versión	V600R007C20SPC300 + V600R007C20SPH315T
Fabricante	Huawei Technologies España
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2021
Revisión de Validez	31/05/2024

Descripción

Los firewalls de nueva generación de la serie Huawei HiSecEngine están diseñados para todo tipo de empresas, instituciones y centros de datos de próxima generación. Los firewalls disponen de capacidades NGFW y se integran con otros dispositivos de seguridad para defenderse de manera proactiva contra amenazas de red, mejorar las capacidades de detección y resolver problemas de deterioro del rendimiento. Proporcionan capacidades de aceleración de procesamiento de servicios de cifrado/descifrado mejorando el rendimiento de los firewalls, la detección de seguridad y los servicios IPSec.

Observaciones

CCN-STIC-1433 PES Huawei USG 6000E Series Firewall

OPNSense	
Versión	21.7
Fabricante	Deciso B.V
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/03/2022
Revisión de Validez	31/08/2022

Descripción

OPNsense es una plataforma de enrutamiento y cortafuegos basada en un sistema operativo BSD de código abierto fortificado, fácil de usar e implantar.
Se trata de un cortafuegos con estado, es decir, un cortafuegos que hace un seguimiento del estado de las conexiones de red (como flujos TCP, comunicación UDP) que viajan a través de él. El producto ofrece una agrupación de reglas de cortafuegos por categoría, una característica excelente para las configuraciones de red más exigentes.
OPNsense incluye la mayoría de las funciones disponibles en los cortafuegos comerciales y más en muchos casos con los beneficios del software de código abierto y verificable.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Forcepoint NGFW 2200 series (N2201, N2205, N2210)	
Versión	6.10
Fabricante	Forcepoint
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2022
Revisión de Validez	30/09/2022

Descripción

Firewalls de Nueva Generación orientados a compañías u organismos de tamaño medio, de tipo appliance físico de 1RU, con capacidades IPS, SD-WAN, URL Filtering y Detección Avanzada de Malware. Dependiendo del modelo concreto de dispositivo se puede disponer de un rendimiento de 13,5 Gbps de Throughput NGFW/NGIPS, 35 millones de conexiones concurrentes y 100 contextos virtuales. Más información en: https://www.forcepoint.com/environments/forcepoint-ngfw-appliances

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Forcepoint NGFW 3400 series (N3401, N3405, N3410)	
Versión	6.10
Fabricante	Forcepoint
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2022
Revisión de Validez	30/09/2022

Descripción

Firewalls de Nueva Generación orientados a grandes redes Campus y Datacenters, de tipo appliance físico de 2RU, IPS, SD-WAN, URL Filtering y Detección Avanzada de Malware. Dependiendo del modelo concreto de dispositivo se puede disponer de hasta un rendimiento de 35 Gbps de Throughput NGFW/NGIPS, 200 millones de conexiones concurrentes y 250 contextos virtuales. Más información en: https://www.forcepoint.com/environments/forcepoint-ngfw-appliances

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Forcepoint NGFW N120 series (N120, N120W, N120WL) y N60	
Versión	6.10
Fabricante	Forcepoint
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2022
Revisión de Validez	30/09/2022

Descripción

Firewalls de Nueva Generación orientados a proteger oficinas remotas o entornos SD-WAN de tipo appliance físico con formato sobremesa, con capacidades IPS, SD-WAN, URL Filtering y Detección Avanzada de Malware. Dependiendo del modelo concreto de dispositivo se puede disponer un rendimiento de hasta 450mbps de Throughput NGFW/NGIPS y 3,2 millones de conexiones concurrentes. Más información en: https://www.forcepoint.com/environments/forcepoint-ngfw-appliances

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Forcepoint Virtual Appliance (ESXi)	
Versión	6.10
Fabricante	Forcepoint
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2022
Revisión de Validez	30/09/2022

Descripción

Firewalls de Nueva Generación orientados a dar servicios de protección perimetral en entornos virtuales, IPS, SD-WAN, URL Filtering y Detección Avanzada de Malware. Dependiendo del número de vCPU asignados se puede disponer de un rendimiento de más de 10GB Gbps de Throughput NGFW/NGIPS. Más información en: https://www.forcepoint.com/environments/forcepoint-ngfw-appliances

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

7.4.4 FAMILIA: PROXIES

Fortinet FortiProxy	
Versión	1.0
Fabricante	Fortinet
Familia	Proxies
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2020
Revisión de Validez	30/04/2022

Descripción

A medida que las ciberamenazas se van haciendo más sofisticadas, las compañías necesitan cada vez más una aproximación integral para proteger a los usuarios del tráfico web malicioso, los websites peligrosos y aquel contenido que pueda suponer una amenazapara ellos. El Secure Web Gateway (SWG) de Fortinet, FortiProxy, aborda esta situación con un único producto que incluye URL filtering, protección contra amenazas avanzadas y malware, filtrado DNS, DLP, IPS… La protección de los usuarios contra amenazasprocedentes de internet facilita el cumplimiento de las políticas corporativas.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Forcepoint On-Premise Security	
Versión	8.5
Fabricante	Forcepoint
Familia	Proxies
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2021
Revisión de Validez	31/10/2023

Descripción

Los dispositivos Forcepoint Web Security realizan la función de proxy de navegación segura integrando múltiples motores de clasificación de contenidos y análisis de seguridad en tiempo real con capacidad de inspección de tráfico seguro y también análisis de datos salientes con capacidad para aplicar políticas frente a fugas de información. Las plataformas funcionan como proxies directos http, https, ftp y SOCKS para la protección y control de usuarios y puestos de conexión. El propósito de estos dispositivos es proporcionar una capa de seguridad entre la red Interna y una o más redes externas (típicamente una red corporativa e Internet), aislando el tráfico de los usuarios a nivel de aplicación y proporcionando además diferentes mecanismos de optimización WAN para el tráfico que procesan.

Observaciones

CCN-STIC-1507 Procedimiento de Empleo Seguro Forcepoint On-premise Security 8.5

INFORMACIÓN IMPORTANTE

McAfee Web Gateway	
Versión	10.0.4-35792
Fabricante	McAfee
Familia	Proxies
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/07/2021
Revisión de Validez	30/04/2022

Descripción

Mcafee Web Gateway proporciona una seguridad web de alto rendimiento a través de un appliance local que puede desplegarse como hardware dedicado o máquina virtual. Implementa directivas de uso de internet, analiza la naturaleza y la intención del contenido y el código activo que entra en las redes. Detecta de forma proactiva el malware zero-day gracias a la cobertura completa del tráfico web, incluido el SSL.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

7.4.5 FAMILIA: DISPOSITIVOS DE RED INALÁMBRICOS

Cisco 5520 Wireless Controller con Cisco Aironet 1560, 2800, 3800 Series Access Points

Versión	8.5
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2020
Revisión de Validez	31/07/2022

Descripción

Los dispositivos Cisco Wireless LAN combinan plataformas específicas de Controlador y Punto de Acceso para crear un Sistema de Acceso WLAN. Estos dispositivos proporcionan a los usuarios inalámbricos acceso seguro a la red de la organización.
Puntos de acceso cualificados:

- Cisco Aironet 1560 Series Access Points: Cisco Aironet 1562i, Cisco Aironet 1562e, Cisco Aironet 1562d,
- Cisco Aironet 2800 Series Access Points: Cisco Aironet 2802i, Cisco Aironet 2802e,
- Cisco Aironet 3800 Series Access Points: Cisco Aironet 3802i, Cisco Aironet 3802e, Cisco Aironet 3802p.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Cisco 8540 Wireless Controller con Cisco Aironet 1560, 2800, 3800 Series Access Points

Versión	8.5
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2020
Revisión de Validez	31/07/2022

Descripción

Los dispositivos Cisco Wireless LAN combinan plataformas específicas de Controlador y Punto de Acceso para crear un Sistema de Acceso WLAN. Estos dispositivos proporcionan a los usuarios inalámbricos acceso seguro a la red de la organización.
Puntos de acceso cualificados:

- Cisco Aironet 1560 Series Access Points: Cisco Aironet 1562i, Cisco Aironet 1562e, Cisco Aironet 1562d,
- Cisco Aironet 2800 Series Access Points: Cisco Aironet 2802i, Cisco Aironet 2802e,
- Cisco Aironet 3800 Series Access Points: Cisco Aironet 3802i, Cisco Aironet 3802e, Cisco Aironet 3802p.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Cisco 9800-80, 9800-40, 9800-L Wireless Controller con Cisco Aironet 1560, 2800, 4800, 3800 Series Access Points	
Versión	IOS-XE 16.12
Fabricante	Cisco Systems
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2022

Descripción

Los dispositivos Cisco Wireless LAN combinan plataformas específicas de Controlador y Punto de Acceso para crear un Sistema de Acceso WLAN. Estos dispositivos proporcionan a los usuarios inalámbricos acceso seguro a la red de la organización.
Puntos de acceso cualificados:

- Cisco Aironet 1560 Series Access Points: Cisco Aironet 1562i, Cisco Aironet 1562e, Cisco Aironet 1562d,
- Cisco Aironet 2800 Series Access Points: Cisco Aironet 2802i, Cisco Aironet 2802e,
- Cisco Aironet 3800 Series Access Points: Cisco Aironet 3802i, Cisco Aironet 3802e, Cisco Aironet 3802p,
- Cisco Aironet 4800 Access Point

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Aruba Mobility Controller Series (7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM y 7280) y Puntos de Acceso	
Versión	ArubaOS 8.5
Fabricante	Aruba
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2020
Revisión de Validez	28/02/2022

Descripción

Aruba Mobility Controller Series funcionan como gateway entre redes cableadas e inalámbricas y proveen funciones de comando y control sobre los puntos de acceso de Aruba (APs) dentro de una red inalámbrica Aruba. Los Mobility Controllers (MC) y Virtual Mobility Controllers (VMC) de Aruba, son switches inalámbricos (Appliance físicos) que proporcionan una amplia gama de servicios y características de seguridad que incluyen la movilidad de red inalámbrica y cableada, seguridad, administración centralizada,auditoría, autenticación, acceso remoto seguro, auto-chequeos de integridad y operación, filtrado de tráfico y funcionalidad de Gateway VPN.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Aruba Mobility Controller (9004, 7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM, 7280) y Puntos de acceso.	
Versión	ArubaOS 8.6
Fabricante	Aruba
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2021
Revisión de Validez	30/04/2022

Descripción

Las familias Aruba Mobility Controllers 7000´s, 7200´s, 9000s y las Virtual Mobility Controller (appliance virtual) junto con los puntos de acceso de las familias 500s, 300s y 200s permiten desplegar redes inalámbricas de máxima seguridad y rendimiento.
Con esta versión se soporta también WPA3 y Wifi-6/802.11ax (con las familias 500s) así como WiFi-5/802.1ac y Wifi-4/802.11n.
Se implementan avanzadas características de seguridad, en el control de acceso a la red así como en la asignación de políticas de seguridad. También se soportan mecanismos de monitorización de espectro. Los Puntos de Acceso en modo pueden trabajar en modo Campus (CAP) y modo Remoto (RAP,lo que permite conectar de forma segura puntos de acceso que cruzan redes ajenas como internet).
Se implementan mejoras en actualizaciones de software sin perdida de servicio. Aruba Multizona permite a un Punto de Acceso dar servicio a varias Mobility Controllers de diferentes dominios o entornos de seguridad. Los Mobility Controllers puede actuar como servidores de túneles IPSEC/SSL para el cliente Aruba VIA.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Ruckus SmartZone WLAN Controllers (SZ-104, SZ-124, SZ 300, vSZ-E , vSZ-H y vSZ-D) & Access Points (R610, R710, R720, T610 y T710	
Versión	v5.1.1.3
Fabricante	Ruckus Wireless
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2021
Revisión de Validez	30/01/2022

Descripción

Ruckus SmartZone controllers and Access points es un sistema de acceso WLAN compuesto por múltiples productos operando en conjunto para proporcionar acceso remoto seguro a redes remotas y cableadas.
El producto proporciona cifrado punto a punto remoto, gestión centralizada y cumplimiento de políticas AAA (autorización, autenticación y accounting).

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Access Controllers (AC6508, AC6605, AC6805, ACU2, AC6800V, AC6507S, AirEngine 9700-M, AirEngine 9700-M1 y AirEngine 9700S-S) con Access Points (AP6050DN, AP6150DN, AP4050DE-M, AP7060DN y AirEngine 5760, 5761, 6760, 6761, 6761 Series)

Versión	AC V200R021C00SPC100 + V200R021C00SPH301
Fabricante	Huawei Technologies España
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2022
Revisión de Validez	30/06/2022

Descripción

Los equipos Huawei Wireless Lan combinan plataformas específicas de Controlador (Access Controller) y Punto de Acceso (Access Points) para crear un sistema de acceso inalámbrico que se adapta a redes de campus, redes de oficinas y redes de área metropolitana (MAN) de cualquier tamaño, y a la cobertura de zonas Wi-Fi, proporcionando acceso seguro a la red a los usuarios inalámbricos.

Puntos de accesos V200R021C00SPC200 + V200R021C00SPH301T cualificados:
• AP6050DN, AP6150DN, AP4050DE-M, AP7060DN
• AirEngine 5760-51, AirEngine 5760-22W, AirEngine 5760-22WD,
• AirEngine5761-11, AirEngine5761S-11, AirEngine5761-11W, AirEngine5761S-11W, AirEngine5761-11WD, AirEngine5761S-21, AirEngine5761-21, AirEngine5761-12W, AirEngine 5761R-11, AirEngine 5761R-11E, AirEngine 5761R-11, AirEngine 5761R-11E, AirEngine 5761S-13, AirEngine 5761S-12, AirEngine 5761-10W, AirEngine 5761S-10W
• AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 6760R-51, AirEngine 6760-X1E, AirEngine 6760R-X1, AirEngine 6760-51EI
• AirEngine6761-21, AirEngine6761-21E, AirEngine 6761-21E, AirEngine 6761S-21
• AirEngine 8760R-X1, AirEngine 8760-X1-PRO y AirEngine 8760R-X1

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Access Controllers (AC6508, AC6605, AC6805, ACU2, AC6800V, AC6507S, AirEngine 9700-M, AirEngine 9700-M1 y AirEngine 9700S-S) con Access Points (AP6050DN, AP6150DN, AP4050DE-M, AP7060DN y AirEngine 5760, 5761, 6760, 6761, 6761 Series)	
Versión	V200R020C00SPC300 + V200R020C00SPH301T
Fabricante	Huawei Technologies España
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2021
Revisión de Validez	30/06/2022

Descripción

Los equipos Huawei Wireless Lan combinan plataformas específicas de Controlador (Access Controller) y Punto de Acceso (Access Points) para crear un sistema de acceso inalámbrico que se adapta a redes de campus, redes de oficinas y redes de área metropolitana (MAN) de cualquier tamaño, y a la cobertura de zonas Wi-Fi, proporcionando acceso seguro a la red a los usuarios inalámbricos.

Puntos de accesos cualificados:
• AP6050DN, AP6150DN, AP4050DE-M, AP7060DN
• AirEngine 5760-51, AirEngine 5760-22W, AirEngine 5760-22WD,
• AirEngine5761-11, AirEngine5761S-11, AirEngine5761-11W, AirEngine5761S-11W, AirEngine5761-11WD, AirEngine5761S-21, AirEngine5761-21, AirEngine5761-12W, AirEngine 5761R-11, AirEngine 5761R-11E, AirEngine 5761R-11, AirEngine 5761R-11E, AirEngine 5761S-13, AirEngine 5761S-12, AirEngine 5761-10W, AirEngine 5761S-10W
• AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 6760R-51, AirEngine 6760-X1E, AirEngine 6760R-X1, AirEngine 6760-51EI
• AirEngine6761-21, AirEngine6761-21E, AirEngine 6761-21E, AirEngine 6761S-21
• AirEngine 8760R-X1, AirEngine 8760-X1-PRO y AirEngine 8760R-X1

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

7.4.6 PASARELAS SEGURAS DE INTERCAMBIO DE DATOS

PSTfile	
Versión	v4.4.2
Fabricante	Autek Ingeniería
Familia	Pasarelas seguras de intercambio de datos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2022





Descripción

PSTfile es un dispositivo de protección de perímetro de la familia PSTgateways. Permite el intercambio controlado de ficheros entre dominios de seguridad. Se establece una correspondencia entre carpetas, en servidores de ficheros de ambas redes y PSTfile,automáticamente, mueve o copia los ficheros del origen al destino. Soporta los protocolos FTP, FTPS, SFTP y SMB. La transferencia de ficheros desde el dominio de alta seguridad al de baja requiere autorización mediante firma digital.

Observaciones

Procedimiento de empleo seguro: CCN-STIC-1401 Configuración segura de pasarelas de AUTEK

PSTmail	
Versión	v3.0.5
Fabricante	Autek Ingeniería
Familia	Pasarelas seguras de intercambio de datos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2022





Descripción

PSTmail es un dispositivo de protección de perímetro de la familia PSTgateways. Permite el intercambio controlado de correo electrónico entre dominios de seguridad. Posibilita el empleo de direcciones de correo de redes externas, desde una red interna, más segura. Soporta las versiones seguras de los protocolos de correo. Los mensajes de salida requieren autorización mediante firma digital (S/MIME).

Observaciones

Procedimiento de empleo seguro: CCN-STIC-1401 Configuración segura de pasarelas de AUTEK

INFORMACIÓN IMPORTANTE

7.4.7 FAMILIA: DIODOS DE DATOS

PSTdiode	
Versión	v1.3.1-A
Fabricante	Autek Ingeniería
Familia	Diodos de datos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2019
Revisión de Validez	31/08/2024



ens Esquema Nacional de Seguridad — ALTA MEDIA BÁSICA — ALTA

Descripción

El diodo de datos hardware PSTdiode es un dispositivo de protección de perímetro que permite la transferencia de información en un único sentido entre dos dominios de seguridad con garantía física de transmisión unidireccional. Su aplicación principal esla introducción de información en una red aislada en entornos clasificados. También se puede aplicar para extraer información de una red de control industrial en entornos de infraestructuras críticas.
En ambos casos se garantiza que no existe tráfico en el sentido inverso.
Existen modelos de transferencia de ficheros y tráfico UDP.

Observaciones

Procedimiento de empleo seguro: CCN-STIC 1408 Procedimiento de empleo seguro Diodo Autek Ingeniería

7.4.8 FAMILIA: REDES PRIVADAS VIRTUALES: IPSEC

Cisco Firepower Threat Defense (FTD) en Firepower 1000 Series (FP1010, FP1120 y FP1140) con FMC y FMCv	
Versión	FTD 6.4 y FMC/FCMv 6.4
Fabricante	Cisco Systems
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2022

CISCO

ens Esquema Nacional de Seguridad — ALTA MEDIA BÁSICA — ALTA

Descripción

Cisco Firepower Threat Defense (FTD) tiene capacidades de firewall, VPN e IPS. Esta plataforma ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).
Compatible con:
-Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)
-FMCv running on ESXi 6.0 or 6.5 on the Unified Computing System (UCS) UCSB-B200-M4, UCSC-C220-M4S, UCSC-C240-M4SX, UCSC-C240-M4L, UCSB-B200-M5, UCSC-C220-M5, UCSC-C240-M5, UCS-E160S-M3 and UCS-E180D-M3

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Cisco Firepower Threat Defense (FTD) en Firepower 2000 Series FP2110, FP2120, FP2130 y FP2140) con FMC y FMCv	
Versión	FTD 6.4 y FMC/FCMv 6.4
Fabricante	Cisco Systems
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2022

Descripción

Cisco Firepower Threat Defense (FTD) tiene capacidades de firewall, VPN e IPS. Esta plataforma ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).
Compatible con:
-Cisco Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9 and FMC4600-K9)
-FMCv running on ESXi 6.0 or 6.5 on the Unified Computing System (UCS) UCSB-B200-M4, UCSC-C220-M4S, UCSC-C240-M4SX, UCSC-C240-M4L, UCSB-B200-M5, UCSC-C220-M5, UCSC-C240-M5, UCS-E160S-M3 and UCS-E180D-M3

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Fortigate FG-30E, FWF-30E, FG-40F, FG-40F-3G4G, FG-50E, FWF-50E, FG-51E, FWF-51E, FG-52E, FG-60E, FG-60E-DSL, FG-60E-PoE, FWF-60E, FWF-60E-DSL, FG-60F, FG-60F-3G4G, FWF-60F, FG-61E, FG-61F, FWF-61E, FWF-61F, FG-80E, FG-80E-PoE, FG-81E y FG-81E-PoE	
Versión	FortiOS 6.2.7
Fabricante	Fortinet
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2022

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos para entornos pequeños y sedes remotas de pocos usuarios. Las funcionalidades de seguridad son similares a las del resto de modelos más grandes (reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf).

Observaciones

CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.

INFORMACIÓN IMPORTANTE

Fortigate FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140E, FG-140E-PoE, FG-200E, FG-201E, FG-300D, FG-300E, FG-301E, FG-400D, FG-400E, FG-401E, FG-500D, FG-500E, FG-501E, FG-600D, FG-601E y FG-900D.	
Versión	FortiOS 6.2.7
Fabricante	Fortinet
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2022

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos para entornos pequeños y sedes remotas de pocos usuarios. Las funcionalidades de seguridad son similares a las del resto de modelos más grandes (reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf).

Observaciones

CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.

Fortigate FG-1000D, FG-1100E, FG-1100E-DC, FG-1101E, FG-1200D, FG-1500D, FG-1500DT, FG-1500D-DC, FG-2000E, FG-2201E y FG-2500E	
Versión	FortiOS 6.2.7
Fabricante	Fortinet
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2022

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos para entornos pequeños y sedes remotas de pocos usuarios. Las funcionalidades de seguridad son similares a las del resto de modelos más grandes (reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf).

Observaciones

CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.

INFORMACIÓN IMPORTANTE

Fortigate FG-3000D, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3600E, FG-3601E, FG-3700D, FG-3800D, FG-3801D, FG-3815D, FG-3960E, FG-3980E, FG-5001E, FG-5001E1, FG-6301F, FG-6501F, FGR-30D, FGR-60F y FGR-60F-3G4G	
Versión	FortiOS 6.2.7
Fabricante	Fortinet
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2022
Descripción	
Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos para entornos pequeños y sedes remotas de pocos usuarios. Las funcionalidades de seguridad son similares a las del resto de modelos más grandes (reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf).	
Observaciones	
CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.	

Fortigate-VM00, Fortigate-VM01, Fortigate-VM02, Fortigate-VM04, Fortigate-VM08, Fortigate-VM16, Fortigate-VM32 y Fortigate-VMUL	
Versión	FortiOS 6.2.7
Fabricante	Fortinet
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2022
Revisión de Validez	31/07/2022
Descripción	
Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos para entornos pequeños y sedes remotas de pocos usuarios. Las funcionalidades de seguridad son similares a las del resto de modelos más grandes (reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf).	
Observaciones	
CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.	

INFORMACIÓN IMPORTANTE

Junos 15.1X49-D60 for SRX platforms SRX300, SRX320, SRX340, SRX345, SRX550M, SRX5400E, SRX5400X, SRX5600E, SRX5600X, SRX5800E and SRX 5800X	
Versión	SW: Junos 15.1X49-D60
Fabricante	Juniper Networks
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2021
Revisión de Validez	31/10/2023

Descripción

La gama de productos SRX de Juniper Networks ofrece, en un solo dispositivo, capacidades de conectividad, conmutación y seguridad que le permiten dar funciones simultaneas de enrutador, switch y cortafuegos de nivel 7, así como dispositivo de detección yprevención de intrusiones. Su sistema operativo Junos, provee de un lenguaje universal con el resto de soluciones de Juniper que facilitan la operación y las tareas de automatización e integración con otras soluciones.

Observaciones

CCN-STIC-1404 “Procedimiento de Empleo Seguro Plataformas SRX Juniper”

Serie SOHO (SOHOW)	
Versión	SonicOS 6.5.2
Fabricante	SonicWall
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2019
Revisión de Validez	30/04/2022

Descripción

Los cortafuegos de la serie TZ SOHO de Sonicwall son una solución adecuada para oficinas pequeñas y domésticas, así como para entornos distribuidos en ubicaciones remotas. Despliegan funcionalidades para construir Secure SD-WAN y conectividad WIFI (opcional). El SOHO 250 proporciona un 50% más de rendimiento sobre su antecesor SOHO, así como acceso a los sandboxes avanzados Capture ATP, con lo que se mejora la seguridad en prevención y detección de malware desconocido en un entorno remoto.

Observaciones

CCN-STIC-1420 Procedimiento de Empleo Seguro Sonicwall SonicOS

INFORMACIÓN IMPORTANTE

SonicWall NSA Serie (2650, 3600, 3650, 4600, 4650, 5600, 5650, 6600, 6650, 9250, 9450, 9650)	
Versión	SonicOS 6.5.2
Fabricante	SonicWall
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2019
Revisión de Validez	30/04/2022

Descripción

Los firewall de la serie NSa de SonicWall están indicados para compañías medianas / grandes (de entre 50 y 3000 usuarios aprox), empresas deslocalizadas geográficamente y datacenters, consolidando tecnologías automatizadas de prevención y detección de amenazas como la inspección de memoria profunda en tiempo real (RTDMI). Desarrollados sobre una arquitectura de hardware de múltiples núcleos con interfaces 10-GbE y 2.5-GbE, la serie NSa cuenta con capacidades basadas en la nube y en el equipo, como descifrado e inspección TLS/SSL, application intelligence y control, SD-WAN segura, visualización en tiempo real y administración de WLAN. Más info en: https://www.sonicwall.com/es-mx/products/firewalls/mid-range

Observaciones

CCN-STIC-1420 Procedimiento de Empleo Seguro Sonicwall SonicOS

SonicWall SM Serie (9200, 9400, 9600, 9800)	
Versión	SonicOS 6.5.2
Fabricante	SonicWall
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2019
Revisión de Validez	30/04/2022

Descripción

Diseñado para grandes empresas, centros de datos, carriers y proveedores de servicios con necesidades multi-gigabit. Dirigido a compañías de entre 1000 y más de 50.000 usuarios (aprox.), realiza detección y prevención de amenazas mediante la combinación de la protección basada en appliances con la inteligencia de la nube en una plataforma de alto desempeño y consolida tecnologías de seguridad que brindan protección contra amenazas a millones de conexiones sin ralentizar el desempeño. Más info en: https://www.sonicwall.com/es-mx/products/firewalls/high-end

Observaciones

CCN-STIC-1420 Procedimiento de Empleo Seguro Sonicwall SonicOS

INFORMACIÓN IMPORTANTE

SonicWall TZ Serie (300/W, 400/W, 500/W, 600)	
Versión	SonicOS 6.5.2
Fabricante	SonicWall
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2019
Revisión de Validez	30/04/2022

Descripción

La serie TZ de SonicWall ofrece seguridad y rendimiento de entorno Enterprise orientado a pequeñas compañías. Enfocado a entornos departamentales o PYMES de entre 5 y 100 usuarios (aprox), incorpora funciones de prevención de intrusiones, antimalware, filtrado de contenidos/URL y control de aplicaciones a través de redes y entornos inalámbricos. Proporciona inspección profunda de paquetes (DPI), SD-WAN y despliegue zero-touch. Opciones de puertos PoE y wifi 802.11ac. Más info en: https://www.sonicwall.com/es-mx/products/firewalls/entry-level

Observaciones

CCN-STIC-1420 Procedimiento de Empleo Seguro Sonicwall SonicOS

Aruba Mobility Controller (9004, 7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM, 7280) y Puntos de acceso.	
Versión	ArubaOS 8.6
Fabricante	Aruba
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2021
Revisión de Validez	30/04/2022

Descripción

Las familias Aruba Mobility Controllers 7000´s, 7200´s, 9000s y las Virtual Mobility Controller (appliance virtual) junto con los puntos de acceso de las familias 500s, 300s y 200s permiten desplegar redes inalámbricas de máxima seguridad y rendimiento.
Con esta versión se soporta también WPA3 y Wifi-6/802.11ax (con las familias 500s) así como WiFi-5/802.1ac y Wifi-4/802.11n.
Se implementan avanzadas características de seguridad, en el control de acceso a la red así como en la asignación de políticas de seguridad. También se soportan mecanismos de monitorización de espectro. Los Puntos de Acceso en modo pueden trabajar en modo Campus (CAP) y modo Remoto (RAP,lo que permite conectar de forma segura puntos de acceso que cruzan redes ajenas como internet).
Se implementan mejoras en actualizaciones de software sin perdida de servicio. Aruba Multizona permite a un Punto de Acceso dar servicio a varias Mobility Controllers de diferentes dominios o entornos de seguridad. Los Mobility Controllers puede actuar como servidores de túneles IPSEC/SSL para el cliente Aruba VIA.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

Aruba Mobility Controller Series (7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM y 7280) y Puntos de Acceso	
Versión	ArubaOS 8.5.
Fabricante	Aruba
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2020
Revisión de Validez	28/02/2022

Descripción

Aruba Mobility Controller Series funcionan como gateway entre redes cableadas e inalámbricas y proveen funciones de comando y control sobre los puntos de acceso de Aruba (APs) dentro de una red inalámbrica Aruba. Los Mobility Controllers (MC) y Virtual Mobility Controllers (VMC) de Aruba, son switches inalámbricos (Appliance físicos) que proporcionan una amplia gama de servicios y características de seguridad que incluyen la movilidad de red inalámbrica y cableada, seguridad, administración centralizada,auditoría, autenticación, acceso remoto seguro, auto-chequeos de integridad y operación, filtrado de tráfico y funcionalidad de Gateway VPN.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Aruba Virtual Intranet Access (VIA) Client	
Versión	3.0
Fabricante	Aruba
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2020
Revisión de Validez	31/05/2022

Descripción

Aruba Virtual Intranet Access (VIA) es un servicio VPN seguro para usuarios que necesitan conectividad corporativa remota desde el hogar, ubicaciones temporales o mientras están en movimiento. Se encuentra disponible como una descarga de software para Google Android, Apple iOS, MacOS, Linux y Windows.
La función cualificada del VIA es la de cliente VPN IPSEC que evalúa y selecciona automáticamente la mejor conexión segura para efectuar la conexión VPN con la organización. A diferencia de las VPN tradicionales que requieren hardware dedicado (terminadores de túneles), Aruba integra servicios VPN directamente en la infraestructura segura existente de Aruba (Mobility Controllers) para simplificar la arquitectura y la administración.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

IS101	
Versión	1.01
Fabricante	ISTRIA SOLUCIONES DE CRIPTOGRAFIA
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2018
Revisión de Validez	31/12/2025



Descripción

El equipo IS101 es un cifrador de altas prestaciones que, sobre una plataforma hardware segura con un FW/SW específico, implementa protocolo IPSec en modo túnel. (con encapsulado ESP y protocolo IKEv2), lo que permite establecer, de forma sencilla y eficiente, redes privadas virtuales (VPN) sobre una red IP no confiable (ya sea pública o privada). Diseñado para sistemas en entornos críticos que manejan información sensible.
Velocidad de transferencia de 2Gbps agregados.

Observaciones

CCN-STIC-1405 "Procedimiento de empleo seguro IS101"

Check Point Security Gateway Serie 15000 (CPAP-SG15400-NGTX, CPAP-SG15600-NGTX)	
Versión	R80.30
Fabricante	Check Point Software Technologies
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2020
Revisión de Validez	31/12/2022

Descripción

Son dispositivos dedicados y que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 76Gbps de inspección Firewall, 13,5Gbps de IPS y 10.1 Gbps para protección ante amenazas avanzadas. Un máximo de 25.6 millones de conexiones concurrentes y 300.000 nuevas por segundo.
https://www.checkpoint.com/downloads/products/15400-security-gateway-datasheet.pdf
https://www.checkpoint.com/downloads/products/15600-security-gateway-datasheet.pdf

Observaciones

CCN-STIC 653 Seguridad en Check Point

INFORMACIÓN IMPORTANTE

Check Point Security Gateway Serie 23000, 26000/26000T y 16000/16000T	
Versión	R80.30 GA 3.10 (take 300)
Fabricante	Check Point Software Technologies
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2020
Revisión de Validez	31/12/2022

Descripción

Son dispositivos dedicados y que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 128Gbps de inspección Firewall, 26Gbps de IPS y 20 Gbps para protección ante amenazas avanzadas. Un máximo de 51,2 millones de conexiones concurrentes y 400.000 nuevas por segundo.
https://www.checkpoint.com/downloads/products/23500-security-gateway-datasheet.pdf
https://www.checkpoint.com/downloads/products/23800-security-gateway-datasheet.pdf
https://www.checkpoint.com/downloads/product-related/datasheets/ds-23900-appliance.pdf

Observaciones

CCN-STIC 653 Seguridad en Check Point

Check Point Security Gateway Serie 3000 (CPAP-SG3100-NGTX, CPAP-SG3200-NGTX)	
Versión	R80.30
Fabricante	Check Point Software Technologies
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2020
Revisión de Validez	31/12/2022

Descripción

Son dispositivos dedicados y que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 4 Gbps de inspección Firewall, 1.1 Gbps de IPS y 510 Mbps para protección ante amenazas avanzadas. Un máximo de 3.2 millones de conexiones concurrentes y 40.000 nuevas por segundo.
https://www.checkpoint.com/downloads/products/3100-security-gateway-datasheet.pdf
https://www.checkpoint.com/downloads/products/3200-security-gateway-datasheet.pdf

Observaciones

CCN-STIC 653 Seguridad en Check Point

INFORMACIÓN IMPORTANTE

Check Point Security Gateway Serie 5000 (CPAP-SG5100-NGTX, CPAP-SG5200-NGTX, CPAP-SG5400-NGTX, CPAP-SG5600-NGTX, CPAP-SG5800-NGTX, CPAP-SG5900-NGTX)

Versión	R80.30
Fabricante	Check Point Software Technologies
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2020
Revisión de Validez	31/12/2022

Descripción

Son dispositivos dedicados y que pueden realizar inspección a nivel de red, de aplicación y de amenaza avanzada, ya sea virus, botnet, ramsonware o zero-day. Ofrece hasta 52 Gbps de inspección Firewall, 7.6 Gbps de IPS y 6.1 Gbps para protección ante amenazas avanzadas. Un máximo de 12.8 millones de conexiones concurrentes y 210.000 nuevas por segundo.
https://www.checkpoint.com/downloads/products/5100-security-gateway-datasheet.pdf
https://www.checkpoint.com/downloads/products/5200-security-gateway-datasheet.pdf
https://www.checkpoint.com/downloads/products/5400-security-gateway-datasheet.pdf
https://www.checkpoint.com/downloads/products/5600-security-gateway-datasheet.pdf
https://www.checkpoint.com/downloads/products/5800-security-gateway-datasheet.pdf
https://www.checkpoint.com/downloads/products/5900-security-gateway-datasheet.pdf

Observaciones

CCN-STIC 653 Seguridad en Check Point

Check Point Security Threat Emulation/Extraction (CPAP-SBTE100X-4VM, CPAP-SBTE250X-8VM, CPAP-SBTE1000X-A-28VM, CPAP-SBTE2000X-40VM , CPAP-SBTE2000X-56VM-HPP)

Versión	R80.30
Fabricante	Check Point Software Technologies
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2020
Revisión de Validez	31/12/2022

Descripción

Equipos dedicados a emulación de ficheros para la detección y prevención de Malware de día Zero, tanto en Navegación (HTTP), como en Correo (SMTP). Permiten la integración con terceros tanto vía API como por protocolo ICAP. Estos equipos según el modelo,son capaces de analizar entre 450 ficheros y 5000 ficheros únicos la hora, soportando desde 450Mbps a más de 4Gbps, permitiendo ampliación hasta 14 puertos 1GbE RJ45, 8 puertos 10GbE de Fibra SFP+. Todos los modelos se pueden configurar con tarjetas de Bypass de 4 puertos 1GbE RJ45 o 2 puertos 10GbE de fibra.

Observaciones

CCN-STIC 653 Seguridad en Check Point

INFORMACIÓN IMPORTANTE

Fortigate FG-30E, FG-50E, FG-51E, FG-52E, FG-60E, FG-60E-DSL, FG-60E-PoE, FG-61E, FG-80E, FG-80E- PoE, FG-81E, FG-81E-PoE	
Versión	FortiOS 6.0
Fabricante	Fortinet
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2021
Revisión de Validez	29/09/2022

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos para entornos pequeños y sedes remotas de pocos usuarios. Las funcionalidades de seguridad son similares a las del resto de modelos más grandes (reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf).
AP Wifi integrado en el dispositivo, para proporcionar cobertura inalámbrica a las oficinas.
Más información en: https://www.fortinet.com/products/next-generation-firewall.htm

Observaciones

CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.

FortiWifi FWF-30E, FWF-50E,FWF-51E, FWF-60E, FWF-60EDSL, FWF-61E	
Versión	FortiOS 6.0
Fabricante	Fortinet
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2021
Revisión de Validez	29/09/2022

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos para entornos pequeños y sedes remotas de pocos usuarios. Las funcionalidades de seguridad son similares a las del resto de modelos más grandes (reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf).
AP Wifi integrado en el dispositivo, para proporcionar cobertura inalámbrica a las oficinas.
Más información en: https://www.fortinet.com/products/next-generation-firewall.htm

Observaciones

CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.

INFORMACIÓN IMPORTANTE

Fortigate FG-100E, FG-100EF, FG-101E, FG-140E, FG-140EPoE, FG-200E, FG-201E, FG-300D, FG-300E, FG-301E, FG-400D, FG-400E, FG-401E,FG-500D, FG-500E, FG- 501E, FG-600D, FG-600E, FG-601E,FG-900D	
Versión	FortiOS 6.0
Fabricante	Fortinet
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2021
Revisión de Validez	29/09/2022

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos para entornos pequeños y sedes remotas de pocos usuarios. Las funcionalidades de seguridad son similares a las del resto de modelos más grandes (reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf).
AP Wifi integrado en el dispositivo, para proporcionar cobertura inalámbrica a las oficinas.
Más información en: https://www.fortinet.com/products/next-generation-firewall.htm

Observaciones

CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.

Fortigate FG-1000D, FG-1100E, FG-1101E,FG-1200D, FG-1500D, FG-2000E, FG-2200E, FG-2201E, FG-2500E	
Versión	FortiOS 6.0
Fabricante	Fortinet
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2021
Revisión de Validez	29/09/2022

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos para entornos pequeños y sedes remotas de pocos usuarios. Las funcionalidades de seguridad son similares a las del resto de modelos más grandes (reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf).
AP Wifi integrado en el dispositivo, para proporcionar cobertura inalámbrica a las oficinas.
Más información en: https://www.fortinet.com/products/next-generation-firewall.htm

Observaciones

CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.

INFORMACIÓN IMPORTANTE

Fortigate FG-3000D, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3600E, FG-3601E,FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG- 3960E, FG-3980E	
Versión	FortiOS 6.0
Fabricante	Fortinet
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2021
Revisión de Validez	29/09/2022

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos para entornos pequeños y sedes remotas de pocos usuarios. Las funcionalidades de seguridad son similares a las del resto de modelos más grandes (reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf).
AP Wifi integrado en el dispositivo, para proporcionar cobertura inalámbrica a las oficinas.
Más información en: https://www.fortinet.com/products/next-generation-firewall.htm

Observaciones

CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.

Fortigate FG-5001D, FG-5001E,FG-5001E1	
Versión	FortiOS 6.0
Fabricante	Fortinet
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/02/2021
Revisión de Validez	29/09/2022

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos para entornos pequeños y sedes remotas de pocos usuarios. Las funcionalidades de seguridad son similares a las del resto de modelos más grandes (reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf).
AP Wifi integrado en el dispositivo, para proporcionar cobertura inalámbrica a las oficinas.
Más información en: https://www.fortinet.com/products/next-generation-firewall.htm

Observaciones

CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.

INFORMACIÓN IMPORTANTE

WatchGuard Fireware on Firebox NGFWs (T35, T40, T80, T55, M270, M370, M470, M570, M670, M4600 y M5600)	
Versión	FirewareOS 12.6.2 Linux Kernel 4.14.83.
Fabricante	WatchGuard Technologies
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2021
Revisión de Validez	30/09/2023

Descripción

Los equipos UTM de WatchGuard están enfocados en ofrecer la mejor seguridad para cualquier empresa y entorno corporativo distribuido. Nuestros dispositivos de seguridad de red están diseñados, desde el inicio, para enfocarse en facilitar el despliegue, el uso y la administración continua.

Proporcionan protección contra ataques de malware avanzado y phishing, así como las protecciones de seguridad tradicionales: prevención de intrusiones (IPS), filtrado de URL, control de aplicaciones, antispam y antivirus, … ofreciendo en todo momento visibilidad del entorno (productividad y seguridad)

Cuentan con capacidades SD-WAN, y VPN.

Están disponibles tanto en equipos físicos como virtuales.
https://www.watchguard.com/es/wgrd-products/network-security

Observaciones

CCN-STIC-1421 Procedimiento de empleo seguro WatchGuard Fireware OS v12.6.2

SonicWall TZ Serie (300P, 350, 350W, 600P)	
Versión	6.5.4.4-44n-federal-12n
Fabricante	SonicWall
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2021
Revisión de Validez	31/01/2024

Descripción

La serie TZ de SonicWall ofrece seguridad y rendimiento de entorno Enterprise orientado a pequeñas compañías. Enfocado a entornos departamentales o PYMES de entre 5 y 100 usuarios (aprox), incorpora funciones de prevención de intrusiones, antimalware, filtrado de contenidos/URL y control de aplicaciones a través de redes y entornos inalámbricos. Proporciona inspección profunda de paquetes (DPI), SD-WAN y despliegue zero-touch. Opciones de puertos PoE y wifi 802.11ac.
Más info en: https://www.sonicwall.com/es-mx/products/firewalls/entry-level.

Observaciones

CCN-STIC-1420 Procedimiento de Empleo Seguro Sonicwall SonicOS

INFORMACIÓN IMPORTANTE

SonicWall SOHO Serie (250, 250W)	
Versión	6.5.4.4-44n-federal-12n
Fabricante	SonicWall
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2021
Revisión de Validez	31/01/2024

Descripción

Los cortafuegos de la serie TZ SOHO de Sonicwall son una solución adecuada para oficinas pequeñas y domésticas, así como para entornos distribuidos en ubicaciones remotas. Despliegan funcionalidades para construir Secure SD-WAN y conectividad WIFI (opcional). El SOHO 250 proporciona un 50% más de rendimiento sobre su antecesor SOHO, así como acceso a los sandboxes avanzados Capture ATP, con lo que se mejora la seguridad en prevención y detección de malware desconocido en un entorno remoto.

Observaciones

CCN-STIC-1420 Procedimiento de Empleo Seguro Sonicwall SonicOS

EMMA VPN	
Versión	CMI/CMIX 1.6.0-23.7153 | Core 1.2.2-0.11643
Fabricante	OpenCloud Factory
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2021
Revisión de Validez	28/02/2024

Descripción

El módulo de concentración de VPNs de EMMA actúa como frontend para la finalización de túneles VPN, mediante un agente. EMMA realiza la autenticación, autorización y auditoría contra el gestor de identidades corporativas del Organismo y permite añadir un segundo factor de autenticación, para minimizar el riesgo de suplantación de identidad. Permite definir y aplicar políticas de acceso en función de una postura de seguridad basada en el nivel de bastionado deseado, además de otros factores, como el horario de la conexión, características del equipo, role de usuario, etc...

Observaciones

CCN-STIC-1105 Procedimiento de empleo seguro EMMA

INFORMACIÓN IMPORTANTE

Palo Alto NGFW (PA-220, PA-220R, PA-820, PA-850, PA-3220, PA-3250, PA-3260, PA-5220, PA-5250, PA-5260, PA-5280, PA-7050, PA-7080, VM-50, VM-100, VM-200, VM-300, VM-500, VM-700 y VM-1000-HV)	
Versión	PAN-OS 10.0.5
Fabricante	Palo Alto
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2021
Revisión de Validez	31/05/2024

Descripción

Firewalls de Nueva Generación orientado a grandes empresas y datacenters, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP. Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido. Soportan hipervisores: vmware ESXi, Citrix SDX, Microsoft Hyper-V, KVM, vmware vCloud Air, Microsoft Azure y Amazon AWS.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

Palo Alto NGFW (VM-50, VM-100, VM-200, VM-300, VM-500, VM-700 y VM-1000-HV)	
Versión	PAN-OS 10.0.5
Fabricante	Palo Alto
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2021
Revisión de Validez	31/05/2024

Descripción

Firewalls de Nueva Generación orientado a grandes empresas y datacenters, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado. Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP. Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido. Soportan hipervisores: vmware ESXi, Citrix SDX, Microsoft Hyper-V, KVM, vmware vCloud Air, Microsoft Azure y Amazon AWS.

Observaciones

CCN-STIC-1413 PES Cortafuegos NGFW Palo Alto Networks

INFORMACIÓN IMPORTANTE

7.4.9 FAMILIA: REDES PRIVADAS VIRTUALES: SSL

SonicWall Secure Mobile Access (SMA)	
Versión	V12.1
Fabricante	SonicWall
Familia	Redes privadas virtuales: SSL
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2021
Revisión de Validez	30/04/2022



Descripción

El SMA (appliances físicos SMA 6210, 7210 y virtual SMA 8200v sobre ESX/ESXI/Hyper-V) ofrece un acceso remoto seguro, completo e integral a los recursos corporativos alojados en centros de datos locales, en la nube e híbridos. Aplica controles de acceso basados en la identidad e impuestos por políticas, autenticación de dispositivos con sensibilidad contextual y VPN a nivel de aplicación para otorgar acceso a datos, recursos y aplicaciones después de establecer la identidad, la ubicación y la confianza del usuario y del dispositivo. Pueden implementarse de forma flexible como un appliance Linux reforzado o dispositivo virtual en nubes privadas en ESXi o Hyper-V, o en entornos de nube pública de AWS o Microsoft Azure, encaja a la perfección en cualquier infraestructura de TI existente, soportando miles de usuarios.

Observaciones

Procedimiento de empleo seguro pendiente de publicación

EMMA VPN	
Versión	CMI/CMIX 1.6.0-23.7153 | Core 1.2.2-0.11643
Fabricante	OpenCloud Factory
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2021
Revisión de Validez	28/02/2022

Descripción

El módulo de concentración de VPNs de EMMA actúa como frontend para la finalización de túneles VPN, mediante un agente. EMMA realiza la autenticación, autorización y auditoría contra el gestor de identidades corporativas del Organismo y permite añadir un segundo factor de autenticación, para minimizar el riesgo de suplantación de identidad. Permite definir y aplicar políticas de acceso en función de una postura de seguridad basada en el nivel de bastionado deseado, además de otros factores, como el horario de la conexión, características del equipo, role de usuario, etc...

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

7.4.10 FAMILIA: HERRAMIENTAS PARA COMUNICACIONES MÓVILES SEGURAS

COMSec	
Versión	V4.2
Fabricante	Indra
Familia	Herramientas para comunicaciones móviles seguras
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2018
Revisión de Validez	31/10/2023



Descripción

COMSec es una solución global de comunicaciones seguras que proporciona servicios cifrados de voz, mensajería instantánea y videoconferencia sobre teléfonos móviles empleando cualquier red celular, inalámbrica o satelital.
Con su alto nivel de seguridad, gran calidad de audio y facilidad de uso protege de forma eficaz cualquier información sensible de la organización. Las llamadas y los datos intercambiados por COMSec son seguros, independientemente del operador móvil utilizado y el país donde se encuentre.
Más información: comsec.indracompany.com

Observaciones

CCN-STIC-1407 Procedimiento de Empleo Seguro de COMSec

7.4.11 FAMILIA: CIFRADORES IP

EP430TX	
Versión	1.04
Fabricante	Epicom
Familia	Cifradores IP
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2022



Descripción

Cifrador de comunicaciones IP hasta 200 Mbps, interoperable con el resto de cifradores de la familia EP430.

Observaciones

Utilización según PE-2016-28 Procedimiento de empleo EP430TX.

INFORMACIÓN IMPORTANTE

EP960	
Versión	1.09.17
Fabricante	Epicom
Familia	Cifradores IP
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2020
Revisión de Validez	31/12/2025

Descripción

Cifrador personal de tamaño reducido (120x80x25mm) para la protección de las comunicaciones. Cuenta con varios interfaces negros (interfaces no seguros donde la información ya está cifrada) : Ethernet, WiFi y 3G/4G. Ofrece un nivel medio de seguridad y proporciona una solución de WiFi seguro.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

IS101	
Versión	1.01
Fabricante	ISTRIA SOLUCIONES DE CRIPTOGRAFIA
Familia	Cifradores IP
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2018
Revisión de Validez	31/12/2025



Descripción

El equipo IS101 es un cifrador de altas prestaciones que, sobre una plataforma hardware segura con un FW/SW específico, implementa protocolo IPSec en modo túnel. (con encapsulado ESP y protocolo IKEv2), lo que permite establecer, de forma sencilla y eficiente, redes privadas virtuales (VPN) sobre una red IP no confiable (ya sea pública o privada). Diseñado para sistemas en entornos críticos que manejan información sensible.
Velocidad de transferencia de 2Gbps agregados.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

EP430GX	
Versión	v.1.07
Fabricante	Epicom
Familia	Cifradores IP
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2022



Descripción

Cifrador de redes IP a 2 Gbps (agregados), interoperable con el resto de cifradores de la familia EP430.

Observaciones

Utilización según PE-2012-49 Procedimiento de Empleo EP430GX.

EP430GX	
Versión	v.1.08
Fabricante	Epicom
Familia	Cifradores IP
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	27/12/2021
Revisión de Validez	31/12/2022



Descripción

Cifrador de redes IP a 2 Gbps (agregados), interoperable con el resto de cifradores de la familia EP430.

Observaciones

Utilización según PE-2012-49 Procedimiento de Empleo EP430GX.

EP430GN	
Versión	1.08.29
Fabricante	Epicom
Familia	Cifradores IP
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2022



Descripción

Cifrador de redes IP a 2 Gbps (agregados).

Observaciones

Este modelo no es compatible con el resto de la familia de cifradores EP430 de EPICOM.
Utilización según P029-PE-2011-33 Operational doctrine EP430GN v2.

INFORMACIÓN IMPORTANTE

EP430TX	
Versión	1.04
Fabricante	Epicom
Familia	Cifradores IP
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2022



Descripción

Cifrador de comunicaciones IP hasta 200 Mbps, interoperable con el resto de cifradores de la familia EP430.

Observaciones

Utilización según PE-2016-28 Procedimiento de empleo EP430TX.

7.4.12 FAMILIA: WEB APPLICATION FIREWALL (WAF)

Pendiente de recepción de solicitudes de productos que cumplan con Requisitos Fundamentales de Seguridad (RFS) correspondientes a esta familia.

7.5 CATEGORÍA: PROTECCIÓN DE LA INFORMACIÓN Y SOPORTES DE INFORMACIÓN

7.5.1 FAMILIA: ALMACENAMIENTO CIFRADO DE DATOS

Cryhod junto con la Tarjeta Criptográfica de la FNMT	
Versión	Q.2020
Fabricante	PrimX/Epicom
Familia	Almacenamiento cifrado de datos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2020
Revisión de Validez	30/04/2023

Descripción

Cryhod es un programa de cifrado moderno que asegura el cifrado completo de los discos duros de las estaciones de trabajo portátiles de la organización. Cryhod implementa mecanismos de autenticación fuerte (doble factor) mediante la tarjeta SmartCard de la FNMT en el Pre-Boot del equipo lo que permite identificar unívocamente a los usuarios del sistema y protegerlo frente a ataques en caso de pérdida o robo.
Además, se está trabajando de la mano del CCN para desarrollar criptografía nacional propia utilizando tecnologías modernas como es XTS para las Administraciones del Estado y para Defensa.

Observaciones

CCN-STIC-1505 Procedimiento de Empleo Seguro CRYHOD de PRIMX

INFORMACIÓN IMPORTANTE

7.5.2 FAMILIA. CIFRADO OFFLINE

EP851	
Versión	2.02 y 2.03
Fabricante	Epicom
Familia	Cifrado offline
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2022





Descripción

Dispositivo portátil USB de cifrado "off-line":
• Compatible con Crypto Token USB de la empresa Datatech.
• Cifrado de ficheros para su posterior envío.
• Almacenamiento interno de la datos cifrados para su transporte.

Observaciones

Utilización según el PE-2008-01 Procedimiento de Empleo TOKEN USB.
Las redes que empleen estos dispositivos, deben sustituirlos por los EP852.

EP852	
Versión	3.04
Fabricante	Epicom
Familia	Cifrado offline
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2021
Revisión de Validez	31/12/2025





Descripción

El EP852 es un cifrador de ficheros fuera de línea que permite el cifrado y descifrado de ficheros y el transporte de información cifrada en el dispositivo. Mejora las prestaciones en cuanto a almacenamiento y velocidad de las versiones anteriores de losToken USB así como la puesta en marcha del dispositivo, carga y distribución de claves.

Observaciones

Utilización según el PE-2020-4 -Procedimiento de Empleo Seguro EP852 -(ESP)

INFORMACIÓN IMPORTANTE

EP852	
Versión	3.05
Fabricante	Epicom
Familia	Cifrado offline
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	27/12/2021
Revisión de Validez	31/12/2025



Descripción

El EP852 es un cifrador de ficheros fuera de línea que permite el cifrado y descifrado de ficheros y el transporte de información cifrada en el dispositivo. Mejora las prestaciones en cuanto a almacenamiento y velocidad de las versiones anteriores de losToken USB así como la puesta en marcha del dispositivo, carga y distribución de claves.

Observaciones

Utilización según el PE-2020-4 -Procedimiento de Empleo Seguro EP852 -(ESP)

EP880	
Versión	2.08.36 y 2.09.35
Fabricante	Epicom
Familia	Cifrado offline
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2021
Revisión de Validez	31/12/2026

Descripción

El EP880 es una aplicación software que se ejecuta sobre ordenador con sistema operativo Windows y que permite realizar, en origen, el cifrado y firma de ficheros de datos “off-line” almacenados en el disco duro del ordenador o dispositivos de almacenamiento externos conectados al ordenador, para su posterior almacenamiento y/o envío de forma segura desde el correo electrónico u otro medio y, en destino, el descifrado y verificación de la integridad de los datos.

Observaciones

Utilización según EP240E880ZZ05 Procedimiento de Empleo Seguro EP880

INFORMACIÓN IMPORTANTE

SMiD Cloud	
Versión	2.1
Fabricante	ENCIFRA
Familia	Cifrado offline
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/04/2022
Revisión de Validez	30/09/2022

Descripción

SMiD cloud es un dispositivo hardware Plu&Play que se integra en una red local SMB de Microsoft y que se encarga del almacenamiento cifrado de los ficheros que se almacenen en él. El uso de SMiD cloud NO requiere la instalación de ningún tipo de software o agente en los equipos que lo utilizan. Los ficheros cifrados pueden almacenarse en local y/o en uno o varios proveedores de almacenamiento en la nube.
Los dispositivos SMiD cloud sólo mantienen copias en claro de los ficheros que están siendo utilizados y retornan cualquier fichero a su estado cifrado cuando se dejan de utilizar.
El arranque de todo dispositivo SMiD cloud requiere la presencia en el arranque de una llave física USB de arranque sin la cual el dispositivo no arranca. Si se configura explícitamente para ello, los dispositivos SMiD cloud pueden ser clonados en el caso de que el original se deteriore, sea sustraído o destruido.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

7.5.3 FAMILIA: BORRADO SEGURO

Blancco Drive Eraser	
Versión	V6.9.1
Fabricante	Blancco
Familia	Herramientas de borrado seguro
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2020
Revisión de Validez	31/01/2023

Descripción

Software de borrado seguro de datos para discos duros HDD y estado sólido SSD en computadoras de escritorio, laptops y almacenamiento masivo con adaptadores IDE, SATA, SAS, SCSI, FIBRA CANAL FC, SSD y Emmc. Ofrece un borrado seguro del 100% del disco duroo por particiones físicas al realizar una sobre escritura en la totalidad de los sectores contenidos en el disco duro. Permite un borrado automatizado, monitorización de las actividades de borrado e informa de todas las actividades de borrado facilitandoel cumplimiento de las Políticas de Seguridad y Retención de Información. El borrado realizado es conforme a los criterios de los órganos normativos gracias a su reporte certificado de auditoría y en cumplimiento con RGPD. Dispone de una instalación flexible y sencilla.

Observaciones

CCN-STIC 1504 Procedimiento de empleo seguro de Blancco Drive Eraser 6.9

INFORMACIÓN IMPORTANTE

Blancco File Eraser	
Versión	v8.3
Fabricante	Blancco
Familia	Herramientas de borrado seguro
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2020
Revisión de Validez	31/08/2022

Descripción

La solución de borrado de archivos Blancco File Eraser permite administrar y automatizar rutinas de borrado de datos en ordenadores de sobremesa, portátiles y servidores.
BENEFICIOS PRINCIPALES
1. Borrado seguro de datos en ficheros.
2. Borrado automatizado.
3. Monitoriza e informa de todas las actividades de borrado.
4. Borrado conforme a los criterios de los órganos normativos gracias a su reporte certificado de auditoría y en cumplimiento con RGPD.
5. Sencilla instalación.
Más información: espana@deletetecnology.com - 91 761 23 70.

Observaciones

CCN-STIC 1502 Procedimiento de empleo seguro de Blancco File Eraser

INFORMACIÓN IMPORTANTE

7.5.4 FAMILIA: PREVENCIÓN DE FUGAS DE DATOS

McAfee Data Loss Prevention (DLP) Endpoint with ePolicy Orchestrator 5.10

Versión	11.1
Fabricante	McAfee
Familia	Sistemas para prevención de fugas de datos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2020
Revisión de Validez	28/09/2022

Descripción

McAfee DLP Endpoint proporciona protección integral para todos los posibles canales de fuga de datos, como dispositivos de almacenamiento extraíbles, la nube, correo electrónico, la mensajería instantánea, la Web, el material impreso, el portapapeles, capturas de pantalla, las aplicaciones para compartir archivos, etc.
Sus principales características son:
- Integración con análisis de comportamientos de usuarios (UEBA) de terceros.
- Clasificación manual.
- Análisis y reparaciones iniciados por el usuario.
- Clasificación flexible, que ofrece diccionarios, expresiones regulares y algoritmos de validación.
- Una exclusiva tecnología de etiquetado para identificar los documentos según su origen, que impide que la información confidencial de las aplicaciones web, las aplicaciones de red y los recursos compartidos de red se duplique, renombre o salga de las instalaciones de la empresa.
- Compatibilidad con virtualización para proteger equipos de sobremesa remotos y soluciones VDI.

Observaciones

CCN-STIC 1503 Procedimiento de Empleo Seguro McAfee Data Loss Prevention 11.1 con ePolicy Orchestrator 5.10

Forcepoint On-Premise Security

Versión	8.5
Fabricante	Forcepoint
Familia	Sistemas para prevención de fugas de datos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2019
Revisión de Validez	31/05/2022

Descripción

Forcepoint On-Premise Security 8.5 es una solución de prevención de fuga de datos en un organismo.Esta solución ofrece una alta escalabilidad de acuerdo con la estrategia del cliente para abordar el robo y la pérdida de datos.

Observaciones

CCN-STIC-1507 Procedimiento de Empleo Seguro Forcepoint On-premise Security 8.5

INFORMACIÓN IMPORTANTE

7.5.5 FAMILIA. HERRAMIENTAS PARA FIRMA ELECTRÓNICA

SIAVAL Safecert Server Signing Sistema	
Versión	v.2.4.02
Fabricante	Sistemas Informáticos Abiertos
Familia	Herramientas para firma electrónica
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2018
Revisión de Validez	23/04/2023

Descripción

Solución de firma centralizada de la familia SIAVAL orientada a facilitar la gestión y el uso de las claves privadas y públicas de los usuarios finales, también identificados como titulares o firmantes. Está diseñado para funcionar como un dispositivo remoto de creación de firma rQSCD, según los requisitos especificados en el Reglamento (UE) nº 910/2014 del Parlamento Europeo (eIDAS: Anexo II), haciendo posible la generación de firmas electrónicas avanzadas (AdES) y de firmas electrónicas cualificadas o reconocidas (QES) en un servidor remoto.

SIAVAL Safecert Server Signing Sistema	
Versión	v.3
Fabricante	Sistemas Informáticos Abiertos
Familia	Herramientas para firma electrónica
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2021
Revisión de Validez	28/02/2024

Descripción

Solución de firma centralizada de la familia SIAVAL orientada a facilitar la gestión y el uso de las claves privadas y públicas de los usuarios finales, también identificados como titulares o firmantes. Está diseñado para funcionar como un dispositivo remoto de creación de firma rQSCD, según los requisitos especificados en el Reglamento (UE) nº 910/2014 del Parlamento Europeo (eIDAS: Anexo II), haciendo posible la generación de firmas electrónicas avanzadas (AdES) y de firmas electrónicas cualificadas o reconocidas (QES) en un servidor remoto.

INFORMACIÓN IMPORTANTE

ADSS Server SAM Appliance	
Versión	6.0
Fabricante	ASCERTIA
Familia	Herramientas para firma electrónica
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2019
Revisión de Validez	30/04/2023

Descripción

El ADSS Server SAM 6.0 es un dispositivo de creación de Firma Remota (rQSCD) de la empresa Ascertia, que cuenta con un certificado Common Criteria EAL4+ que cumple con la regulación Protection Profile EN 419241-2 con Level 2 Sole Control y que, junto a laaplicación de móviles Go>Sign de Ascertia, proporciona a sus usuarios la firma Remota Avanzada y Cualificada.

Observaciones

Procedimiento de empleo pendiente de publicación.

7.5.6 FAMILIA. HARDWARE SECURITY MODULE (HSM)

Thales Luna K7 Cryptographic Module (808-000048-002, 808-000073-001, 808-000066-001, 808-000069-001 y 808-000070-001)	
Versión	7.7.0 (bootloader versions 1.1.1, 1.1.2 y 1.1.4)
Fabricante	Thales
Familia	Hardware Security Module (HSM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2021
Revisión de Validez	28/02/2024

Descripción

Los Módulos de Seguridad Hardware (HSM) de Thales, son criptoprocesadores dedicados que están diseñados específicamente para la protección del ciclo de vida de las claves criptográficas. La administración, el procesamiento y el almacenamiento de claves criptográficas se realiza dentro del dispositivo reforzado a prueba de manipulaciones, aumentando el rendimiento y manteniendo la seguridad.
Con los módulos de seguridad de hardware de Thales, puede:
- Abordar los requisitos de cumplimiento con soluciones para Blockchain, GDPR, IoT, iniciativas de papel a digital, PCI DSS, firmas digitales, eIDAS, DNSSEC, almacenamiento de claves en hardware, aceleración transaccional, firma de certificados, firma de código o documentos, generación de claves masivas, cifrado de datos y más.
- Las claves siempre se generan y almacenan en el dispositivo validado a prueba de intrusiones y manipulaciones, que proporciona los niveles más altos de control de acceso.
- Posibilidad de crear particiones lógicas en los HSM de red, con Oficiales de Seguridad dedicados por partición, y segmentando la gestión con una separación total de las claves.

Observaciones

Solicitar al fabricante la guía de configuración utilizada en la certificación Common Criteria. Configurar el producto para la utilización de funciones, algoritmos y protocolos aprobados por el Centro Criptológico Nacional, según la guía 'CCN-STIC-807 Criptología de empleo en el ENS'.

INFORMACIÓN IMPORTANTE

nShield Solo XC Hardware Security Module	
Versión	v12.60.15
Fabricante	Entrust Solutions
Familia	Hardware Security Module (HSM)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2021
Revisión de Validez	30/04/2024

Descripción

Los módulos de seguridad hardware (HSM) nShield XC son dispositivos físicos con certificación FIPS 140-2 nivel 3 y Common Criteria EAL4+ (EN 419 221-5) que permiten realizar operaciones criptográficas de forma segura.
A su vez, el diseño de estos equipos, ofrece una serie de funcionalidades que facilita la gestión de material criptográfico:
- Protección prácticamente ilimitada de claves privadas.
- Flexibilidad en la creación de copias de seguridad de las claves al no necesitar equipos adicionales ni acceso directo a los HSM.
- Capacidad de ejecutar código dentro del HSM mediante CodeSafe.

Desde un punto de vista funcional, los HSM nShield XC son plataformas resistentes a la manipulación (tamper resistant) que realizan de forma segura funciones de generación y protección de claves y firma digital para una gran variedad de aplicaciones, como:
- Autoridades de certificación
- Procesos de negocio
- Firma de código
- Servicios en la nube
- Blockchain privadas y públicas
- Establecimiento de comunicaciones seguras

Observaciones

Solicitar al fabricante la guía de configuración utilizada en la certificación Common Criteria. Configurar el producto para la utilización de funciones, algoritmos y protocolos aprobados por el Centro Criptológico Nacional, según la guía 'CCN-STIC-807 Criptología de empleo en el ENS'.

INFORMACIÓN IMPORTANTE

7.6 CATEGORÍA: PROTECCIÓN DE EQUIPOS Y SERVICIOS

7.6.1 FAMILIA: DISPOSITIVOS MÓVILES

Samsung Galaxy A51 (SM-A515F)



Versión	Android 11
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2020
Revisión de Validez	13/12/2022

Descripción

Galaxy A51 es un teléfono móvil basado en Android que incorpora la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzadoy monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1611 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 11)

Samsung Galaxy A52 5G (SM-A526B)



Versión	Android 11
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/01/2022
Revisión de Validez	30/06/2024

Descripción

El modelo Galaxy A52 5G es un teléfono móvil basado en Android que incorpora la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1611 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 11)

INFORMACIÓN IMPORTANTE

Samsung Galaxy Note10 (SM-N970F), Note10+ (SM-N975F), Note10+ 5G (SM-N976B)

Versión	Android 11
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2019
Revisión de Validez	01/08/2022





Descripción

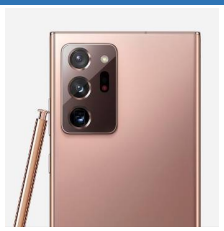
Los dispositivos de la Gama S10 son el fruto de 10 años de innovación en smartphones, y están preparados para afrontar los desafíos de cualquier sector empresarial. Toda la gama S10 cuenta con las mismas características a nivel empresarial: seguridad garantizada gracias a Samsung Knox, pantalla Infinita para una mejor experiencia de trabajo, un potente procesador, carga rápida e inalámbrica, sensor de huella (ultrasónico en el caso de S10+ y S10), y unas capacidades de altas prestaciones.
Versión de Android soportada actualmente: Android 10
Fecha fin de soporte prevista:
SM-G970F: 01/03/2022
SM-G970F Enterprise Edition: 01/03/2023
SM-G975F: 01/03/2022
SM-G976B: 01/03/2022

Observaciones

CCN-STIC 1611 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 11)

Samsung Galaxy Note20 4G (SM-N980F), Note20 5G (SM-N981B), Note20 Ultra 5G (SM-N986B)

Versión	Android 11
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2020
Revisión de Validez	27/07/2023





Descripción

La familia de dispositivos de la gama Galaxy Note20 son teléfonos móviles basados en Android que incorporan la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.
Fecha fin de soporte prevista:
- SM-N980F: 24/07/2023
- SM-N981B: 24/07/2023
- SM-N981B Enterprise Edition: 01/07/2024
- SM-N986B: 22/07/2023

Observaciones

CCN-STIC 1611 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 11)

INFORMACIÓN IMPORTANTE

Samsung Galaxy S10 (SM-G973F Enterprise Edition), S10e (SM-G970F Enterprise Edition)



Versión	Android 11
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/08/2019
Revisión de Validez	01/03/2023

ens Esquema Nacional de Seguridad — ALTA MEDIA BÁSICA — ALTA

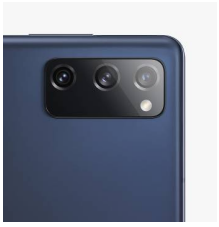
Descripción

Los dispositivos de la Gama S10 son el fruto de 10 años de innovación en smartphones, y están preparados para afrontar los desafíos de cualquier sector empresarial. Toda la gama S10 cuenta con las mismas características a nivel empresarial: seguridad garantizada gracias a Samsung Knox, pantalla Infinita para una mejor experiencia de trabajo, un potente procesador, carga rápida e inalámbrica, sensor de huella (ultrasónico en el caso de S10+ y S10), y unas capacidades de altas prestaciones.

Observaciones

Expediente: 2021-47

Samsung Galaxy S20 FE 4G (SM-G780F), S20 FE 5G (SM-G781B)



Versión	Android 11
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2020
Revisión de Validez	17/09/2023

ens Esquema Nacional de Seguridad — ALTA MEDIA BÁSICA — ALTA

Descripción

La familia de dispositivos de la gama Galaxy S20 FE son teléfonos móviles basados en Android que incorporan la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1611 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 11)

INFORMACIÓN IMPORTANTE

Samsung Galaxy S20+ 5G (SM-G986B), S20 5G (SM-G981B), S20 Ultra 5G (SM-G988B), S20+ 4G (SM-G985F), S20 4G (SM-G980F)



Versión	Android 11
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2020
Revisión de Validez	04/02/2023

Descripción

La familia de dispositivos de la gama Galaxy S20 son teléfonos móviles basados en Android que incorporan la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datosen Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.
Fecha fin de soporte prevista:
- SM-G986B Enterprise Edition: 04/02/2024
- SM-G986B: 04/02/2023
- SM-G981B: 04/02/2023
- SM-G988B: 07/02/2023
- SM-G985F Enterprise Edition: 04/02/2024
- SM-G985F: 04/02/2023
- SM-G980F Enterprise Edition: 04/02/2024
- SM-G980F: 04/02/2023

Observaciones

CCN-STIC 1611 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 11)

Samsung Galaxy S21 5G(SM-G991B), S21 + 5G (SM-G996B), S21 Ultra+ 5G (SM-G998B)



Versión	Android 11
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2021
Revisión de Validez	31/12/2024

Descripción

La familia de dispositivos de la gama Galaxy S21 son teléfonos móviles basados en Android que incorporan la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datosen Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1611 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 11)

INFORMACIÓN IMPORTANTE

Samsung Galaxy Tab Active 3 (SM-T570 / SM-T575)



Versión	Android 11
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2020
Revisión de Validez	29/10/2024



Descripción

Galaxy Tab Active 3 es una tableta rugerizada basada en Android que incorpora la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1611 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 11)

Samsung Galaxy Tab S6 (SM-T860, SM-T865)



Versión	Android 11
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2020
Revisión de Validez	05/08/2022



Descripción

Galaxy Tab S6 es una tableta empresarial basada en Android que incorpora la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el controlavanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1611 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 11)

INFORMACIÓN IMPORTANTE

Samsung Galaxy Tab S7 (SM-T870 / SM-T875), Tab S7+ (SM-T970 / SM-T976B)



Versión	Android 11
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2020
Revisión de Validez	17/07/2023

Descripción

Galaxy Tab S7 / S7+ es una tableta empresarial basada en Android que incorpora la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.
Fecha fin de soporte prevista:
SM-T870: 28/07/2023
SM-T875: 24/07/2023
SM-T875 Enterprise Edition: 24/07/2024
SM-T970: 21/07/2023
SM-T976B: 17/07/2023

Observaciones

CCN-STIC 1611 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 11)

Samsung Galaxy XCoverPro (SM-G715FN)



Versión	Android 11
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2020
Revisión de Validez	10/01/2023

Descripción

Galaxy XCover Pro es un teléfono móvil rugerizado basado en Android que incorpora la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.
Fecha fin de soporte prevista:
SM-G715FN: Enterprise Edition: 10/01/2024
SM-G715FN: 10/01/2023

Observaciones

CCN-STIC 1611 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 11)

INFORMACIÓN IMPORTANTE

Samsung Galaxy Z Flip (SM-F700F / SM-F707B)



Versión	Android 11
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2020
Revisión de Validez	05/02/2023

Descripción

Galaxy Z Flip es un teléfono móvil basado en Android que incorpora la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.
Fecha Fin de Soporte prevista:
SM-F700F: 05/02/2023
SM-F707B: 08/07/2023

Observaciones

CCN-STIC 1611 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 11)

Samsung Galaxy Z Fold2 5G (SM-F916B)



Versión	Android 11
Fabricante	Samsung Electronics
Familia	Dispositivos móviles
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2020
Revisión de Validez	28/08/2023

Descripción

Galaxy Z Fold2 5G es un teléfono móvil basado en Android que incorpora la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Observaciones

CCN-STIC 1611 Procedimiento de Empleo Seguro de dispositivos Samsung Galaxy (Android 11)

INFORMACIÓN IMPORTANTE

7.6.2 FAMILIA: SISTEMAS OPERATIVOS

Windows Server 2012 R2	
Versión	Standard Edition, Datacenter Edition
Fabricante	Microsoft Corporation
Familia	Sistemas Operativos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2018
Revisión de Validez	10/10/2023
Descripción	
Sistema Operativo para servidores	
Observaciones	
CCN-STIC-870A y CCN-STIC-870B	

Windows Server 2016	
Versión	Datacenter Edition
Fabricante	Microsoft Corporation
Familia	Sistemas Operativos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2018
Revisión de Validez	09/01/2024
Descripción	
Sistema Operativo para servidores	
Observaciones	
CCN-STIC-570A, CCN-STIC-570B Anexo A	

INFORMACIÓN IMPORTANTE

Windows 10 1909	
Versión	Entreprise Edition
Fabricante	Microsoft Corporation
Familia	Sistemas Operativos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2021
Revisión de Validez	10/05/2022

Descripción

Sistema operativo para puesto de trabajo cliente, tanto para entorno real como virtualizado.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

SUSE Linux Enterprise	
Versión	Server 15 SP2
Fabricante	SUSE Software Solutions
Familia	Sistemas Operativos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/10/2021
Revisión de Validez	31/04/2022

Descripción

SUSE® Linux Enterprise Server (SLES) 15 SP2 es un sistema operativo (SO) modular que ayuda a simplificar el entorno IT, modernizar la infraestructura IT y acelerar la innovación. SLES se adapta a cualquier entorno operativo a la vez que satisface los requisitos de rendimiento, seguridad y confiabilidad. Es una plataforma fácil de administrar para desarrolladores y administradores que permite implementar cargas de trabajo críticas para el negocio en las instalaciones, en la nube y en el perímetro.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

7.6.3 FAMILIA: PROTECCIÓN DE CORREO ELECTRÓNICO

FortiMail Appliances FML-2000E, FML-3000E, FML-3200E	
Versión	Firmware 6.0.2
Fabricante	Fortinet
Familia	Protección de correo electrónico
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2019
Revisión de Validez	30/11/2022

Descripción

Sistema de seguridad de correo electrónico que proporciona una protección multicapa contra spam, virus, gusanos y spyware. El motor de filtrado empleado en FortiMail bloquea el spam y el malware antes de que pueda afectar a las redes y usuarios.

Observaciones

CCN-STIC-1614 Procedimiento de empleo seguro Fortimail
Requiere Fortinet Entropy Token V1

7.6.4 FAMILIA: TARJETAS INTELIGENTES

Pendiente de publicación los Requisitos Fundamentales de Seguridad (RFS) de esta familia.

7.6.5 FAMILIA: COPIAS DE SEGURIDAD

Pendiente de recepción de solicitudes de productos que cumplan con Requisitos Fundamentales de Seguridad (RFS) correspondientes a esta familia.

7.6.6 FAMILIA: PLATAFORMAS CONFIABLES

Pendiente de recepción de solicitudes de productos que cumplan con Requisitos Fundamentales de Seguridad (RFS) correspondientes a esta familia.

7.6.7 FAMILIA: VIRTUALIZACIÓN

Pendiente de recepción de solicitudes de productos que cumplan con Requisitos Fundamentales de Seguridad (RFS) correspondientes a esta familia.

INFORMACIÓN IMPORTANTE

7.6.8 FAMILIA: BALANCEADORES DE CARGA

LTM+APM (Bourne 1035v-F, Shuttle i5000 (i5600, i5800, i5820-DF), Shuttle i7000 (i7600, i7800, i7820-DF), Shuttle i10000 (i10600, i10800), Shuttle i11000 (i11600-DS, i11800-DS), Shuttle i15000 (i15800, i15600-DS), VIPRION B2250 y VIPRION B4450)	
Versión	14.1.0.3 BUILD bigip-14.1.0.3.75.6-ENG with Hotfix-BIGIP-14.1.0.3.0.75.6-ENG
Fabricante	F5 Networks Iberia,S.L.
Familia	Balanceadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2021
Revisión de Validez	30/04/2022
Descripción	
F5 BIG-IP es una herramienta clave en la publicación y entrega de las aplicaciones. Optimiza su disponibilidad mejorando la velocidad y fiabilidad de las mismas a través de las capas de aplicación y de red.	
Observaciones	
Procedimiento de empleo seguro pendiente de publicación.	

LTM+AFM (Bourne 1035v-F, Shuttle i5000 (i5600, i5800, i5820-DF), Shuttle i7000 (i7600, i7800, i7820-DF), Shuttle i10000 (i10600, i10800), Shuttle i11000 (i11600-DS, i11800-DS), Shuttle i15000 (i15800, i15600-DS), VIPRION B2250 y VIPRION B4450)	
Versión	14.1.0.3 BUILD bigip-14.1.0.3.75.6-ENG with Hotfix-BIGIP-14.1.0.3.0.75.6-ENG
Fabricante	F5 Networks Iberia,S.L.
Familia	Balanceadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2021
Revisión de Validez	30/04/2022
Descripción	
F5 BIG-IP es una herramienta clave en la publicación y entrega de las aplicaciones. Optimiza su disponibilidad mejorando la velocidad y fiabilidad de las mismas a través de las capas de aplicación y de red.	
Observaciones	
Procedimiento de empleo seguro pendiente de publicación.	

7.6.9 FAMILIA: HERRAMIENTAS CASB

Pendiente de recepción de solicitudes de productos que cumplan con Requisitos Fundamentales de Seguridad (RFS) correspondientes a esta familia.

INFORMACIÓN IMPORTANTE

7.6.10 FAMILIA: HIPERCONVERGENCIA

KATUA SDI PLATFORM	
Versión	1.0.6
Fabricante	KRC ESPAÑOLA S.A.
Familia	Hiperconvergencia
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2021
Revisión de Validez	29/02/2024

Descripción

Katua®SDI Platform es una plataforma hiperconvergente escalable y segura, basada en el concepto Software Define Infraestructure, donde todos los elementos que conforman un CPD se definen en una única plataforma hardware y software. Permite el despliegue rápido de servicios (xaaS), consolidación de CPDs, SDN y tiene capacidad de instalación desde equipos móviles hasta grandes centros de procesos de datos. Su flexibilidad permite que se puedan desplegar servicios cloud sobre la plataforma de forma sencilla y eficiente. Dispone de la capacidad para generar bibliotecas de sistemas preconfigurados para su despliegue con un click a través de su interfaz web. Las capacidades de optimización del hipervisor aseguran un rendimiento máximo de la plataforma, haciendo uso de todos los recursos disponibles y ofreciendo de esta forma capacidad de instalación en nodos pequeños y configuraciones hardware básicas. Su capacidad para integrarse con sistemas de almacenamiento masivos, ya sean locales o remotos permite escalar la solución en función de las necesidades. Para más información de la plataforma, vista nuestra web https://www.krc.es.

Observaciones

CCN-STIC-1610 Procedimiento de Empleo Seguro KATUA SDI Platform

INFORMACIÓN IMPORTANTE

7.6.11 FAMILIA: HERRAMIENTAS DE VIDEOCONFERENCIA

PEXIP Infinity

Versión	v.25.4 (Build 59565.0.0); Client software v1.6.2
Fabricante	PEXIP
Familia	Herramientas de videoconferencia
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/03/2022
Revisión de Validez	31/08/2023

Descripción

Plataforma de infraestructura de videoconferencia virtualizada y distribuida, para gestionar equipos de videoconferencia de sala H.323/SIP y clientes de escritorio PC, Mac, Linux, con cliente WebRTC.
Actúa de Call Control, consta de firewall traversal, unidad multiconferencia (MCU), sistema de gestión de terminales y aloja usuarios de escritorio y móviles. Proporciona bridge para interoperar con usuarios de Microsoft Teams CVI, Google Meet, Skype for Business, Webex y WebRTC, y hace streaming y recording.
Integra Outlook y Google Calendar para la planificación de sesiones, SSO, certificados y LDAP. Consta de una amplia librería de APIs.
La arquitectura se basa en 3 tipos de nodos:
- Management Node para gestionar y configurar la plataforma, las políticas de llamadas y la monitorización.
- Transcoding Nodes, donde se procesan y alojan las conferencias y multiconferencias. Proporciona redundancia y es resistente a pérdida de paquetes y bajos ratios de transferencia.
- Edge Nodes en donde se negocia la señalización con redes externas y donde securiza el tráfico y oculta la topología de red interna.
Esta arquitectura es escalable y permite la securización de las comunicaciones mediante cifrado. Permite la privacidad de datos, equipos y usuarios.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

7.7 CATEGORÍA: HERRAMIENTAS PARA EL DESARROLLO DE PRODUCTOS DE SEGURIDAD

TRNG-P200 Physical True Random Number Generator

Versión	1.11
Fabricante	BERTEN DSP S.L.
Familia	-
Tipo	Producto
Categoría ENS	-
Fecha Inclusión	01/10/2020
Revisión de Validez	31/03/2023

Descripción

El IP Core TRNG-P200 es un Generador de Números Aleatorios Verdaderos (TRNG, True Random Number Generator) implementable en cualquier diseño criptográfico basado en FPGA, SoC o ASIC. Utiliza una fuente física de entropía no determinista basada en osciladores multifase, que genera números aleatorios de alta calidad estadística en un área mínima. Genera simultáneamente la secuencia aleatoria de la fuente de entropía, y dos salidas post procesadas con un filtro de paridad y un codificador polinómico configurable.
Es portable a cualquier dispositivo Xilinx, Intel o Microsemi y cumple con los requisitos definidos en las baterías de test Diehard, NIST 800-22 y AIS-31 PTG.2. Además, implementa un conjunto de pruebas de integridad (health tests), de acuerdo con NIST 800-90B, FIPS 140-2 y AIS-31. La generación de secuencias es monitorizada continuamente, activando alarmas en caso de fallos.
El TRNG-P200 incluye interfaces AMBA-AXI y un mapa de registros con parámetros programables para configurar la velocidad de salida, el codificador polinómico, las pruebas de integridad, y la gestión de las alarmas. El producto incluye funciones ANSI C para la configuración de estos registros en el sistema criptográfico.
https://www.bertendsp.com/products/trng-p200/

Observaciones

No aplica

Biblioteca Criptográfica BOTAN-CCN

Versión	2.15.2
Fabricante	Centro Criptológico Nacional
Familia	-
Tipo	Producto
Categoría ENS	-
Fecha Inclusión	01/10/2020
Revisión de Validez	31/03/2023

Descripción

La biblioteca criptográfica BOTAN-CCN implementa los mecanismos criptográficos aceptados por el CCN para su uso en el desarrollo de productos de seguridad. Incluye código fuente y binarios compatibles con sistemas Windows y Linux. Incluye generadores de ruido y test de todas los mecanismos implementados

Observaciones

No aplica

INFORMACIÓN IMPORTANTE

7.8 CATEGORÍA: OTRAS HERRAMIENTAS

authUsb safeDoor	
Versión	2.0.0.8
Fabricante	authUSB
Familia	Otras Herramientas
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2019
Revisión de Validez	30/11/2022





Descripción

AuthUsb safeDoor es un dispositivo hardware que actúa como barrera entre las memorias USB y los equipos de una organización, identificando amenazas a tres niveles:

-Eléctrico: identificando y deteniendo ataques destructivos de sobretensión tipo UsbKiller.

-Hardware: detectando y desactivando ataques de la familia BadUsb, ataques HID (rubber ducky y similares), falsas tarjetas de red, interfaces compuestas, etc.

-Software: antivirus integrado que realiza un análisis previo a la descarga de cualquier contenido.

Observaciones

CCN-STIC 1201 Procedimiento de empleo seguro AuthUsb SafeDoor

Personal Code	
Versión	2020.3.2
Fabricante	HUBOX
Familia	Otras Herramientas
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/09/2021
Revisión de Validez	30/04/2022





Descripción

PERSONAL CODE es una solución de identidad digital que resuelve el problema de fraudes por suplantación de identidad. Véase la solución como una secuencia de bits que almacena, de forma segura, características biométricas e información biográfica de un individuo. Estos datos son firmados y reconocidos por una autoridad y se protegen mediante criptografía asimétrica para su posterior verificación a través de una aplicación que no requiere conectividad ni consultas a bases de datos. PERSONAL CODE implementa su solución en forma de dos librerías o DLLs, una librería de generación que se encarga de procesar la información del individuo y otra de verificación para la posterior extracción y validación de los datos.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

7.9 CATEGORÍA: SEGURIDAD OT

ÁGATA	
Versión	2.3.3
Fabricante	Ágata Technology
Familia	-
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/12/2021
Revisión de Validez	31/05/2022

Descripción

Ágata es una plataforma software que permite la digitalización, optimización y automatización de procesos de negocio, poniendo la tecnología al servicio de las personas. Ágata integra en un único entorno tecnológico todos los procesos y servicios de una organización permitiendo gestionarlos de manera sencilla, eficiente, sostenible y segura.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

INFORMACIÓN IMPORTANTE

8. PRODUCTOS APROBADOS

PRODUCTOS APROBADOS



8.1 CATEGORÍA: CONTROL DE ACCESO

8.1.1 FAMILIA: CONTROL DE ACCESO A RED (NAC)

Citrix ADC (formerly NetScaler) MPX 14030 FIPS, MPX 14060 FIPS y MPX 14080 FIPS

Versión	Platinum Edition Version 11.1
Fabricante	Citrix Systems
Familia	Control de Acceso a Red (NAC)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/04/2020
Revisión de Validez	30/09/2022



Descripción

Citrix ADC (antes NetScaler) es un Application Delivery Controller con funciones específicas de seguridad para el control de acceso a la red corporativa de usuarios y dispositivos, permitiendo discriminar en el acceso no solo por usuario sino también porel estado de la seguridad en el momento de la conexión y durante la misma. Tanto en accesos SSL VPN como mediante un portal completo de aplicaciones servido al usuario -donde están sus aplicaciones internas, SaaS y aplicaciones y desktops virtuales-, se autenticará al usuario (con opción de múltiples factores, incluso con OTP Nativo sin necesidad de otro OTP adicional) contra un sistema corporativo o mediante federación de identidades, se tendrá en cuenta su perfil (usuario, grupos, atributos en el Directorio), y se comprobará la seguridad del dispositivo (antivirus, firewall, dominio, procesos activos, etc.) y la de la conexión (punto de acceso, ubicación desde la que se accede, etc.), para aplicar según el resultado unas políticas de acceso granulares,ya sea en el propio appliance o en un dispositivo de red posterior como un firewall. De esta forma se garantiza el acceso a cada recurso interno únicamente de aquellas combinaciones aprobadas de usuario/dispositivo/conexión.

Observaciones

Procedimiento de empleo pendiente de publicación.

Cisco Identity Services Engine (ISE)	
Versión	2.6
Fabricante	Cisco Systems
Familia	Control de Acceso a Red (NAC)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/07/2020
Revisión de Validez	31/12/2022

Descripción

Cisco ISE es una plataforma de control de acceso que combina la autenticación, autorización y trazabilidad (AAA), así como la gestión de usuarios, en un appliance. ISE permite control de acceso seguro en las conexiones cableadas, inalámbricas y VPN. Permite realizar búsquedas en la red para dar visibilidad sobre quién o qué accede a los distintos recursos.Productos cualificados:
- Cisco Identity Services Engine Appliance 3515, 3595, 3615, 3655, 3695
- Cisco Identity Services Engine Virtual Machine (ISE-VM) en ESXi 6.7 ejecutado sobre UCSC-C220-M5SX
- Cisco Identity Services Engine ejecutado sobre Cisco Application Deployment Engine (ADE) Release 3.0 operating system (ADE-OS)

Observaciones

CCN-STIC-1104 Procedimiento de Empleo CISCO ISE 2.6

EMMA	
Versión	-
Fabricante	OpenCloud Factory / CCN
Familia	Control de Acceso a Red (NAC)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/05/2020
Revisión de Validez	31/10/2022

Descripción

EMMA es una solución de Visualización de activos en una red, su autenticación y segregación, así como la automatización de auditorías de seguridad de la infraestructura. El alcance de la cualificación abarca los siguiente módulos de EMMA:
Visibilidad, Control / Respuesta, Segmentación, Cumplimiento, BYOD y Gestión de invitados.
Se recoge el inventario y perfilado del equipo que se podrá utilizar en las políticas de acceso a la conexión remota. Adicionalmente, permite definir y aplicar políticas de acceso en función de una postura de seguridad basada en el nivel de bastionado, además de otros factores (horario de la conexión, características del equipo, role de usuario etc.).
EMMA se integrará con soluciones del ecosistema CCN-CERT: ROCIO y ANA.
https://www.ccn-cert.cni.es/pdf/documentos-publicos/4153-datasheet-emma/file.html

Observaciones

CCN-STIC-1105 Procedimiento de empleo seguro EMMA

ClearPass Policy Manager (C1000, C2000, C3000)	
Versión	6.9
Fabricante	Aruba
Familia	Control de acceso a red (NAC)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/07/2019
Revisión de Validez	31/08/2022

Descripción

La familia de productos ClearPass de seguridad para el control de acceso a la red ofrece elaboración de perfiles, autenticación y autorización para usuarios, sistemas y dispositivos que intentan acceder a los recursos de TI. ClearPass se ha diseñado paraabordar los retos de seguridad asociados con una organización TI: Acceso seguro a la red (802.1X y Radius), funciones de NAC, Implementación de portal de Invitados e interno, soporte de funcionalidades BYOD, integración con Firewalls (PaloAlto, CheckPoint, Forninet y mas) todo ello mediante la integración múltiples fuentes de autenticación (Directorios activos, LDAP, BBDD y provedores externos de identidad)

Observaciones

CCN-STIC-1103 Procedimiento de empleo seguro ClearPass 6.9

8.1.2 FAMILIA: SERVIDORES DE AUTENTICACIÓN

ClearPass Policy Manager (C1000, C2000, C3000)	
Versión	6.9
Fabricante	Aruba
Familia	Servidores de Autenticación
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/07/2019
Revisión de Validez	31/08/2022

Descripción

La familia de productos ClearPass de seguridad para el control de acceso a la red ofrece elaboración de perfiles, autenticación y autorización para usuarios, sistemas y dispositivos que intentan acceder a los recursos de TI. ClearPass se ha diseñado paraabordar los retos de seguridad asociados con una organización TI: Acceso seguro a la red (802.1X y Radius), funciones de NAC, Implementación de portal de Invitados e interno, soporte de funcionalidades BYOD, integración con Firewalls (PaloAlto, CheckPoint, Forninet y mas) todo ello mediante la integración múltiples fuentes de autenticación (Directorios activos, LDAP, BBDD y provedores externos de identidad)

Observaciones

CCN-STIC-1103 Procedimiento de empleo seguro ClearPass 6.9

8.1.3 FAMILIA: GESTIÓN DE ACCESO PRIVILEGIADO (PAM)

Thycotic Secret Server Government Edition	
Versión	10.1
Familia	Gestión de acceso privilegiado (PAM)
Fabricante	Thycotic
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/05/2019
Revisión de Validez	30/11/2022

Descripción

Thycotic Secret Server es una solución de gestión de cuentas privilegiadas que permite descubrir, securizar, administrar y auditar contraseñas, credenciales así como monitorizar y grabar las sesiones privilegiadas. Permite gestionar el acceso a cada cuenta privilegiada y activo crítico, automatizar las mejores prácticas de seguridad y cumplir las regulaciones normativas.

Las capacidades de PAM de Secret Server para la administración de las cuentas privilegiadas incluyen:

- Gestión del Ciclo de Vidade las credenciales con privilegios:
  - Descubrimiento Automatizado de cuentas privilegiadas y “onboarding” de las mismas en un Repositorio central seguro
  - Rotado automático de las credenciales y Gestión, control y auditoria de las sesiones privilegiadas
- Análisis del comportamiento del usuario privilegiado
- Gestión de cuentas de servicio
- Políticas de acceso basadas en RBAC y Gestión de políticas de seguridad.
- Arquitectura escalable. Alta Disponibilidad y DR. Integración con múltiples plataformas Out-Of-The-Box
- Módulo de Reporting capaz de generar informes totalmente a medida
- Securización de los procesos de DevOps.

Observaciones

CCN-STIC-1101 Procedimiento de Empleo Seguro SECRET SERVER de THYCOTIC

8.1.4 FAMILIA: GESTIÓN DE IDENTIDADES (IM)

One Identity Manager	
Versión	v8.1
Fabricante	One Identity
Familia	Gestión de identidades (IM)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/11/2020
Revisión de Validez	30/04/2023

Descripción

One Identity Manager es una solución de gobierno y gestión de identidades (IAM) que permite automatizar la gestión de los accesos de los usuarios, permitiendo que accedan a las aplicaciones y a los datos estrictamente necesarios para desempeñar su trabajo. La solucion permite que la administración de los usuarios, sus identidades digitales y sus accesos puedan ser impulsadas por otros departamentos como RRHH.

• Gestione el acceso a recursos en las instalaciones, en la nube e híbridos desde cualquier departamento de la organización

• Reduzca el riesgo al asegurarse de que los usuarios tengan solo los accesos que necesitan

• Satisfaga auditorías e iniciativas de cumplimiento con políticas de confirmación/recertificación

Otorgue derechos de acceso en función de roles, reglas y políticas definidas. Establezca procesos estándares de aprovisionamiento y desaprovisionamiento para sus empleados y proveedores. Administre de forma rápida y fácil el acceso a recursos a medida que las responsabilidades del usuario evolucionen con la empresa.

Observaciones

CCN-STIC-1107 Procedimiento de Empleo Seguro One Identity Manager 8.1

IBM Secret Server Government Edition	
Versión	10.7
Fabricante	IBM
Familia	Gestión de acceso privilegiado (PAM)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/05/2020
Revisión de Validez	30/11/2022

Descripción

IBM Secret Server es una solución de gestión de cuentas privilegiadas que permite descubrir, securizar, administrar y auditar contraseñas, credenciales así como monitorizar y grabar las sesiones privilegiadas. Permite gestionar el acceso a cada cuenta privilegiada y activo crítico, automatizar las mejores prácticas de seguridad y cumplir las regulaciones normativas.

Las capacidades de PAM de Secret Server para la administración de las cuentas privilegiadas incluyen:

- Gestión del Ciclo de Vida de las credenciales con privilegios:
  - Descubrimiento Automatizado de cuentas privilegiadas y “onboarding” de las mismas en un Repositorio central seguro
  - Rotado automático de las credenciales y Gestión, control y auditoria de las sesiones privilegiadas
- Análisis del comportamiento del usuario privilegiado
- Gestión de cuentas de servicio
- Políticas de acceso basadas en RBAC y Gestión de políticas de seguridad.
- Arquitectura escalable. Alta Disponibilidad y DR. Integración con múltiples plataformas Out-Of-The-Box
- Módulo de Reporting capaz de generar informes totalmente a medida
- Securización de los procesos de DevOps.

Observaciones

CCN-STIC-1101 Procedimiento de Empleo Seguro SECRET SERVER de THYCOTIC

CyberArk Privileged Account Security Solution	
Versión	10.4
Fabricante	CyberArk
Familia	Gestión de acceso privilegiado (PAM)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/07/2020
Revisión de Validez	31/12/2022

Descripción

CyberArk Core PAS es una solución de seguridad que permite proteger, controlar y monitorizar el acceso privilegiado a infraestructura locales, en la nube e híbridas. Permite a las organizaciones administrar y proteger las credenciales de las cuentas privilegiadas y los derechos de acceso, monitorizar y controlar la actividad de las cuentas privilegiadas, identificar las actividades sospechosas y responder a las amenazas.

• Asegurar y controlar centralmente el acceso a las credenciales privilegiadas basadas en políticas de seguridad definidas administrativamente.

• Aislar y asegurar sesiones de usuarios privilegiados. Las capacidades de monitorización y grabación permiten a los equipos de seguridad ver sesiones privilegiadas en tiempo real, suspender automáticamente y terminar remotamente las sesiones sospechosas.

• Detectar, alertar y responder a actividades privilegiadas anómalas.

• Controlar el acceso de privilegios mínimos para * NIX y Windows. La solución permite a los usuarios con privilegios ejecutar comandos administrativos autorizados desde sus sesiones nativas de Unix o Linux, a la vez que se eliminan los privilegios de raíz innecesarios.

• Proteger los controladores de dominio de Windows.

Observaciones

CCN-STIC-1108 Procedimiento de empleo seguro CyberArk Privileged Account Security Solution 10.4

8.2 CATEGORÍA: SEGURIDAD EN LA EXPLOTACIÓN

8.2.1 FAMILIA: ANTI-VIRUS/EPP (ENDPOINT PROTECTION PLATFORM)

ESET Endpoint Security	
Versión	7.2.2055.3
Fabricante	ESET SPOL S.R.O
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/04/2020
Revisión de Validez	30/07/2022

Descripción

ESET Endpoint Security es una solución fácil de implementar y utilizar, administrable de forma centralizada, con protección multicapa que se basa en tres pilares básicos: primar el rendimiento del sistema, una detección eficaz y no importunar al usuario con falsos positivos. Este enfoque de protección multicapa permite a ESET detectar y/o bloquear diferentes tipos de amenazas, como ransomware, ataques sin archivos, botnets, ataques de red o exploits.
Los componentes de protección que han sido analizados en el proceso de cualificación son:
1) Antivirus y antiespía: Elimina todo tipo de amenazas tales como virus, rootkits, gusanos y software espía.
2) Sistema avanzado de prevención de intrusiones (HIPS): Permite controlar los procesos, archivos y claves deregistro a través de reglas. Protege frente a modificaciones no autorizadas y detecta las amenazas basándose en su comportamiento en el sistema.
3) Análisis avanzado de memoria: Monitoriza el comportamiento de todos los procesos y los analiza cuando seejecutan en memoria. Esto permite una prevención más efectiva contra las infecciones, incluso en el caso de que estén especialmente diseñadas para evitar su detección.
4) Protección contra botnets: Evita que los equipos de tu empresa formen parte de una

Observaciones

CCN-STIC 1204 Procedimiento de empleo seguro ESET Endpoint Security 7

Intercept X Advanced with EDR	
Versión	2.5.4 BETA/ 10.8.6/2.0.16 BETA
Fabricante	Sophos
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/03/2020
Revisión de Validez	31/08/2022

Descripción

Sophos Intercept X Advanced con EDR es una solución que ofrece protección avanzada de puesto trabajo y servidores. Está especialmente diseñada para detener la gran mayoría de ataques y hacer frente a nuevas amenazas como ransomware, fileless, o ataques zero-day. Con diferentes capas de protección, las primeras están diseñadas para reducir la superficie de ataque a través del control de USBs, control de aplicaciones, control de navegación y DLP. Posteriormente tiene capas que detectan, primero lo malo conocido a través de las firmas que desarrollan los Sophos LABS y, segundo, lo malo desconocido, como el ransomware, gracias a la monitorización de procesos, el control de comportamiento, utilizando la tecnología única de Deep Learning que permite detectar malware no identificado previamente, y la detección de técnicas de explotación/ataque y de post compromiso. Además, la solución cuenta con capacidades avanzadas de detección y respuesta inteligentes (EDR) que permiten a la organización hacer investigaciones y threat hunting para ser proactivo a la hora de identificar amenazas e investigar posibles eventos maliciosos, así como comprender el alcance y el impacto o buscar los indicadores de amenazas en toda la red. Todo ello desde una única consola de gestión

Observaciones

CCN-STIC 1207 Procedimiento de Empleo Seguro Sophos Central Intercept X

McAfee Endpoint Security	
Versión	10.6 with ePolicy Orchestrator 5.3.3
Fabricante	McAfee
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/08/2020
Revisión de Validez	31/01/2023

Descripción

El endpoint de McAfee integra capacidades de antivirus, aprendizaje automático, prevención de exploits, firewall y control web. Proporciona una gestión centralizada y una visualización integral de las amenazas para reforzar las defensas y realizar cambiosen las políticas globales de protección. Las actividades de escaneo en tiempo real, análisis en la nube, contención de aplicaciones y la corrección de reversión trabajan juntas para limitar el impacto de los archivos sospechosos y el malware de día cero.Las detecciones y remediaciones manuales se reemplazan por análisis, contención y remediación automáticos para detener las amenazas antes de que se propaguen y devuelvan los endpoints a un estado saludable. Dispone de una tecnología sencilla, integrada,automatizada y adaptable de detección y respuesta de terminales (EDR). Las investigaciones guiadas por IA facilitan las tareas a los analistas con cualquier nivel de experiencia.

Observaciones

CCN-STIC-1208 Procedimiento de Empleo Seguro Mcafee Endpoint

Checkpoint Endpoint Security (Sandblast Agent)

Versión	E82.40 (82.40.1159)
Fabricante	Check Point Software Technologies
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/05/2020
Revisión de Validez	31/10/2022



ens Esquema Nacional de Seguridad — ALTA / MEDIA / BÁSICA — MEDIA

Descripción

Check Point SandBlast Agent es una solución de protección avanzada para endpoints y navegadores de Internet, garantiza protección completa contra los diferentes vectores de amenazas con capacidades de prevención, detección y respuesta. Incorpora una gestión integrada disponible en nube o instalación local. Prestaciones:

- Emulación de amenazas (Sandbox) y Extracción (Entrega archivos limpios a usuarios en tiempo real)
- Anti-Ransomware (prevención y reparación) y defensa contra ciberextorsión
- Anti-Bot,
- Anti-Exploit
- Anti-Malware.
- Análisis de comportamientos (detección y bloqueo)

Observaciones

CCN-STIC-1214 Procedimiento de Empleo Seguro Checkpoint Endpoint Security (SBA)

Deep Security (Manager y Agente/Relay Linux/Windows)

Versión	11
Fabricante	Trend Micro
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/12/2021
Revisión de Validez	31/05/2024

ens Esquema Nacional de Seguridad — ALTA / MEDIA / BÁSICA — ALTA

Descripción

Deep Security es la respuesta de Trend Micro para proteger el cloud híbrido ya sean servidores físicos o virtuales. Gracias a su agente ligero, el cual incorpora funcionalidades: EDR (con respuesta frente a amenazas conocidas, zero-day), reputación web, control de aplicaciones, supervisión de logs, Supervisión de Integridad (FIM), Firewall de Host y Host IPS (que incorpora la tecnología de parcheado virtual), ayuda a mejorar la postura de seguridad proporcionando seguridad, visibilidad y control. La cualificación abarca los siguientes componentes: Manager, Agente/Relay Linux y el Agente/Relay Windows. El *Virtual Appliance* no está cualificado.

Observaciones

CCN-STIC-1216 PES Trendmicro Deep Security

Panda Adaptive Defense 360	
Versión	3.71 (Protection Agent v8.0)
Fabricante	Panda Security
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/09/2020
Revisión de Validez	28/02/2023

Descripción

Panda Adaptive Defense 360 es una solución de seguridad completa para los puestos de trabajo, portátiles y servidores que además de proteger contra amenazas conocidas, avanzadas y zero-day, ransomware y ataques de seguridad fileless (en memoria) y malwareless, incluye firewall personal, IPS/IDS, anti-spam, anti-spam en correo, filtrado y categorización en navegación web y control de dispositivos, entre otras técnicas de seguridad y control de productividad.
Sus capacidades de protección avanzada cubrentodas fases de la Seguridad Adaptativa: Prevención, Detección, Respuesta y Remediación, gracias a los servicios gestionados: servicio de clasificación del 100% de los programas, procesos y ejecutables en los endpoints y el servicios de Threat Hunting y Análisis Forense, que permite una enforzamiento de la seguridad corporativa continua.

Observaciones

CCN-STIC-1213 PES Panda Adaptive Defense 360

8.2.2 FAMILIA: EDR (ENDPOINT DETECTION AND RESPONSE)

Intercept X Advanced with EDR	
Versión	2.5.4 BETA/ 10.8.6/2.0.16 BETA
Fabricante	Sophos
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/03/2020
Revisión de Validez	31/08/2022

Descripción

Sophos Intercept X Advanced con EDR es una solución que ofrece protección avanzada de puesto trabajo y servidores. Está especialmente diseñada para detener la gran mayoría de ataques y hacer frente a nuevas amenazas como ransomware, fileless, o ataques zero-day. Con diferentes capas de protección, las primeras están diseñadas para reducir la superficie de ataque a través del control de USBs, control de aplicaciones, control de navegación y DLP. Posteriormente tiene capas que detectan, primero lo malo conocido a través de las firmas que desarrollan los Sophos LABS y, segundo, lo malo desconocido, como el ransomware, gracias a la monitorización de procesos, el control de comportamiento, utilizando la tecnología única de Deep Learning que permite detectar malware no identificado previamente, y la detección de técnicas de explotación/ataque y de post compromiso. Además, la solución cuenta con capacidades avanzadas de detección y respuesta inteligentes (EDR) que permiten a la organización hacer investigaciones y threat hunting para ser proactivo a la hora de identificar amenazas e investigar posibles eventos maliciosos, así como comprender el alcance y el impacto o buscar los indicadores de amenazas en toda la red. Todo ello desde una única consola de gestión

Observaciones

CCN-STIC 1207 Procedimiento de Empleo Seguro Sophos Central Intercept X

McAfee Endpoint Security

Versión	10.6 with ePolicy Orchestrator 5.3.3
Fabricante	McAfee
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/08/2020
Revisión de Validez	31/01/2023

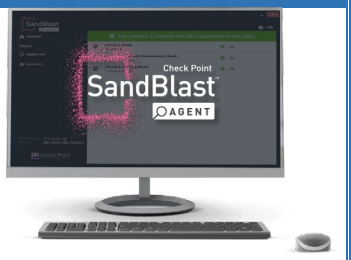
Descripción

El endpoint de McAfee integra capacidades de antivirus, aprendizaje automático, prevención de exploits, firewall y control web. Proporciona una gestión centralizada y una visualización integral de las amenazas para reforzar las defensas y realizar cambiosen las políticas globales de protección. Las actividades de escaneo en tiempo real, análisis en la nube, contención de aplicaciones y la corrección de reversión trabajan juntas para limitar el impacto de los archivos sospechosos y el malware de día cero.Las detecciones y remediaciones manuales se reemplazan por análisis, contención y remediación automáticos para detener las amenazas antes de que se propaguen y devuelvan los endpoints a un estado saludable. Dispone de una tecnología sencilla, integrada,automatizada y adaptable de detección y respuesta de terminales (EDR). Las investigaciones guiadas por IA facilitan las tareas a los analistas con cualquier nivel de experiencia.

Observaciones

CCN-STIC-1208 Procedimiento de Empleo Seguro Mcafee Endpoint

Checkpoint Endpoint Security (Sandblast Agent)



Versión	E82.40 (82.40.1159)
Fabricante	Check Point Software Technologies
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/05/2020
Revisión de Validez	31/10/2022



Descripción

Check Point SandBlast Agent es una solución de protección avanzada para endpoints y navegadores de Internet, garantiza protección completa contra los diferentes vectores de amenazas con capacidades de prevención, detección y respuesta. Incorpora una gestión integrada disponible en nube o instalación local. Prestaciones:

- Emulación de amenazas (Sandbox) y Extracción (Entrega archivos limpios a usuarios en tiempo real)
- Anti-Ransomware (prevención y reparación) y defensa contra ciberextorsión
- Anti-Bot,
- Anti-Exploit
- Anti-Malware.
- Análisis de comportamientos (detección y bloqueo)

Observaciones

CCN-STIC-1214 Procedimiento de Empleo Seguro Checkpoint Endpoint Security (SBA)

Deep Security (Manager y Agente/Relay Linux/Windows)	
Versión	11
Fabricante	Trend Micro
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/12/2021
Revisión de Validez	31/05/2024

Descripción

Deep Security es la respuesta de Trend Micro para proteger el cloud híbrido ya sean servidores físicos o virtuales. Gracias a su agente ligero, el cual incorpora funcio
alidades: EDR (con respuesta frente a amenazas conocidas, zero-day), reputación web, control de aplicaciones, supervisión de logs, Supervisión de Integridad (FIM), Firewall de Host y Host IPS (que incorpora la tecnología de parcheado virtual), ayuda a mejorar la postura de seguridad proporcionando seguridad, visibilidad y control. La cualificación abarca los siguientes componentes: Manager, Agente/Relay Linux y el Agente/Relay Windows. El *Virtual Appliance* no está cualificado.

Observaciones

CCN-STIC-1216 PES Trendmicro Deep Security

Panda Adaptive Defense 360	
Versión	3.71 (Protection Agent v8.0)
Fabricante	Panda Security
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/09/2020
Revisión de Validez	28/02/2023

Descripción

Panda Adaptive Defense 360 es una solución de seguridad completa para los puestos de trabajo, portátiles y servidores que además de proteger contra amenazas conocidas, avanzadas y zero-day, ransomware y ataques de seguridad fileless (en memoria) y malwareless, incluye firewall personal, IPS/IDS, anti-spam, anti-spam en correo, filtrado y categorización en navegación web y control de dispositivos, entre otras técnicas de seguridad y control de productividad.

Sus capacidades de protección avanzada cubren todas fases de la Seguridad Adaptativa: Prevención, Detección, Respuesta y Remediación, gracias a los servicios gestionados: servicio de clasificación del 100% de los programas, procesos y ejecutables en los endpoints y el servicios de Threat Hunting y Análisis Forense, que permite una enforzamiento de la seguridad corporativa continua.

Observaciones

CCN-STIC-1213 PES Panda Adaptive Defense 360

8.2.3 FAMILIA: SISTEMAS DE GESTIÓN DE EVENTOS DE SEGURIDAD

IBM Qradar	
Versión	v7.3.2
Familia	Sistemas de gestión de eventos de seguridad
Fabricante	IBM
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/09/2019
Revisión de Validez	30/04/2022

Descripción

La familia de productos QRadar, plataforma de seguridad inteligente líder en el mercado SIEM, ofrece una visibilidad absoluta y unificada de la seguridad en tiempo real, aplicando tanto en entornos IT como OT.
QRadar recolecta, consolida y correlaciona información de todos los endpoints, dispositivos de red, entornos de las nubes, aplicaciones e incluso de diferentes data-lakes.
Aplica análisis avanzado para priorizar las amenazas y clasificarlas con mayor precisión. Adicionalmente, nuestra tecnología ofrece facilidades de búsquedas profundas para ayudar a encontrar nuevas amenazas de forma proactiva.
QRadar proporciona todas las funcionalidades que una organización necesita para abordar los desafíos de seguridad más importantes, ya sean amenazas avanzadas, amenazas internas, riesgos en la nube u otras vulnerabilidades.
https://www.ibm.com/support/knowledgecenter/es/SS42VS_7.3.2/com.ibm.qradar.doc/qradar_IC_welcome.html

Observaciones

CCN-STIC-1203 Procedimiento de empleo seguro IBM QRadar Security Intelligence Platform

LogICA5 Next Generation SIEM	
Versión	v7.1
Fabricante	Grupo ICA Sistemas y Seguridad
Familia	Sistemas de gestión de eventos de seguridad
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/01/2020
Revisión de Validez	30/06/2023

Descripción

La plataforma española Next Generation SIEM LogICA permite a los analistas de ciberseguridad recopilar logs e información ilimitada de seguridad, detectar ataques basados en anomalías y comportamientos desconocidos así como automatizar la respuesta anteincidentes en entornos IT, OT e IoT.
LogICA NG SIEM recopila información de cualquier fuente interna y externa a la empresa (comercial, propietaria, aplicaciones, cloud), correlando y analizando en tiempo real esa información, permitiendo contextualizary priorizar los incidentes de seguridad tanto internos como externos. Combina los casos de uso de detección más sofisticados con la información más precisa de amenazas y vulnerabilidades zero day gracias a la información de fuentes externas de inteligencia, threat hunting y anomalías de red/usuario. Incorpora, además, un cuadro de mando de gestión del servicio, centralizando la información y facilitando su consumo por parte de la organización.
LogICA permite adaptarse a las necesidades de despliegue de las organizaciones, en modo on-premise, virtual o entorno cloud.

Observaciones

CCN-STIC-1206 PES NGSIEM LogICA

NetWitness	
Versión	v.11
Fabricante	RSA
Familia	Sistemas de gestión de eventos de seguridad
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/12/2019
Revisión de Validez	31/05/2022

Descripción

La plataforma RSA Netwitness es la solución de SIEM evolucionado, con capacidades de visibilidad completa gracias a su modelo de datos unificado pudiendo capturar logs, netflow, tráfico de red y end point de forma integrada, bajo un único motor de análisis y correlación avanzada. Además, incluye funcionalidades necesarias por un SOC para hacer frente a amenazas complejas. RSA Netwitness Platform cuenta además con componentes adicionales como UEBA y SOAR. La solución permite capturar todo tipo de información, permitiendo el análisis avanzado de amenazas, priorización en base al contexto de negocio y haciendo más eficiente el trabajo del analista. Es una plataforma que, gracias su capacidad de análisis, muestra el alcance completo de un ataque a los analistas. Además, gracias a su estrategia Run Anywhere, la plataforma se puede desplegar en cualquier entorno (virtual, cloud, físico, híbrido), así como hacer frente a arquitecturas altamente distribuidas. RSA Netwitness incluye en todos sus clientes +50 feeds de inteligencia, agente para endpoints ilimitados así como el despliegue ilimitado de dispositivos para cubrir cualquier forma de despliegue. https://www.rsa.com/en-us/products/threat-detection-response.

Observaciones

CCN-STIC-1210 Procedimiento de Empleo Seguro RSA Netwitness Platform

8.2.4 FAMILIA: DISPOSITIVOS PARA GESTIÓN DE CLAVES CRIPTOGRÁFICAS

EP543N	
Versión	V.1.7
Familia	Dispositivos para gestión de claves criptográficas
Fabricante	Epicom
Clasificación	RESERVADO
Fecha Inclusión	27/12/2021
Revisión de Validez	31/12/2024



Descripción

Centro de Gestión de cifradores IP EP430GN sobre ordenador seguro EP1140.

Observaciones

EP543X	
Versión	SW v 4.15
Familia	Dispositivos para gestión de claves criptográficas
Fabricante	Epicom
Clasificación	SECRETO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2022



Descripción

Centro de Gestión sobre la plataforma EP1140, que da soporte a los cifradores de la familia EP430, incluidos los modelos EP430TX y EP430GX.

Observaciones

Utilización según PE-2012-49 Procedimiento de Empleo EP430GX v2

8.2.5 FAMILIA: CAPTURA, MONITORIZACIÓN Y ANÁLISIS DE TRÁFICO

GigaVUE (HD8, HD4, HC3, HC2, HC1)	
Versión	version 5.1.01
Fabricante	Gigamon
Familia	Captura, Monitorización y Análisis de Tráfico
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/11/2019
Revisión de Validez	30/04/2022

Descripción

Network Packet Brokers HC/HD Series. Network Packet Brokers de alto rendimiento con soporte de puertos 1g/10g/25g/40g/100g en fibra multimodo o/y monomodo y 100m/1000m/10g en cobre y funcionalidades de filtrado de trafico L2-3-4-7 con motor de DPI, generación de Netflow/IPFix/Metadatos, Cifrado/Descifrado de SSL/TLS (incluyendo protocolos RSA, DHE, ECC, y PFS), Terminación de túneles (GRE, VXLAN, ERSPAN, GMIP), Truncado de paquetes, Eliminación de cabeceras, Enmascarado, De-Duplicación, Clustering, Balanceo, Captura de tráfico para entornos virtuales (VMWare ESX/NSX, Openstack, Kubernetes, AWS, GCP, Azure, Nutanix), simetrización de tráfico para arquitectura HA, Inline Bypass con Heartbeat positivo y negativo, Cambio de medio y velocidad, Bypass HW, TAPsintegrados.

Observaciones

CCN-STIC-1301-Procedimiento de Empleo Seguro Giga VUE-OS 5.1.01 Gigamon

GigaVUE (TA10, TA40, TA100)	
Versión	version 5.1.01
Fabricante	Gigamon
Familia	Captura, Monitorización y Análisis de Tráfico
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/11/2019
Revisión de Validez	30/11/2020

Descripción

Agregadores TA Series (TA10/TA40/TA100)
Agregadores de alto rendimiento con soporte de puertos 1g/10g/25g/40g/100g en fibra multimodo o/y monomodo y 100m/1000m/10g en cobre y funcionalidades de filtrado de trafico L2-3-4, Terminación de túneles (GRE, VXLAN, ERSPAN, GMIP), Clustering, Balanceo, Cambio de medio y velocidad

Observaciones

CCN-STIC-1301-Procedimiento de Empleo Seguro Giga VUE-OS 5.1.01 Gigamon

GigaVUE (GVS-HC101, GVS-HC102, GVS-HC301, GVS-HC302, GVS-HC2A1 y GVS-HC2A2)	
Versión	version 5.9
Fabricante	Gigamon
Familia	Captura, Monitorización y Análisis de Tráfico
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/03/2022
Revisión de Validez	31/08/2024

Descripción

Network Packet Brokers HC Series. Network Packet Brokers de alto rendimiento con soporte de puertos 1g/10g/25g/40g/100g en fibra multimodo o/y monomodo y 100m/1g/10g en cobre y funcionalidades de filtrado de trafico L2-3-4-7 con motor de DPI, generación de Netflow/IPFix/Metadatos, Cifrado/Descifrado de SSL/TLS (incluyendo protocolos RSA, DHE, ECC, y PFS), Terminación de túneles (GRE, VXLAN, ERSPAN, GMIP), Truncado de paquetes, Eliminación de cabeceras, Enmascarado, De-Duplicación, Clustering, Balanceo, Captura de tráfico para entornos virtuales (VMWare ESX/NSX, Openstack, Kubernetes, AWS, GCP, Azure, Nutanix), simetrización de tráfico para arquitectura HA, Inline Bypass con Heartbeat positivo y negativo, Cambio de medio y velocidad, Bypass HW, TAPs integrados.

Observaciones

CCN-STIC-1301 Procedimiento de Empleo Seguro GigaVUE-OS 5.1.01

GigaVUE (GVS-TAC21 y GVS-TAC22)	
Versión	version 5.9
Fabricante	Gigamon
Familia	Captura, Monitorización y Análisis de Tráfico
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/03/2022
Revisión de Validez	31/08/2024

Descripción

Agregadores TA Series. Agregadores de alto rendimiento con soporte de puertos 1g/10g/25g/40g/100g en fibra multimodo o/y monomodo y 100m/1g/10g en cobre y funcionalidades de filtrado de trafico L2-3-4, Terminación de túneles (GRE, VXLAN, ERSPAN, GMIP), Clustering, Balanceo, Cambio de medio y velocidad y Timestamping

Observaciones

CCN-STIC-1301 Procedimiento de Empleo Seguro GigaVUE-OS 5.1.01

8.3 CATEGORÍA: MONITORIZACIÓN DE LA SEGURIDAD

8.3.1 FAMILIA: DISPOSITIVOS DE PREVENCIÓN DE INTRUSIONES

McAfee Network Security Platform (IPS-NS9100, IPS-NS9200, IPS-NS9300 P, IPS-NS9300 S, PS-NS7150, IPS-NS7250, IPS-NS7350, IPS-NS7100, IPS-NS7200, IPS-NS7300, PS-NS5200, IPS-NS5100, IPS-NS3200, IPS-NS3100 y NSM-MAPL-NG)	
Versión	NS Sensor v 9.1.17.100 and NSM v9.1.21.20
Fabricante	McAfee
Familia	Dispositivos de prevención y detección de intrusiones
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/05/2020
Revisión de Validez	31/10/2022

Descripción

McAfee® Network Security Platform (NSP) es un sistema de detección y prevención de intrusiones (IDPS) de próxima generación que descubre y bloquea amenazas de malware sofisticadas en la red. Emplea técnicas avanzadas de detección y emulación, y va más allá de la comparación con patrones para ofrecer protección contra los ataques ocultos con un alto grado de precisión. Para satisfacer las necesidades de las redes más exigentes, la plataforma puede adaptarse hasta 40 Gbit/s con un solo dispositivo y hasta 100 Gbit/s con dispositivos apilados. La integración de la solución de IPS simplifica las operaciones de seguridad mediante la combinación de la información en tiempo real de McAfee Global Threat Intelligence y los datos contextuales completos sobre usuarios, dispositivos y aplicaciones, con el fin de responder de manera rápida y precisa a los ataques que se propagan por la red.
Otras funciones: Administración centralizada, cifrado SSL, y alta disponibilidad y protección de recuperación ante desastre.

Observaciones

CCN-STIC 1302 Procedimiento de Empleo Seguro de McAfee Network Security Platform (NSP)

8.4 CATEGORÍA: PROTECCIÓN DE LAS COMUNICACIONES

8.4.1 FAMILIA: ENRUTADORES

MIL2004-2xHSR-L3



Versión	19.12
Fabricante	SoCe System-on-Chip engineering - Novatronic
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/04/2020
Revisión de Validez	30/09/2022

Descripción

Router Switch gestionado, rugerizado de alta disponibilidad, de 20 puertos cobre 1Gb + 4 puertos fibra hasta 10 GbE. COTS potente, abierto y flexible con capacidades Edge-Computing gracias a sus procesadores multicore CPU, GPU y FPGA Ultrascale. Su arquitectura reconfigurable permite tecnologías HSR y PRP para asegurar el 100% de la transmisión de datos sin interrupciones ni retrasos en la entrega de paquetes incluso cuando hay fallos de red. Cuenta con TSN para una interoperabilidad con ancho de banda garantizado y latencia determinista, sincronización IEEE 1588 v2 PTP y el máximo nivel de seguridad ante ciberataques y otras amenazas. Certificado MIL-STD-461G y MIL-STD-810G, entre otros, está equipado con sistemas electrónicos auxiliares activos y de supervisión, indispensables para los programas de próxima generación, proporcionando una mayor seguridad de la carga útil, un mayor control del sistema y una fácil integración. El chasis cuenta con filtros EMI/EMC, protección de voltajes y temperaturas extremos.

Observaciones

CCN-STIC-1416 Procedimiento de Empleo Seguro MIL2004-2xHSR-L3 SoCe-Novatronic

Aruba 2930F y 2930M Switch Series



Versión	Aruba OS version 16.04
Fabricante	Aruba
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2022

Descripción

Familia de switches y routers para Centros de Datos y Border Routing enfocada a operadores, proveedores de servicios y empresas. Se soportan tecnologías tales como MPLS/VPLS, Carrier Ethernet y EVPN, con equipos dotados de buffer ultra-profundos. Los equipos son compactos y proporcionan gran densidad de puertos a velocidades 1/10/25/40/50/100 Gbps en una unidad de rack.

El despliegue de soluciones IP Fabric para datacenter puede automatizarse desde una máquina virtual residente en el propio switch. Se soportan arquitecturas Clos (Leaf and Spine) sin necesidad de controlador externo. También se soporta la interconexión de Datacenters mediante Leaf especializados

Observaciones

CCN-STIC-647C Seguridad en conmutadores HPE Aruba

Aruba 3810M Switch Series



Versión	Aruba OS version 16.04
Fabricante	Aruba
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2022

Descripción

Familia de switches y routers para Centros de Datos y Border Routing enfocada a operadores, proveedores de servicios y empresas. Se soportan tecnologías tales como MPLS/VPLS, Carrier Ethernet y EVPN, con equipos dotados de buffer ultra-profundos. Los equipos son compactos y proporcionan gran densidad de puertos a velocidades 1/10/25/40/50/100 Gbps en una unidad de rack.

El despliegue de soluciones IP Fabric para datacenter puede automatizarse desde una máquina virtual residente en el propio switch. Se soportan arquitecturas Clos (Leaf and Spine) sin necesidad de controlador externo. También se soporta la interconexión de Datacenters mediante Leaf especializados

Observaciones

CCN-STIC-647C Seguridad en conmutadores HPE Aruba

Aruba 5400R Switch Series



Versión	Aruba OS version 16.04
Fabricante	Aruba
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2022

Descripción

Familia de switches y routers para Centros de Datos y Border Routing enfocada a operadores, proveedores de servicios y empresas. Se soportan tecnologías tales como MPLS/VPLS, Carrier Ethernet y EVPN, con equipos dotados de buffer ultra-profundos. Los equipos son compactos y proporcionan gran densidad de puertos a velocidades 1/10/25/40/50/100 Gbps en una unidad de rack.

El despliegue de soluciones IP Fabric para datacenter puede automatizarse desde una máquina virtual residente en el propio switch. Se soportan arquitecturas Clos (Leaf and Spine) sin necesidad de controlador externo. También se soporta la interconexión de Datacenters mediante Leaf especializados

Observaciones

CCN-STIC-647C Seguridad en conmutadores HPE Aruba

Dell EMC Networking SmartFabric (Modelos: S3048-ON, S4048-ON, S4048T-ON, S4112F-ON, S4112T-ON, S4128F-ON, S4128T-ON, S4148F-ON, S4148T-ON, S4148U-ON, MX5108n, S4248FB-ON, S4248FBL-ON, S6010-ON, Z9100-ON, MX9116n, S5212F-ON, S5224F-ON, S5232F-ON, S5248F-ON

Versión	OS 10 Build: 10.5.1.3.
Fabricante	Dell Computer
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/12/2020
Revisión de Validez	31/05/2022

Descripción

Dell EMC Smart Fabric OS10 es el sistema operativo de red (NOS) que se utiliza en las familias de enrutadores y conmutadores de las serie N (algunos modelos), serie S, serie Z y serie MX de Dell EMC Networking (las plataformas HW que actualmente soportanOS10 son N3200, S3048-ON, S4048-ON, S4048T-ON, S4112F-ON, S4112T-ON, S4128F-ON, S4128T-ON, S4148F-ON, S4148T-ON, S4148U-ON, S4248FB-ON, S4248FBL-ON, S6010-ON, S5212F-ON, S5224F-ON, S5232F-ON, S5248F-ON, S5296F-ON, Z9100-ON, Z9264F-ON, Z9332F-ON, MX5108n yMX9116n). Dell EMC SmartFabric OS10 es un sistema operativo de red (NOS) que admite múltiples arquitecturas y entornos. La solución SmartFabric OS10 permite la desagregación en varias capas de la funcionalidad de red. SmartFabric OS10 comprende la administración, monitorización y funcionalidad completa y estándar de la industria de redes de nivel 2 y nivel 3 a través de interfaces CLI, SNMP y REST. Los usuarios pueden elegir sus propias aplicaciones de organización, gestión, supervisión y redes de terceros. Para desarrollar redes escalables L2 y L3, SmartFabric OS10 ofrece una solución modular y desagregada en una única imagen binaria.

Observaciones

CCN-STIC-1429 PES DELL EMC Networking

SLX Product Series (SLX 9740 y SLX 9540)

Versión	20.2.1aa
Fabricante	Extreme Networks
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/09/2021
Revisión de Validez	31/07/2023



Descripción

Familia de switches y routers para Centros de Datos y Border Routing enfocada a operadores, proveedores de servicios y empresas. Se soportan tecnologías tales como MPLS/VPLS, Carrier Ethernet y EVPN, con equipos dotados de buffer ultra-profundos. Los equipos son compactos y proporcionan gran densidad de puertos a velocidades 1/10/25/40/50/100 Gbps en una unidad de rack.

El despliegue de soluciones IP Fabric para datacenter puede automatizarse desde una máquina virtual residente en el propio switch. Se soportan arquitecturas Clos (Leaf and Spine) sin necesidad de controlador externo. También se soporta la interconexión de Datacenters mediante Leaf especializados

Observaciones

CCN-STIC-1430 PES Switches Extreme Networks SLXOS

SLX Product Series (SLX9150, SLX9250 y SLX9640)	
Versión	20.1.1aa
Fabricante	Extreme Networks
Familia	Enrutadores
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/02/2021
Revisión de Validez	31/07/2023





Descripción

Familia de switches y routers para Centros de Datos y Border Routing enfocada a operadores, proveedores de servicios y empresas. Se soportan tecnologías tales como MPLS/VPLS, Carrier Ethernet y EVPN, con equipos dotados de buffer ultra-profundos. Los equipos son compactos y proporcionan gran densidad de puertos a velocidades 1/10/25/40/50/100 Gbps en una unidad de rack.

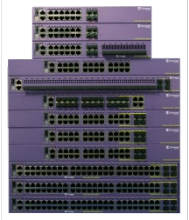
El despliegue de soluciones IP Fabric para datacenter puede automatizarse desde una máquina virtual residente en el propio switch. Se soportan arquitecturas Clos (Leaf and Spine) sin necesidad de controlador externo. También se soporta la interconexión de Datacenters mediante Leaf especializados.

Observaciones

CCN-STIC-1430 PES Switches Extreme Networks SLXOS

8.4.2 FAMILIA: SWITCHES

Summit X440-G2 Series: X440-G2-12t-10GE4, X440-G2-12p-10GE4, X440-G2-24t-10GE4 X440-G2-24p-10GE4, X440-G2-48t-10GE4, X440-G2-48p-10GE4, X440-G2-24t-10GE4-DC, X440-G2-48t-10GE4-DC, X440-G2-24x-10GE4, X440-G2-24fx-GE4, X440-G2-12t8fx-GE4, X440-G2-24t-GE4	
Versión	EXOS v22.3.1.4-patch1CC-2
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/06/2019
Revisión de Validez	31/08/2022



Descripción

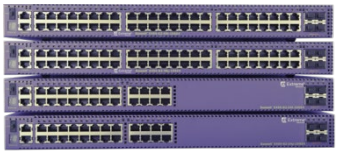
Conmutador apilable de alto rendimiento, posicionado como equipo de acceso. Proporciona conmutación inteligente de Nivel 2 y routing básico de Nivel 3, con interfaces 10/100/1000 Mbps así como 10 Gb. Existen versiones PoE y no PoE y de puertos de fibra óptica y puede apilarse también con otras familias de switches Extreme Networks

Observaciones

CCN-STIC-642B Seguridad en Extreme Networks EXOS

Summit x450-G2 Series:
X450-G2-24t-GE4, X450-G2-24p-GE4, X450-G2-48t-GE4, X450-G2-48p-GE4, X450-G2-24t-10GE4, X450-G2-24p-10GE4, X450-G2-48t-10GE4, X450-G2-48p-10GE4, X450-G2-24p-10GE4-FB-715-TAA, X450-G2-48p-10GE4-FB-1100-TAA,X450-G2-24t-GE4-FB-TAA, X450

Versión	EXOS v22.3.1.4-patch1CC-2
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/06/2019
Revisión de Validez	31/08/2022



Descripción

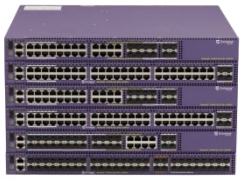
Conmutador apilable de alto rendimiento, posicionado como equipo de acceso de altas prestaciones. Proporciona conmutación avanzada de Nivel 2 y routing de Nivel 3, con interfaces 10/100/1000 Mbps, así como 10Gb. Existen versiones PoE y no PoE, y puede apilarse con otras familias de switches Extreme Networks.

Observaciones

CCN-STIC-642B Seguridad en Extreme Networks EXOS

Summit X460-G2 Series:
X460-G2-24t-10GE4, X460-G2-48t-10GE4, X460-G2-24p-10GE4, X460-G2-48p-10GE4, X460-G2-24x-10GE4, X460-G2-48x-10GE4, X460-G2-24t-GE4, X460-G2-48t-GE4, X460-G2-24p-GE4, X460-G2-48p-GE4

Versión	EXOS v22.3.1.4-patch1CC-2
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/06/2019
Revisión de Validez	31/08/2022



Descripción

Conmutador apilable de alta rendimiento, posicionado como equipo de acceso de altas prestaciones y backbone de redes medias. Proporciona conmutación avanzada de Nivel 2 y de Nivel 3, con soporte de protocolos de alta complejidad (BGP, MPLS, etc). con interfaces 10/100/1000 Mbps, así como 10Gb y 40 Gb. Existen versiones PoE y no PoE, y puede apilarse con otras familias de switches Extreme Networks.

Observaciones

CCN-STIC-642B Seguridad en Extreme Networks EXOS

Summit X620 Series:
X620–16x, X620–16t, X620–10x, X620–8t-2x



Versión	EXOS v22.3.1.4-patch1CC-2
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/06/2019
Revisión de Validez	31/08/2022

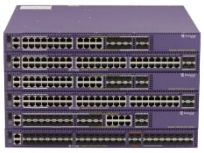
Descripción

Conmutador apilable de alto rendimiento, proporcionando servicios avanzados de switching y enrutamiento básico. Destinado como concentrador de redes pequeñas y también para conexión de servidores. Soporta interfaces 100Mb, 1Gb y 10Gb. Asimismo puede proporcionar PoE. El equipo es apilable también con otras familias de switches Extreme Networks.

Observaciones

CCN-STIC-642B Seguridad en Extreme Networks EXOS

Summit x670-G2 Series:
X670-G2-72x, X670-G2-48x-4q, X670-G2-48x-4q-FB-AC-TAA



Versión	EXOS v22.3.1.4-patch1CC-2
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/06/2019
Revisión de Validez	31/08/2022

Descripción

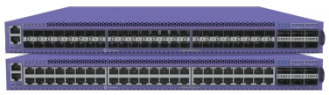
La familia de productos x670-G2 proporciona servicios avanzados de switching y routing, pudiendo utilizarse como equipo concentrador o bien como una solución Top of Rack para una granja de servidores, gracias a su baja latencia y capacidades avanzadas. Se soportan interfaces 10Gb y 40Gb. El equipo es apilable también con otras familias de switches Extreme Networks.

Observaciones

CCN-STIC-642B Seguridad en Extreme Networks EXOS

Summit X690 Series:
(X690-48x-2q-4c, X690-48t-2q-4c)

Versión	EXOS v22.3.1.4-patch1CC-2
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/06/2019
Revisión de Validez	31/08/2022



Descripción

La familia de productos x690 proporciona servicios avanzados de switching y routing, pudiendo utilizarse como equipo concentrador o bien como una solución Top of Rack para una granja de servidores, gracias a su baja latencia y capacidades avanzadas. Se soportan interfaces 10Gb, 25Gb, 40Gb, 50 Gb y 100Gb. El equipo es apilable también con otras familias de switches Extreme Networks.

Observaciones

CCN-STIC-642B Seguridad en Extreme Networks EXOS

Summit X870 Series:
(X870-32c, X870-96x-8c)

Versión	EXOS v22.3.1.4-patch1CC-2
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/06/2019
Revisión de Validez	31/08/2022



Descripción

La familia de productos x870 proporciona servicios de switching y de routing. Soporta velocidades de 10 Gb, 25Gb, 40GB, 50Gby 100GB en un formato compacto de 1U. La conmutación directa de baja latencia y un conjunto de características avanzadas lo hacenideal para centros de datos de alto rendimiento. El equipo es apilable también con otras familias de switches Extreme Networks.

Observaciones

CCN-STIC-642B Seguridad en Extreme Networks EXOS

MIL2004-2xHSR-L3



Versión	19.12
Fabricante	SoCe System-on-Chip engineering - Novatronic
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/04/2020
Revisión de Validez	30/09/2022

Descripción

Router Switch gestionado, rugerizado de alta disponibilidad, de 20 puertos cobre 1Gb + 4 puertos fibra hasta 10 GbE. COTS potente, abierto y flexible con capacidades Edge-Computing gracias a sus procesadores multicore CPU, GPU y FPGA Ultrascale. Su arquitectura reconfigurable permite tecnologías HSR y PRP para asegurar el 100% de la transmisión de datos sin interrupciones ni retrasos en la entrega de paquetes incluso cuando hay fallos de red. Cuenta con TSN para una interoperabilidad con ancho de banda garantizado y latencia determinista, sincronización IEEE 1588 v2 PTP y el máximo nivel de seguridad ante ciberataques y otras amenazas. Certificado MIL-STD-461G y MIL-STD-810G, entre otros, está equipado con sistemas electrónicos auxiliares activos y de supervisión, indispensables para los programas de próxima generación, proporcionando una mayor seguridad de la carga útil, un mayor control del sistema y una fácil integración. El chasis cuenta con filtros EMI/EMC, protección de voltajes y temperaturas extremos.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

Alcatel-Lucent Enterprise OmniSwitch Serie 6465 (OS6465-P6, OS6465-P12, OS6465-P28, OS6465T-P12 y OS6465T-12)



Versión	AOS 8.6.R11.
Fabricante	Alcatel-Lucent Enterprise
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/04/2021
Revisión de Validez	30/09/2023

Descripción

Familia de conmutadores L2+ con puertos 1G y 10G, preparados para entorno industrial, con amplio rango de temperaturas de funcionamiento (-40ºC a +75ºC). Diseñados como equipos de acceso en redes de tipo industrial, transportes o utilities.
https://www.al-enterprise.com/es-es/productos/conmutadores

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS

Alcatel-Lucent Enterprise OmniSwitch Serie 6560 (OS6560-P24Z8, OS6560-P24Z24, OS6560-P48Z16, OS6560-24Z8, OS6560-24Z24, OS6560-24X4, OS6560-P24X4, OS6560-48X4, OS6560-P48X4 y OS6560-X10)



Versión	AOS 8.6.R11.
Fabricante	Alcatel-Lucent Enterprise
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/04/2021
Revisión de Validez	30/09/2023

Descripción

Familia de conmutadores L3 compactos apilables con alta densidad de puertos 1GE, Multigigabit ethernet 1/2.5 GigE y enlaces 10GE, diseñados como equipos de acceso en redes convergentes de alta capacidad.
https://www.al-enterprise.com/es-es/productos/conmutadores

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS

Alcatel-Lucent Enterprise OmniSwitch Serie 6860 (OS6860-24, OS6860-P24, OS6860-48, OS6860-P48, OS6860E-24, OS6860E-P24, OS6860E-48, OS6860E-P48, OS6860E-U28 y OS6860E-P24Z8)



Versión	AOS 8.6.R11.
Fabricante	Alcatel-Lucent Enterprise
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/04/2021
Revisión de Validez	30/09/2023

Descripción

OS6860: Familia de conmutadores L3+ compactos apilables con alta densidad de puertos 1GE, Multigigabit ethernet 1/2.5/5/10 GigE y enlaces 10GE, 25GE y 100GE, diseñadas para redes convergentes. Con funciones de Acceso unificado avanzadas que permiten la creación de redes orientadas a las aplicaciones. Puede supervisar y controlar las aplicaciones de la red mediante capacidades de Deep Packet Inspection (DPI).
https://www.al-enterprise.com/es-es/productos/conmutadores

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS

Alcatel-Lucent Enterprise OmniSwitch Serie 6865 (OS6865-P16X, OS6865-U12X y OS6865-U28X)	
Versión	AOS 8.6.R11.
Fabricante	Alcatel-Lucent Enterprise
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/04/2021
Revisión de Validez	30/09/2023



Descripción

Familia de conmutadores L3+ con puertos 1G y 10G, preparados para entorno industrial o redes de misión crítica como transportes y utilities, con amplio rango de temperaturas de funcionamiento (-40ºC a +75ºC).
https://www.al-enterprise.com/es-es/productos/conmutadores

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS

Alcatel-Lucent Enterprise OmniSwitch Serie 6900 (OS6900-X20, OS6900-X40, OS6900-T20, OS6900-T40, OS6900-X72, OS6900-Q32, OS6900-V72 y OS6900-C32)	
Versión	AOS 8.6.R11.
Fabricante	Alcatel-Lucent Enterprise
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/04/2021
Revisión de Validez	30/09/2023



Descripción

Familia de conmutadores L3+ compactos apilables de alta densidad 10GE, 25GE, 40GE y 100GE. Diseñadas para que sean flexibles. Pueden instalarse como conmutadores convergentes situados en la parte superior del bastidor (TOR) o tipo spine para entornos de Data Centers y también como dispositivos de agregación y de núcleo en una red de campus.
https://www.al-enterprise.com/es-es/productos/conmutadores

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS

Alcatel-Lucent Enterprise OmniSwitch Serie 9900 (OmniSwitch 9907 Chassis, OS9907-CFM, OS99-CMM, OS99-XNI-48, OS99-XNI-U48, OS99-GNI-48, OS99-GNI-P48, OS99-CNI-U8, OS99-XNI-P24Z8, OS99-XNI-P48Z16, OS99-XNI-U12Q, OS99-XNI-U24, OS99-XNI-U48 y OS99-XNI-UP24Q2)



Versión	AOS 8.6.R11.
Fabricante	Alcatel-Lucent Enterprise
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/04/2021
Revisión de Validez	30/09/2023

Descripción

Conmutador LAN L3+ con chasis modular de alta capacidad de interfaces 1GE, 10GE y 100GE para conmutación segura y con alta disponibilidad en el núcleo de las redes empresariales, campus y redes Metro Ethernet.
https://www.al-enterprise.com/es-es/productos/conmutadores

Observaciones

CCN-STIC-1410 Procedimiento de Empleo Seguro OMNISWITCH AOS

Series AlliedWare Plus x930 (x930-28GTX, x930-28GPX, x930-28GSTX, x930-52GTX, x930-52GPX) y x950 (x950-28XSQ y x950-28XTQm)



Versión	Software Version 5.5.0-0.6
Fabricante	Allied Telesys
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/10/2019
Revisión de Validez	30/04/2022

Descripción

Switches apilables Layer 3 con puertos Gigabit. Ofrecen flexibilidad, fiabilidad y alto rendimiento al estar orientados a soluciones de core y distribución de redes. Vienen con opciones de 24 y 48 puertos con uplinks de 10G y 40G. Son apilables hasta 8 unidades gracias a la tecnología Virtual Chassis Stacking (VCStack™) que permite crear pilas con equipos separados hasta 40 km.Están equipados con el sistema operativo AlliedWare Plus. Entre sus características más reseñables, destacan:

- Soporte de AMF para gestión avanzada de redes convergentes
- Protocolos para redes flexibles como EPSR, G.8032 o UDLD
- Monitorización activa de fibra (AFM)
- Análisis de tráfico sFlow
- POE continuo
- Layer 3: RIP, OSPF, BGP, VRF
- Controlador wireless

Observaciones

CCN-STIC-1422 Procedimiento de empleo Seguro AlliedWare Plus (AW+) versión 5.5.0-0.6

Series AlliedWare Plus x550 (X550-18XTQ, X550-18XSQ, X550-18XSPQm) y x530-x530L (X530-28GPXm, X530-28GPXm, X530-52GTXm, X530-52GPXm, X530L-28GTX, X530L-28GPX, X530L-52GTX, X530L-52GPX)



Versión	Software Version 5.5.0-0.6
Fabricante	Allied Telesys
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/10/2019
Revisión de Validez	30/04/2022

Descripción

Switches apilables Layer 3 con puertos Gigabit. Ofrecen flexibilidad, fiabilidad y alto rendimiento al estar orientados a soluciones de core y distribución de redes. Vienen con opciones de 24 y 48 puertos con uplinks de 10G y 40G. Son apilables hasta 8 unidades gracias a la tecnología Virtual Chassis Stacking (VCStack™) que permite crear pilas con equipos separados hasta 40 km.Están equipados con el sistema operativo AlliedWare Plus. Entre sus características más reseñables, destacan:

- Soporte de AMF para gestión avanzada de redes convergentes
- Protocolos para redes flexibles como EPSR, G.8032 o UDLD
- Monitorización activa de fibra (AFM)
- Análisis de tráfico sFlow
- POE continuo
- Layer 3: RIP, OSPF, BGP, VRF
- Controlador wireless

Observaciones

CCN-STIC-1422 Procedimiento de empleo Seguro AlliedWare Plus (AW+) versión 5.5.0-0.6

Series AlliedWare Plus x230 (X230-10GP, X230-10GT, X230-18GP, X230-18GT, X230-28GP, X230-28GT, X230L-17GT, X230L-26GT) y x200 (X220-28GS, X220-52GP, X220-52GT)



Versión	Software Version 5.5.0-0.6
Fabricante	Allied Telesys
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/10/2019
Revisión de Validez	30/04/2022

Descripción

Switches apilables Layer 3 con puertos Gigabit. Ofrecen flexibilidad, fiabilidad y alto rendimiento al estar orientados a soluciones de core y distribución de redes. Vienen con opciones de 24 y 48 puertos con uplinks de 10G y 40G. Son apilables hasta 8 unidades gracias a la tecnología Virtual Chassis Stacking (VCStack™) que permite crear pilas con equipos separados hasta 40 km.Están equipados con el sistema operativo AlliedWare Plus. Entre sus características más reseñables, destacan:

- Soporte de AMF para gestión avanzada de redes convergentes
- Protocolos para redes flexibles como EPSR, G.8032 o UDLD
- Monitorización activa de fibra (AFM)
- Análisis de tráfico sFlow
- POE continuo
- Layer 3: RIP, OSPF, BGP, VRF
- Controlador wireless

Observaciones

CCN-STIC-1422 Procedimiento de empleo Seguro AlliedWare Plus (AW+) versión 5.5.0-0.6

Series AlliedWare Plus SBX81CFC960 (SBx81CFC960, SBx81GP24, SBx81GT24, SBx81GS24a, SBx81GC40, SBx81XLEM) y SBX908 GEN2 (XEM2-8XSTm, XEM2-12XTm, XEM2-12XT, XEM2-12XS, XEM2-4QS, XEM2-1CQ)

Versión	Software Version 5.5.0-0.6
Fabricante	Allied Telesys
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/10/2019
Revisión de Validez	30/04/2022



Descripción

Switches apilables Layer 3 con puertos Gigabit. Ofrecen flexibilidad, fiabilidad y alto rendimiento al estar orientados a soluciones de core y distribución de redes. Vienen con opciones de 24 y 48 puertos con uplinks de 10G y 40G. Son apilables hasta 8 unidades gracias a la tecnología Virtual Chassis Stacking (VCStack™) que permite crear pilas con equipos separados hasta 40 km.Están equipados con el sistema operativo AlliedWare Plus. Entre sus características más reseñables, destacan:

- Soporte de AMF para gestión avanzada de redes convergentes
- Protocolos para redes flexibles como EPSR, G.8032 o UDLD
- Monitorización activa de fibra (AFM)
- Análisis de tráfico sFlow
- POE continuo
- Layer 3: RIP, OSPF, BGP, VRF
- Controlador wireless

Observaciones

CCN-STIC-1422 Procedimiento de empleo Seguro AlliedWare Plus (AW+) versión 5.5.0-0.6

Series AlliedWare Plus x510 (X510-28GSX)



Versión	Software Version 5.5.0-0.6
Fabricante	Allied Telesys
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/10/2019
Revisión de Validez	30/04/2022

Descripción

Switches apilables Layer 3 con puertos Gigabit. Ofrecen flexibilidad, fiabilidad y alto rendimiento al estar orientados a soluciones de core y distribución de redes. Vienen con opciones de 24 y 48 puertos con uplinks de 10G y 40G. Son apilables hasta 8 unidades gracias a la tecnología Virtual Chassis Stacking (VCStack™) que permite crear pilas con equipos separados hasta 40 km.Están equipados con el sistema operativo AlliedWare Plus. Entre sus características más reseñables, destacan:

- Soporte de AMF para gestión avanzada de redes convergentes
- Protocolos para redes flexibles como EPSR, G.8032 o UDLD
- Monitorización activa de fibra (AFM)
- Análisis de tráfico sFlow
- POE continuo
- Layer 3: RIP, OSPF, BGP, VRF
- Controlador wireless

Observaciones

CCN-STIC-1422 Procedimiento de empleo Seguro AlliedWare Plus (AW+) versión 5.5.0-0.6

Dell Networking C-Series (C9010 y C1048P)

Versión	V9.14
Fabricante	Dell Computer
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/06/2020
Revisión de Validez	30/11/2022

Descripción

Este switch ofrece una plataforma de conmutación modular, de varias velocidades. Puede admitir redes de grandes empresas, medianas empresas y campus. Su plataforma de 8U cuenta con ranuras para hasta 10 módulos de tarjetas de línea, 2 módulos de procesadores de ruta, 3 módulos de ventiladores y 4 módulos de fuente de alimentación. El chasis viene equipado con un plano posterior integrado y compatible con varias velocidades 100GbE. El C1048 incluye 48 puertos 10/100/1000Base-T POE+ para el acceso de usuario y 2 puertos uplink SFP+ para la conectividad con el C9010

Observaciones

CCN-STIC-1402 Procedimiento de empleo seguro DELL EMC OS 9.14

Dell Networking S-Series 10GbE (S5048F, S4048-ON, S4048T-ON)	
Versión	V9.14
Fabricante	Dell Computer
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/06/2020
Revisión de Validez	30/11/2022

Descripción

Estos switches 10GbE flexibles ofrecen las siguientes prestaciones:
- S4048-ON es un switch de baja latencia y alta densidad para la parte superior del rack con 48 puertos 10GbE SFP+ y 6 puertos 40 GbE (o 72 puertos 10 GbE en modo de transición), así comoun rendimiento de 720 Gb/s máscimo. Es compatible con el entorno Open Network Install Environment (ONIE).
- S5000 ofrece un diseño modular que permite añadir módulos Ethernet y Fibre Channel. El módulo Fibre Channel es compatible con el modo NPG los servicios completos de estructura Fibre Channel. Admite 4 módulos.

Observaciones

CCN-STIC-1402 Procedimiento de empleo seguro DELL EMC OS 9.14

Dell Networking S-Series 1GbE (S3124, S3124P, S3124F, S3148, S3148P, S3048-ON)	
Versión	V9.14
Fabricante	Dell Computer
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/06/2020
Revisión de Validez	30/11/2022

Descripción

Estos switches 1GbE ofrecen las siguientes prestaciones:
- Proporcionan baja latencia y alta densidad con redundancia de hardware y software..
- Ofrecen diseños de Active Fabric con el uso de switches principales de la serie S o Z para crear una arquitectura de red de centro de datos 1/10/40GbE de dos niveles.

Observaciones

CCN-STIC-1402 Procedimiento de empleo seguro DELL EMC OS 9.14

Dell Networking S-Series 25/40/50/100GbE (S6010-ON, S6100-ON)	
Versión	V9.14
Fabricante	Dell Computer
Familia	Switches
Tipo	Producto
Categoría ENS	ALTA
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/06/2020
Revisión de Validez	30/11/2022

Descripción

Los Swtiches Serie S ofrecen una solución preparada para redes definidas por software, con las siguientes pestaciones:
- Alta densidad para las implementaciones basadas en 25/40/50/100GbE para la parte superior del rack, en medio de la fila o al final dela fila.
- Selección de switches 40GbE S5048F-ON, S6000-ON y S6010-ON, además del switch modular 10/25/40/50/100GbE S6100-ON.
- Módulos S6100-ON que incluyen: 16 puertos 14GbE, 8 puertos 100GbE, módulo combinado de 4 puertos 100GbE CXP y 4 puertos 100GbE

Observaciones

CCN-STIC-1402 Procedimiento de empleo seguro DELL EMC OS 9.14

Dell Networking Z-Series (Z9100-ON)	
Versión	V9.14
Fabricante	Dell Computer
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/06/2020
Revisión de Validez	30/11/2022

Descripción

Este switch Open Networking de formato fijo y preparado para redes definidas por software (SDN) se ha diseñado para centros de datos y ofrece las siguientes prestaciones:
- Switch multivelocidad con opciones 10/25/40/50/100GbE.
- Alta densidad con hasta32 puertos 100GbE en 1U.
- Selección de los principales sistemas operativos de red.
- Vía de acceso fácil a las SDN para una parte o la totalidad de su entorno de producción.

Observaciones

CCN-STIC-1402 Procedimiento de empleo seguro DELL EMC OS 9.14

SLX Product Series (SLX9150, SLX9250 y SLX9640)	
Versión	20.1.1aa
Fabricante	Extreme Networks
Familia	Switches
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/02/2021
Revisión de Validez	31/07/2023





Descripción

Familia de switches y routers para Centros de Datos y Border Routing enfocada a operadores, proveedores de servicios y empresas. Se soportan tecnologías tales como MPLS/VPLS, Carrier Ethernet y EVPN, con equipos dotados de buffer ultra-profundos. Los equipos son compactos y proporcionan gran densidad de puertos a velocidades 1/10/25/40/50/100 Gbps en una unidad de rack.

El despliegue de soluciones IP Fabric para datacenter puede automatizarse desde una máquina virtual residente en el propio switch. Se soportan arquitecturas Clos (Leaf and Spine) sin necesidad de controlador externo. También se soporta la interconexión de Datacenters mediante Leaf especializados.

Observaciones

CCN-STIC-1430 PES Switches Extreme Networks SLXOS.

8.4.3 FAMILIA: CORTAFUEGOS

Stormshield Network Security UTM/NG-Firewall (Appliances desde SN200 a SN6100 en 4 compilaciones distintas: S, M, L y XL).	
Versión	3.10.1
Fabricante	Stormshield SAS
Familia	Cortafuegos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/06/2020
Revisión de Validez	30/09/2022



Descripción

Firewalls de nueva generación de capa 7, IPS y concentrador de túneles VPN. Con capacidades de bloqueo de amenazas avanzadas, ataques de día cero, filtrado de navegación web o gestión de vulnerabilidades.
El mismo equipamiento realiza inspección profundade protocolos OT, además de IT.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

8.4.4 FAMILIA: PROXIES

Forcepoint On-Premise Security	
Versión	8.5
Fabricante	Forcepoint
Familia	Proxies
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/05/2021
Revisión de Validez	31/10/2023

Descripción

Los dispositivos Forcepoint Web Security realizan la función de proxy de navegación segura integrando múltiples motores de clasificación de contenidos y análisis de seguridad en tiempo real con capacidad de inspección de tráfico seguro y también análisis de datos salientes con capacidad para aplicar políticas frente a fugas de información. Las plataformas funcionan como proxies directos http, https, ftp y SOCKS para la protección y control de usuarios y puestos de conexión. El propósito de estos dispositivos es proporcionar una capa de seguridad entre la red Interna y una o más redes externas (típicamente una red corporativa e Internet), aislando el tráfico de los usuarios a nivel de aplicación y proporcionando además diferentes mecanismos de optimización WAN para el tráfico que procesan.

Observaciones

CCN-STIC-1507 Procedimiento de Empleo Seguro Forcepoint On-premise Security 8.5

8.4.5 FAMILIA: PASARELAS DE INTERCAMBIO DE DATOS

PSTfile	
Versión	v4.4.2
Fabricante	Autek Ingeniería
Familia	Pasarelas seguras de intercambio de datos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2022



Descripción

PSTfile es un dispositivo de protección de perímetro de la familia PSTgateways. Permite el intercambio controlado de ficheros entre dominios de seguridad. Se establece una correspondencia entre carpetas, en servidores de ficheros de ambas redes y PSTfile,automáticamente, mueve o copia los ficheros del origen al destino. Soporta los protocolos FTP, FTPS, SFTP y SMB. La transferencia de ficheros desde el dominio de alta seguridad al de baja requiere autorización mediante firma digital.

Observaciones

Procedimiento de empleo seguro: CCN-STIC-1401 Configuración segura de pasarelas de AUTEK

PSTmail	
Versión	v3.0.5
Fabricante	Autek Ingeniería
Familia	Pasarelas seguras de intercambio de datos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2022



Descripción

PSTmail es un dispositivo de protección de perímetro de la familia PSTgateways. Permite el intercambio controlado de correo electrónico entre dominios de seguridad. Posibilita el empleo de direcciones de correo de redes externas, desde una red interna, más segura. Soporta las versiones seguras de los protocolos de correo. Los mensajes de salida requieren autorización mediante firma digital (S/MIME).

Observaciones

Procedimiento de empleo seguro: CCN-STIC-1401 Configuración segura de pasarelas de AUTEK

8.4.6 FAMILIA: DIODOS DE DATOS

PSTdiode	
Versión	v1.3.1-A
Fabricante	Autek Ingeniería
Familia	Diodos de datos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/09/2019
Revisión de Validez	31/08/2024



Descripción

El diodo de datos hardware PSTdiode es un dispositivo de protección de perímetro que permite la transferencia de información en un único sentido entre dos dominios de seguridad con garantía física de transmisión unidireccional. Su aplicación principal esla introducción de información en una red aislada en entornos clasificados. También se puede aplicar para extraer información de una red de control industrial en entornos de infraestructuras críticas.
En ambos casos se garantiza que no existe tráfico en el sentido inverso.
Existen modelos de transferencia de ficheros y tráfico UDP.

Observaciones

Procedimiento de empleo seguro: CCN-STIC 1408 Procedimiento de empleo seguro Diodo Autek Ingeniería

8.4.7 FAMILIA: REDES PRIVADAS VIRTUALES: IPSEC

Bittium SafeMove VPN Client for Android	
Versión	Android (genérico): 1.2.159, Android (Bittium Tough Mobile R): 2020-04-27 @ granite @ c5e05cb
Fabricante	Bittium SafeMove Oy
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/04/2021
Revisión de Validez	30/06/2023

Descripción

SafeMove Mobile VPN forma parte de la Bittium Secure Suite. Proporciona los servicios de firewall y VPN IPSec a las plataformas Android y Windows conectadas de forma remota a la infraestructura corporativa, y está concebido para ser un servicio siempre activo y aplicado a todo el tráfico de red que entra y sale del dispositivo. Nada sensible se escapa, nada dañino puede entrar. La SafeMove Mobile VPN es una solución cliente-servidor. El cliente instalado en el dispositivo se conecta a la puerta de enlace Bittium SafeMove VPN Gateway instalada en el servidor, con el resto de los componentes de la Bittium Secure Suite, que son el gestor de dispositivos (MDM), el gestor de las aplicaciones instaladas en los dispositivos (solo Android) y los servicios de comprobación de la integridad (solo Android). Usado en combinación con los smartphones de la familia Bittium Tough Mobile proporciona servicios de recuperación de los registros de auditoría y actualización OTA del firmware de los dispositivos.
Más información de Bittium SafeMove® Mobile VPN:
https://www.bittium.com/secure-communications-connectivity/bittium-safemove-mobile-vpn

Observaciones

PE-2021-7-Procedimiento de empleo seguro Bittium SafeMove VPN (Android y Windows)

Bittium SafeMove VPN Client for Windows	
Versión	4.11.722
Fabricante	Bittium SafeMove Oy
Familia	Redes privadas virtuales: IPSec
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/04/2021
Revisión de Validez	30/06/2023

Descripción

SafeMove Mobile VPN forma parte de la Bittium Secure Suite. Proporciona los servicios de firewall y VPN IPSec a las plataformas Android y Windows conectadas de forma remota a la infraestructura corporativa, y está concebido para ser un servicio siempre activo y aplicado a todo el tráfico de red que entra y sale del dispositivo. Nada sensible se escapa, nada dañino puede entrar. La SafeMove Mobile VPN es una solución cliente-servidor. El cliente instalado en el dispositivo se conecta a la puerta de enlace Bittium SafeMove VPN Gateway instalada en el servidor, con el resto de los componentes de la Bittium Secure Suite, que son el gestor de dispositivos (MDM), el gestor de las aplicaciones instaladas en los dispositivos (solo Android) y los servicios de comprobación de la integridad (solo Android). Usado en combinación con los smartphones de la familia Bittium Tough Mobile proporciona servicios de recuperación de los registros de auditoría y actualización OTA del firmware de los dispositivos.
Más información de Bittium SafeMove® Mobile VPN: https://www.bittium.com/secure-communications-connectivity/bittium-safemove-mobile-vpn

Observaciones

PE-2021-7-Procedimiento de empleo seguro Bittium SafeMove VPN (Android y Windows)

8.4.8 FAMILIA: HERRAMIENTAS PARA COMUNICACIONES MÓVILES SEGURAS

COMSec Admin +	
Versión	v4.2
Fabricante	Indra
Familia	Herramientas para comunicaciones móviles seguras
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/05/2021
Revisión de Validez	31/10/2023



Descripción

COMSec Admin+ es una solución global de comunicaciones seguras que proporciona servicios cifrados de voz, mensajería instantánea y videoconferencia sobre teléfonos móviles empleando cualquier red celular, inalámbrica o satelital.
Con su alto nivel de seguridad, gran calidad de audio y facilidad de uso protege de forma eficaz información clasificada (hasta difusión limitada) de la organización. Las llamadas y los datos intercambiados por COMSec son seguros, independientemente del operador móvil utilizado y el país donde se encuentre.
Más información: comsec.indracompany.com

Observaciones

Utilización según el PE-2018-24 Procedimiento de empleo COMSec Admin + v2
Para su empleo en entornos tácticos o desplegables, este producto deberá emplearse sobre un dispositivo móvil perteneciente a la familia “plataformas y dispositivos tácticos confia

8.4.9 FAMILIA: CIFRADORES IP

Centro de gestión 543U/B	
Versión	2.01
Fabricante	Epicom
Familia	Cifradores IP
Tipo	Producto
Clasificación	CONFIDENCIAL
Fecha Inclusión	01/09/2020
Revisión de Validez	28/02/2023



Descripción

El Centro de Gestión EP543U/B es el elemento de gestión remota del cifrador EP430 GU/B. El único procedimiento permitido para gestionar de manera remota un EP430GU/B es a través de una conexión remota segura (Canal Seguro) desde la aplicación del Centro de Gestión.

Observaciones

Utilización según PE-2019-9 Procedimiento de Empleo EP430GU/B

EP430GN



Versión 1.08.29

Fabricante Epicom

Familia Cifradores IP

Tipo Producto

Clasificación RESERVADO

Fecha Inclusión 01/12/2017

Revisión de Validez 31/12/2022

Descripción

Cifrador de redes IP a 2 Gbps (agregados).

Observaciones

Este modelo no es compatible con el resto de la familia de cifradores EP430 de EPICOM.
Utilización según P029-PE-2011-33 Operational doctrine EP430GN v2.

EP430GU/B



Versión 2.01

Fabricante Epicom

Familia Cifradores IP

Tipo Producto

Clasificación CONFIDENCIAL

Fecha Inclusión 01/09/2020

Revisión de Validez 28/02/2023

Descripción

El cifrador IP EP430 GU/B está basado en el cifrador IP EP430GU, sobre el que se han sustituido los mecanismos criptográficos por algoritmos tipo B. Está compuesto por una plataforma de comunicaciones EP430G+ y un módulo cripto EP940+ programado como EP940U/B (software y firmware). Es un cifrador a 1Gpbs, diseñado para operar en la capa 3 del modelo OSI, lo que permite el despliegue de redes privadas virtuales (VPN, Virtual Private Networks) de una forma completamente segura.

Observaciones

Utilización según PE-2019-9 Procedimiento de Empleo EP430GU/B

EP430GX



Versión v.1.07

Familia Cifradores IP

Fabricante Epicom

Clasificación SECRETO

Fecha Inclusión 01/12/2017

Revisión de Validez 31/12/2022

Descripción

Cifrador de redes IP a 2 Gbps (agregados), interoperable con el resto de cifradores de la familia EP430.

Observaciones

Utilización según PE-2012-49 Procedimiento de Empleo EP430GX.

EP430GX	
Versión	v.1.08
Familia	Cifradores IP
Fabricante	Epicom
Clasificación	SECRETO
Fecha Inclusión	27/12/2021
Revisión de Validez	31/12/2022



Descripción

Cifrador de redes IP a 2 Gbps (agregados), interoperable con el resto de cifradores de la familia EP430.

Observaciones

Utilización según PE-2012-49 Procedimiento de Empleo EP430GX.

EP430TX	
Versión	1.04
Fabricante	Epicom
Familia	Cifradores IP
Tipo	Producto
Clasificación	SECRETO
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2022



Descripción

Cifrador de comunicaciones IP hasta 200 Mbps, interoperable con el resto de cifradores de la familia EP430.

Observaciones

Utilización según PE-2016-28 Procedimiento de empleo EP430TX.

8.5 CATEGORÍA: PROTECCIÓN DE LA INFORMACIÓN Y SOPORTES DE INFORMACIÓN

8.5.1 FAMILIA: CIFRADO OFFLINE

EP851

Versión 2.02 y 2.03

Familia Cifrado offline

Fabricante Epicom

Clasificación CONFIDENCIAL

Fecha Inclusión 01/12/2017

Revisión de Validez 31/12/2022



Descripción

Dispositivo portátil USB de cifrado "off-line":
• Compatible con Crypto Token USB de la empresa Datatech.
• Cifrado de ficheros para su posterior envío.
• Almacenamiento interno de la datos cifrados para su transporte.

Observaciones

Utilización según el PE-2008-01 Procedimiento de Empleo TOKEN USB.
Las redes que empleen estos dispositivos, deben sustituirlos por los EP852.

EP852

Versión 3.04

Familia Cifrado offline

Fabricante Epicom

Clasificación CONFIDENCIAL

Fecha Inclusión 20/07/2020

Revisión de Validez 31/12/2025



Descripción

El EP852 es un cifrador de ficheros fuera de línea que permite el cifrado y descifrado de ficheros y el transporte de información cifrada en el dispositivo. Mejora las prestaciones en cuanto a almacenamiento y velocidad de las versiones anteriores de losToken USB así como la puesta en marcha del dispositivo, carga y distribución de claves.

Observaciones

Utilización según el PE-2020-4 -Procedimiento de Empleo Seguro EP852 -(ESP)

EP852	
Versión	3.05
Familia	Cifrado offline
Fabricante	Epicom
Clasificación	CONFIDENCIAL
Fecha Inclusión	27/12/2021
Revisión de Validez	31/12/2025



Descripción

El EP852 es un cifrador de ficheros fuera de línea que permite el cifrado y descifrado de ficheros y el transporte de información cifrada en el dispositivo. Mejora las prestaciones en cuanto a almacenamiento y velocidad de las versiones anteriores de losToken USB así como la puesta en marcha del dispositivo, carga y distribución de claves.

Observaciones

Utilización según el PE-2020-4 -Procedimiento de Empleo Seguro EP852 -(ESP)

EP880	
Versión	2.08.36 y 2.09.35
Fabricante	Epicom
Familia	Cifrado offline
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/07/2021
Revisión de Validez	31/12/2026

Descripción

El EP880 es una aplicación software que se ejecuta sobre ordenador con sistema operativo Windows y que permite realizar, en origen, el cifrado y firma de ficheros de datos “off-line” almacenados en el disco duro del ordenador o dispositivos de almacenamiento externos conectados al ordenador, para su posterior almacenamiento y/o envío de forma segura desde el correo electrónico u otro medio y, en destino, el descifrado y verificación de la integridad de los datos.

Observaciones

Utilización según EP240E880ZZ05 Procedimiento de Empleo Seguro EP880

8.5.2 FAMILIA: SISTEMAS PARA PREVENCIÓN DE FUGAS DE DATOS

McAfee Data Loss Prevention (DLP) Endpoint with ePolicy Orchestrator 5.10	
Versión	11.1
Fabricante	McAfee
Familia	Sistemas para prevención de fugas de datos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/04/2020
Revisión de Validez	28/09/2022

Descripción

McAfee DLP Endpoint proporciona protección integral para todos los posibles canales de fuga de datos, como dispositivos de almacenamiento extraíbles, la nube, correo electrónico, la mensajería instantánea, la Web, el material impreso, el portapapeles, capturas de pantalla, las aplicaciones para compartir archivos, etc.
Sus principales características son:
- Integración con análisis de comportamientos de usuarios (UEBA) de terceros.
- Clasificación manual.
- Análisis y reparaciones iniciados por el usuario.
- Clasificación flexible, que ofrece diccionarios, expresiones regulares y algoritmos de validación.
- Una exclusiva tecnología de etiquetado para identificar los documentos según su origen, que impide que la información confidencial de las aplicaciones web, las aplicaciones de red y los recursos compartidos de red se duplique, renombre o salga de las instalaciones de la empresa.
- Compatibilidad con virtualización para proteger equipos de sobremesa remotos y soluciones VDI.

Observaciones

CCN-STIC 1503 Procedimiento de Empleo Seguro McAfee Data Loss Prevention 11.1 con ePolicy Orchestrator 5.10

8.5.3 FAMILIA: HERRAMIENTAS PARA FIRMA ELECTRÓNICA

Keyone	
Versión	v 4.0
Fabricante	Safelayer
Familia	Herramientas para firma electrónica
Tipo	Producto
Clasificación	Conf. DL Int. Res.
Fecha Inclusión	01/12/2017
Revisión de Validez	31/12/2023

Descripción

Aplicación para la gestión de infraestructura de clave pública.
Aprobado para proteger la confidencialidad hasta Difusión Limitada y la integridad (Firma digital) hasta Reservado.

Observaciones

Utilización según el PE-2015-38 Operational Doctrine KeyOne System.

8.6 CATEGORÍA: PROTECCIÓN DE EQUIPOS Y SERVICIOS

8.6.1 FAMILIA: DISPOSITIVOS MÓVILES

Färist Mobile System	
Versión	V4.1, Dispositivo: BQ Aquaris X2
Familia	Dispositivos móviles
Fabricante	Tutus
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	27/12/2021
Revisión de Validez	31/12/2022



Descripción

Sistema de comunicación seguro de terminales móviles basado en S.O. Android. El Färist Mobile System además de proteger la comunicación protege la plataforma (BQ Aquaris X2) para almacenar información clasificada hasta el grado de Difusión Limitada.

Observaciones

Utilización según PE-2019-30 Operational Doctrine Farist Mobile v4.1 DL Rel to EU.
Comercializado en España por la empresa Epicom.

8.6.2 FAMILIA: SISTEMAS OPERATIVOS

Windows 10	
Versión	Enterprise LTSC 2019
Fabricante	Microsoft Corporation
Familia	Sistemas Operativos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/10/2019
Revisión de Validez	09/01/2029

Descripción

Sistema Operativo para estaciones de trabajo, tanto en entornos reales como virtualizados.

Observaciones

Procediminento de empleo: CCN-STIC-599A19 y CCN-STIC-599B19

Windows 10	
Versión	Enterprise 2015 LTSB
Fabricante	Microsoft Corporation
Familia	Sistemas Operativos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/12/2018
Revisión de Validez	14/10/2025

Descripción

Sistema Operativo para estaciones de trabajo, tanto en entornos reales como virtualizados.

Observaciones

CCN-STIC-599A Anexo B
CCN-STIC-599B Anexo B

Windows 10	
Versión	Enterprise 2016 LTSB
Fabricante	Microsoft Corporation
Familia	Sistemas Operativos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/12/2018
Revisión de Validez	13/10/2026

Descripción

Sistema Operativo para estaciones de trabajo, tanto en entornos reales como virtualizados.

Observaciones

CCN-STIC-599A18 Anexo B
CCN-STIC-599B18 Anexo B

Windows Server 2012 R2	
Versión	Standard Edition, Datacenter Edition
Fabricante	Microsoft Corporation
Familia	Sistemas Operativos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/12/2018
Revisión de Validez	10/10/2023

Descripción

Sistema Operativo para servidores

Observaciones

CCN-STIC-870A y CCN-STIC-870B

Windows Server 2016	
Versión	Datacenter Edition
Fabricante	Microsoft Corporation
Familia	Sistemas Operativos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/12/2018
Revisión de Validez	09/01/2024

Descripción

Sistema Operativo para servidores

Observaciones

CCN-STIC-570A, CCN-STIC-570B Anexo A

8.6.3 FAMILIA: PROTECCIÓN DE CORREO ELECTRÓNICO

FortiMail Appliances FML-2000E, FML-3000E, FML-3200E	
Versión	Firmware 6.0.2
Fabricante	Fortinet
Familia	Protección de correo electrónico
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/06/2019
Revisión de Validez	30/11/2022

Descripción

Sistema de seguridad de correo electrónico que proporciona una protección multicapa contra spam, virus, gusanos y spyware. El motor de filtrado empleado en FortiMail bloquea el spam y el malware antes de que pueda afectar a las redes y usuarios.

Observaciones

CCN-STIC-1614 Procedimiento de empleo seguro Fortimail
Requiere Fortinet Entropy Token V1

8.6.4 FAMILIA: HIPERCONVERGENCIA

KATUA SDI PLATFORM

Versión	1.0.6
Fabricante	KRC ESPAÑOLA S.A.
Familia	Hiperconvergencia
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/09/2021
Revisión de Validez	29/02/2024

Descripción

Katua®SDI Platform es una plataforma hiperconvergente escalable y segura, basada en el concepto Software Define Infraestructure, donde todos los elementos que conforman un CPD se definen en una única plataforma hardware y software. Permite el despliegue rápido de servicios (xaaS), consolidación de CPDs, SDN y tiene capacidad de instalación desde equipos móviles hasta grandes centros de procesos de datos. Su flexibilidad permite que se puedan desplegar servicios cloud sobre la plataforma de forma sencilla y eficiente. Dispone de la capacidad para generar bibliotecas de sistemas preconfigurados para su despliegue con un click a través de su interfaz web. Las capacidades de optimización del hipervisor aseguran un rendimiento máximo de la plataforma, haciendo uso de todos los recursos disponibles y ofreciendo de esta forma capacidad de instalación en nodos pequeños y configuraciones hardware básicas. Su capacidad para integrarse con sistemas de almacenamiento masivos, ya sean locales o remotos permite escalar la solución en función de las necesidades. Para más información de la plataforma, vista nuestra web https://www.krc.es.

Observaciones

CCN-STIC-1610 Procedimiento de Empleo Seguro KATUA SDI Platform
La herramienta no ha sido aprobada para garantizar el aislamiento de recursos y convivencia en una misma infraestructura de sistemas de diferentes dominios y niveles de clasificación de Información Clasificada.

8.7 CATEGORÍA: COMUNICACIONES TÁCTICAS SEGURAS

8.7.1 FAMILIA: PLATAFORMAS Y DISPOSITIVOS TÁCTICOS CONFIABLES

BITTIUM TOUGH MOBILE C	
Versión	HW version: 9304809A03 SW version: Android 5.1.1 Kernel version: 3.4.0 Build: S2_BSOS_1.1.5C_MR22_sapphire2
Fabricante	BITIUM
Familia	Plataformas y dispositivos tácticos confiables
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/06/2019
Revisión de Validez	30/11/2022



Descripción

Teléfono móvil rugerizado (IP67, MIL-STD- 810G) basado en S.O. Android diseñado para dar soporte a usuarios civiles y militares. Cubre 9 bandas LTE, incluida la Banda 14 para seguridad pública. Dual-sim para redes LTE privadas y públicas. Este dispositivo se considera una plataforma confiable donde ejecutar aplicaciones software de forma protegida. Incluye una VPN para la protección de la información en tránsito.

Observaciones

Procedimiento de configuración y empleo seguro pendiente de publicación.

GETAC F110	
Versión	G4 con firmware GETAC R1.12.070520
Fabricante	GETAC
Familia	Plataformas y dispositivos tácticos confiables
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/06/2019
Revisión de Validez	13/10/2023



Descripción

Tableta robusta diseñada para dar soporte a usuarios civiles y militares. Este dispositivo se considera una plataforma confiable donde ejecutar aplicaciones software de forma protegida (p.ej.: aplicaciones de mando y control).
El sistema operativo de la tableta es Windows 10 Enterprise 1607 LTSB. La tableta incluye un TPM 2.0.

Observaciones

Configuración y empleo seguro según la CCN-STIC-1605.
Para protección de las comunicaciones en tránsito es necesario un producto aprobado perteneciente a la familia “soluciones para protección de las comunicaciones tácticas”.

GETAC F110



Versión	G5 con firmware GETAC 12.0.45.1509
Fabricante	GETAC
Familia	Plataformas y dispositivos tácticos confiables
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/06/2021
Revisión de Validez	13/10/2023

Descripción

Tableta robusta diseñada para dar soporte a usuarios civiles y militares. Este dispositivo se considera una plataforma confiable donde ejecutar aplicaciones software de forma protegida (p.ej.: aplicaciones de mando y control).
El sistema operativo de la tableta es Windows 10 Enterprise 1607 LTSB. La tableta incluye un TPM 2.0.

Observaciones

Configuración y empleo seguro según la CCN-STIC-1609.
Para protección de las comunicaciones en tránsito es necesario un producto aprobado perteneciente a la familia "soluciones para protección de las comunicaciones tácticas".

Unidad de Comunicaciones Seguras (UCS) con módulo de seguridad TZ-501



Versión	UCS v2.4 con TZ-501 (versión SW 4.26)
Fabricante	TECNOBIT, S.L. y RF Española, S.A.
Familia	Soluciones para protección de las comunicaciones tácticas
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/09/2021
Revisión de Validez	31/12/2023

Descripción

La UCS es un gestor de comunicaciones para su uso en entornos tácticos militares en los que se requiere contar con comunicaciones seguras tanto de voz táctica CNR como de de datos IP. La UCS permite la conexión de varias radios tácticas, u otros medios CIS, que actuan como medio de transporte. El sistema incorpora un módulo de gestión de radiofonía, un módulo para la gestión de la interfonía y un servidor de telefonía de Voz IP para la integración con equipos telefónicos SIP, todo ello acompañado de un módulo de cifrado seguro, denominado TZ-501. El TZ-501 es el módulo encargado de cifrar la voz táctica según estándares OTAN, así como los datos IP unicast y multicast. La UCS cuenta con una "Crypto Ignition Key" (CIK) para el arranque seguro del equipo, y que además facilita el transporte y almacenamiento del equipo (sin la CIK la UCS se considera un equipo no clasificado).
La cifra del TZ-501 es compatible con la cifra del TZ-1001R en modo "slave-crypto" y con la cifra del TZ-2001.

Observaciones

Utilización según el Procedimiento de Empleo Seguro T00741600PDE001 V3.

HP Elitebook 840 G7 y G8	
Versión	G7 y G8
Fabricante	HP PRINTING AND COMPUTING SOLUTIONS SL
Familia	Plataformas y dispositivos tácticos confiables
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/09/2021
Revisión de Validez	29/02/2024

Descripción

Equipos portátiles con sistema operativo Windows 10 Enterprise, Versión 20H2, Compilación (19042.1023) securizable mediante la aplicación de las guías STIC para manejo de información clasificada.

Observaciones

Plataforma bastionada según CCN-STIC 599B19

8.7.2 FAMILIA: SOLUCIONES PARA PROTECCIÓN DE LAS COMUNICACIONES TÁCTICAS

COMSec Admin +	
Versión	v4.2
Fabricante	Indra
Familia	Soluciones para protección de las comunicaciones tácticas
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/05/2021
Revisión de Validez	31/10/2023



Descripción

COMSec Admin+ es una solución global de comunicaciones seguras que proporciona servicios cifrados de voz, mensajería instantánea y videoconferencia sobre teléfonos móviles empleando cualquier red celular, inalámbrica o satelital.
Con su alto nivel de seguridad, gran calidad de audio y facilidad de uso protege de forma eficaz información clasificada (hasta difusión limitada) de la organización. Las llamadas y los datos intercambiados por COMSec son seguros, independientemente del operador móvil utilizado y el país donde se encuentre.
Más información: comsec.indracompany.com

Observaciones

Utilización según el PE-2018-24 Procedimiento de empleo COMSec Admin + v2
Para su empleo en entornos tácticos o desplegables, este producto deberá emplearse sobre un dispositivo móvil perteneciente a la familia “plataformas y dispositivos tácticos confia

TZ-1001R

Versión	V4.26
Familia	Soluciones para protección de las comunicaciones tácticas
Fabricante	TECNOBIT
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/10/2020
Revisión de Validez	31/12/2023



Descripción

El TZ-1001R es un cifrador táctico de pequeño tamaño para la protección de las comunicaciones sobre redes de bajo ancho de banda y sin estabilidad de enlace garantizada. Cuenta con dos modos de operación diferenciados: como cifrador en línea (modo “tactical crypto”), o alternativamente en modo “slave crypto” como elemento de cifra esclavo de otro elemento que gestiona la interacción con los medios de transmisión y con el usuario (caso del Gestor de Comunicaciones del ET).

El TZ-1001R tiene capacidad para cifrar de forma simultánea varios flujos de voz táctica (“push to talk”) según varios estándares OTAN, pudiendo elegirse en cada caso el más adecuando según el tipo de radio por el que se va a realizar la transmisión. Simultáneamente también puede cifrar datos IP unicast y multicast. Cuando el cifrador se configura en modo “tactical crypto” implementa IPSec con asociaciones de seguridad manuales. En configuración “slave crypto” el TZ-1001R implementa un protocolo específico de cifra IP para facilitar la integración con los sistemas CIS de dotación.

En modo “slave crypto” la cifra del TZ-1001R es interoperable con la cifra del TZ-501 (módulo de seguridad de la UCS) y con la aplicación de cifrado para S.O. Windows TZ-2001.

Observaciones

Utilización según el Procedimiento de empleo T90431000PDE003 v2.0

Bittium SafeMove VPN Client for Android	
Versión	Android (genérico): 1.2.159, Android (Bittium Tough Mobile R): 2020-04-27 @ granite @ c5e05cb
Fabricante	Bittium SafeMove Oy
Familia	Soluciones para protección de las comunicaciones tácticas
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/04/2021
Revisión de Validez	30/06/2023

Descripción

SafeMove Mobile VPN forma parte de la Bittium Secure Suite. Proporciona los servicios de firewall y VPN IPSec a las plataformas Android y Windows conectadas de forma remota a la infraestructura corporativa, y está concebido para ser un servicio siempre activo y aplicado a todo el tráfico de red que entra y sale del dispositivo. Nada sensible se escapa, nada dañino puede entrar. La SafeMove Mobile VPN es una solución cliente-servidor. El cliente instalado en el dispositivo se conecta a la puerta de enlace Bittium SafeMove VPN Gateway instalada en el servidor, con el resto de los componentes de la Bittium Secure Suite, que son el gestor de dispositivos (MDM), el gestor de las aplicaciones instaladas en los dispositivos (solo Android) y los servicios de comprobación de la integridad (solo Android). Usado en combinación con los smartphones de la familia Bittium Tough Mobile proporciona servicios de recuperación de los registros de auditoría y actualización OTA del firmware de los dispositivos.
Más información de Bittium SafeMove® Mobile VPN:
https://www.bittium.com/secure-communications-connectivity/bittium-safemove-mobile-vpn

Observaciones

PE-2021-7-Procedimiento de empleo seguro Bittium SafeMove VPN (Android y Windows)

Bittium SafeMove VPN Client for Windows	
Versión	4.11.722
Fabricante	Bittium SafeMove Oy
Familia	Soluciones para protección de las comunicaciones tácticas
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/04/2021
Revisión de Validez	30/06/2023

Descripción

SafeMove Mobile VPN forma parte de la Bittium Secure Suite. Proporciona los servicios de firewall y VPN IPSec a las plataformas Android y Windows conectadas de forma remota a la infraestructura corporativa, y está concebido para ser un servicio siempre activo y aplicado a todo el tráfico de red que entra y sale del dispositivo. Nada sensible se escapa, nada dañino puede entrar. La SafeMove Mobile VPN es una solución cliente-servidor. El cliente instalado en el dispositivo se conecta a la puerta de enlace Bittium SafeMove VPN Gateway instalada en el servidor, con el resto de los componentes de la Bittium Secure Suite, que son el gestor de dispositivos (MDM), el gestor de las aplicaciones instaladas en los dispositivos (solo Android) y los servicios de comprobación de la integridad (solo Android). Usado en combinación con los smartphones de la familia Bittium Tough Mobile proporciona servicios de recuperación de los registros de auditoría y actualización OTA del firmware de los dispositivos.
Más información de Bittium SafeMove® Mobile VPN: https://www.bittium.com/secure-communications-connectivity/bittium-safemove-mobile-vpn

Observaciones

PE-2021-7-Procedimiento de empleo seguro Bittium SafeMove VPN (Android y Windows)

Bittium Tough SDR Handheld – Soldier Radio	
Versión	9400132
Fabricante	Bittium Wireless Ltd.
Familia	Soluciones para protección de las comunicaciones tácticas
Tipo	Producto
Clasificación	DIFUSIÓN LIMITADA
Fecha Inclusión	01/08/2021
Revisión de Validez	30/06/2023



Descripción

El producto Bittium Tough SDR Handheld es una radio táctica militar V-UHF de mano basada en tecnología SDR conforme a la arquitectura ESSOR SCA. Esta radio, en función de la forma de onda empleada, proporciona diferentes servicios de comunicaciones de voz y datos con unas prestaciones determinadas en términos de ancho de banda, alcance, número de nodos soportados en la red radio, etc.

La Tough SDR Handheld cubre la banda de frecuencias desde 30 MHz hasta 2,5 GHz y puede ejecutar formas de onda tanto de banda estrecha como de banda ancha, las cuales incluyen diferentes mecanismos de protección COMSEC, TRANSEC y NETSEC. La aprobación para la protección de información clasificada nacional de grado DIFUSIÓN LIMITADA es aplicable cuando el producto se emplee con la forma de onda ESSOR High Data Rate Waveform.

Observaciones

Utilización según el PE-2021-21 “Procedimiento de empleo seguro de la radio táctica Bittium Tough SDR Hand-Held”.

8.8 CATEGORÍA: OTRAS HERRAMIENTAS

8.8.1 FAMILIA: OTRAS HERRAMIENTAS

authUsb safeDoor	
Versión	2.0.0.8
Familia	Otras Herramientas
Fabricante	authUSB
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/05/2019
Revisión de Validez	30/11/2022



Descripción

AuthUsb safeDoor es un dispositivo hardware que actúa como barrera entre las memorias USB y los equipos de una organización, identificando amenazas a tres niveles:

-Eléctrico: identificando y deteniendo ataques destructivos de sobretensión tipo UsbKiller.

-Hardware: detectando y desactivando ataques de la familia BadUsb, ataques HID (rubber ducky y similares), falsas tarjetas de red, interfaces compuestas, etc.

-Software: antivirus integrado que realiza un análisis previo a la descarga de cualquier contenido.

Observaciones

CCN-STIC 1201 Procedimiento de empleo seguro AuthUsb SafeDoor

8.9 CATEGORÍA: TEMPEST

8.9.1 FAMILIA: ARMARIOS APANTALLADOS

SHATEM - SHELTER ARPA TEMPEST MULTIPROPOSITO



Versión

Fabricante ARPA, EQUIPOS MÓVILES DE CAMPAÑA S.A.U.

Familia Armarios apantallados

Tipo Producto

Clasificación APTO ZONA 0

Fecha Inclusión 01/01/2020

Revisión de Validez 31/05/2022

Descripción

Contenedor shelter para alojamiento y/o operación de equipos informáticos, electrónicos, optrónicos de telecomunicaciones y asimilables para entornos CIS. Equipado con los elementos de filtrado y protección EMI necesarios en acometidas de potencia, datosy servicios para disponer de apantallamiento intergral TEMPEST frente a emanaciones comprometedoras radiadas y conducidas.

Observaciones

P.AT-02D



Versión

Fabricante CONSUEGRA S. COOP.

Familia Armarios apantallados

Tipo Producto

Clasificación Apto ZONA 0

Fecha Inclusión 01/12/2017

Revisión de Validez 31/05/2022

Descripción

Armario apantallado de 19" y hasta 730 mm de longitud. Puertas delanteras acristaladas y puertas laterales ciegas. Filtros de alimentación independientes de 6A. Aireación mediante electroventiladores. Apto para instalación en locales con clasificación deZONA 0 con equipos clasificados ZONA 2.

Observaciones

P.AT-06D



Versión

Fabricante CONSUEGRA S. COOP.

Familia Armarios apantallados

Tipo Producto

Clasificación Apto ZONA 0

Fecha Inclusión 01/12/2017

Revisión de Validez 31/05/2022

Descripción

Armario apantallado ciego de 25U. Dimensiones 1524x625x1000 mm. Ventilación a través de 2 ventiladores con termostatos independientes con caudal de hasta 2.700 m3/h. Distribuidor interno con diferencial y automático. Apto para instalación en locales con clasificación de ZONA 0.

Observaciones

P.AT-06E



Versión

Fabricante CONSUEGRA S. COOP.

Familia Armarios apantallados

Tipo Producto

Clasificación Apto ZONA 0

Fecha Inclusión 01/12/2017

Revisión de Validez 31/05/2022

Descripción

Armario apantallado ciego de 38U. Dimensiones 2102x625x1000 mm. Ventilación a través de 2 ventiladores con termostatos independientes con caudal de hasta 2.700 m3/h. Distribuidor interno con diferencial y automático. Apto para instalación en locales con clasificación de ZONA 0.

Observaciones

P.AT-07

Versión

Fabricante CONSUEGRA S. COOP.

Familia Armarios apantallados

Tipo Producto

Clasificación Apto ZONA 0



Fecha Inclusión 01/12/2017

Revisión de Validez 31/05/2022

Descripción

Armario apantallado para CPU. Dispone de bandeja extraible, ventilación y filtrado de las líneas de datos y alimentación. Apto para instalación en locales con clasificación ZONA 0.

Observaciones

P.AT07D

Versión

Fabricante CONSUEGRA S. COOP.

Familia Armarios apantallados

Tipo Producto

Clasificación Apto ZONA 0



Fecha Inclusión 01/04/2019

Revisión de Validez 30/09/2022

Descripción

Armario Tempest de sobremesa de dimensiones reducidas con dos posibles opciones. El armario PAT 07D ofrece alta protección electromagnética para que el cliente incluya su propia CPU, convirtiendo el conjunto en una CPU Tempest aceptada para procesar información clasificada en locales ZONA 0. CONSUEGRA se ocupa de las adaptaciones necesarias para su correcta instalación y funcionamiento. Posteriormente, si el cliente deseara cambiar la CPU por una más actualizada, CONSUEGRA también puede ocuparse de su instalación y funcionamiento. CONSUEGRA también ofrece la posibilidad de suministrar e instalar la CPU solicitada por el cliente como parte del pedido, en este caso, el producto se codifica como P.COMPT0-03.

Observaciones

8.9.2 FAMILIA: MONITORES

P.MONT0-11



Versión

Fabricante CONSUEGRA S. COOP.

Familia Monitores

Tipo Producto

Clasificación SDIP-27 Level A

Fecha Inclusión 01/12/2021

Revisión de Validez 31/05/2023

Descripción

Monitor LED Full HD de 22" y resolución 1920 x 1080p con formato panorámico.

Observaciones

8.9.3 FAMILIA: PERIFÉRICOS

P.KVMT0-01



Versión

Fabricante CONSUEGRA S. COOP.

Familia Periféricos

Tipo Producto

Clasificación SDIP-27 Level A

Fecha Inclusión 01/12/2017

Revisión de Validez 31/05/2022

Descripción

Conmutador KVM para dos sistemas. Basado en BELKIN SECURE OMNIVIEW F1DN102Uea con certificación NIAP EAL 4+.

Observaciones

P-RATT0-04	
Versión	
Fabricante	CONSUEGRA S. COOP.
Familia	Periféricos
Tipo	Producto
Clasificación	SDIP-27 Level A
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2022



Descripción

Ratón óptico USB

Observaciones

P.TECT0-07	
Versión	
Fabricante	CONSUEGRA S. COOP.
Familia	Periféricos
Tipo	Producto
Clasificación	SDIP-27 Level A
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2022



Descripción

Teclado QWERTY español. Conexión USB.

Observaciones

8.9.4 FAMILIA: CPU

P.COMT0-01



Versión

Fabricante CONSUEGRA S. COOP.

Familia CPU

Tipo Producto

Clasificación SDIP-27 LEVEL A

Fecha Inclusión 01/06/2018

Revisión de Validez 30/11/2022

Descripción

CPU de sobremesa tempestizada del modelo comercial HP ELITE 8000. Aprobado para su uso combinado con periféricos TEMPEST de la empresa CONSUEGRA S. COOP. en locales con clasificación de ZONA 0.

Observaciones

P.COMPT0-06



Versión

Fabricante CONSUEGRA S. COOP.

Familia CPU

Tipo Producto

Clasificación SDIP-27 LEVEL A

Fecha Inclusión 01/12/2021

Revisión de Validez 31/05/2023

Descripción

CPU de sobremesa tempestizada del modelo comercial HP PRODESK 600 G5 SFF. Aprobado para su uso combinado con periféricos TEMPEST de la empresa CONSUEGRA S.COOP. en locales con clasificación de ZONA 0.

Observaciones

8.9.5 FAMILIA: IMPRESORAS

P.IMPT0-04



Versión	
Fabricante	CONSUEGRA S. COOP.
Familia	Impresoras
Tipo	Producto
Clasificación	SDIP-27 Level A
Fecha Inclusión	01/12/2021
Revisión de Validez	31/05/2023

Descripción

Impresora TEMPEST basada en el model HP Color LaserJet Enterprise M553dn.

Observaciones

9. PRODUCTOS Y SERVICIOS DE CONFORMIDAD Y GOBERNANZA DE LA SEGURIDAD

PRODUCTOS Y SERVICIOS DE CONFORMIDAD Y GOBERNANZA DE LA SEGURIDAD



9.1 FAMILIA: GOBERNANZA Y PLANIFICACIÓN DE LA SEGURIDAD

ANA	
Versión	2.3.2.2
Fabricante	Centro Criptológico Nacional
Familia	Gobernanza y Planificación de la Seguridad
Tipo	Producto
Fecha Inclusión	01/01/2022
Revisión de Validez	31/05/2022

Descripción

ANA es una solución de gobernanza técnica de la seguridad TIC que mediante la evaluación de la Superficie de Exposición proporciona indicadores sobre la criticidad de los hallazgos encontrados. Permite reducir los tiempos en la gestión de la seguridad TICal ofrecer recomendaciones para un tratamiento oportuno de las amenazas detectadas en base a su severidad.
Características principales:
• Permite acceder en tiempo real a amenazas localizadas, identificarlas y seguir su evolución en el tiempo.
• Genera dinámicamente informes del estado real de la entidad por departamento, servidor, aplicación o cualquier activo definido.
• Organiza la información proporcionando múltiples vistas/cuadros de mandos a los usuarios.
• Centraliza y normaliza todas las inspecciones de seguridad realizadas.
• Proporciona mecanismos de alerta temprana mediante interacción directa y detallada con las amenazas encontradas permitiendo una notificación oportuna sin dilación indebida.

Observaciones

Para más información, contactar con ana@ccn-cert.cni.es.
Procedimiento de empleo seguro pendiente de publicación.

9.2 FAMILIA: NORMATIVA DE SEGURIDAD Y CONFORMIDAD

CLARA ENS WINDOWS	
Versión	2.0.2.1
Fabricante	SIDERTIA / Centro Criptológico Nacional
Familia	Normativa de Seguridad y Conformidad
Tipo	Producto
Fecha Inclusión	01/11/2021
Revisión de Validez	30/04/2024

Descripción

CLARA es una herramienta para analizar las características de seguridad técnicas en equipos Windows definidas por el Esquema Nacional de Seguridad. El análisis del cumplimiento está basado en las normas proporcionadas a través de las plantillas de seguridad de las guías de configuración segura de equipos Windows (la CCN-STIC-599, entre otras).

Observaciones

Para más información, contactar con clara@ccn-cert.cni.es.

9.3 FAMILIA: NOTIFICACIÓN Y GESTIÓN DE CIBERINCIDENTES

LUCIA	
Versión	4.1
Fabricante	CSA / Centro Criptológico Nacional
Familia	Notificación y Gestión de Ciberincidentes
Tipo	Producto
Fecha Inclusión	01/11/2021
Revisión de Validez	30/04/2024

Descripción

LUCIA es una herramienta para la Gestión de Ciberincidentes en las entidades del ámbito de aplicación del Esquema Nacional de Seguridad. Con ella, se pretende mejorar la coordinación entre el CERT Gubernamental Nacional y los distintos organismos y organizaciones con las que colabora. LUCIA ofrece un lenguaje común de peligrosidad y clasificación del incidente y mantiene la trazabilidad y el seguimiento del mismo. El sistema permite, además, automatizar las tareas e integrarse con otros sistemas ya implantados.

Observaciones

Para más información, contactar con lucia@ccn-cert.cni.es.

9.4 FAMILIA: FORMACIÓN Y CONCIENCIACIÓN EN CIBERSEGURIDAD

PSAT – Proofpoint Security Awareness Training	
Versión	-
Fabricante	Proofpoint
Familia	Formación y Concienciación de Ciberseguridad
Tipo	Servicio
Fecha Inclusión	01/03/2022
Revisión de Validez	30/06/2023

Descripción

PSAT -Proofpoint Security Awareness Training- es una solución de formación y capacitación de concienciación en materia de seguridad. La solución, basada en un enfoque cíclico de evaluación, educación, refuerzo y medición, enseña a los usuarios las mejores prácticas y les muestra cómo emplearlas cuando se enfrentan a amenazas de seguridad, ayudándoles a evitar que los ciberataques consigan su objetivo y convirtiéndolos en la última línea de defensa de las organizaciones.

Características Principales:
• Identifica el riesgo de los usuarios mediante Simulaciones de Phishing y evaluaciones de conocimiento.
• Permite cambiar el comportamiento de los usuarios, mediante más 350 módulos de formación interactivos que ofrecen ejercicios prácticos para que los usuarios reconozcan y eviten los ataques de phishing y otros fraudes de ingeniería social.
• Reduce la exposición de la organización, mediante un complemento para cliente de correo, los usuarios pueden denunciar los mensajes sospechosos con un solo clic
• Evalúa y analiza los resultados, la solución ofrece una visibilidad detallada y de alto nivel que permite medir el progreso, evaluar el desempeño e identificar el riesgo a nivel de organización, departamento y usuario.

Observaciones

CCN-STIC-1701 Procedimiento de Empleo Seguro PSAT

10. REFERENCIAS

[1] CCN-STIC-106 Procedimiento de inclusión de productos de seguridad TIC cualificados en el CPSTIC.

[2] CCN-STIC-140 Taxonomía de referencia para productos de Seguridad TIC.

[3] CCN-STIC-102 Procedimiento para la Aprobación de Productos de seguridad TIC para manejar información Nacional clasificada.

[4] CCN-STIC-130 Requisitos de Aprobación de Productos de Cifra para Manejar Información Nacional Clasificada.

[5] CCN-STIC-151 Evaluación y Clasificación TEMPEST de equipos.

11. ABREVIATURAS

CC	*Common Criteria*
CCN	*Centro Criptológico Nacional*
CPSTIC	*Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación*
EDR	*Endpoint Detection and Response*
ENECSTI	*Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información*
ENS	*Esquema Nacional de Seguridad.*
EPP	*Endpoint Protection Platform*
IDS	*Intrusion Detection System*
IPS	*Intrusion Prevention System*
PES	*Procedimiento de Empleo Seguro*
RFS	*Requisitos Fundamentales de Seguridad*
STIC	*Seguridad de las Tecnologías de la Información y la Comunicación*
TIC	*Tecnologías de la Información y la Comunicación*

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA SUBSECRETARÍA DE DEFENSA SECRETARÍA GENERAL TÉCNICA SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL