Apuntes de ItCetas

Copia de la página original de ItCetas http://itcetas.blogspot.com.es

CURSO FORTINET 4.3

RECOMENDACIONES



- No utilizar la última versión de Forti
- Versiones recomendadas EN la web de soporte
- Si tienes el interfaz wan con dhcp y coge automáticamente el gw es recomendable igualmente generar la ruta estática 0.0.0.0 0.0.0.0 next-hop x.x.x.x

USB-AUTOINSTALL

Para cargar configs y soft via USB

System>config>Advanced y defines el nombre de los ficheros que estarán el USB.

Si luego pones un USB (Forti apagado) con un fichero de conf y una imagen lo enciendes y cargará esta version y config. Tienen que coincidir los nombres de los ficheros con los antes definidos

UPDATES Fortios

Desde el dashboard



Normalmente guarda como mínimo dos versiones en dos particiones diferentes. cada una con su última config con su respectivo sistema operativo

LOGGING y BACKUP

FAMS - Logging y análisis forense en la nube(de pago), pasará a llamarse FORTICLOUD

- Recomendado Forti OS 4.3.7+
- se pueden enviar los logs en

tiempo real o programado cuando estos tengan disco duro

- Se pueden hacer backups de las

configs de los FortiGates

- alertas

- graficas
- reporting

-***Solo puede recibir información

de Fortigate, y no otros productos de Fortinet

 $\ensuremath{\mathsf{FAZ}}$ - Fortianalyzer - logs e informes de todos los productos de Fortinet y terceros

- Puede ser en maquina virtual incluso sobre vm player

LOCAL - Local en el FW

FORTIGUARD

A۷

IPS

Estos tres funcionan a nivel de proxy, cuidado con el dimensionamiento.

APP CONTROL

Web Filter y AntiSpam - NO se usa proxy.

Web Filter cache y AntiSpam cache -- guarda en memoria una web categorizada o una reputación de ip para ahorrar consultas a Fortiguard, se puede modificar el tiempo que estarán las entradas en cache

PASSWORD RECOVERY FORTIGATE

Físicamente desde la consola

Nada más salir el login poner user: maintainer y password: bcpb<nºde serie>

Ya estaremos en modo admin FORTIGATE#

INTERFACES

Varios ip con el mismo direccionamiento en interfaces, por ejemplo para hacer de proxy arp para varias ip publicas en la wan

Config system settings --- set allow subnet overlaps

Si tienes HA no puedes tener interfaces en dhcp o ppoe.

ZONAS

Si agrupas interfaces en una zona para administrar reglas luego no podrás crear reglas a interfaces individuales de esta zona

2025/10/12 15:35 3/21 Apuntes de ltCetas

REPLACEMENT MESSAGES

Cambiar los mensajes de notificación del FW como alerta de virus o pagina no permitida, login ssl vpn, etc... config system replace messages

ADMIN PROFILES

Generar perfiles de administración dando permisos a diferentes apartados de configuración que luego asignaras a usuarios

BALANCEO EN SALIDA

En router settings

Hay varios métodos (un único método global)

Source IP

Peso (Weight) - esta se asigna dentro de la config del

interfaz

Spillover - Balanceo por ancho de banda - se asigna dentro del

interfaz

***ojo con las métricas y prioridades ya que puede aplicar a routing asimétrico

Dead gateway detection - métodos para detectar la caída de uno de nuestros routers balanceados

Tiempo de vida (TTL) de las conexiones 3600 segundos por ip origen

POLICY ROUTING

Prioritario sobre cualquier otro tipo de routing

Se puede hace por red/host origen, tipo de tráfico, etc...

OBJETOS

De zona geográfica - objeto de país para utilizarlo en las reglas

TRAFIC SHAPPING

SHARED

	Por defecto el Forti pone el tráfico en
categoría alta	

Hay 3 niveles

Alta - 10 Media - 3 Baja - 1

Ejemplo, por cada diez conexiones

categorizadas como altas envía 3 medias y 1 baja

A parte está el garantizar o limitar por ancho

de banda.

Se puede hacer de dos modos
Per policy - se aplica por
política sumando todas las conexiones de esa política
all policies - suma todas las
políticas que tengan aplicadas el objeto de traffic Shapping

Per-ip

Se aplica por cada dirección ip, por ejemplo limitar a 1MB de internet a un usuario

VIP -

Así se realizan los nats en fortigate

Virtual IP - nat estatico que luego aplicas en las políticas por puerto o por ip completa ip pool - se utiliza para hacer pat con una ip que no es la del interface, por ejemplo para salir a internet con una Publica concreta

LOAD BALANCE

Creamos el Healt Check (monitor) que puede ser ping, tcp o http

Creamos el virtual Server y le asociamos el Healt Check creado. Le configuramos la IP que responderá, el puerto, Tipo de balanceo, persistencia, etc...

1. SSL offloading - puedes poner un certificado para que el Forti cierre el https y hacia dentro vaya por http por ejemplo.

Creamos el Real Server en el que asociamos el virtual server, marcamos el puerto real del servicio, el peso, y otras opciones

2025/10/12 15:35 5/21 Apuntes de ItCetas

Mode- active - está activo - standby - solo se activa si otro servidor real asociado no está activo

Como no hace PAT el servidor real siempre tendrá que tener como GW el Fortigate.

Tipos de balanceo

- 1. first alive elige el servidor real que se ha creado primero y el siguiente entrará cuando el primero caiga
- 2. Least RTT por ping calcula el tiempo de respuesta y elige el más rápido (no vale si el Healt es HTTP)
- 3. Least sessions el que tenga el menor número de sesiones
- 4. https host te balancea en función del http host (búsqueda en la cabecera http) y que está asociado a un campo en el real server

VDOMS

Dominios virtuales o Fortigate's Virtuales

Como mínimo hay que tener un puerto físico o lógico dedicado a un vdom

A partir de la versión 4 además de que se reparten los recursos a nivel hardware se puede asignar recursos de configuración Como que un VDOM no pueda crear más de 10 políticas.

Vdom link, te crea interfaces entre VDOMs para dar conectividad entre VDOMs. Hay que crear políticas en los VDOMs links de un vdom y de otro, como Por ejemplo dar salida a internet al vdom 3 a través de un puerto del Vdom 1.

Para crear un vdom no puede haber ninguna regla ni ruta u otra config que haga referencia a un interface.

*No se recomienda repetir direccionamientos entre interfaces de diferentes VDOMs aunque puede hacerse con: Config system settings — set allow subnet overlaps "en el Vdom global" Para crear un usuario de admin de un único vdom hay que crearlo como prof_admin y asociarlo al vdom concreto *Switch management - hay que marcarle el que tenga acceso a internet para que se actualice el Fortiguard, por defecto es el root y no puede ser el global.

Para cambiarlo se hace desde el global y en VDOMs RESOURCE LIMITS - Editando o creando un VDOM puedes asignar por ejemplo nº de reglas configurables en ese VDOM o limite de VPN's, etc...

AUTENTICACIÓN

REMOTE

LDAP
RADIUS --- En estas 3 hay que validarse
manualmente por http,telnet,
TACACS+

FSSO

WINDOWS

eDirectory novell

+collector en ADirectory - es un soft que se
integra en el ADirectory para que la info entre este y el Forti sea a tiempo
real

Este puede estar en el mismo AD o
no. El collector con el AD trabaja por el puerto 8002 y el collector con el
Forti por el 8000.

Para crear una regla de FW con autenticación en local:

1ºCrear un usuario en user > user 2ºCrear un grupo que incluya este usuario 3ºEditar o crear política marcando en esta el check identity based policy 4ºAñadir los grupos de usuarios

Para crear un objeto LDAP ir a user > remote > LDAP

```
1ºcreate new e introducir los campos
name
ip
Port
cn --- también puede ser SamAccountName y con
este en user vale con que pongas DN=usuario@dominio y su password
DN ej. DC=xxxxxx,DC=local
Type regular
User DN ej.
cn=administrator,cn=users,dc=xxxxxxxx,dc=local ---- recomendado NO USAR
Administrator si no mejor uno que tenga permisos de lectura
password ej. xxxxxxxxx
```

SOFTWARE FSSO - SE INSTALA EN UN SERVIDOR O EN EL MISMO ACTIVE DIRECTORY Y SIRVE PARA CORRELAR EN TIEMPO REAL LOS EVENTOS DEL AD CON EL FORTIGATE

```
0J0, HAY QUE REINICIAR EL SERVIDOR PARA INSTALAR una vez instalado el agente en el servidor ir al fortigate > users > Single sign-on > FFSO agent ponerle un nombre una ip y el password (por defecto - fortinetcanada) cuidado a veces
```

falla una vez creado debería aparecer la flechita azul de desplegable en el objeto FSSO si no es así, hacer check en esta y darle a refresh un par de veces

Luego tendremos que crear un grupo de users de Fortinet SSO y elegir los grupos de nuestro active Directory
Una vez hecho ir la política correspondiente y asignarle el grupo de FFSO dentro del identity based policy

VPN SSL

Iremos a VPN > SSL > CONFIG

Desde aquí podemos configurar:

ip pools - pools de ip "dhcp" para los clientes que se conecten con el cliente vpn, no requerido para tipo portal Server certificate - Certificado que utilizaremos para realizar la conexión/encriptación, se pueden añadir otros.

Require client certificate - esto es para realizar la conexión forzando a un cliente tener certificado concreto, se aplica de forma global y es para todos los perfiles

TIPO PORTAL

Vamos a portal

settings

Desde aquí

configuraremos distintos parámetros de configuración del portal vpn Clean cache -- limpia la cache de tu navegador antes de entrar

Después crearíamos un grupo de

usuarios local o remoto

Users > group >

crear uno y marcar que es para SSL VPN y marcarle a este el portal que queremos

Después hay que crear la política ej., source wan

any, dest lan any, service any, action ssl-vpn después de marcar action ssl-vpn añadiremos el grupo de usuarios a autenticar

Una vez hecho todo esto ya

tendremos el portal creado para dar servicio

Por ejemplo para

smb/cifs pondremos \\ip_Servidor\loquesea

TIPO TUNEL

Se puede hacer que todo el tráfico, incluido internet, pase por el fortigate remoto o con split tunneling para que solo te enrute por el túnel vpn el tráfico deseado Para empezar crearemos un objeto de pool de ip's genérico por ejemplo un /24 y lo elegiremos desde la config global de SSLVPN Crearemos otros pools más concretos dentro de este rango global para luego discriminar.

Después hay que crear un portal con el Widget

Tunnel mode

En este editamos el widget de tunnel y le marcamos split tunnel si es el caso y asignamos el pool que corresponda para este portal concreto marcando

la opción user group y así poder tener diferentes grupos de usuarios dentro de una misma política

Ahora tendremos que crear las políticas

 1° la de wan a la red que deseamos

llegar, una regla por cada segmento interno que queramos permitir y action vpn-ssl

a esta regla hay

que añadirle los grupos de usuarios

 $$2^{\circ}$$ otra regla o reglas con origen ssl.root con los diferentes pools de ip's remotos y destino deseado, la acción ya no será SSL_VPN

3º (opcional) si interesa habría que crear una política desde una red interna del Forti a ssl.root Después necesitaremos crear rutas correspondientes a los pools de ip's que asigna a los clientes remotos a través del interface ssl.root

VPN IPSEC

Se pueden hacer en modo tunnel o con políticas y ambas site-to-site o client-to-fortigate

Doble encapsulación

Phase 1

Negociación de la preshared key, en un primer momento se conocen ambas preshared key pero pasado el keylife se regenera una nueva clave

que solo saben los peers. Cuanto menos keylife más segura será la Phase 1

Phase 2

Se encripta el tráfico que circula por el túnel y es la fase que se encarga de enrutar las redes de extremo a extremo

Pueden haber dos entornos

Que el router por delante del

Forti tenga la ip publica

En este caso hay

que redirigir los puertos 4500 (NAT-T) y 500 (IKE), ambos UDP, a nuestra "wan" en el Forti

Εl

nat-t nos sirve para decir en la encapsulación que la red contra la que se

2025/10/12 15:35 9/21 Apuntes de ItCetas

monta el túnel no es el primer segmento si no el que está detrás del nat.

!!!Nota - si uno de los extremos no tiene ip estática se puede configurar con el DYN-DNS !!!Para VoIP sobre vpn recomendado subir el keylife para evitar posibles cortes en la voz cuando se regenera la clave.

Para empezar iremos a VPN > IPSec > auto key >

new Phase 1

nombre

remote gateway -

elegimos entre ip estática, dyndns, o dialup-user que es para los clientes vpn ipsec (forticlient)

ip address - ip del

peer remoto para el caso site-to-site

local interface -

interfaz en el que se montará el túnel, normalmente wanX.

Mode - agressive

- va sin encriptar el primer paquete de autenticación , recomendado para clientes remotos
- main va encriptado el primer paquete de autenticación, recomendado para site-to-site

Authentication

method - preshared key o RSA signature (Certificado)

Enable ipsec

interface mode - sin habilitar es modo políticas, y habilitado modo túnel

P1 Proposal

encriptación - si conocemos el otro extremos recomendado dejar solo un tipo DH

group - si lo soportan ambos extremos cuanto más alto mejor keylife - comprobar que ambos extremos es lo mismo

Dead

peer detection - comprueba si el túnel esta caido o no

new Phase 2

nombre y phasel

asociada

encriptación

pfs - reenvío de la

generación de claves

Quick mode selector

(split tunnel) - De Forti a Forti no es necesario ya que se hace
con las políticas

- De Forti a otro fabricante si habría que marcarlo

Si queremos establecer el túnel contra un equipo de terceros necesitaremos una Phase 2 por cada red que

queramos enrutar por el túnel con estos definidos en el quick mode selector, además de hacerlo también en la política

Modo política

Nueva política

Hay que hacer una

política de Internal a wan (solo en un sentido no hace falta la vuelta)

Recomendado poner

las políticas de vpn al principio de todo, no afectan al demás tráfico.

Modo túnel

Se crean la Phase 1 y 2 igual excepto en la Phase 1 que hay que marcar Enable IPSEC interface mode

después las reglas se harán entre el interfaz interno y el nuevo Int virtual que se habrá creado dentro del wan y también otra con la vuelta del tráfico, no tendrás que poner action vpn-ipsec

Además habrá que poner las rutas correspondientes a las redes remotas a través del interface virtual

MODO CONCENTRADOR

Sirve para interconectar las site-to-site que tengas configuradas, pero solo pueden hacerse con las que son modo policy $VPN \,>\, IPSEC \,>\, CONCENTRATOR$

FORTIGUARD UTM

ANTIVIRUS

Para hacer la inspección por defecto utiliza el modo proxy, y según el equipo tendrá un límite mayor o menor de conexiones, así que hay que ir con cuidado en el dimensionamiento.

	Se recomienda en equipos pequeños ponerlo en modo flow-based
que	
	el modo en que trabaja es analizar en tiempo real sin parar la conexión mirando únicamente las firmas. Ganas en ancho de banda pero por ejemplo si hay un virus dentro de varios
niveles	
	de un .Zip no lo detecta

La base de antivirus es propietaria de Fortinet

UTM> antivirus > profile

Podemos crear varios perfiles para poder asignar a diferentes segmentos de red

Podemos marcar que los virus se vayan a la

cuarentena

WEB-FILTER

Cada petición que haga el usuario se pregunta a Fortiguard Puede trabajar en modo proxy o en modo flow

UTM> WEB FILTER> PROFILE

Categorías de Fortiguard

Elegiremos el modo de operación,

proxy o flow

Marcaremos Fortiguard Categories y

elegiremos y aplicaremos acciones correspondientes sobre estas categorías

Enable safe search - nos bloqueara

resultados en búsquedas de categorías o palabras bloqueadas

HTTPS Scaning - habilita el

escaneo https

Advanced Filter

Web url Filter -

aquí elegiremos la lista de url manual que hayamos creado

web content Filter

- lista para declarar palabras que queremos bloquear o permitir dentro del contenido de una web

UTM> WEB FILTER> URL FILTER

Desde aquí podemos crear listas customizadas

Creamos una lista y dentro de esta

vamos dando de alta diferentes url manualmente y asignándole una acción

Podemos hacerlo con

tipo:

Simple: www.mundodeportivo.com -- tiene que contener exactamente esta url,

por ejemplo www.mundodeportivo.com/barça no lo bloquearía

Regex: con expresiones regulares de Perl --- mirar documento de referencia

Wildcard: www.mundodeportivo.com/* bloquearía o permitiría todos los

dominios

ACCIONES: block

Permit

Exempt - realiza una excepción si por otra regla, por ejemplo de Fortiguard web Filter, lo está bloqueando

RATING OVERRIDES

Podemos categorizar url's concretas para sacarlas de una categorización automática

!!!!Podemos pedir

que nos valoren de nuevo una url determinada si creemos que es incorrecta desde la parte de Fortiguard > web Filter

APP CONTROL

Va con la licencia de IPS

UTM>Application control

Con esto podemos crear perfiles para controlar mediante policy que aplicaciones podemos usar o no, trabaja con unas 4000 firmas

Se puede filtrar

por Application o por filtro

Por

Application lo haces con la App concreta

Por

Filter puedes generalizar y por ejemplo bloquear todo el p2p

Podemos aplicar el traffic

Shapping por aplicación para no bloquear pero si limitar

Con Session TTL - prevalece este

sobre otro configurado para por ejemplo el ftp en otro apartado del Firewall

Una vez hecho aplicaremos este

perfil en la política de navegación por ejemplo

IPS — Podemos crear diferentes sensores para aplicar a diferentes flujos de tráfico

UTM> IPS SENSOR

Cuando creamos/editamos un sensor podemos:

Hacemos un filtro o añadimos por aplicación

concreta

action -- de las aplicaciones filtradas podemos

aceptar, monitorizar o bloquear

quear

Debajo de action la línea semejante a la superior habilitamos todas las firmas, las deshabilitamos o las dejamos por defecto y entonces algunas estarán activas y otras no

ej. si ponemos Disable all la

action superior no valdrá de nada excepto para monitorizar

packet Logging te analiza a nivel de paquete -

puedes sacar por scp este fichero para analizarlo (wireshark)

Quarantine - mete en la Banned list a la sesión,

usuario, etc...

Hay tres tipos:

atacker ip

 te banea la ip para el servicio bloqueado los demás seguirán funcionando atacker and victim ip por ejemplo si hay un ataque HTTP el ftp dejaría pasarlo para esa ip.

attack incoming interface

- Te bloquea todo el interface cuidado!

***Para ver los baneos y poder eliminarlos ir a USERS> Banned User

Después aplicaremos este profile a una policy

DoS Sensor

Con esto creamos perfiles de denegación de

servicio

aplicamos la política sobre policy> DoS policy Se crean políticas separadas que se asignan al interfaz por donde llega el ataque

!!!!!!!!!!Recomendado, empezar con un sensor en modo Monitor y después de un tiempo analizar el tráfico y a partir de ahí empezar a bloquear

EMAIL FILTER

Perfiles para bloquear el spam en el correo

Analiza, IMAP, POP3, SMTP y seguros, pero

recomendado no utilizar los seguros sin certificado firmado (hace man in the middle)

Casi todos los chequeos son en

base a listas de reputación de ip o dominios

Banned word

Con esto marcamos palabras para poder realizar

acciones sobre mails que las contengan

Por ejemplo porno score 10

Marcamos un peso a

esta palabra y luego en el profile de e-mail

marcamos el

threshold para bloquear si por ejemplo es igual o

supera el valor de

20 (en este caso con que porno saliese dos veces la bloquearía)

DLP — Data leak prevention

Protección de fuga de datos

Te protege por ejemplo para que no puedas enviar un email con un número de cuenta o palabras clave que tú quieras Por ejemplo también podemos

etiquetar documentos con [confidential] y que estos no puedan salir de la compañía

UTM> DLP

Rules: Reglas con expresiones regulares para

marcar lo que nos interese

Compound: Sería un grupo de las rules anteriores

Sensor: En este aplicaremos las rules y

compounds que me interese

Document Finguerprint (solo windows-share de

momento)

Podemos analizar un

directorio de un servidor de ficheros para que

después en función

de los patrones podamos saber si un fichero de

ese directorio está

saliendo de la red

Pondremos la Ip, servidor y un user y password con permiso de lectura También el pattern que tendrá que coincidir con el nombre del fichero que buscamos

Rules

action

block, none, exempt

Quarantine user - bloquea al user solo en ese servicio, por ejemplo un

correo de pepito@xxx.com

Quarantine ip - bloquea la ip

Quarantine interface - bloquea toda la interface

Ban - bloquea la ip y solo al servicio concreto

Archive

none

summary - te da info de lo bloqueado

full - te envía el fichero con todos los datos al Fortianalyzer o equipos

con disco duro (cuidado con la LOPD)

NAC —

Control de pc's, se necesita el forticlient endpoint instalado aunque utilices un antivirus de terceros

Haces que el usuario tenga que cumplir una serie de requisitos para entrar en la red

Application sensor - creamos grupos de

aplicaciones a detectar y acciones a aplicar

Profile - asignas a este profile el sensor

creado

- puedes obligar al

usuario que tenga el antivirus, fw, etc...

- notify host

Policy - tendremos que aplicar el profile anteriormente creado

Application Database - base de datos de aplicaciones detectables por el nac

Forticlient - opciones concretas para el cliente

PROTOCOL OPTIONS

Podemos crear perfiles para modificar protocolos para que por ejemplo el App control no mire solo el puerto 80 para http sino por ejemplo en el 80,8080,8082,etc... o todos los puertos directamente

Dentro de http

Confort Clients - Agiliza la conexión si se está utilizando algún tipo de proxy del Forti, por ejemplo antivirus. Si estuviésemos viendo youtube no pararía la conexión hasta que revise si tiene virus si no que la cargaría más lentamente en función del tamaño de bytes que envías en cada interval

Oversize File/email

Puedes indicar que a partir de un

cierto tamaño no analice la conexión (cuidado)

PARA VER LA CUARENTENA

2025/10/12 15:35 15/21 Apuntes de ItCetas

Log report, Quarantine archive

ANALISIS HTTPS

Hace un man-in-the-middle

Entrega un certificado al cliente y cierra la conexión con este y después abre otra contra la web final

Es posible que de fallo con

algunas páginas de banco o con mucha protección.

Se recomienda poner un certificado firmado para que no aparezca a los usuarios el error típico de certificado

HA – En fortigate funciona a través de arp, solo utiliza una ip por interface en ambos equipos (hasta 5 equipos)

Prerrequisitos - mismo hardware y mismo firmware Tipos - activo/pasivo

1. activo/activo

No es un balanceo entre dos maquinas, uno es el master y recibe

todas las conexiones y se encarga

de balancearlas entre los dos

Cuidado porque si

hay switchs por delante habría que deshabilitar

la comprobación de

macs ya que el paquete después vuelve con una

mac diferente no

con la virtual

Se podría hacer un balanceo real con el comando "config ha > set load-balance-all enable" pero también hay

problemas con el arp

Se puede modificar

el método de balanceo de este "set Schedule": Round-robin - recomendado, reparte por sesión

ip

- hash por dirección ip origen

ipport - igual que ip pero también por puerto

random

least-connection

weight round robin - por peso

Mejor no tener VDOMs antes de

hacer el HA

Por orden mira

1º Nº de puertos, el que más

puertos tenga levantado es master	
	2º Tiempo de vida maquina, el que
más tiempo lleve activo es master	
	3º Device priority el que mas es
master	
	4º Nº Serie más antiguo master

Configuración

system> config> HA

mode

priority - el

master es mayor

group name y

password tienen que coincidir en ambos equipos

enable Session

pickup - replica las sesiones tcp al Slave para un failover mas rápido

port monitor
puertos que monitoriza para hacer un failover en caso de caída

heartbit - puertos

por los que pasa el Healt y el tráfico, a menor priority MAYOR prioridad

Recomendación para añadir un Slave a un standalone existente

	Configurar en el nuevo solo la parte de ha no monitorizar los puertos durante la conexión Conectar solo lo puertos de heartbit en el Slave Una vez se vea el cluster en el master conectar
los cables del Slave	
	No puedes tener un interface en DHCP para montar
НА	

CLI Troubleshoot y demás en HA

execute ha disconect - desconecta el equipo desde el que lo hagas del cluster, cuidado porque se pondrán los dos activos... quitar antes los cables de servicio ha sync - fuerzas resincronización ha Manage - te permite saltar al otro dispositivo Diagnose debug Application hasync 6 Diagnose debug Application hatalk 6 -- niveles de debug Diagnose debug enable

OPTIMIZACIÓN WAN

2025/10/12 15:35 17/21 Apuntes de ItCetas

Mejora de rendimiento en redes wan Dos modos de funcionamiento

modo peer - mallado entre equipos (se hace una vpn ipsec) modo activo pasivo - permite:

- activo pasivo entre Fortigate y forticlient connect con licencia optimización WAN
- activo pasivo entre FortiGates, uno es el activo y los demás pasivos (concentrador)

Es capaz de comprimir FTP,CIFS,FTP

Config -

Desde wan opt.& cache Creamos un nombre de ID local - local Peer host ID Damos de alta los FortiGates a los que te vayas a unir poniendo el ID y la IP Authentication group - aquí haremos la autenticación entre los peers name - todos los que queramos interconectar tienen que tener el mismo nombre de grupo podemos elegir por certificado o preshared-key password Accept defined peers - conectara contra todos los declarados anteriormente Rule - crearemos las reglas parecidas a VPN Full optimization - para mas protocolos source - red local dest - red remota port - podemos marcar puertos concretos auto detect - off - modo peer passive o active para el otro modo protocol - puede ser todo tcp peer - elegir el otro extremo Transparent mode - si marcamos esto no hace falta policy de Firewall byte catching - me traigo solo a cache los bites que hayan cambiado enable ssl - es para montarlo por el 443 enable secure túnel - ipsec auth group - elegir el grupo antes creado Hay que repetir esta regla en el sentido opuesto

PRACTICA VDOMS CON SALIDA A INTERNET COMPARTIDA

WAN1 Va a ser la salida a internet compartida entre dos VDOMs, el 1 y el root

Primero creamos el Vdom1 y le asignamos el interface wan2 como
Internal para este desde el vdom Global
Creamos un Vdom Link desde interface (desde vdom global)
Configuramos el interface 0 como el local, vdom1
con ip 1.1.1.2/30
Configuramos el interface 1 como el remoto, vdom
root con ip 1.1.1.1/30
Creamos una ruta por defecto en el vdom1 hacia la ip 1.1.1.1
del vdom link
Creamos una regla en el vdom1 desde wan2 al vdom link
correspondiente al root con permiso any y nat (pat), así no necesitamos ruta
de vuelta y el root no nos ve nuestro direccionamiento en vdom1
Creamos una regla en el vdom root desde vdom link
correspondiente al vdom1 a wan1 con permiso any y nat (pat)
OPCIONAL - Creamos un pool dhcp en el interface wan2(Internal

DIAGNOSE CLI

SNIFFER - EJEMPLO

vdom1) Desde Vdom1

```
FG50BH3G09600089 # diagnose sniffer packet any icmp 4 -- con el 4 por ejemplo marcamos que nos aparezcan los interfaces interfaces=[any]
filters=[icmp]
6.953015 Internal in 192.168.1.110 ->
212.0.97.82: icmp: 192.168.1.110 udp port 64173 unreachable
6.953067 wan1 out 172.29.62.174 -> 212.0.97.82: icmp: 172.29.62.174 udp port 64173 unreachable
6.953078 eth0 out 172.29.62.174 -> 212.0.97.82: icmp: 172.29.62.174 udp port 64173 unreachable
6.953113 Internal in 192.168.1.110 ->
212.0.97.81: icmp: 192.168.1.110 udp port 64173 unreachable
6.953146 wan1 out 172.29.62.174 -> 212.0.97.81: icmp: 172.29.62.174 udp port 64173 unreachable
6.953156 eth0 out 172.29.62.174 -> 212.0.97.81:
```

2025/10/12 15:35 19/21 Apuntes de ltCetas

icmp: 172.29.62.174 udp port 64173 unreachable

6 packets received by Filter

0 packets dropped by kernel
FG50BH3G09600089 #

TEST LDAP

diagnose test authserver ldap "nombre_del_remote_ldap" username
password

TROUBLESHOOT VPN

diagnose debug Application ike 6 -- nivel más alto de debug diagnose debug enable

DIAGNOSE TEST APPLICATION

Desde aquí podemos hacer troubleshoot para los diferentes proxys del fortigate y otras aplicaciones ej. FG50BH3G09600089 # config global

FG50BH3G09600089 (global) #
FG50BH3G09600089 (global) #
FG50BH3G09600089 (global) # diagnose test
Application

DIAGNOSE SYS SESSION? —- Relacionado con sessiones

Filter
port
ip dest o source
duration
protocol
policy
etc... Revisar con el interrogante

DIAGNOSE SYS TOP - Es como un top en linux para ver la ocupación de los servicios

				Run Time: 0 days, 4 hours and 17
minutes				
				0U, 0S, 98I; 502T, 152F, 113KF
sshd	182 S	1.3	2.1	
newcli	190	R 0.	3 2.7	
httpsd	71	S 0.	1 3.7	
				ipsengine
49	S < 0.0	19.2		
httpsd	62	S 0.	0 3.9	
cmdbsvr	15	S 0	.0 3.7	•
httpsd	189	S 0.	0 3.0	

	narawai	cirortigatentee	tas http://mtrasos.imo/aoka.ph		
httpsd 30 S newcli 183 S	0.0 0.0	3.0 2.7			
fgfmd 67 S	0.0	2.6			
miglogd 28 S	0.0	2.5		scanunitd	
58 S < 0.0 2.	3				
57 S < 0.0 2.	3			scanunitd	
sqldb 90 S	0.0	2.2			
iked 51 S	0.0	2.2			
37 S < 0.0 2.	2			scanunitd	
5. 5 . 5.5	_			urlfilter	
47 S 0.0 2.	2				
46 S 0.0 2.	2			forticron	
	_		merged_daemons	44	S
0.0 2.1					
fdsmgmtd 54 S		2.1			
authd 48 S updated 52 S	0.0 0.0	2.1 2.1			
upua teu 52 5	0.0	2.1	zebos_launcher	22	S
0.0 2.1					
dhcpd 56 S	0.0	2.1			
dhcpcd 59 S	0.0	2.1			
quard 64 S	0.0	2.1			
snmpd 55 S dnsproxy 66 S	0.0	2.1 2.1			
dnsproxy 66 S sshd 61 S	0.0	2.1			
33114 01 3	0.0	210		wad_diskd	
36 S 0.0 2.	0			_	
ntpd 60 S <	0.0	2.0		_	
65 6 0.0 2	0			alertmail	
65 S 0.0 2.	U			cauploadd	
68 S 0.0 2.	0			cauptoauu	
getty 42 S <	0.0	2.0			
reportd 91 S	0.0	2.0			
uploadd 27 S	0.0	2.0			
43 S 0.0 2.	0			ipsmonitor	
43 S 0.0 2. proxyd 35 S	0.0	2.0			
miglogd 29 S	0.0	2.0			
telnetd 63 S	0.0	2.0			
httpclid 50 S	0.0	2.0			
0.0 3.0			initXXXXXXXXXXX	1	S
0.0 2.0			n	roxyworker	
39 S 0.0 1.	4		ρ	. oxy nor her	

DIAGNOSE SYS KILL - matar servicios

2025/10/12 15:35 21/21 Apuntes de ItCetas

ej. FG50BH3G09600089 (global) # diagnose sys kill -9 182

NOTAS!!!

Para saltar por cli desde el root al vdom

	FG50BH3G09600089 # FG50BH3G09600089 # FG50BH3G09600089 # config vdom
	FG50BH3G09600089 (vdom) # edit <vdom> Virtual Domain Name VD0M1 root</vdom>
VDOM1	FG50BH3G09600089 (vdom) # edit current vf=VD0M1:1
diagnose sniffer packet any icmp	FG50BH3G09600089 (VD0M1) # FG50BH3G09600089 (VD0M1) # interfaces=[any] filters=[icmp]
	<pre>0 packets received by Filter 0 packets dropped by kernel</pre>
	FG50BH3G09600089 (VD0M1) #

Códigos de protocolo

tcp - 6 all - 0 udp -17

From:

http://intrusos.info/ - LCWIKI

Permanent link:

http://intrusos.info/doku.php?id=hardware:fortigate:itcetas

Last update: 2023/01/18 14:36

