Manual de usuario servicio FortiPortal

11



5

Grupo Euskaltel

Contenido

1	Introducción a FortiPortal								
2		Divis	sión p	por tipo de cliente					
3		Port	al we	2b					
4		Dasł	nboa	rd 9					
5		Polít	ica F	irewall11					
	5.:	alación de políticas15							
	5.2	2	Reg	a de acceso18					
6		Obje	etos F	Firewall					
	6.:	1	Zon	e/Interface					
	6.2	2	Fire	wall Objects					
	6.3	3	Secu	rity Profiles					
		6.3.3	1	Antivirus					
		6.3.2	2	Control de Aplicaciones					
		6.3.3	3	Data Leak Prevention					
		6.3.4	1	Email Filter					
		6.3.	5	IPS					
		6.3.0	5	Web Filter					
	6.4	4 Us		r & Device					
7		Viev	v						
	7.:	1	Арр	lication View					
	7.2	2	Atta	ck 44					
	7.3	3	Sand	dbox45					
8		Rep	orts.						
9 Audit									
1(10 Recursos adicionales								
11 Wifi									
	11	1	Mar	aged AP					
	11	2	WiF	i Monitor					
	i Profile								

R

euskaltel 🔇

12	SDV	VAN.		53
12	2.1	SD-۱	WAN status y opciones avanzadas	54
12	2.2	Con	figuración SD-WAN	55
	12.2	2.1	Configuración de interfaces	55
	12.2	2.2	Configuración de SLA	56
	12.2	2.3	Reglas SD-WAN	59
12	2.3	Мо	nitorización SD-WAN	61
12	2.4	Plar	itillas SD-WAN	61





1 Introducción a FortiPortal

Este documento es un manual detallado de las operativas que puede realizar autónomamente un usuario final en la política de seguridad de su firewall virtual en la plataforma ofrecida por Euskaltel, a través de la nueva herramienta Fortiportal.

Fortiportal refleja a través de un portal web interactivo, todas las características de la política de seguridad y aporta visibilidad de los flujos que gestiona dicha política a través de cuadros de mando, gráficos de tráfico, análisis de logs y reportes de datos agregados.

Dispone de acciones tanto de análisis como de cambios en la política que pueden realizarse de forma sencilla.

2 División por tipo de cliente

euskaltel 🔇

No todos los clientes tienen los mismos privilegios para realizar los cambios en los diferentes componentes de la política de seguridad de su firewall virtual.

3

Estos componentes principalmente son:

- **Política Firewall** (reglas de acceso)
- NAT
- Control de aplicaciones
- Web filter (navegación)
- Antispam
- Antivirus
- IPS
- ATP (Advanced Threat Prevention)
- Wifi y FortiAP
- SDWAN

Para organizar dichos privilegios se han seleccionado 3 tipos de clientes, que mostramos a continuación, por orden de menor a mayor número de funcionalidades adquiridas:

- **Cliente Avanzado:** Además de los permisos de acceso y modificación de la política firewall, también maneja los perfiles de Control de Aplicaciones.
- **Cliente con Navegación:** Posee los mismos permisos que el cliente avanzado, a los que añade los de definición de filtrado web (URL Web Filtering) y antivirus para navegación.
- **Cliente Premium:** el perfil más avanzado incluye todos los permisos anteriores, más el control sobre la política de IPS (Intrusion Prevention) y ATP o sandboxing en cloud.

Además existen dos tipos de cliente centrados en dos características concretas de la política de seguridad:

- Cliente administrador FortiAPs
- Cliente administrador SDWAN

Estos dos perfiles de cliente se pueden asignar como único perfil para ese cliente o añadir a los perfiles de administración de política generales, vistos más arriba.

La siguiente tabla recoge la comparativa de los perfiles según sus privilegios de administración y cambios en cada una de las características de su política de seguridad:

		Le	ctura y Escritu	ra	
	Avanzado	Navegación	Premium	FortiAPs	SDWAN
Dashboards	✓	✓	✓	✓	✓
Reportes	✓	✓	✓	✓	✓
Logs View	✓	✓	✓	✓	✓
Auditoria	✓	✓	\checkmark	\checkmark	\checkmark
FW Policy	✓	✓	\checkmark		
Control APP	✓	✓	\checkmark		
URL web filter		✓	\checkmark		
Antivirus		✓	✓		

Tabla 1



5

telecable

IPS		\checkmark		
ATP		\checkmark		
WIFI y FortiAP			✓	
SDWAN				\checkmark

3 Portal web

El servicio de FortiPortal es accesible a través de la URL:

https://fwvirtualportal.com

La página de acceso presenta la siguiente apariencia:

GRUPO EUSKALTEL	
	Portal Firewall Virtual
	Username or email
	Password
	Login Forgat password
	Language English V



En la misma podemos elegir el idioma en el que se mostrarán los diferentes menús:

- Inglés
- Español
- Italiano
- Rumano
- Portugués
- Francés
- Alemán

euskaltel 🔇





Ilustración 2

Tras rellenar los datos de usuario y contraseña, podemos acceder a los menús del portal:

Por	tal Fire	ewall	Virtual
Usernam	e or email		
diente			
Password	I.		
•••••	•••		
		Login	
Forgot p	assword		
		Faciliate	

Si no recordamos la contraseña, existe la posibilidad de recuperarla mediante correo electrónico, de modo temporal, pulsando sobre "Forgot password":







Una vez autenticados, accedemos a la información sobre el firewall virtual, en una ventana como la siguiente:



Ilustración 4

Podemos distinguir las siguientes partes:

1. Barra de usuario

Está en el extremo superior derecho, y contiene los siguientes botones de acceso:



De izquierda a derecha:

Help > Abre una nueva ventana con el manual de usuario como ayuda contextual.

Alerts > Muestra en un pop-up las alertas que afectan al portal o la configuración del firewall virtual

Change Password > Abre una ventana de diálogo que permite cambiar la contraseña de acceso de nuestro usuario. Para ello debemos proporcionar la contraseña antigua y una nueva:





Change Password 😧		×
*Old Password:		
* New Password: 0		
Confirm New Password:		
		Change
llustra	ción 6	

Exit > Cierra la sesión actual en FortiPortal.

2. Panel de administración

M	Dashboard
2	Policy & Objects
≡	Device Manager
۰	View
	Reports
■.	Audit

Incluye los principales menús de acceso a la información sobre el firewall virtual:

• **Dashboard** muestra el cuadro de mando con la información más relevante del estado del firewall virtual y el tráfico que gestiona

~

- **Policy & Objects** da acceso a la política de seguridad del firewall para revisar su configuración y modificarla si se tienen permisos suficientes
- View muestra información relativa a los eventos de seguridad recogidos en los logs de la plataforma. Esta información se puede filtrar o ahondar en ella de modo que podamos investigar en mayor profundidad el tráfico.
- **Reports** accede a los diferentes reportes disponibles desde FortiAnalyzer.
- Audit ofrece un listado de acciones efectuadas por los administradores sobre la política y configuración del firewall virtual.

El panel se oculta si pulsamos sobre (<<) Collapse Sidebar

3. Panel central

euskaltel 🔇

Muestra la información seleccionada en cada uno de los menús, de forma interactiva.

8

A continuación, pasamos a revisar la información que muestra cada uno de los menús generales.

4 Dashboard

Es un cuadro de mando que aglutina toda la información sobre tráfico y eventos en varios gráficos y tablas que llamamos widget.



Mediante los controles de la parte superior, podemos:

- + Widget, añadir un nuevo cuadro de información
- **Refresh**, refrescar la información desde FortiAnalyzer. Está en la esquina superior derecha.
- Scope, cambia la vista de los widgets: All (todos), para un site concreto o Wireless (wifi y FortiAP). En nuestro caso no existe más de un site, por lo que All y site mostrarán la misma información.
- **Filter**, filtra los datos por ventana de tiempo (última hora, último día, última semana o un filtro personalizado)





10

telecable



Ilustración 8

Los widgets que podemos añadir son:

- Top Countries: los países más visitados por la navegación de los usuarios
- Top Threats: las mayores amenazas de intrusión o problemas
- Top Sources: los orígenes con mayor número de conexiones
- Top Destinations: las direcciones IP públicas que más visitan los usuarios
- Top Applications: las aplicaciones más usadas.
- Policy Hits: las reglas con más uso.
- Admin Logins: los últimos accesos de administradores a la configuración
- System Events: logs de los problemas que detecta el sistema.
- Resource Usage: uso de los recursos asignados por la plataforma.

Los widgets son editables al pulsar sobre la barra superior el icono con forma de lápiz

0 <mark>/</mark> 2 🛍

euskaltel 🔇

Por ejemplo, podemos modificar el tipo de gráfico, el número de elementos en el top, y el criterio para ordenarlos:

Top Countries		0/20
Chart Types	map	~
Тор	10	~
Sort by	sessions	~
		CANCEL
		<u> </u>
	Ilustración 9	

Si pulsamos sobre el icono en forma de cubo de basura, eliminamos ese widget del cuadro de mando.

5 Política Firewall

Recoge las reglas de acceso de modo secuencial tal y como están aplicadas en el firewall.

Es accesible desde el menú "Policy & Objects" del cliente:

	IPO EUSKALTEL
Ltd. Dashboard	Policy & Objects
Policy & Objects	Policy Objects
 Device Manager View 	Search
I Reports	
🖻 Audit	

En la pestaña "**Policy**" aparecerá las políticas disponibles. Normalmente sólo hay una, pero pueden ser varias si hay más de un firewall asignado, o si hay varias versiones de política en un mismo entorno.

Las características de cada una se pueden revisar, pulsando el botón derecho sobre el nombre y eligiendo "**View Package Settings**". Sólo si el usuario tiene permisos sobre la política podrá modificar el nombre, si usa o no **Central NAT** y el tipo de Inspección que utiliza globalmente para revisar el tráfico: modo **Flow** (fluido, más rápido para que el usuario no observe cortes de la comunicación) o el modo **Proxy** (la conexión se almacena en un buffer para una inspección más profunda y se sirve al destino cuando acaba esta inspección. El usuario puede notar un poco de retraso). Por defecto será el modo **Proxy**:





Policy Package "DCFW5_SIGIngEKT" ×								
Name	DCFW5_SIGIngEKT							
Central NAT	\checkmark							
Inspection Mode	Flow Provy							
		OK						
	Ilustración 10							

Se puede elegir una de las políticas o paquetes de política, y aparecerá a la derecha, las reglas de dicha política:

Refrest Policy	Refreah Revision Backup Installation P Policy Review																
Show 1	0 In Setti	v entri	ies	Search S	Search (Search b) All												
Seq.#	ID	Name	Source	Destination	Schedule	Service	Authentication	Action	Log	NAT	Web Filter	Application Control	DLP	Email Filter	IPS	SSL/SSH Inspection	Proxy Options
1	11		* all	* all	* always	KALL	ana a oscar a satec a victor	Accept	٥	0	victor_webfilter					deep-inspection	🍘 default
2	5		* all	🖷 LAN	* always	4LL	3 RDPLabo	⊘ Accept	۲	9					😥 default	ertificate- inspection	🙀 default
3	8		* all	🖷 LAN	* always	🔇 ALL	 a Raquel a Web2 a WebAccess a pruebaRaq a pruebaRaq2 a pruebar1 	Accept	ø	٥						certificate- inspection	🕧 default

Ilustración 11

Aparecen dos números asociados a cada regla:

euskaltel 🔇

- **Número de secuencia (Seq. #):** es el número secuencial que indica el orden de la regla dentro de la política.
- Número ID de la regla: es el número unívoco que se genera al crear una nueva regla y que se le asignar para siempre. Si la regla se borra, ese número ID no vuelve a reasignarse.

Hay tres opciones que podemos realizar de forma general con la política y que aparecen encima de la misma:



Ilustración 12

Refresh: actualiza la política desde los firewalls, mostrando en el portal la más actual y sincronizada con los firewalls.



Revision backup: guarda una copia de la política a modo de backup, para volver a ella rápidamente, si realizamos algún cambio erróneo en la misma, posterior al backup.

Si pulsamos sobre este botón, aparece un menú donde podemos ver la copia de seguridad disponible.

Si pulsamos sobre "+Create" se generará un nuevo backup, <u>sobrescribiendo el anterior</u>. Solo es posible una copia de seguridad almacenada a la vez.

Revision Backup						
+ Create						
ID	Name	Creation Time	Comments			
30	WORSKSHOP	1591782741				



Si pulsamos sobre el backup con el botón derecho, aparece el menú de recuperación del mismo ("**Restore**"). Al pulsarlo se carga la política anterior, eliminando los cambios hechos hasta ahora en el paquete de política.

+ Create	2		
ID	Nan	1e	Creation Time
30	WO	RSKSHOP	1591782741
		e Restore	



Ploy Package

Image: Statistic in target

Image: Statistic in target

Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
Image: Statistic in target
I

13

Installation nos muestra las últimas instalaciones y el botón para lanzar una nueva:

Además, existen dos pestañas:

Policy, con la política que tiene guardada el Portal (y sincronizada con FMG).

Review muestra en un formato compacto toda la información sobre las reglas que componen la política y los objetos firewall definidos y UTM en la misma:

Po	² olicy												
ID	Source Interface	Destination Interface	Source	Destination	Action	Status	NAT	Service	Schedule	Authentication	Log	Security Profiles	Comments
11	sslvpn_tun_intf	* any	• all	- all	accept	enable	enable	ALL	* always	ana oscar satec victor	Enable	Victor_webfilter deep-inspection	Clone of 5 test WORK
6	sslvpn_tun_intf	* any	• all	LAN	accept	enable	enable	ALL	* always	RDPLabo	Enable	 Ø default Ø default Ø certificate-inspection Ø default 	
8	sslvpn_tun_intf	* any	• all	LAN	accept	enable	enable	ALL	* always	Raquel Web2 WebAccess pruebaRaq pruebaRaq2 pruebar1	Enable	 Ø default B certificate-inspection M default 	
17	sslvpn_tun_intf	* any	• all	LAN_MAQUETA_SD_WAN VPRN_WAN	accept	enable	enable	ALL	• always	Infovista	Log Security Events	ertificate-inspection default	
2	• any	* any	LAN LAN SD-WAN LAN SOLUCION EMPRESA VPRN_WAN	* all	accept	enable	enable	ALL	* always		Enable	AV-flow default certificate-inspection default_sc	
7	• any	• any	• all	VIP_SRV_10.10.2.10_FTP	accept	enable	enable	FTP FTP_20	• always		Enable	ertificate-inspection default	
9	• any	Vlan_367	LAN	AzureNetwork	accept	enable	disable	ALL	• always		Enable	ertificate-inspection default	
10	Vlan_367	Vlan_320	AzureNetwork	LAN	accept	enable	disable	ALL	• always		Enable	ertificate-inspection default	
13	• any	• any	• all	VIP_10.71.32.2_SDWAN_S3	accept	enable	enable	HTTPS	• always		Log Security Events	 ertificate-inspection default 	
19	• any	• any	* all	VIP_10.110.255.14_SDWAN_S1	accept	enable	enable	HTTPS	• always		Log Security Events	 certificate-inspection default 	comentario test
20	* any	* any	• all	VIP_10.110.255.22_SDWAN_S2	accept	enable	enable	HTTPS	• always		Log Security Events	 ertificate-inspection default 	

Ilustración 16





Address

Name	Туре	Interface	Default Mapping	Comments
AzureNetwork	Address	Vlan_387	IP/MASK:10.250.252.0/255.255.255.0	
FIREWALL_AUTH_PORTAL_ADDRESS	Address	any	IP/MASK:0.0.0.0/0.0.0.0	
LAN	Address	any	IP/MASK:10.10.2.0/255.255.255.0	
LAN SD-WAN	Address	any	IP/MASK:10.110.255.0/255.255.255.0	
LAN SOLUCION EMPRESA	Address	any	IP/MASK:10.200.200.0/255.255.255.0	
LAN_HUB	Address	any	IP/MASK:172.16.0.0/255.255.255.0	
LAN_MAQUETA_SD_WAN	Address Group		LAN_HUB, LAN_SPOKE_1, LAN_SPOKE_2	
LAN_SPOKE_1	Address	апу	IP/MASK:172.16.1.0/255.255.255.0	
LAN_SPOKE_2	Address	any	IP/MASK:172.16.2.0/255.255.255.0	
SSLVPN_TUNNEL_ADDR1	Address	sslvpn_tun_intf	IP Range:10.212.134.200-10.212.134.210	
SSLVPN_TUNNEL_ADDR1_201_124	Address	any	IP Range:10.212.134.200-10.212.134.210	
SSLVPN_TUNNEL_IPv6_ADDR1	IPv8 Address		IP/Netmask:fdff:ffff::/120	
VPRN_WAN	Address	any	IP/MASK:192.168.71.0/255.255.255.0	
all	Address	any	IP/MASK:0.0.0.0/0.0.0.0	
all	IPv6 Address		IP/Netmask:::/0	
autoupdate.opera.com	Address	any	FQDN:autoupdate.opera.com	
google-play	Address	any	FQDN:play.google.com	
none	Address	any	IP/MASK:0.0.0.0/255.255.255.255	
none	IPv8 Address		IP/Netmask:::/128	
swscan.apple.com	Address	апу	FQDN:swscan.apple.com	
update.microsoft.com	Address	any	FQDN:update.microsoft.com	
Service				

Name	Category	Туре	Details	Comments
AFS3	File Access	Firewall Service	TCP/7000-7009 UDP/7000-7009	
АН	Tunneling	Firewall Service	IP/51	
ALL	General	Firewall Service	IP/0	

Ilustración 17

5.1 Instalación de políticas

euskaltel 🔇

Hemos activado en FortiManager el modo **workspace**, de modo que un usuario desde FortiPortal y otro desde FortiManager, no puedan trabajar en un mismo ADOM, <u>en una misma</u> <u>política</u>. Así se evita sobrescribir los cambios de otro usuario.

Es por ello, que, si se hacen los cambios desde FortiManager, tenemos que hacer el bloqueo de la política para poder modificarla.

Para ello, basta con pulsar sobre el botón "Lock" que aparece al lado de nuestro ADOM:



Ilustración 18

Cuando lo pulsemos, cambiará a color verde el icono de candado que aparece al lado del mismo:

Device Manager 🗸 De	evice & Groups Firmware License	Provisioning Templates Scripts SD-WAN				ADOM: SIGIngE	CT Unlock 🚺 🔘
Add Device	oup 🗸 🗎 Save 🖪 Install Wizard 🗙	Tools 🗸					
Managed FortiGate	1 Des Totz	vices al	O Devices Connection Down	2 Devices Device Config Mo	-	B	O Devices Policy Package Modified
	🗹 Edit 📋 Delete 🗉 Import I	Policy 🕹 Install 🗸 🚦 More 🗸 🕫 Column	Settings -				
	Device Name	Config Status	Policy Package Status	Firmware Version	Host Name	IP Address	Platform
	DCFW5	A Modified (recent auto-updated)		FortiGate 6.0.5,build0268 (GA)	DC809FW5	10.114.35.136	FortiGate-1500D
	SIGIngEKT [NAT]	A Modified	OCFW5_SIGIngEKT	FortiGate 6.0.5,build0268 (GA)			vdom
	I	1	lustración 19				

Una vez acabados los cambios, deberemos pulsar sobre "Unlock" para liberar la política y que sea modificada por otro usuario.

A veces, puede estar bloqueada por cambios desde el FortiPortal. En tal caso, aparecerá con un candado rojo al lado del nombre del ADOM, y no nos permitirá hacer cambios. Si pulsamos sobre el ADOM, nos muestra el mensaje de quién tiene bloqueada la configuración. En este caso nos indica que es el usuario del FortiPortal:



Ilustración 20

Si lanzamos la instalación desde FortiManager, tenemos antes que guardar los cambios, con el botón SAVE que aparece en la pestaña de Policy & Objects. Si no los guardamos, no permite hacer la instalación.

euskaltel 🔇





17

telecable

Policy & Objects	~	Polic	cy Packages	¢
 Policy Package 🗸	H	Save	\pm Install \checkmark	

Ilustración 21

Si no está bloqueada por un usuario en el FortiManager, podemos lanzar una instalación, desde FortiPortal.

Para ello, accedemos a la pestaña **Policy**, y luego pulsamos sobre el botón **Instalation**. Aparece el **Installation target** y el estado. Si pulsamos el botón **Install**, se inicia la instalación.

olicy Pa	ackage	
Please s	elect the installation target:	
	Installation Target	Policy Package Status
	DCFW5[SIGIngEKT]	installed
		Install
	11	han sián 22

 Retest
 Revision Badup
 Installation
 Policy

 Policy
 Review

 Policy
 Destination Interface
 Source
 Destination
 Action
 Status
 NAT
 Service

 10
 Interface
 Destination Interface
 Source
 Destination
 Action
 Status
 NAT
 Service

 11
 sslvpn_tun_intf
 Reinstall Packages
 *
 e enable
 ALL
 ENPRESA
 ENPRESA
 ENPRESA
 ENPRESA
 ENPRESA
 Entry
 Entry

Tras pulsarlo, comienza una instalación, y se muestra su avance en una barra:

Ilustración 23

Finalmente muestra el resultado satisfactorio:

euskaltel 🔇

Reinstall Pa	ackages	×
Index	Installation Target	Policy Package Status
1	DCFW5[SIGIngEKT]	install and save finished status = OK

Ilustración 24

Ahora los cambios realizados en la política del portal están realmente instalados en la política de los Firewall Fortigate.

5.2 Regla de acceso

Cada regla se compone de los siguientes elementos, todos ellos editables, al seleccionar la regla con el botón derecho y pulsar "**Edit**":

	Edit Policy:1	
Name		
Groups(s)	a Click to add	~
User(s)	4 of 15 selected	-
Source Device Type	Click to add	-
Incoming Interface	sslvpn_tun_intf	T
Source Internet Service		
Source Address	* all	0
Outgoing Interface	👼 any ,	~
Destination Internet Service		
Destination Address	* all (D
Schedule	💿 always	•
Service	Kall (Ð
Action	▲ACCEPT	•
Obynamic IP Pool Logging Options No Log OLog Security Events @Log All Sessions Capture Packets Enable Web Cache Enable WAN Optimization	n Session Starts	
Enable Disclaimer		
Resolve User Names Usin	g FSSO Agent	

Ilustración 25





Security Profiles							
Enable Web Filter	😵 victo	r_webfliter	~				
Enable Application Control	tefa	uit	~				
Enable IPS	👩 defa	uit	~				
Enable Email Filter	😰 defa	uit	~				
Enable DLP Sensor	📙 defa	uit	~				
Enable VoIP	🗿 defa	uit	~				
Enable ICAP	🐚 defa	uit	~				
Enable SSL/SSH Inspection	📧 deep	-Inspection	~				
Proxy Options	🔞 defa	uit	~				
Traffic Shaping		Click to add		~			
Reverse Direction Traffic Sh	aping	Click to add		~			
Per-IP Traffic Shaping		Click to add		~			
Comments Clone of 5 test WO	RK		.il) 22/1023				

Ilustración 26

1. Regla de acceso:

Define que conexiones son permitidas o no por el firewall:

Name		
Groups(s)	a Click to add	~
User(s)	4 of 15 selected	~
Source Device Type	Click to add	~
Incoming Interface	選 sslvpn_tun_intf	~
Source Internet Service		
Source Address	* all	0
Outgoing Interface	🕦 any	~
Destination Internet Service		
Destination Address	* all	0
Schedule	🧔 always	~
Service	S ALL	0
Action	✓ ACCEPT	~



Se componer de:

euskaltel 🔇

a. Group(s) y User(s): define qué usuarios o grupos de usuarios autenticados pueden acceder al destino definido en la regla, desde los orígenes definidos y por los servicios designados.

19



User(s)	4 of 15 selected	*
	Check all XUncheck all	
	🔲 a Infovista	^
	RDPLabo	
	Raquel	
	Web2	
	Ca WebAccess	~

Ilustración 28

b. Source Device Type: indica qué tipo de dispositivo es el permitido como dispositivo origen. Se puede elegir uno o varios entre los disponibles:

Source Device Type	🕞 Click to add	~
	Check all XUncheck all	
	Mobile Devices	^
	Network Devices	
	Chers Others	
	🔲 all	
	amazon-device	
		~

Ilustración	29
-------------	----

c. Incoming/Outgoing interface: son los interfaces desde los que tiene que venir la petición de conexión y por donde tiene que salir la petición hacia el destino. Cualquier petición de acceso, que venga por otro interfaz o salga hacia otro interfaz será rechazada, aunque esté aceptada por el resto de la regla (origen/destino/servicio)

Incoming Interface	I Vlan_367	~
Outgoing Interface	i Vlan_320	~

Ilustración 30

euskaltel 🔇

- d. Source/Destination Addres: las direcciones IP de los orígenes válidos y los destinos alcanzables a través de la regla. Se pueden elegir entre los objetos de red previamente definidos.
- e. Service: protocolo y servicio que usará la conexión para acceder al destino. Se puede elegir entre los servicios anteriormente definidos.

20

f. Action: define qué acción realiza el firewall con la conexión que cumple todas las condiciones anteriores. Las disponibles son:

ACCEPT (acepta la conexión) DENY (elimina la conexión sin enviar respuesta)

Action	✓ ACCEPT	~
	- 🗸 ACCEPT	^
	O DENY	~

Ilustración 31

Si la acción es **Accept**, aparecerá la opción de NAT, que se ven a continuación.

Si es **Deny**, aparece la opción de guardar los logs de las conexiones que intentan acceder y se rechazan, lo que supone una violación ("**Log violation Traffic**").

2. NAT:

Define si se aplica NAT de origen a la conexión que ha sido aceptada por la regla.

≤NAT

Our Content of the second s

ODynamic IP Pool

Ilustración 32

Hay dos opciones:

- Use Destination Interface Access está habilitado por defecto, y cambia la dirección IP origen por la dirección IP definida en el interfaz de salida de la conexión. Se puede forzar que el puerto de servicio no cambie el puerto origen de la conexión, activando la función "Fixed port"
- Dynamic IP pool, aplica el NAT definido en un IP pool específico. Al seleccionarlo aparece un desplegable con todos los ip pool definidos en el equipo, para seleccionar el deseado.

3. Opciones de logging

Un log por cada sesión iniciada bajo una regla en concreto se genera en el firewall y se almacena en la plataforma.



Podemos elegir entre no guardar ese log (**No Log**), guardar sólo los eventos de seguridad (**Log Security Events**) como son los eventos de antivirus, control de aplicaciones, etc., o guardar todos los logs de todas las sesiones (**Log All Sessions**).

En este último caso, podemos además guardar una captura de paquetes de la conexiones que sean aprobadas por esta regla (**Capture Packets**).

Normalmente el log de la sesión se genera cuando la sesión finaliza. Si queremos que se genere al inicio de la conexión, deberemos seleccionar **Generate Logs when Session Starts.**

Logging Options No Log Log Security Events Cog All Sessions Generate Logs when Session Starts Capture Packets

Ilustración 33

4. Caché

En cada regla hay dos opciones de caché para todo el tráfico que es aceptado en dicha regla. Puede aplicarse al tráfico de navegación web (**Enable Web Cache**) o a todo el tráfico (**Enable WAN Optimization**):

Enable Web Cache

Enable WAN Optimization

Ilustración 34

La caché habilitada permite almacenar en un buffer las páginas web y ficheros que descargan los usuarios para proveerlo rápidamente a otro usuario que pida el mismo recurso.

No se recomienda habilitar ninguna de estas dos opciones.

5. Disclaimer

euskaltel 🔇

Tampoco está permitido habilitar esta opción, ya que no se ha definido una política de **disclaimer** (aviso) cuando se navega a través de esta regla.

22

telecable

Enable Disclaimer
Redirect URL

Ilustración 35

6. Resolución de nombre usando FSSO

La autenticación de usuarios mediante FSSO permite conocer el equipo desde el que está conectado, de cara a la autenticación en la regla.

Si este servicio está activo, Grupo Euskaltel procederá a habilitar las reglas con esta opción.

No está permitido que el cliente lo habilite sin consultarlo.

Resolve User Names Using FSSO Agent

Ilustración 36

7. Securtity profiles

Permite seleccionar los perfiles de seguridad (Antivirus, Web Filter, Control de Aplicaciones, IPS, Email Filter, DLP, VoIP, ICAP, Inspección SSL/SSH y opciones de proxy) que podemos aplicar

Security Profiles		
✓Enable Web Filter	Victor_webfilter	~
Enable Application Control	default 👘	~
Enable IPS	🕞 default	~
Enable Email Filter	📧 default	~
Enable DLP Sensor	📴 default	~
Enable VolP	🚛 default	~
Enable ICAP	😰 default	~
✓Enable SSL/SSH Inspection	a deep-inspection	~
Proxy Options	🝓 default	~

Ilustración 37

Solo serán editables los permisos asignados al perfil del cliente, contratados por el mismo.

Para aquellos perfiles de seguridad permitidos, podremos elegir cual aplica a la regla en cada caso, entre los predefinidos en el firewall.

Dichos perfiles de seguridad podrán ser editados, creados y eliminados por el cliente siempre que estén habilitados según su perfil.

La inspección SSL/SSH y las opciones de proxy no deben modificarse para no afectar al tráfico de la regla. Si se quieren modificar, se debe notificar a Grupo Euskaltel.





8. Conformado de tráfico

Se puede aplicar a las reglas una limitación de tráfico por caudal (Mbps). Podemos seleccionar entre un perfil de conformado (**Traffic Shaping**) compartido por todas las conexiones permitidas por dicha regla, o un perfil de conformado que aplique sus límites sobre las conexiones provenientes de una misma ip (Per-IP TRaffic Shaping).

Además, en la primera opción (general), podemos aplicar también los límites del conformado al flujo inverso (destino>origen), seleccionando la opción **Reverse Direction Traffic Shaping.**

□Traffic Shaping	🖬 Click to add	~
Reverse Direction Traffic Shaping	Click to add	~
Per-IP Traffic Shaping	Click to add	~

Ilustración 38

9. Comentario

euskaltel 🔇

Por último, podemos añadir a la regla un comentario que ayude a identificar su propósito.

No puede superar los 1023 caracteres.

Comments	Clone of 5 test WORK	
COMMENTS	(=	

Ilustración 39

Todas estas características son visibles en la política por cada una de las reglas. Podemos elegir cuales se ven en la vista general de la política, pulsando sobre "**Column Settings**" y activando las columnas que necesitemos:



25

telecable



Ilustración 40

6 Objetos Firewall

euskaltel

Este menú recoge todos los objetos que son modificables en la política de seguridad.

Se accede desde la pestaña de Objetcs en la vista "Policy & Objects"

Allí podemos ver qué tipo de objetos están disponibles para su edición, agrupados en 4 tipos:

Policy & Objects



Ilustración 41

- **Zone/interface:** hace referencia a los interfaces de red del firewall y las zonas a las que están asociados. Dichas zonas son asociaciones de interfaces
- **Firewall objects:** son los objetos de red y servicios que se aplican en la definición de las reglas de acceso
- Security & Profiles: incluye los perfiles de seguridad avanzados y su definición
- User & Device: define los usuarios, grupos y tipos de dispositivos que se utilizan para autenticar las conexiones a través de la política de acceso.

6.1 Zone/Interface

Muestra los interfaces definidos en la política y a qué interfaces físicos o lógicos está asociados en el firewall virtual.

DCges2fmanagereus/SIGIngEKT	~ 0			
			Search Search by All	
Interface	1 Default Mapping	11 Per-Device Mapping	1 Description	
 Interface (6) 				^
any				
sslvpn_tun_intf				
sd-wan				
Vlan_320		DCFW5 (SIGIngEKT) : Vlan_320		~
Showing 1 to 6 of 6 entries				



6.2 Firewall Objects

euskaltel 🔇

Su administración está permitida por los tres perfiles: navegación, avanzado y premium.

Incluye la definición de objetos de los siguientes tipos:







A. Address

Cada objeto define una red o host en formato IP, FQDN o un país.

DCges2/managereus/SIGIngEKT v 0 Show 10 v entries			Search Search by All	
Name	Туре	Interface	Default Mapping	Comments
AzureNetwork	Address	Vlan_367	IP/MASK:10.250.252.0/255.255.255.0	
E FIREWALL_AUTH_PORTAL_ADDRESS	Address	any	IP/MASK:0.0.0/0.0.0.0	
E LAN	Address	any	IP/MASK:10.10.2.0/255.255.255.0	
LAN SD-WAN	Address	any	IP/MASK:10.110.255.0/255.255.255.0	
LAN SOLUCION EMPRESA	Address	any	IP/MASK:10.200.200.0/255.255.255.0	
E LAN_HUB	Address	any	IP/MASK:172.16.0.0/255.255.255.0	
E LAN_MAQUETA_SD_WAN	Address Group		LAN_HUB, LAN_SPOKE_1, LAN_SPOKE_2	
LAN_SPOKE_1	Address	any	IP/MASK:172.16.1.0/255.255.255.0	
LAN_SPOKE_2	Address	any	IP/MASK:172.16.2.0/255.255.255.0	
SSLVPN_TUNNEL_ADDR1	Address	sslvpn_tun_intf	IP Range:10.212.134.200-10.212.134.210	
Showing 1 to 10 of 21 entries				First Previous 1 2 3 Next Last



Puede ir asociada a un interfaz o a ninguno en concreto (any):

Edit Address: LA	N_SPOKE_2	×
"Name: Comments: "Color:	LAN_SPOKE_2	.il 0/255
*Type: *IP/Netmask:	IP/Netmask 172.16.2.0/255.255.255.0	~]
*Interface:	any	~
	s	ave Cancel
	Ilustración 45	

Debemos definir el nombre, y la IP y máscara de red, como podemos ver arriba.

Para los grupos, basta con definir el nombre, el color del objeto y los miembros:





Edit Address	Group: LAN_MAQUETA_SD_WA	N 3	ĸ
* Name:	LAN_MAQUETA_SD_WAN		^
Comments:		0/255	
*Color:	1		
Members:	LAN_HUB X		
	LAN_SPOKE_1 X		v
		Save	

Ilustración 46

B. Schedule

Es el periodo de tiempo en el que una regla está activa.

Puede ser recurrente o aplicado a una única ventana de tiempo.

Si es recurrente, podemos estipular la hora de comienzo y final, y los días de la semana en los que está activo:

	Schedule Type Recurring One Time	
	*Name: always	
	*Color: 🐻	
	* Day: 🗹 Sun 🗹 Mon 🗹 Tue 🗸 Wed 🗸 Thu	Friv Sat
	* Start Time: 0 V Hour 0 V Minute	
	* Stop Time: 0 🗸 Hour 0 🗸 Minute	
tes: If the stop time is	et earlier than the start time, the stop time will be during next day. If the start time	ne is equal to the stop time, the schedule will run for 24 hours.

Ilustración 47

C. Service

Son los servicios IP (TCP/UDP/ICMP etc) asociados a un puerto de destino:





DCges2fmanagereus/SIGIngEKT 🗸 🛛						
Show 10 v entries				Search Search by All		
Name	Category	Туре	Details			Comments
G AFS3	File Access	Firewall Service	TCP/7000-7009 UDP/7000-7009			
K AH	Tunneling	Firewall Service	IP/51			
6 ALL	General	Firewall Service	IP/0			
G ALL_ICMP	General	Firewall Service	ICMP / ANY:ANY			
C ALL_ICMP6	General	Firewall Service	ICMP6 / ANY:ANY			
S ALL_TCP	General	Firewall Service	TCP/1-85535			
C ALL_UDP	General	Firewall Service	UDP/1-65535			
4 AOL		Firewall Service	TCP/5190-5194			
6 BGP	Network Services	Firewall Service	TCP/179			
CVSPSERVER		Firewall Service	TCP/2401 UDP/2401			
Showing 1 to 10 of 93 entries				First Pre	vious 1 2 3 4 5	10 Next Last

Ilustración 48

Para definirlo debemos seleccionar un nombre, el tipo de protocolo (normalmente TCP/UDP/SCTP) y los puertos de origen y destino.

Se pueden añadir varias combinaciones de puertos, para un mismo servicio, mediante el botón **Add** que aparece en la definición del servicio.

Edit Service: HTTPS					×
	*Name: Comments: *Color: Service Type: *Category:	HTTPS	v/255		
Protocol	Protocol:	TCP/UDP/SCTP	Destination Port		
TCP V	Low	High 65535	Low 443	High 443	
					Save Cancel

Ilustración 49

D. Virtual IP

Recoge la lista de NATs disponibles para aplicar en la política.

DCges2fmanagereus/SIGIngEKT 🗸			
Name	Туре	Interface	Details
VIP_SRV_10.10.2.10_FTP	Virtual IP	any	62.99.88.142 -> 10.10.2.10-10.10.2.10
VIP_10.71.32.2_SDWAN_S3	Virtual IP	any	62.99.89.228 -> 10.71.32.2-10.71.32.2
VIP_10.110.255.14_SDWAN_S1	Virtual IP	any	62.99.89.228 -> 10.110.255.14-10.110.255.14
VIP_10.110.255.22_SDWAN_S2	Virtual IP	any	62.99.89.228 -> 10.110.255.22-10.110.255.22

Ilustración 50

Pueden ser de tres tipos:

euskaltel 🔇



 Virtual IP es un NAT de entrada que cambia la IP destino pública por una privada. Sirve para natear las conexiones destinadas a un servidor publicado en Internet.

Edit Virtual IP: v	ip-62.99.88.14	1		,
*Name:	vip-62.99.88.14	11		
Comments:				
				đ
	0 / 255			
Color:	(
*External Interface:	any		\sim	
Type:	statio-nat		\sim	
External IP	62.99.89.141			
Address Honge.	62.99.89.141			
Mapped IP Address/Range:	172.18.226.10]		
	172.18.226.10			
Port Forwarding:	disable		\sim	
Enable ARP Reply:	enable		\sim	
Per-Device Mapping	Name	VDom	Details	
	No data availat	le		
			Save	ncel

Ilustración 51

• **Virtual IP Group** es un conjunto de Virtual IP aplicables a una regla, que se asocian para una mejor operabilidad.

create new VIP	Group		×
*Group Name:	VIP-GROUP		
Comments:			
i i) / 255		
Color:	6		
External Zone:			\sim
*Members:	Available	_	Selected
	Search	>	Search
	vip-62.99.88. ^	>>	^
		<	
	\checkmark		\sim
Per-Device Mapping	Name V	Dom	Details
	No data available		
			Save
llustra	ación 52		





En la nueva versión, se pueden añadir diferentes mapeados o asignaciones de VIP según el FW en el que se apliquen (Per-Device Mapping)

Device:	DCFW5[SIGPrueb	92]	\sim
Comments			
	0 / 255		
External	07235		
Interface:			\sim
*Members:	Available	_	Selected
	Search	>	Search
	vip-62.99.88. ^	>>	
	~	<<	

• IP pool es un NAT de salida, para dar acceso a las redes internas a la red pública.

create new IPv4	Pool		×
*Name:	Public-1.1.	1.1	
Comments:			
c) / 255		,d
Type:	overload		\sim
External IP Range From:	0.0.0.0		
External IP Range To:	0.0.0.0		
Enable ARP Reply:	enable		\sim
Per-Device Mapping	Name	VDom	Details
	No data av	ailable	
			Save Cancel

Ilustración 54

Se debe asignar la dirección IP pública a la que se natea. Así como el tipo:

euskaltel 🔇

 Overload. Asigna dinámicamente las conexiones a puertos origen traducidos (PAT), de modo que con una IP púnlica se puedan atender 60416 conexiones.

telecable

- One-to-one. Es un NAT estático que asocia una IP privada con una pública y no mediante la asignación de puertos concretos, como en el caso de overload.
- Fixed-port-range. Define un grupo de puertos asignados a cada una de las ips origen privadas que utilicen el NAT. Es un caso particular del overload.
- Port block allocation. Permite seleccionar el tamaño de bloques de puertos utilizados en PAT y el número de bloques por IP origen. Es como el caso anterior, pero aquí podemos definir el tamaño de los rangos.

Por defecto siempre se utilizará la opción Overload.

Se permite también en esta versión el mapeado por FW.

La opción de **ARP Reply** permite que se envíen respuestas ARP cuando se recibe una petición para una IP contenida en el pool. Se debe dejar marcada por defecto.

6.3 Security Profiles

Como hemos comentado anteriormente, los perfiles de seguridad no están accesibles para todos los clientes. Es por ello por lo que indicaremos en cada funcionalidad qué perfiles tienen acceso para gestionar la misma.



Ilustración 55

6.3.1 Antivirus

Está habilitado para los perfiles de Navegación y Premium.





DCges2fmanagereus/SIGPrueba2 v	0	
Show 10 v entries		
Name		Comments
Demo-flow		flow-based scan and delete virus
() default		Scan files and block viruses.
le sniffer-profile		Scan files and monitor viruses.
🛞 wifi-default		Default configuration for offloading WiFi traffic.

Ilustración 56

Podemos modificar los perfiles de Antivirus, editando los siguientes parámetros:

dit Antivirus Filter I	Profile: Demo-flow
*Name:	Demo-flow
Comments:	flow-based scan and delete virus
Inspection Mode:	Flow-based Proxy
Scan Mode:	● Full ◯ Quick
Detect Viruses:	Block O Monitor
Send Files to S	andbox for Inspection
Please confirm that sandb Sandbox can be enabled ft	ox feature is enabled for the devices to be affected by thischange. or the devices in site management form.
Include Mobile	Malware Protection
Include Mobile	Malware Protection



- Inspection Mode: Es el modo de inspeccionar el flujo de comunicación de una conexión. El modo Flow-based analiza el tráfico de modo fluido en pequeñas porciones de este, comparando con firmas de virus conocidos. El modo proxy hace uso de un buffer de memoria para almacenar temporalmente los archivos que se descargan o envían y cuando lo tiene completo, procede al análisis.
 El modo recomendado es Flow-based, porque evita que el usuario final experimente retrasos en la descarga y la potencia de escaneo es suficiente.
- **Scan Mode:** Permite elegir entre un modo rápido (**Quick**) de escaneo de archivos en búsqueda de virus, o un modo más exhaustivo (**Full**)
- Detect Viruses: Indica la acción a realizar con la conexión en la que se ha encontrado un virus: bloquear dicha conexión (Block) o dejarla pasar y solo generar un log de evento virus (Monitor)
- Send Files to Sandbox for Inspection: Permite el envío de los ficheros analizados a una segunda inspección en un sandbox o ATP que analice las acciones que genera el archivo al ser ejecutado en un pc, y poder catalogarlo como virus si el comportamiento es extraño.
- Include Mobile Malware Protection: Habilita la base de datos de virus que afectan a equipos móviles.

telecable

euskaltel 🔇

34

telecable

6.3.2 Control de Aplicaciones

Está habilitado para los perfiles Avanzado, Navegación y Premium.

Permite controlar qué aplicaciones son las que funcionan a través de un flujo habilitado en una regla.

DCges2fmanagereus/SIGIngEKT 🗸 🔮			
Show 10 v entries		Search	Search by All
Name	Comments		
åi block-high-risk			
는 default	Monitor all applications.		
a sniffer-profile	Monitor all applications.		
a wifi-default	Default configuration for offloading WiFi traffic.		

Ilustración 58

A dicha regla se le aplicará un sensor de aplicaciones (**Application Sensor**), que no es más que una secuencia de reglas de bloqueo o Monitorización, de aplicaciones agrupadas por los siguientes campos:

- Category: habilita las categorías predefinidas, según la finalidad de la aplicación (tráfico P2P, Mensajería instantánea, etc).
- Vendor: se aplicarán todas las aplicaciones creadas por este fabricante.
- Risk: agrupadas por su potencial peligrosidad
- Technology: agrupa por el SO donde se ejecuta la aplicación
- Popularity: en diferentes grupos según su uso popular
- **Application:** por la aplicación en concreto.

Para las categorías, podemos elegir entre las siguientes:

- Botnet
- Business
- Cloud.IT
- Collaboration
- Email
- Game
- General.Interest
- Mobile
- Network.Service
- P2P
- Proxy
- Remote.Access
- Social.Media
- Storage.Backup
- Update
- Video/Audio

euskaltel 🔇

35

telecable

- VolP
- Web.Clients
- Unknown Applications

Una vez que hemos seleccionado las aplicaciones mediante los filtros, procedemos a elegir la acción que aplicará a la conexión en la que se ha detectado una aplicación:

- Allow permite el paso
- Monitor permite el paso, pero genera un evento de seguridad que queda resistrado
- Block no permite el paso y la conexión no se establece

*Name:									
bl	ock-high-risk								
Comments:									
			-ii 0/25	5					
Categories									
Business	Cloud.IT		Collaboration		Email		Game		
Allow	✓ Ø Allow	~	Allow	~	Allow	~	Allow	~	
eneral.Interest	Mobile		Network.Service		P2P		Proxy		
📀 Allow	✓ Ø Allow	~	Allow	~	🖉 Block	~	🔗 Block	~	
emote.Access	Social.Media		Storage.Backup		Update		Video/Audio		
2 Allow	✓ Ø Allow	~	Allow	~	Allow	~	Allow	~	
IP	Web.Client		Unknown Applicatio	ns					
2 Allow	✓ Ø Allow	*	🥝 Allow 🗸 🗸						
pplication Overrid	des								
Application					Category				Action
					No data ava	ailable			
Options									
Deep Inspection	of Cloud Application	ns							
Allow and Log D	ONS Traffic								
	-								

Ilustración 59

6.3.3 Data Leak Prevention

euskaltel 🔇

No es un servicio habilitado para ninguno de los perfiles de cliente.

6.3.4 Email Filter

No es un servicio habilitado para ninguno de los perfiles de cliente.

6.3.5 IPS

Está habilitado para los clientes con perfil Premium.

Policy Objects			
With Firewall Objects With Address With Schedule	DCges2fmanagereus/SIGPrueba2 V Show 10 V entries		
Ca Service	Name	Comments	
G Security Profiles Antivirus Profile Antivirus Profile Antivirus Profile Antiverse Sensor Web Filter Profile	@ all_default	All predefined signatures with default setting.	
	@ all_default_pass	All predefined signatures with PASS action.	
	@ default	Prevent critical attacks.	
Rating Overrides	@ high_security	Blocks all Critical/High/Medium and some Low severity vulnerabilities	
🕀 💾 User & Device	@ protect_client	Protect against client-side vulnerabilities.	
	@ protect_email_server	Protect against email server-side vulnerabilities.	
	@ protect_http_server	Protect against HTTP server-side vulnerabilities.	
	@ sniffer-profile	Monitor IPS attacks.	
	@ wifi-default	Default configuration for offloading WiFi traffic.	

Ilustración 60

De un modo parecido al control de aplicaciones, podemos agrupar las protecciones IPS sobre perfiles, utilizando filtros para seleccionar sólo las protecciones necesarias y requeridas.

Un perfil con muchas protecciones aplicadas no es efectivo, porque tiene que analizar todas ellas sobre un mismo flujo, y ralentiza la conexión.

Es por ello por lo que es importante aplicar sólo las protecciones adecuadas para cada flujo.

Por ejemplo, para una regla que protege el acceso a un servidor web, aplicaremos el perfil **protect_http_server** que excluye protecciones para otros tipos de servidores, como SQL servers, por ejemplo.

Edit IP:	dit IPS Sensor: protect_http_server												
* Name: Comments:		[protect_http_serv	er									
		: 	Protect against HTTP server-side vulnerabilities.										
						Sear	ch						
	Seq.#	Name	Exempt IPs	Severity	Target	os	Action	Status	Packet Logging	Applications	ID	Revision	Matched Signatures
	1		0	all	server	all	Default	default	0	all	1		9084

Ilustración 61

Cada regla de IPS sensor puede filtrar las protecciones por:

euskaltel 🔇

- Severity: según las consecuencias del ataque hasta la caída del servicio.
- Target: divide entre las intrusiones con objetivo un servidor concreto o pc de usuarios (client)
- OS: asocia las protecciones para equipos que comparten sistema operativo (Windows, Linux, etc).

telecable

36

Una vez seleccionadas las protecciones, debemos indicar la acción a aplicar sobre la conexión sospechosa:

- **block** rechaza la conexión
- pass, la permite
- **reject** reinicia la conexión. El atacante recibe ese **reset** y puede saber que se le ha detectado.
- **default** aplica la acción por defecto definida para cada protección, que puede ser bloquear o permitir.

6.3.6 Web Filter

euskaltel 🔇

Policy Objects

Está habilitado para los clientes con perfil de navegación y perfil premium.

Permite crear filtros sobre URLs no permitidas.

Firewall Objects	DCges2fmanagereus/SIGPrueba2 🗸 🗸	
- 🔝 Address - 70 Schedule	Show 10 v entries	
Circle Ci	Name	Comments
G Security Profiles	😵 Prueba_Demo	default web filtering
	Prueba_Demo_Acceso_Limitado	default web filtering
Web Filter Profile	Prueba_Demo_Acceso_Total	default web filtering
del Category del Cat	🐌 default	Default web filtering.
🕀 🛃 User & Device	🐌 monitor-all	Monitor and log all visited URLs, flow-based.
	🐌 sniffer-profile	Monitor web traffic.
	🕉 wifi-default	Default configuration for offloading WiFi traffic.

Ilustración 62

Se aplica mediante categorías y subcategorías. Cada URL es categorizada en una de ellas, y a las conexiones contra esa URL se le aplica la acción definida en su categoría:

Edit Web Filter Profile: Prueba_Demo_Acceso_Limitado	×
Name: Prueba_Demo_Acceso_Limit Comments: default web filtering 21/255 Inspection Mode: Flow-based ● Proxy Seq. ↑1 ID ↑1 URL ↑1 Type ↑1 Action ↑1 Status ↑1 No data available (Right click to create new) No Status ↑1 Status ↑1	FortiGuard Categories FortiGuard Categories Fortentially Liable OF Child Abuse OF Discrimination OF Drug Abuse OF Extremist Groups Hacking OHacking OHacking
llustrac	Save Cancel



38

telecable

Hay dos categorías especiales que debemos tener en cuenta:



Ilustración 64

La primera es **Unrated** (No categorizadas). Aquí se incluyen todas las URLs que no pertenecen a ninguna categoría. Podemos elegir entre dejar pasar la conexión o bloquearla.

La categorización se hace mediante base de datos de Fortinet, donde hay millones de URLs asignadas a las categorías predefinidas.

La segunda categoría especial es **Local Category.** Se trata de una categoría personalizada donde podemos incluir las URLs que necesitemos para aplicar una acción específica.

Pueden ser tantas categorías locales como necesitemos. Se crean en el menú Local Category:

Policy Objects		
Kirewall Objects Kirewall Objects G Schedule	DCges2fmanagereus/SIGPru Show 10 v entries	ebs2 🗸 🖌
Construction Construction	ID	Name
🕞 🍓 Security Profiles – 🛞 Antivirus Profile	140	custom1
- 🚋 Application Sensor - 🝺 IPS Sensor	141	custom2
- 🐨 Web Filter Profile	142	Url_denegada_a_permitir
Rating Overrides Viser & Device		



Se modificarán en Rating Override.

Rating Override

euskaltel 🔇

Para añadir URLs a la categoría local, o a cualquier otra categoría, se habilita la funcionalidad **Rating Override.** Para ello basta con indicar la URL y la categoría a la que la queremos añadir.

olicy Objects			
Birewall Objects Galactic Address Galactic Address Galactic Address	DCges2fmanagereus/SIGPrueba2 v • Show 10 v entries		
Cirtual IP	URL	Status	Category
G Security Profiles ──────────────────────────────────	www.888.com	enable	Url_denegada_a_permitir
- 🕼 IPS Sensor - 🥨 Web Filter Profile			
Web Filter Profile Gal Category GRating Overrides			

Ilustración 66

Si la URL estaba incluida en otra categoría, dejará de estar en ella, para incluirse en la nueva. Si no estaba categorizada (unrated), se incluirá en la nueva categoría.

6.4 User & Device

Aquí podremos habilitar los usuarios locales o remotos (LDAP, RADIUS, TACACS+)

licy Objects							
Eirewall Objects Good Schedule	DCges2fmanagereus/SIGPrueba2 v Show 10 v entries						
- Ca Service	Name	Туре	Two-factor Authentication				
Security Profiles	a Sigpruebs2	LOCAL	disable				
	3 User_Provision	LOCAL	disable				
	3 User_Provision2	LOCAL	disable				
C Local Category	a UsuarioAccesoLimitado	LOCAL	disable				
User & Device	3 UsuarioAccesoTotal	LOCAL	disable				
- 🍓 User Group	a UsuarioSinAcceso	LOCAL	disable				
	a guest	LOCAL	disable				
	a josune	LOCAL	Email based two-factor authentication				
	a tuboplast	LOCAL	disable				

Ilustración 67

Si es un usuario remoto, deberemos especificar el servidor de autenticación que esté previamente definido (en FMG o en los propios FGT).

No está permitido crear nuevos servidores remotos desde el Portal.





Create New User Profi	file >	•
Type User Name	O LOCAL O LDAP O RADIUS O TACACS+	
LDAP	Gick to add	
Contact Info		
Enable Two-factor Au EartiTokon Control Content	uthentication	
EndiToken C En	Cife be add	
	Save	
	Ilustración 68	
	Please Select LDAP ×	
	Search	
	Name No data available	
	Ok Cancel	

Ilustración 69

Si el usuario no está en uso, podemos marcarlo como deshabilitado (Disable).

Por ahora **no está implementado** un segundo factor de autenticación para los usuarios, por lo que esta funcionalidad debe dejarse sin habilitar.





7 View

Permite investigar los eventos de seguridad y logs de tráfico generados por las conexiones manejadas por el firewall.

Podemos aplicar varios filtros para obtener sólo los eventos deseados:

Application v All v Last 5 Minutes v 🕒								
Appression Source Destination								
Show 10 ventries								
Application Name	1 Application ID	1 Category	Sent Bytes	Received Bytes	Sent Packets	Received Packets	11 Users	11 Service
udp/123 (Spain)		Unscenned	110656	110732	1456	1457		UDP/123
udp/123 (Spain)		Unscanned	110428	110580	1453	1455		UDP/123
udp/5060 (Spain)		Unscanned	25142714	19308391	61425	29430		UDP/5060
udp/5080 (Spain)		Unscanned	23307588	17782821	59185	27084		UDP/5080
udp/5060 (Spain)		Unscanned	25140100	19306419	61417	29427		UDP/5080
udp/5080 (Spain)		Unscanned	23302924	17779114	59156	27079		UDP/5080

Ilustración 70

El principal filtro es la diferencia entre eventos agrupados por **Application** (Aplicación), **Attack** (Ataque, IPS) y **Sandbox** (ATP).

También permite seleccionar desde más de un firewall virtual (no aplica en nuestro caso, porque solo hay uno) y el periodo de tiempo donde se han dado los eventos (última hora, día, semana, o algo más específico):



Ilustración 71

Tras seleccionar el filtro de información, podemos seleccionar cómo ordenar los eventos, seleccionando una de las pestañas que aparecen justo debajo:

euskaltel 🔇



Application	~ All		\sim	Last 5 Minutes	\sim	0
Application	Source	Destination				
Show 10	 entries 					

Ilustración 72

En el caso de aplicación, podemos ordenar los eventos por la aplicación concreta, por origen o por destino. La información aparecerá ordenada justo debajo.

Vemos a continuación la información que presenta cada tipo de evento:

7.1 Application View

euskaltel 🔇

Muestra los eventos que han activado el control de aplicaciones, ordenados por aplicación:

Application Source Destination									
Show 10 entries									
Application Name	1 Application ID	1 Category	1 Sent Bytes	1 Received Bytes	Sent Packets	1 Received Packets			
udp/123 (Spain)		Unscanned	110858	110732	1456	1457			
udp/123 (Spain)		Unscanned	110428	110580	1453	1455			
udp/5060 (Spain)		Unscanned	25142714	19308391	81425	29430			
udp/5060 (Spain)		Unscanned	23307566	17782621	59165	27084			
udp/5060 (Spain)		Unscanned	25140100	19306419	61417	29427			
udp/5060 (Spain)		Unscanned	23302924	17779114	59156	27079			

Ilustración 73

Para cada entrada podemos ver el ID de aplicación, la categoría, los detalles de paquetes enviados y recibidos y el servicio que usó la conexión:

Category	1 Sent Bytes	1 Received Bytes	1 Sent Packets	Received Packets	1 Users	Service
Unscanned	110656	110732	1458	1457		UDP/123
Unscanned	110428	110580	1453	1455		UDP/123
Unscanned	25142714	19308391	61425	29430		UDP/5060
Unscanned	23307566	17782621	59165	27084		UDP/5060
Unscanned	25140100	19306419	61417	29427		UDP/5060
Unscanned	23302924	17779114	59156	27079		UDP/5060



Si pulsamos sobre cualquier fila, se aplica un filtro sobre las sesiones mostradas, según pulsemos sobre origen, destino o aplicación.

Ese filtro coincide con el seleccionado arriba entre Application, Source y Destination.

Por ejemplo, para aplicación, se ordena filtra por la aplicación (o servicio) seleccionada, y podemos ordenar por el resto de variables: origen y destino, pulsando las pestañas laterales debajo del filtro:



Application	✓ All ✓ Last 5 Minutes ✓ Ø							
Application	Source Destination							
Application (u	Application (udp122 (Spain)) O							
Source	Show 10 v entries							
Destination			Search gearch by Source (or) User Name					
	Source Country	Source	1 Source Port	11 Source Interface	1 Sent Bytes			
	Reserved	192.168.71.99	123	Vlan_320	111340			
	Reserved	192.168.71.99	123	Vlan_320	111340			

Ilustración 75

Para filtrar por origen o destino, pulsamos sobre el origen o destino de una sesión:

Source (10.20	0.200.20) 🖸						
Application	Show 10 v entries						
Destination				Search Sea	rch by Application (or) Country/Category/Risk		
	Application Name	1. Application ID	1 Category	1 Sent Bytes	1 Received Bytes	1 Sent Packets	1 Received Packets
	udp/5060 (Spain)		Unscanned	25173276	19332024	61496	29466
	udp/5060 (Spain)		Unscanned	25168634	19328498	61487	29461
	udp/5060 (Spain)		Unscanned	25165626	19326116	61478	29457
Source (10.200.	200.20) O						
Application	Show 10 v entries						
Destination				Search Search by Destination			
	Destination Country	Destination	t	Destination Port	1 Destination Inte	erface	1 Received Bytes
	Spain	212.142.129.90		5060	Vlan_367		19332024
	Spain	212.142.129.90		5060	Vlan_307		19328498
	Spain	212.142.129.90		5080	Vlan_387		19326116

Ilustración 76

Para quitar el filtro, basta con pulsar el aspa que aparece al lado del filtro en la barra sombreada:

Source (10.200.200.20) 3

Si aplicamos el filtro de origen y destino, aparecerán listadas las sesiones por tiempo, y podremos ampliar la información mediante el botón desplegar (en amarillo):





Source (10.200	200.20) 😋 > Destination (212.142.129.9	0) 😋	
Application	Show 10 v entries		
	†↓ Time	11	Source
	2020-08-10 15:55:21		10.200.200.20
	-Security Level notice Source	2	
	-Country Reser	ved	
	Ilustració	on 77	

Aquí podemos ver mucha más información detallada sobre tiempo, duración, NAT, etc.

00.200.20) O > Destination (212.1	42.129.90) 🛛						
Show 10 V entries							
			Search	Search by Application (or) Country/Category/Risk			
† Time		1 Source	1 Source Interface	1 Destination	1 Destination Interface	1 Application Name	1. Policy II
2020-08-10 15:	55:21	10.200.200.20	Vian_320	212.142.129.90	Vian_367	udp/5080	2
Beauty Level Security Level Source Country Country Course Name Course Type Endpoint ID Endpoint ID Pare Ant Tpe Ant Tpe Ant Tpe Ant Tpe Ant Tpe Ant Tpe Course Co	notice Reserved For KCT019800288 CCXVS 3 0 10 200 200 20 Viar_320 42 99 228 64178 5050 20 900 716 20408 61486 61486 61485 40 MILTS 4 MIS			deneral - cog D - cog D - session - cog D - session - cog D - session - cos D - cos D	000000020 1177325811 1177325811 1177325811 1177325811 1277427 100 1111112 111112 11112 12174273 100 1111112 1111112 111111111111111111		
2020-08-10 15:	traffic 53:01	10.200.200.20	Vian_320	212.142.129.90	Vlan_387	udp/5080	2
2020-08-10 15:	50:51	10.200.200.20	Vlan_320	212.142.129.90	Vlan_367	udp/5080	2

Ilustración 78

7.2 Attack

De manera similar a la vista de aplicaciones, podemos ver la vista de ataques, con los filtros que queramos aplicar:

Attack V All V Last 5	Minutes 🗸 😝					
Attack Source Destination						
Show 10 entries						
Attack Name	†↓ Count	11 Level	11 Device ID	1 Attack ID	1. Policy ID	1. Service
No matching records found						

Ilustración 79

Podemos ver el ataque, el nivel de criticidad de este, cuántas veces se ha producido, la IP del atacante y la política que lo reporta.

Se ordenan de nuevo por tipo de ataque, origen y destino:



Attack	Source	Destination
Show 10	∨ en	tries

Ilustración 80

7.3 Sandbox

Por último, podemos ver los eventos de sandboxing.

Podemos aplicar los mismos filtros temporales y ordenación por evento, origen o destino:

Sandbox V All V Last 5 Minutes	• •						
Sandbox Source Destination							
Show 10 S white							
Device ID	1 Matware Name	1 Level	1 Client Device	1 Risk			
		Ma analytican second forward					

Ilustración 81

De cada evento, se muestra el Malware encontrado, la IP del cliente infectado y el riesgo asociado:

Sandbox Source Destination				
Show 10 v entries				
Device ID	1 Malware Name	1 Level	1 Client Device	11 Risk

8 Reports

euskaltel

El enlace **Reports** del menú principal proporciona el acceso a los reportes <u>generados en</u> <u>FortiAnalyzer</u>, que pueden ser descargados por desde el enlace proporcionado (el icono de flecha bajo la columna Action):

Last 1 Month 0 Show 10 0 entries		Search Search by Report Name	
Created (Europe/Brussels)	Report Name		Action
2020-08-10 05:01:27	DCges2fanalyzereus/SiGingEKT/Cyber Threat Assessment-2020-08-10-0301_5131		*
2020-08-03 05:01:25	DCges2fanalyzereus/SIGIngEKT/Cyber Threat Assessment-2020-08-03-0301_5039		Download
2020-07-27 05:01:24	DCges2fanalyzereus/SiGingEKT/Cyber Threat Assessment-2020-07-27-0301_4783		
2020-07-20 05:04:02	DCges2fanalyzereus/SIGIngEKT/Cyber Threat Assessment-2020-07-20-0303_4715		
2020-07-13 05 00 50	DCges2fanalyzereus/SIGIngEKT/Cyber Threat Assessment-2020-07-13-0300_4593		

Ilustración 82

Podemos filtrar por tiempo, de modo que solo se muestren los reportes generados dentro de la ventana elegida (hoy, ayer, la última semana, el último mes o una ventana específica):



46

telecable



Ilustración 83

El reporte se puede descargar en formato PDF.



Ilustración 84

9 Audit

euskaltel 🔇

Muestra la actividad de los usuarios administradores de la política y los cambios que han aplicado sobre la misma, como pueden ser instalaciones, cambios en objetos, etc.

M. Dashboard	Audit Log List 😡					
Polloy & Objects Device Manager View	Last 1 Day V Show 10 V entries					Search Search by Level User Name/Event Type/Client IP Address/Message
Reports	Date (Europe/Brussels)	Level	User Name	Event Type	Client IP Address	Message
Audit	2020-08-10 00:26:55	info	spuser	Policy Install Progress	10.240.240.3	installation progress for taskid:10846 is completed warning:0, error:0, success:3
	2020-08-10 00:28:38	info	spuser	Policy Install	10.240.240.3	Policy package DCFW5_SIGIngEKT install to device null started with taskid 10840

Ilustración 85

Dispone de una ventana de diálogo para realizar búsquedas por tipo de evento, usuario administrador, IP desde la que se ha conectado un administrador, el mensaje del evento, etc.

Search	Search by Level/User Name/Event Type/Client IP Address/Message					
Message						
installation progress for taskld:10846 is completed warning:0, error:0, success:3						
Policy package DCFW5_SIGIngEKT install to device null started with taskId 10846						

Ilustración 86

Así como un filtro temporal, con las opciones que ya hemos visto (última hora, último día, semana o ventana temporal concreta)



Ilustración 87

10 Recursos adicionales

Aquí se muestran accesos o enlaces web a recursos relacionados con el servicio, como las peticiones de cambios, de nuevos reportes, etc.

Por el momento no se ha implementado ningún enlace.





11 Wifi

Toda la administración de **APs (access points)**, **perfiles de administración WiFi y SSIDs**, se pueden revisar en esta pestaña.

Solo es accesible para los clientes que **han contratado el servicio WiFi** en FortiPortal, que se puede añadir a su perfil de cliente (Avanzado, Navegación o Premium).

11.1 Managed AP

ADOM_WiFi_Test/FW90DP3Z14002610/root +

Muestra los **APs** conectados al firewall, el SSID que utiliza y los canales y perfiles que utiliza cada uno de ellos.

	Access Point	Connect Via	SSID	Channel	Clients	OS Version	AP Profile
Search Managed AP	FP320B3X13002882		Radio 1: FPC-Test2 Radio 2: FPC-Test1	Radio 1: 0 Radio 2: 0	Radio 1: 0 Radio 2: 0		clone-1
🦾 💭 Managed AP	FAP320		Radio 1: Radio 2:	Radio 1: 0 Radio 2: 0	Radio 1: 0 Radio 2: 0		clone-1
🦾 🚛 WiFi Profile	FW90DP-WIFI0		Radio 1: Radio 2:	Radio 1: 44	Radio 1: 0		11n-only

Ilustración 88

Cada uno de los AP puede ser editado (pulsando sobre el mismo, con el botón derecho y seleccionando editar). Cuando estén realizados los cambios, basta con pulsar sobre el botón "Save" para guardarlos.

También con el botón derecho sobre un AP, nos da la opción de borrarlo.





49

telecable

11.2 WiFi Monitor

Permite monitorizar el servicio Wifi, mediante los tres menús que mostramos a continuación:



Ilustración 89

Rogue AP

Muestra la lista de eventos de AP no autorizados que intentan acceder al servicio WiFi. Se puede filtrar por tiempo o hacer una búsqueda por tipo u otra característica:

Rogue AP Li	st La	st 1 Day		~ 📑							
Show 10 • entries Search Search by All (Exception: On Wire?/Signal Strength)											
Detected by	SSID	Mac Id	Status	Security Type	On Wire?	First Seen	Last	Seen	Vendor Info	Channel	Signal Strength
No data available											

FAP

Muestra el listado de FortiAPs registrados en el firewall virtual:

euskaltel 🔇



Ilustración 90

50

telecable

Podemos ampliar información sobre cada equipo FAP, pulsando sobre el icono de cruz verde (más):

FAP Details (FAP320)				3
			C Refre	esh
▼ FAP Details				
Name	FAP320	Serial Number	FP320B3X13002883	
Admin Mode		Status	disconnected	
Connection State	Disconnected	Clients	0	
AP Profile	clone-1	Connection From	0.0.0.0	
OS Version		Board Mac	00:00:00:00:00	
WTP Id	FP320B3X13002883	Mesh Uplink	ethernet	
Join Time		Last Reboot Time		
Last Failure	0 N/A	Reboot Last Day	false	
Last Failure Time		Last Poll on	2019-01-09 17:02:39.0	
► SSID: FPC-Test1	(Radio Id:1)			
▹ SSID: FPC-Test1	(Radio Id:2)			

Ilustración 91

<u>SSID</u>

Muestra los APs ordenados por SSID

euskaltel 🔇

Show 10 ▼ entries.			Search	Search by Site/Ne	twork Name/FAP	
		Status	Bandwidth In		Bandwidth Out	
😑 🔘 FPC-Test1						<u>^</u>
😑 🏾 💻 site1		•	0.00 MB	0.03	B MB	
😑 🕤 n	etwork1					
	FAP320	0	0 Bytes	0 Ву	rtes	
	FP320B3X13002882	0	0 Bytes	0 Ву	rtes	- 1
	FW90DP-WIFI0	0	0 Bytes	29.4	14 KB	-

Ilustración 92

Si pulsamos sobre un nombre de FAP, la información se amplía:

FAP Details (FAP320)				3
			C Refr	esh
▼ FAP Details				
Name	FAP320	Serial Number	FP320B3X13002883	
Admin Mode		Status	disconnected	
Connection State	Disconnected	Clients	0	
AP Profile	clone-1	Connection From	0.0.0.0	
OS Version		Board Mac	00:00:00:00:00	
WTP Id	FP320B3X13002883	Mesh Uplink	ethernet	
Join Time		Last Reboot Time		
Last Failure	0 N/A	Reboot Last Day	false	
Last Failure Time		Last Poll on	2019-01-09 17:02:39.0	
SSID: FPC-Test1	(Radio Id:1)			
SSID: FPC-Test1	(Radio Id:2)			

Ilustración 93

11.3 WiFi Profile

Permite actualizar y borrar perfiles AP, así como manejar los SSIDs en la política WiFi del firewall.



Ilustración 94

AP Profile

Muestra los diferentes perfiles de AP, con sus características de radio.

Cada uno de ellos puede ser modificado o borrado.





Seq.	Name	Platform	Radio 1	Radio 2	Comment
1	11n-only	FortiWiFi local radio	2.4GHz 802.11n/g/b		
2	AP-11N-default	Default 11n AP	2.4GHz 802.11n/g/b		
3	Clone of FAP320B_for_test	FAP320B	5GHz 802.11n/a	2.4GHz 802.11n/g/b	
4	FAP112B-clone	FAP112B	2.4GHz 802.11n/g/b		
5	FAP112B-default	FAP112B	2.4GHz 802.11n/g/b		
6	FAP112D-default	FAP112D	2.4GHz 802.11n/g/b		
7	FAP11C-default	FAP11C	2.4GHz 802.11n/g/b		
8	FAP14C-default	FAP14C	2.4GHz 802.11n/g/b		
9	FAP210B-default	FAP210B	2.4GHz 802.11n/g/b		
10	FAP21D-default	FAP21D	2.4GHz 802.11n/g/b		
11	FAP220B-default	FAP220B/221B	5GHz 802.11n/a	2.4GHz 802.11n/g/b	
12	FAP221C-default	FAP221C	2.4GHz 802.11n/g/b	5GHz 802.11ac/n/a	

Ilustración 95

SSID

Se muestran los **SSIDs configurados**. Se pueden modificar y borrar con el menú que aparece al pulsar el botón derecho sobre uno de ellos.

Seq.	Name	SSID	Traffic Mode	Security Mode	Schedule	Data Encryption	Maximum Clients
1	DFS_323C	DFS_323C	Local Bridge	Open	Always	AES	0
2	FPC-Captive-0	fortinet	Tunnel	WPA2 Only Personal	Always	AES	0
3	FPC-Test1	FPC-Test1	Tunnel	WPA2 Only Personal	Always	AES	0
4	FPC-Test2	FPC-Test2	Tunnel	WPA2 Only Personal	Always	AES	0
5	S311_DFS	S311S_DFS_VAP	Local Bridge	Open	Always	AES	0
6	wifi	fpc_test	Tunnel	WPA2 Only Personal	Always	AES	0

Ilustración 96

Para crear uno nuevo, se debe configurar el nombre, el pool de direcciones IP, la PSK, servidores de autenticación, y VLAN pooling.





53

telecable

Create New SSID			
* Interface Name			
	The Interface Name field is required.		
Alias	5:		
Traffic Mode	e: 🖲 Tunnel 🔍 Bridge 🔍 Mesh		
Addres	s		
* IP/Network Mask	^{CC} 0.0.0/0.0.0.0		
DHCP Server			
WiFi Setting	s		
* SSID	fortinet		
Security Mode	WPA2 Only Personal	•	
* Pre-shared Key			
	The Pre-shared Key field is required.		
Broadcast SSID	: 🖉		
Schedule	always	•	
Block Intra-SSID Traffic	. 🗌		
Filter Clients by MA Addres	C s		
RADIUS Server			
VLAN Pooling	Disable	Ŧ	
Quarantine Hos	t: 📃		

Save	Cancel

Ilustración 97

12 SDWAN

Es una característica de Device Manager, que sólo está accesible para los clientes que lo soliciten explícitamente.

SD-WAN o software-defined wide area, permite crear dos interfaces WAN redundantes para acceso a internet, de forma que la navegación esté balanceada entre ambos. También aporta redundancia en caso de que uno de ellos caiga.

El menú es accesible desde Device Manager, en la barra de acciones principal:

Device Manager \Theta								
SIGIngEKT/DCFW5/SIGIngEKT	•							
Search		SD-WAN			SD-VAN Status: On	Advanced Options	fail-alert-interface: None fail-detect: Enable	✓ Edit
	Interface Members							
- Configuration	Seq.	ID	Port	Status	Weight	Gateway	Ingress Spillover	Spillover
- D Template	No data available							
Chuth Server Settings								
🗄 🗅 System	Performance SLA							
	Seq.	Name	Detect Server		Detect Protocol	Failu	re Threshold	Recovery Threshold
	No data available							
	SD-WAN Rules							
	Seq.	Name		Source	Destination		Criteria	Members
	1	sd-wan		All	All		Source IP Based	All

Ilustración 98

Desde FortiPortal podemos realizar las siguientes opciones:

euskaltel 🔇

- Editar el estado de SD-WAN y opciones avanzadas
- Configurar los interfaces que participan, los SLAs aplicados y las reglas SD-WAN
- Monitotizar SD-WAN a través de las interfaces que participan
- Crear Plantillas SD-WAN para aplicarlas a un ADOM

12.1 SD-WAN status y opciones avanzadas

El panel SD-WAN muestra el estado de este (on/off) y las opciones avanzadas:

- Fail-alert-interface
- Fail-detect

a Internet).

euskaltel 🔇

- SD-WAN	
SD-WAN Status: On	
Advanced Options	
fail-alert-interface: None	
fail-detect: Disable	
	Edit

Ilustración 99

Para habilitarlo pulsamos sobre el botón "Edit" y aparece este cuadro de diálogo:

*SD-WAN Status: Advanced Options fail-alert-interface:	⊖ Enable (● Disable Available		Selected	
	Search		Search	
	ssl.TestDCU IX_MX_TESTDCU IX_TESTDCU_EDGE any	> > <		^
*fail-detect:	Disable		~	
			Save	Cancel

Seleccionamos "**Enable**" en **SD-WAN Status** en primer lugar. A continuación, seleccionamos el **interfaz físico** que queremos monitorizar, **fail-alert-interface** (o también puede ser None o Any, para ninguno o todos) y hablitamos **fail-detect** (detección de caída del interfaz o el acceso

Las dos opciones de configuración y monitorización aparecen debajo de la carpeta de SD-WAN en **Device Manager**

Device Manager	0
TestDCU/OV08SPR	FG01A/TestDCU
Search	
D SE VPN	
- IPSec Phase	≘ 1
- IPSec Phase	≥ 2
🕀 🚍 Router	
🕂 🗀 SD-WAN	
- 🖿 Configura	ation
– 🗀 Monitorir	ng
- 🗅 Template	2
🗆 🗀 Interface	Members
🕂 🗀 Auth Server	Settings
🗄- 🗀 System	

Ilustración 101

12.2 Configuración SD-WAN

Debemos seguir los siguientes pasos:

12.2.1 Configuración de interfaces

Habilitamos los siguientes puntos para la Configuración (Configuration) SD-WAN:

- Interface members son los interfaces entre los que se hará el balanceo
- **Performance SLA** define las características que debe cumplir el interfaz para ser considerado como activo dentro del grupo SD-WAN
- **SD-WAN rules** definen la prioridad de los flujos y sesiones que están establecidas a través de los interfaces físicos que comprenden el servicio SD-WAN

Interface Members										
Seq.	ID	Port	Status	Weight	Gateway	Ingress Spillover	Spillover			
No data available										
Performance SLA										
Seq.	Name Detect Server		Detect Protocol		Failure Threshold	Recovery Threshold				
No data available										
SD-WAN Rules										
Seq.	Name		Source	Destination		Criteria	Members			
1	sd-wan		All	All		Source IP Based	All			

Ilustración 102

En Interface Members añadimos tantos interfaces como necesitemos.

Para definir sus parámetros utilizamos el siguiente cuadro:





Create New Interfac	e Member	×
*Member:	~	
Weight:	The interface field is required.	
Gateway IP:	0.0.0.0	
Status:	🖲 enable 🔘 disable	
Estimated Upstream	۲	
Bandwidth:		
Downstream		
Bandwidth:		
Advanced Options	~	
gateway6:		
priority:	0	
seq-num:	ŧ	
source:	0.0.0.0	
source6:	::	
volume-ratio:	0	
		Save Cancel



- Member permite seleccionar uno de los interfaces físicos disponibles
- Weight da un peso sobre el reparto de carga a este interfaz. El mínimo es 0 y el máximo 255, y mientras más alto es, mayor carga soporta.
- **Gateway IP** es la dirección IP del default gateway para este interfaz. Normalmente es el definido para acceso a Internet en este interfaz.
- Status habilita y deshabilita este intefaz dentro del SD-WAN
- **Estimated Upstream/Downstream Bandwidth** define el ancho de banda de subida y bajada teórico para este interfaz. Se tendrá en cuenta para el reparto de carga.
- Opciones avanzadas:
 - Gateway6 es la dirección IPv6 del gateway en caso de que se utilice IPV6
 - **Priority** asigna una prioridad en el reparto de carga. Mientras más alto el número, mayor prioridad tiene este interfaz.
 - Seq-num es el número de secuencia en el reparto de carga entre los interfaces. Va de 0 a 4294967295.
 - o Source es la dirección origen IPv4 del interfaz
 - **Source6** es la dirección origen IPv6
 - Volumen-ratio es el valor de carga total que soporta el interfaz (por ejemplo: 20, entre una suma de 100 repartidos por los interfaces, da un 20%)

12.2.2 Configuración de SLA

A continuación, activamos el **SLA** que deben cumplir la conexión a través de los interfaces:



ate New Performance SLA			
"Name:			
	The Name field is required.		
*Detect Protocol:	Ping ~		
*Detect Server.	0.0.0.0		
Detect Server 2:			
Members	Availahie	Selecter	
	Search	Search	
		~	
		×	~
SLA:			
D Jitter Threshold (Milliseconds)	Latency Threshold (Milliseconds)	Packet Loss Threshold(%)	
vo data available			
Link Status			
Interval:	1		
	Seconds		
Failure Before inactive:	5		
	(max 10)		
Restore Link After:	5		
	(max 10)		
Action When inactive	(
Update Static Route:			
Update Cascade Interface:			
	enable disable		
Advanced Options	enable disable		
Advanced Options http-get:	enable O disable v		
Advanced Options http-get: http-match:			
Advanced Options http-get. http-match: interval:			
Advanced Options http-get. http-match: interval:			
Advanced Options http-get. http-match: interval: packet-size:			
Advanced Options http-get. http-match: interval: packet-size: threshold-alert-jitter:			
Advanced Options http-get. http-match: Interval: packet-size: threshold-alert-latency:			
Advanced Options http-get. http-match: Interval: packet-size: threshold-alert-latency. threshold-alert-latency.			
Advanced Options http-get. http-match: interval: packet-size: threshold-alert-latency: threshold-alert-latency: threshold-alert-latency: threshold-alert-latency.	(disable (disable		
Advanced Options http-get. http-match: Interval: packet-size: threshold-alert-latency: threshold-alert-latency: threshold-alert-latency: threshold-alert-latency: threshold-alert-latency: threshold-warning-jitter:			
Advanced Options http-get. http-match: Interval: packet-size: threshold-alert-latency: threshold-alert-latency. threshold-alert-packetoss. threshold-warming-jater;			
Advanced Options http-get. http-match: interval: packet-size: threshold-alert-latency: threshold-alert-latency: threshold-alert-packetoss. threshold-warming-jatency.			



Si todos los interfaces cumplen con el SLA, se elegirá el primer link por prioridad, aunque no sea el de mejor ancho de banda. Si ese interfaz deja de cumplir uno de los criterios del SLA, pasará al siguiente con mayor prioridad que sí los cumpla.

Los parámetros para definir el SLA son los siguientes:

- Name o nombre del SLA

euskaltel 🔇

- **Detect Protocol** es el protocolo que se va a utilizar para probar el interfaz. Puede ser PING, TCP ECHO, UDP ECHO, HTTP o TWAMP
- **Detect Server** es la IP de un servidor externo al que se va a intentar acceder con el protocolo de pruebas

57

telecable

- Detect Server 2 es la IP de un segundo servidor de test.



- **Members** permite seleccionar entre los interfaces de SD-WAN, los que se le va a aplicar este cumplimiento de condiciones
- SLA fields son los parámetros físicos para evaluar el interfaz, con sus valores umbrales máximos
 - Link-cost factor permite elegir entre uno o varios criterios de calidad:
 - Jitter o variación de los retardos
 - Latency o retardo
 - **Packet loss** o pérdida de paquetes
 - Thresholds son los valores máximos permitidos para jitter, latency y packets loss:

"link-cost-factor:	Jitter Threshold 🖌 Latency Thresh	nold
	Packet Loss Threshold	
Jitter Threshold:	5	
Latency Threshold:	5	•
Packet Loss Threshold:	0	•

Ilustración 105

- Link status es relativo al estado del interfaz según el SLA
 - Interval es el periodo de tiempo tras el cual se intenta conectar al servidor para comprobar la calidad. Por defecto es 5 segundos, pero puede configurarse entre 1 y 3600 segundos.
 - **Failure before inactive** es el número de fallos tras el cual se considera que el interfaz es inválido. Puede ser entre 1 y 10. Por defecto es 5.
 - Restore link after es el número mínimo de respuestas correctas desde el servidor para considerarlo como recuperado. Tiene los mismos valores que el anterior.

- Action when Inactive

- **Update Static Route** permite cambiar las rutas estáticas tras la caída del interfaz como interfaz válido.
- Update Cascade Interface habilita el update en cascada desde el interfaz.

- Advanced Options

euskaltel 🔇

o http-get es la URL que debe utilizar en vez de ip la sonda si el servidor es HTTP

58

- **http-match** es el string de respuesta del servidor que esperamos para HTTP
- o Interval es el tiempo que esperará la sonda entre pregunta y
- Packet-size es el tamaño de paquete para twapt. El rango es 64-1024

A partir de ahí podemos configurar los umbrales de las tres medidas de calidad (jitter, latencia y pérdida de paquetes), para lanzar alerta de sobrepasado o un aviso (warning) por estar cerca. El valor para jitter y latencia es entre 0 y 4294967295 ms y la pérdida entre 0 y 100 porciento:

- Threshold-alert-jitter
- Threshold-alert-latency
- $\circ \quad \text{Threshold-alert-packetloss}$
- Threshold-alert-jitter
- Threshold-alert-latency
- Threshold-alert-packetloss

12.2.3 Reglas SD-WAN

Y por último añadimos las reglas de SD-WAN para balanceo y prioridad (también conocidas como servicios). Podemos editarlas, borrarlas o crearlas según pulsemos sobre **Edit, Delet o Create New.**

Pulsando sobre Create New, aparecerá el menú de configuración de una nueva regla:





60

telecable

reate New SD-WAN Rules				×
*blowe				
	The Name field is required.			
Souro	• ·			
Address	C Available		Selected	
	dearch		Generation	
	FIREWALL_AUTH_FORTAL_ADDRESS SSLVPN_TUNNEL_ADDR1			
	all	10		
	autoupdate.opera.com	~		
	googie-pray.	44		
	swscan.apple.com			
	update.microsoft.com			
Use	- Available		Selected	
	Search		Search	
	quest	>		
	Baarer	10		
User group	: Available		Selected	
	Search		Search	
	Guest-group	>		
	SSO_Guest_Users	10		
		~		
		**		
"Destination	O Address O Internet Service			
*Address	: Available		Selected	
	search		Search	
	FIREWALL_AUTH_PORTAL_ADDRESS	>		
	all	10		
	autoupdate.opera.com	~		
	google-play			
	swscan.apple.com			
	update.microsoft.com			
Protoco	C TOR O UDR @ ANY O Receive			
*Outgoing Interface	Best Quality () Mnimum Quality (SLA)			
*Interface Members	z Available		Selected	
	Search		Search	
	dmz1	>		
	dmz2	304		
	wan2	-		
*Status Check	۲ ۲			

Ilustración 106

- Name es el nombre de la regla
- Source es el origen de las conexiones a las que aplicaremos la regla. Es la combinación de:
 - Address o la dirección IP origen
 - $\circ \quad \textbf{User} \ o \ usuario$

euskaltel 🔇

- User group o grupos de usuarios
- **Destination** es el destino de las conexiones, formado por la elección de una dirección IP o un servicio:
 - o Address o dirección IP destino
 - o Internet Service predefinido
 - o Internet Service Group también predefinido
 - o Protocol o protocolo utilizado en las conexiones

- **Application** en el caso de Servicio, designa la aplicación de las conexiones verificadas.
- **Application Group** es el conjunto de aplicaciones para verificar en las conexiones.
- Outgoing interface es el criterio para elegir el mejor interfaz de salida entre los miembros del SD-WAN:
 - **Best Quality** mejor calidad en general
 - Minimum Quality (SLA) requiere que llegue a los estándares del SLA
- **Status Check** aparece en el caso de que hayamos elegido mejor calidad es donde se permite elegir el SLA requerido
- **Required SLA Target** aparece en el caso de elegir mínima calidad, para elegir el SLA de la lista de predefinidos.

12.3 Monitorización SD-WAN

En la pestaña de monitorización SD-WAN podemos encontrar el estado de cada una de las reglas de SDWAN en activo, con los parámetros de calidad del enlace y el número de sesiones:

Table Map											
Device	Template	Interface	Packet Loss	Volume(TX)	Volume(RX)	Session	Performace	Jitter	Latency	Bandwidth(TX)	Bandwidth(RX)
FGT60D4613055589(root)		dmz	0%	0	0	0	Ping_gateway	0	0	0	0
							Ping_FAZ	0	0	0	0
							SaaS_SLA	0	0	0	0
FGT60D4613055589(root)		wan2	0%	25.21 KB	3.59 MB	0	Ping_gateway	0	0	0	0
							Ping_FAZ	0	0	0	0
							SaaS_SLA	0	0	0	0



12.4 Plantillas SD-WAN

Permite crear plantillas para aplicar en distintos tiempos sobre el ADOM del cliente. Solo un perfil SDWAN puede estar aplicado en el entorno, a la vez.

La configuración es igual a la vista en el punto 12.2, donde nos permite identificar:

- Los interfaces donde se aplica
- El SLA que tiene que cumplir
- Las reglas SD-WAN
- El modo de fail-over entre interfaces
- El modo de balanceo

-

euskaltel 🔇



create new Template				×
*Name:				
Description	Name is required.			
Description.	0 / 255		1	
Status:	enable	T		
Interface Members	Sequence Number		Member	
	No data available			
Performance SLA	Name Detect Server	Detect Protocol	Fail Time	recovery time
	No data available			
SD-WAN Rule	Name Source Addre	ss Destination Add	iress Criter	ia Members
	No data available			
Fail Alert Interfaces:		*		
Fail-Detect:	disable	•		
Load Balance Mode:	source-ip-based	v		

Ilustración 108



