Cercanía para llegar lejos.

Manual de usuario servicio Fortimanager

11



Grupo Euskaltel

Índice

0.	Introducción	3
1.	Servicio de Fortimanager	4
1.	1. Creación de objetos	4
1.2	2. Creación de servicios	7
1.3	3.Creación de VIPS	8
1.4	4. Creación de objetos IP Pools	10
1.3	5.Configuración política básica de navegación	12
1.0	6.Configuración política básica de navegación con NATs es	pecíficos 14
1.7	7.Integración de políticas en FortiGate	16
1.8	8.Configuración de políticas con calidad de servicio (QoS)	18
1.9	9. Creación de usuarios y grupos locales	20
1.	10. Configuración URL Filtering	22
1.	11.Configuración Control de aplicaciones	24
1.	12.Configuración IPS	26
1.	13.Configuración perfiles antivirus para navegación	29
1.	14.Configuración VPN SSL	30
1.	15.Configuración VPN IPSEC	34
1.	16.Configuración Política DLP	42
1.	17.Políticas de navegación por grupo de usuarios	46
1.	18.Proxy Web	47
1.	19.Balanceadores de carga	51
	1.19.1 Definición del servicio balanceado	51
	1.19.2. Creación de la granja de servidores	53
	1.19.3. Utilización en la política	54

R

telecable

0. Introducción

Dentro del proceso de actualización y mejora del servicio de firewall virtual, el grupo Euskaltel proporciona un nuevo portal de acceso web para la gestión, y monitorización de las políticas, que además de permitir a los clientes acceder a un panel único, aporta las siguientes características y ventajas:

- Nuevo Interface más sencillo, e intuitivo para ayudar a la identificación y respuesta a incidentes de seguridad.
- Administración centralizada: mediante un amplio conjunto de herramientas que permite gestionar todos los dispositivos Fortinet del cliente.
- Realizar copias de seguridad de la configuración.

A continuación, se describe cómo realizar las acciones más habituales de gestión y monitorización de la política del firewall.







1. Servicio de Fortimanager

Para poder realizar cambios sobre las políticas y objetos es necesario bloquearlo.



Para ello sobre el menú de la izquierda nos ponemos sobre IPv4 Policy, botón derecho y seleccionamos **Lock.** Esto permitirá hacer cambio sobre la política, objetos, profiles de seguridad...







Policy	y & Objects ✓	Policy Pa
🖹 Policy	Install Wizard	
Search	New Package	
	Clone Package	
- Prox	New Folder	
Insta 🗠 🕒 Insta	Lock	
	Unlock	
	View Locked Pa	ackages
	Move	
	Edit	
	Delete	
	Delete Policy Check	
	Delete Policy Check Run Script	
	Delete Policy Check Run Script Export to Exce	

Al hacerlo aparecerá un candado en verde indicando que se ha bloqueado y ya podremos realizar nuevas configuraciones.





telecable

μ	Search	Q
÷ 🔒	DCFW5_SIGIng	
	- IPv4 Policy	
	Proxy Policy	
	Installation Targets	
÷ 🗜	default	

Antes de aplicar cualquier cambio, es decir, ejecutar un Install, tendremos que hacer click sobre el botón Save, que como se puede ver, cambia de color cuando se detecta algún cambio.



1.1. Creación de objetos

euskaltel 🔇

Un objeto es una referencia, en la que viene definido habitualmente una dirección IP.

1. Seleccionar en el menú principal la opción de "Policy & Objects".



2. Seleccionar en el menú superior la opción "Object Configurations".

Policy & Objects V Policy	Packages	Object Configurations			
🛎 Policy Package 🗸 👌 Install 🔊	∕ ⊕ AD	OM Revisions 🛛 🍄 Tools 🗸	📌 Collapse	All ≸≣ Object	Selector 🗸
😫 Search Q	Create	e New 🗸 🛛 🗹 Edit 🗸 🖞	Delete 🔳 S	ection 🗸 🤹 🥵	Column Settings -
🖻 🖻 default		201			
 IPv4 Policy 	- #	Name	From	То	Source
Installation Targets		Implicit (1-1 / Total:1)			
	1	Implicit Deny	🗘 any	🗘 any	🗘 all

3. Elegir en el menú lateral izquierdo la opción de "Firewall Objects" y "Addresses".







4. Hacer click en la pestaña "Create new" y en la opción de "Address".



- 5. Procedemos a crear el objeto:
- En el campo Address Name incluiremos un nombre identificativo para el objeto a crear.
- En el campo Type, elegiremossubnet.
- En el campo IP/Netmask especificamos la IP del objeto con su correspondiente máscara.
- En el campo Interface elegiremos "any" No será necesario especificar la interfaz en la creación del objeto. Si se desea utilizar será aquella interfaz a través de la cual se enrutará el tráfico para alcanzar la dirección del objeto que se está creando.

Policy & Objects 🗸 🕴	Policy i	Packages Object Configurations		
ADOM Revisions	Tools 🗸	· · · · · · · · · · · · · · · · · · ·		
Zone/Interface	>	Create New Address		
Firewall Objects	~	Address Name	1	
Addresses		Туре	Subnet	
Wildcard FQDN Addresses		IP/Netmask		
Services		Interface	O anv	
Schedules		Static Route Configuration	OFF	
Virtual IPs		Comments		
IP Pools				
Traffic Shapers				
Security Profiles	>	Add To Groups	Click her	e to select
℁ Security Fabric	>	Advanced Options >		
a User & Device	>	Per-Device Mapping	OFF	







telecable

1.2. Creación de servicios

1. Seleccionar en el menú principal la sección "Policy & Objects" y en la parte superior "Object Configurations". En el panel izquierdo, dentro de "Firewall Objects" seleccionar "Services".

Policy & Objects 🗸 P	olicy	Packa	ges Object Config	urations
🖶 ADOM Revisions 🔅 1	Tools \	/		
Zone/Interface	>	+	Create New 🗸 🛛 🗹	Edit 🍵 Delete 🗔 Colum
Firewall Objects	8		Name	Туре
Addresses			ALL	Custom Service
Wildcard FODN Addresses			ALL_TCP	Custom Service
Windcard F QDIN Addresses			ALL_UDP	Custom Service
Services			ALL_ICMP	Custom Service
Schedules			ALL_ICMP6	Custom Service
Virtual IPs			GRE GRE	Custom Service
IP Pools			GTP	Custom Service
11 1 0015			I AH	Custom Service
Traffic Shapers			ESP ESP	Custom Service
Security Profiles	>		AOL	Custom Service
Security Fabric	>		😰 BGP	Custom Service
6 Liser & Devise	>		DHCP	Custom Service
Coser & Device		1771		Custom Service

2. Para la creación: seleccionar el botón "Create New" y dentro del desplegable la opción "Service".

Policy & Objects 🗸	Policy P	acka	ges Object Config	urations	
ADOM Revisions	🌣 Tools 🗸				
Zone/Interface	>	+	Create New 🗸 🛛 🖉	វ្វEdit 📋 De	lete 🔹 Colun
E Firewall Objects	~	5	ervice	Туре	
Addresses		S	ervice Group	Custom	Service
Wildcard EODN Address	ac	10	W ALL_ICP	Custom	Service
Wildcard PQDIV Address	cs.		ALL_UDP	Custom	Service
Services			ALL_ICMP	Custom	Service
Schedules			ALL_ICMP6	Custom	Service
Virtual IPs			GRE GRE	Custom	Service
ID De ele			GTP	Custom	Service
IP POOIS			🛛 AH	Custom	Service
Traffic Shapers			ESP ESP	Custom	Service
Security Profiles	>		AOL	Custom	Service
X Security Fabric	>		BGP	Custom	Service
6 UL C D I			DHCP	Custom	Service
Coser & Device	1	100	DNS	Custom	Service

- 3. Una vez dentro de la configuración, distinguimos los campos siguientes:
- Name: Nombre significativo con el que se verá el servicio en el editor de políticas.
- Service Type: Por defecto Firewall.

- Category: Nombre de la categoría en la que queremos añadir el servicio nuevo. Normalmente se añadirá en Uncategorized.
- Protocol type: Lo más habitual seleccionar la opción "TCP/UDP/SCTP"
- Protocol: Seleccionamos el protocolo correspondiente "TCP/UDP/SCTP".
- Source Port: Rango de Puertos Origen, por defecto [1-65535].
- Destination Port: Este campo es el que define el servicio, si únicamente se quiere especificar un puerto sería [8080–8080] .

ADOM Revisions	Tools	~		
Zone/Interface	>	Create New Service		
Firewall Objects	~	Name	1	
Addresses		Comments	e	0/25
Wildcard FQDN Addresses				
Services				1
Schedules		Service Type	Firewall OProxy	
Virtual IPs		Category	Uncategorized	Y
IP Pools		Protocol Type	TCP/UDP/SCTP	Y
Traffic Shapers		IP/FQDN	0.0.00	
Security Profiles	>	Add To Groups	Click here to select	
Security Fabric	>	Protocol Source Port	Destination Port	
User & Device	>			
			· · ·	

1.3. Creación de VIPS

Una dirección IP virtual (VIP) es una dirección IP que no corresponde a una interfaz de red física real.

Se establecerá una correspondencia entre una IP pública y una IP privada, de forma que todo el tráfico con destino a esa IP pública se traducirá a la IP privada. Esta traducción se podrá hacer para todos los puertos y protocolos o bien se podrá traducir únicamente un puerto. Incluso cabe la posibilidad de utilizar una única IP para publicar varias IPs privadas, con distintos servicios en cada una de ellas. Por ejemplo, es posible redirigir el puerto SMTP a la dirección privada del servidor de correo, con distinta IP del servidor web, al que se dirigirá el tráfico http.

1. Seleccionar en el menú principal la sección "Policy & Objects" y en la parte superior "Object Configurations". En el panel izquierdo, dentro de "Firewall Objects" seleccionar "Virtual IPs".





telecable



2. Para la creación: seleccionar el botón "Create New" y dentro del desplegable la opción "Virtual IP".



3. Una vez dentro de la configuración, distinguimos los campos siguientes:

- Name: Nombre significativo con el que se verá el objeto en el editor de políticas.
- Interface: En caso de escoger una interfaz específica, solo se podrá utilizar este VIP en aquellas reglas cuya interfaz origen sea la seleccionada.
- Type: Por defecto NAT Estático.
- External IP Address/Range: IP pública que se va a ver internet y sobre las que se van a establecer las conexiones, será traducida por el Firewall a la IP privada.
- Mapped IP Address/Range: IP privada a la que se va a traducir.







T ADOM REVISIONS	10015	~		
W Zone/Interface	>	Create New Virtual IP		
Firewall Objects Addresses Wildcard FQDN Addresses Services	~	Name Comments Color		0/25
Schedules		latarfaca	(a	
IP Pools Traffic Shapers Security Profiles	>	Configure Default Value Network Type	Static NAT ODNS Tra	nslation () FQDN
IP Pools Traffic Shapers Security Profiles Security Fabric	>	Configure Default Value Network Type External IP Address/Range	Static NAT ODNS Tra	nslation OFQDN 0.0.0.0
IP Pools Traffic Shapers Security Profiles Security Fabric User & Device	> > >	Configure Default Value Network Type External IP Address/Range Mapped IP Address/Range	ON OStatic NAT ODNS Tra 0.0.0.0 0.0.0.0	nslation O FQDN 0.0.0.0 0.0.0.0
IP Pools Traffic Shapers Security Profiles Security Fabric Luser & Device	> > >	Configure Default Value Network Type External IP Address/Range Mapped IP Address/Range Source Interface Filter Optional Filters Port Forgarding	ON Static NAT ODNS Tra 0.0.0,0 0.0.0,0 Click to add OFF OFF	nslation OFQDN 0.0.0.0 0.0.0.0
IP Pools Traffic Shapers Security Profiles Security Fabric	> > >	Configure Default Value Network Type External IP Address/Range Mapped IP Address/Range Source Interface Filter Optional Filters Port Forwarding Enable ARP Reply	ON OStatic NAT ○DNS Tra 0.0.0.0 0.0.0.0 Click to add OFF OFF OFF	nslation () FQDN 0.0.0 0.0.0

1.4. Creación de objetos IP Pools

euskaltel 🔇

Se indicará una IP o un rango de IPs que se utilizarán para traducir las direcciones orígenes de la regla, normalmente cuando esas direcciones IPs origen sean privadas y quieran tener acceso a Internet.

1. Seleccionar en el menú principal la sección "Policy & Objects" y en la parte superior "Object Configurations". En el panel izquierdo, dentro de "Firewall Objects" seleccionar "IP Pools".

Policy & Objects 🗸	Policy P	Packages	Object Co	nfigurations	
ADOM Revisions	🌣 Tools 🗸	e -			
Zone/Interface	>	+ Crea	te New 🗸	🗹 Edit 👔	🖞 Delete 🗄
E Firewall Objects	~	Na	me		Туре
Addresses					
Wildcard FQDN Addresse	25				
Services					
Schedules					
Virtual IPs					
IP Pools					
Traffic Shapers					
Security Profiles	>				
X Security Fabric	>				
12 User & Device	>				



telecable

2. Para la creación: seleccionar el botón "Create New" y dentro del desplegable la opción "IPv4 Pool".

Policy & Objects 🗸	Policy Pa	ckages Ob	oject Co	nfiguratio	ns	
ADOM Revisions	🎾 Tools 🗸					
Zone/Interface	>	+ Create N	New 🗸	🗹 Edit	歯 Delete	to C
E Firewall Objects	~	IPv4 Pool	I.	-	Туре	
Addresses		IPv6 Pool	L			
Wildcard FQDN Addresses	i					
Services						
Schedules						
Virtual IPs						
IP Pools						
Traffic Shapers						
Security Profiles	>					
Security Fabric	>					
🙎 User & Device	>					

3. Una vez dentro de la configuración, distinguimos los campos siguientes:

- Name: Nombre significativo con el que se verá el objeto en la edición de la regla.
- Type: Podemos definir varias opciones para la asignación de la IP o rango públicos a las IPs privadas, hacer una asignación uno-a-uno, con sobrecarga, un rango de puerto fijo o la asignación de bloque de puertos.
- External IP Range: IP o Rango de IPs con las que se va a salir a Internet, normalmente será una IP únicamente pero podría definirse un rango o una subred.

Policy & Objects 🗸	Policy	Packages Object Configuration	5				
ADOM Revisions	🌣 Tools	~					
Zone/Interface	>	Create New IPv4 Pool					
B Firewall Objects	~	Name	[]				
Addresses		Comments					0/2
Wildcard FQDN Address	es						
Services							1
Schedules		Туре	Overload	One-to-One	Fixed Po	rt Range	Port Block Allocation
Virtual IPs		External IP Range	0.0.0.0			0.0.0.0	
IP Pools	1	Enable ARP Reply					
Traffic Shapers		Advanced Options >					
Security Profiles	>	Per-Device Mapping	OFF				

euskaltel

1.5. Configuración política básica de navegación

Una política se trata de un conjunto de reglas que definen los accesos permitidos de internet a los servicios internos y viceversa. Estas reglas se definen como una IP o grupo de IPs origen y una IP o grupo de IPs destino así como uno o varios servicios y puertos y la acción que se quiere que se lleve a cabo cuando a través del Firewall se detecte un tráfico que coincide con lo especificado en la regla.

Dicha acción podrá ser básicamente aceptar o rechazar la conexión.

Las reglas se ejecutan de forma secuencial en orden, es decir, se empiezan a aplicar desde la regla más baja, la 1 hasta que se encuentre la primera coincidencia. Habitualmente la última regla es una de denegación total.



1. Seleccionar en el menú principal la opción de "Policy & Objects".

2. Aparecemos directamente en el menú de las políticas, por lo que hacemos click en "Create new".







3. Procedemos a crear la política.

⊙ any	0
○ any	8
OFF	
○ all	8
+	
+	
+	
OFF	
○ all	0
♦ ALL	0
• always	8
	 any any oFF all + + OFF all ALL always

- En el campo Name introduciremos el nombre (se recomienda que sea identificativo) de la política.
- En Incoming Interface se seleccionará la interfaz de entre aquellas configuradas desde donde se recibirá el tráfico proveniente de las IPs origen.
- En Outgoing interface se seleccionará la interfaz de entre aquellas configuradas por la cual el firewall enviará el tráfico hacia la IP destino de la conexión.
- En Source Address se especificará el objeto creado previamente para representar la IP, rango, red o grupos de IPs que será el origen de la conexión establecida.
- En Destination Address se especificará el objeto creado previamente para representar la IP, rango, red, grupos de IPs o IP virtual que será el destino de la conexión establecida.
- En Service se seleccionará el servicio, predefinido o personalizado, o grupo de ellos, que representa el protocolo al que se dará acceso o se rechazará en el destino de la conexión.
- En Action básicamente las acciones que se aplicarán serán ACCEPT, en caso de la que conexión deba ser permitida, o DENY en caso de que sea rechazada.

4. Por último, terminamos haciendo click en OK para crear la regla.





1.6. Configuración política básica de navegación con NATs específicos

El NAT, es una funcionalidad que nos permite realizar una traducción de direcciones para convertir las IPs privadas de la red local de cliente en IPs públicas que tengan acceso a Internet. De forma inversa nos permitirá publicar en Internet una dirección privada de algún servidor al que se tenga que tener acceso desde una red pública.

Esta funcionalidad no siempre será requerida. Se habilitará el NAT si es necesario realizar una traducción de las IPs origen de la regla. Si simplemente se activa esta casilla, se traducirán automáticamente con la IP de la interfaz de destino en el firewall. En caso de que se quiera utilizar otra IP se marcará la opción "Dynamic IP Pool" y se escogerá una de entre las disponibles que se hayan configurado previamente.



1. Seleccionar en el menú principal la opción de "Policy & Objects".

2. Aparecemos directamente en el menú de las políticas, por lo que hacemos click en "Create new".







telecable

3. Procedemos a crear la política.

eate New IFV4 Folicy		
Name		
Incoming Interface	Oany	٥
Outgoing Interface	• any	0
Source Internet Service	OFF	
Source Address	♦ all	۵
Source User	+	
Source User Group	+	
Source Device	+	
Destination Internet Service	OFF	
Destination Address	€all	0
Service	♦ ALL	0
Schedule	• always	0
Action	Deny Accept IPSEC	
Log Traffic	✓ Log Violation Traffic	
	Generate Logs when Session Starts	
Comments		

En el campo Name introduciremos el nombre (se recomienda que sea identificativo) de la política.

- En Incoming Interface se seleccionará la interfaz de entre aquellas configuradas desde donde se recibirá el tráfico proveniente de las IPs origen.
- En Outgoing interface se seleccionará la interfaz de entre aquellas configuradas por la cual el firewall enviará el tráfico hacia la IP destino de la conexión.
- En Source Address se especificará el objeto creado previamente para representar la IP, rango, red o grupos de IPs que será el origen de la conexión establecida.
- En Destination Address se especificará el objeto creado previamente para representar la IP, rango, red, grupos de IPs o IP virtual que será el destino de la conexión establecida
- En Service se seleccionará el servicio, predefinido o personalizado, o grupo de ellos, que representa el protocolo al que se dará acceso o se rechazará en el destino de la conexión.
- En Action básicamente las acciones que se aplicarán serán ACCEPT, en caso de la que conexión deba ser permitida, o DENY en caso de que sea rechazada.
- Para la aplicación de una NAT específica, se habilitará la opción de NAT y podremos elegir dos opciones, que la NAT se realice mediante la ip de la interfaz de salida, o con un Ip Pool dinámico que nosotros hayamos creado.

telecable

Destination Address	👽 all	8
Service	♦ ALL	٢
Schedule	• always	٢
Action	Deny Accept IPSEC	
Log Traffic	○No Log ●Log Security Events ○Log All Sessions	
	Generate Logs when Session Starts	
	Capture Packets	
NAT		
	●Use Destination Interface ☐ Fixed Port Address	
	O Dynamic IP Pool	
Security Profiles		
Shared Shaper	+	
Reverse Shaper	+	
Per-IP Shaper	+	
-		
	OK Cancel	

4. Por último, terminamos haciendo click en OK para crear la regla.

1.7. Integración de políticas en FortiGate

Una vez tenemos creadas un conjunto de políticas, agrupadas en un paquete, hay que integrarlas con el Fortigate. Para ello debemos ir al apartado de Policy & Objects. En el lateral izquierdo de la pantalla y podemos comprobar que tenemos tantos paquetes de políticas como hayamos creado. En nuestro caso tenemos 2 grupos, uno para un firewall y otro para un firewall distinto.



Una vez tenemos creado una política de red para nuestro firewall, debemos incluir dicho firewall en el apartado de Installation Targets. Para ello debemos hacer click en Add.

euskaltel

telecable



Entonces se nos desplegará una pantalla con los posibles objetivos de la instalación del paquete de políticas, de las que deberemos elegir el que deseemos.

In the second second	Trend	Confee Status	Delley Deckney Status
installation	target	Coning Status	Policy Package Status
- FW1809	263	A Modified	@ Unknown
0	[NAT]	✓ Synchronized	A Never installed
0	[NAT]	✓ Synchronized	A Never installed
0	[NAT]	 Synchronized 	A Never installed
6	[NAT]	 Synchronized 	A Never installed
4	[NAT]	Synchronized	A Never installed
6	[NAT]	Synchronized	A Never installed
0	[NAT]	 Synchronized 	A Never installed
@ root []	NAT] (Management)	A Modified	A Never installed
All Group	•		
An Manager	1 FortiGate		
			1/22

El siguiente paso sería instalar dicho paquete de políticas en el objetivo. Para ello desde la pantalla de Policy Packages, hacemos click en Install, y elegimos Install Wizard.

Policy & Objects 🗸	Policy Packages	Object Configurations
🕭 Policy Package 🗸 🛃	Install 🗸 🕀 AD	OM Revisions 🌾 Tools 🗸 🖌 Collapse All 🛛 f≣ Object Selector 🗸
La Search	Install Wizard	ew 🗸 🗹 Edit 🗸 🍵 Delete 🖼 Section 🗸 🎜 Column Settings 🗸
IPv4 Policy	Re-install Policy V	Name From To Source
Proxy Policy Installation Targets Prw_2 IPv4 Policy Proxy Policy Installation Targets default	. 1	Securitas-Egaña (1-5 / Total:5)

Ahora se nos muestra una pantalla donde debemos elegir cual es el paquete de políticas que queremos instalar.

telecable

Install Policy Package & Device Sett	lings		
Install a selected policy package.	Any device specific settings for devi	es associated with the package will	also be installed.
Policy Package	FW1809bl3_	2.0	
Comment		٩	
	default		
L] Create ADOM Revision	FW1809bl3		
Schedule Install	Fw_2		
Jortall Device Sattions (only)	L		

Por último, en función del paquete de políticas que hayamos elegido, y de los Installation Targets que le hayamos asignado, se nos dispondrán unas opciones u otras para instalar dicho paquete de políticas, de las que se podrán elegir como objetivo tantas unidades como queramos.

Install Wizard - Policy Package and Device Setting FW1809bl3

A Device Name	IP Address	Platform
III THE COMPANY OF THE OWNER	CONTRACTOR OF THE OWNER	FortiGate-1500D
450,00x870(Hef)		vdom

Una vez hayamos hecho click en Next, comenzará la carga del paquete en la unidad elegida.

1.8. Configuración de políticas con calidad de servicio (QoS)

QoS (Quality of Service en ingés) es un conjunto de mecanismos utilizados para asegurar la priorización de tráfico y garantizando un ancho de banda mínimo para la correcto funcionamiento del servicio. QoS básicamente mide el ancho de banda y prioriza los paquetes de tráfico en función de las colas de prioridad.

No debemos confundir QoS con limitador de ancho de banda ya que, básicamente el limitador limita la conexión independientemente del tipo de tráfico que haya pero no realiza priorización de los paquetes en la cola.

Para la creación de políticas con calidad de servicio el proceso a seguir es el mismo que el anterior.

Antes de hacer click en OK para terminar de crear la regla nos fijaremos en

una de las últimas opciones dentro de la creación de políticas. Aquí será donde elegiremos cómo queremos

Security Profiles	
Shared Shaper	+
Reverse Shaper	+
Per-IP Shaper	+
Comments	

Esto nos permitirá limitar el ancho de banda en las políticas. En caso de habilitar Shared Shaper se limitará la subida o el tráfico saliente y en caso de que sea Reverse Shaper limitará la descarga o el tráfico entrante.

También existe la posibilidad de limitarlo para una ip en concreto y no para todos los objetos que entren dentro de esa regla. Para su elección dispondemos de Shapers ya creados por defecto o en caso de querer crear uno podremos hacer click en el "+" de arriba a la derecha.

Traffic Shaper	+•	r ^{it}		×
Search				Q
SHARED SHAPER (5) 🗸				
guarantee-100kbps Guaranteed: 100 Kbps, Maximum: 1048576 Kbp	s, Traffic P	riorit	y: H	
• high-priority Guaranteed: 0 Kbps, Maximum: 1048576 Kbps,	Traffic Prio	rity: I	High	
low-priority Guaranteed: 0 Kbps, Maximum: 1048576 Kbps,	Traffic Prio	rity: I	low	
• medium-priority Guaranteed: 0 Kbps, Maximum: 1048576 Kbps,	Traffic Prio	rity: I	Med	
 shared-1M-pipe Guaranteed: 0 Kbps, Maximum: 1024 Kbps, Traff 	ic Priority:	High	1	

Entonces se nos abrirá una ventana para la creación de un nuevo Shaper.

Para su configuración lo único que necesitamos es asignarle un nombre y dos anchos de banda. Uno de ellos es el "Guaranteed Bandwidth" que nos permitirá establecer un ancho de banda mínimo, es decir, la política que tenga dicho shaper asociado dispondrá siempre de un bando de ancha garantizado a su elección. El otro es "Maximum Bandwidth" que limitará el ancho de banda de la regla que lo tenga asociado a la elegida.

Create New Shared Toffs: Shapers		
Name	8	
Apply Shaping	CPer Policy @For all policies using this shaper	
Bandwidth Unit	KDan More Class	
Guaranteed Bandwidth (0 - 16775000)	a	
Maximum Blandwidth (0 - 16776000)	8	
Traffic Priority	High Medium Low	
DDSCP (000000 - 311111)	000000	





telecable

1.9. Creación de usuarios y grupos locales

1. Seleccionar en el menú principal la opción de "Policy & Objects".



2. Seleccionar en el menú superior la opción "Object Configurations".

Policy & Objects 🗸	Policy P	ckages Object	Configurations			
A Policy Package 🗸 🔥	Install 🗸	ADOM Revis	ions 🗘 Tools 🗸	/ Collapse Al	I IE Object	Selector 🗸
11 Search.,	Q.	Create New ~	ØEdit∨ ₫	Delete 🗐 Sect	ion∨ for	Column Settings -
A default 1894 Folicy	_	0.1	Name	From	To	Source
 Installation Targets 		= - Implicit (1	-1 / Totak1)			
		a 1	Implicit Deny	🗢 any	♦ any	tha 🗘

3. En el menú lateral izquierdo elegimos la opción de "User definition" primeramente para crear un usuario y hacemos click en "Create New".



telecable

- 4. Una vez abierto el menú para crear el usuario introduciremos:
- En el campo de Type, el tipo de usuario,local por defecto.
- En el campo de User Name el nombre del usuario asociado.
- En el campo de Password la contraseña asociada a dicho usuario

vpe	LOCAL LDAP RADIUS TACACS+	
Jer Name		
Disable	0	
Password		
Contact infu		
Email		
SMS	● FortiGuard Messaging Service O Custom	
	Country/Region	
	Phane Number	
Two-factor	Climble	
Two-factor Authentication	OFortToken	
Two-factor Authentication	CFortToken CEmail based two-factor authentication	,
Two-factor Authentication	Disable OFortiToken OEmail based two-factor authentication OSMS based two-factor authentication	

El resto de los campos se obviarán por ahora.

5. Por último, haremos click en OK para finalizar la creación del usuario.

6. Para la segunda parte, la creación de grupos, nos situaremos de nuevo en la pestaña en la que estábamos antes, donde elegimos User definition, pero en este caso elegiremos User Groups y haremos click en Create New.

7. Aquí solo tendremos que especificar un nombre para el grupo en el campo "Group Name" y los miembros de dicho grupo en el campo "Members".

8. Por último hacemos click en OK y el grupo se crearía.

telecable



1.10. Configuración URL Filtering

Este módulo nos permitirá definir a qué páginas de internet pueden navegar nuestros usuarios y cuales tendrán denegadas. Podremos aplicar este filtrado por categoría de página y también podremos crear varios perfiles de navegación: básica, avanzada o navegación VIP.

1. Seleccionar en el menú principal la opción de "Policy & Objects".

2. En la barra superior elegir la opción de "Object Configurations".

3. En el menú lateral izquierdo elegir "Web Filter", dentro de "Security Profiles" y hacemos click en "Create New".

4. Una vez estamos creando un nuevo filtro habilitamos las siguientes opciones:

euskaltel 🔇

• FortiGuard Categories: esto permitirá o bloqueará ciertas páginas en

telecable

función de la categoría que tengan asociada por Forti.

Adva	anced	New Web Filter Profile Inced Options > ection Mode Proxy Flow-based			
Insp	ection	Mode Proxy Flow-based			
Ou	Advanced Options > Inspection Mode Proxy Flow-based Log all URLs FortiGuard Categories Expand All Category Authenticate Categories Categories Categories Adult/Mature Content Security Risk				
D R	Expa	and Categories		(All	
-	CADA	ing our Proceeding of the		1.00	
		Category	Authenticate		
		Local Categories			
	*	la Potentially Liable			
		Adult/Mature Content			
		Bandwidth Consuming			
		26 Security Risk			
0		C General Interest - Personal			
0					
	:	General Interest - Business			

 URL Filter: aquí incluiremos URL's específicadas y creadas por nosotros pudiendo indicar la acción que queremos que se haga: allow, que la permitirá; block, que la bloquerá; monitor, que la monitorizará y exempt, que lo que hace es pasar por alto cualquier acción adicional en la lista de filtros para toda conexión que coincida con el dominio en la entrada URL.



Block malicious URLs discovered by Fortslandbox Web Content Filter



⁺ Create 🗹 Edit 📋 Delete

10.000	100 C 100 C 100 C			
URL	Filter	: En	tries	

Entry	-3		
URL.			
Type	simple	*	
Action	exempt	*	
Referrer Host	1	9	
Enable	allow		
	block		
	exempt	100	÷.
	monitor	En al	

 Allow Websites When a Rating Error Occurs: se recomienda habilitar para permitir el acceso a páginas web que devuelven un error de clasificación del servicio de filtro web FortiGuard. Si su unidad FortiGate no puede ponerse en contacto con el servicio FortiGuard temporalmente, esta configuración determina qué acceso permite la unidad FortiGate hasta que se restablezca el contacto. Si está habilitado, los usuarios tendrán acceso completo sin filtros a todos los sitios web. Si está desactivado, los usuarios no podrán acceder a ningún sitio web.

Rating Options

Allow Websites When a Rating Error Occurs

Rate URLs by Domain and IP Address

Rate Images by URL (Blocked images will be replaced with blanks)

1.11. Configuración Control de aplicaciones

El control de aplicaciones de Fortinet protege equipos y servidores permitiendo y denegando el uso de aplicaciones basándose en políticas establecidas por el administrador de la red.

1. Para acceder a la configuración del Control de Aplicaciones, dentro de "Policy & Objects" 2 "Object Configurations" y en el panel izquierdo seleccionamos "Security Profiles" 2 "Application Control".





telecable

Policy & Objects - Pol	cy Pa	ickages	Object	Configura	tions		
ADOM Revisions & Too	ls v				- 19		
Zone/Interface	>	+ Cre	ate New	🕑 Edit	B Delete	Column Setting	s ∽ 🚦 More ∽
▶ Firewall Objects	>	Na	me			Comments	
Security Profiles	-	. 0	block-high	h-risk			
AntiVirus		0	default			Monitor all	applications.
DNS Filter			sniffer-pro wift-defau	ofile /It		Monitor all Default con	applications. figuration for office
Web Application Firewall	1						
Web Filter							
Application Control							
Intrusion Prevention							

En esta pantalla podemos ver todos los perfiles de Control de aplicaciones, si queremos editar alguno, hacemos click encima del perfil y seleccionamos el botón "Edit". Para crear un perfil nuevo, seleccionamos el botón "Create New".

2. Una vez dentro de la configuración inicial, distinguimos los campos siguientes:

• Name: el nombre del perfil.

- Categories: se selecciona la acción para cada una de las categorías: Allow, Monitor, Block, Traffic Shaping, Quarantine, or Reset.
- Application Overrides: permite seleccionar aplicaciones individuales.
- Filter Overrides: permite seleccionar grupos de aplicaciones y anular la configuración de la firma de la aplicación para ellas.
- Deep Inspection of Cloud Applications: realizar una inspección profunda de aplicaciones en la nube.
- Allow and Log DNS Traffic: permitir y registrar el tráfico DNS.
- Replacement Messages for HTTP-based Applications: mensajes de reemplazo para aplicaciones basadas en HTTP.

THE PROPERTY OF	-	and a	Statute of the local division of the	di					
ADOH Revision 4	0.	terror and							
2 Serve Setterface	. 0	Create New Applic	alter Cartral Profile						
R Firmul Oljecty	1.4	-	li.						
Security Problem AntiView DND Filter		Converts			0.288				
Week Again allow Pressal		Categories							
Vea faur	_	(QMunitur	+ Bastress	Q Marrier General Interest	+	Annual Access	+	Q Normal	4 Matt
And and a second se		University	+ Onatif	Mantar	+ Moltie	C Marittan	+ Sound Marile	U Montton	+ Industrial
(8) Security Fabric	1	Mutter	+ Collaboration	Method Service	•	Wonthar Marina	•)	Wester	+ Vell-Client
A User & Deven	1	Gitteriur	+ Enal	Wheeler	+ 2(2	C Maximi	+ Montane	O Aldree University Appl	a diata a second
		QMuster	+)Gane	Clinick	+ Press	C Marillar	i Vdenikalie		

telecable

1.12. Configuración IPS

La configuración del protocolo IPS (Intrusion Prevention System), nos permitirá proteger nuestra red de ataques externos. Un IPS es un sistema de prevención/ protección contra las intrusiones y no solo para reconocerlas e informar acerca de ellas. El IPS tiene la habilidad de bloquear inmediatamente las intrusiones, sin importar el protocolo de transporte empleado y sin reconfigurar un dispositivo externo. Esto significa que el IPS puede filtrar y bloquear paquetes de manera nativa (al utilizar técnicas como la caída de una conexión, la caída de paquetes ofensivos, el bloqueo de un intruso, etc.).

En este protocolo se lleva a cabo una defensa basada en firmas contra ataques o vulnerabilidades conocidas. El atacante en estos casos tratará de comunicarse con un host para ganar acceso al mismo, para lo cual hará uso de una serie de comandos particulares. Las firmas IPS incluyen estos comandos, de forma que permiten al Fortigate detectar y parar el ataque.



1. Seleccionar en el menú principal la opción de "Policy & Objects".

2. En la barra superior elegir la opción de "Object Configurations".

euskaltel 🔇

Policy & Objects - Policy I	ackages Object	Configurations			
🕭 Policy Package 🗸 👍 Install 🗸	ADOM Revis	ions 🗘 Tools 🗸	/ Collapse	All IE Object	Selector 🗸
It Search Q	Create New ~	ØEdt~ ₫	Delete 🗐 S	ection v 6	Column Settings -
🗄 🖻 default		Alama	From	To	Fourte
Installation Targets	a - Implicit (1	-1 / Totak1)	Prom	10	- source
	a 1	Implicit Deny	🗢 any	🗢 any	O all

3. En el menú lateral izquierdo hacemos click en "Intrusion Prevention", dentro de la categoría de "Security Profiles" y pulsamos "Create New".

telecable



4. Los campos que tenemos para configurar un perfil IPS serían los siguientes:

Create New IPS Profile							
Name Comments		M210					
#5.Spatures							
+ Antiqueures (2 Los (2 Los							
C None Lengt Ps Severity To	larget Service Of Action Status	Packet Logging Ling Arts	ex Comut Byte	Matter Rate-Court	Byte Duration Decombil	Applications 01	Series .
Anther States 0.0	1.1.	Relations		144.44	ah Connai		
Care of the Annual Contractor							
Rate Based Signatures							
Evalue Signature	Threathand	Duration/Seconds)	Tech By	Arten	Bioth Deretton		
No-mante hand							
Advanced Dation: >							

• Name: Donde indicaremos el nombre del escaner IPS.

- Comment: en caso de querer establecer algún comentario.
- IPS Signatures: para añadir una firma hacer click en Add Signatures. Estas firmas nos permiten proteger los equipos frente a ciertas amenazas concretas. Dichas firmas se actualizan automáticamente. En el caso de ejemplo disponemos de casi 13000 firmas.

Agregar Flemas

40	and Filler								6
6	Derfigeration de Columnas -								ିୟ
D	Partiet	Serectad.	Olythia	08	01	feretis 2	Autor	Talatas	01-0
	10-Sector (AAChine) Local Bulley (Decelore Depilat)	millert	arrent diami	(Industrial)	Westings .	TOTAL TRADE AND	AD DOUBL	O mindre	2
	100+CVS Manhold PVP File Policies:	10	441947	Dennisi	Wetters Unu BI	TONHITP	C sout	O multit.	
	(2000) Wester, Buster XOD Parment Read	module	errert chert	Extended	31940	TOOMTY .	C DOWN	O make	CVE-2007-408
	30% Phone Reserve (WE), Deping Armines a Plan Lipst	ne .		Extended	Westingt	TOTALTY.	Cinck	O multik	
	3Care 3CDestroy / 74 Server Buffer Doerflow	ings .	-betteph	Begulas, Extended	Westmen	TCH/TH	Chinese	O analate.	CNE 2009-007
	Kirsh Miller and Philler and Deliver	- Norm	others.	Repaire Extended	Wighteen	TOAITH	@ Marth	C stuble	CVE 2000-0075
	Marth Intelligent Management & Carrier & Rectarbase	market .	-	Angular, Extended	Wittines	TCR/HTTP .	Charles !!	O student	
	Karn Office Servert ADD, Wennes French Root	mailure .	407107	Arguine, Centrelad	Emut.	TOWTH	C Month	O analyse	
	3D J. Ph. Player-WebPlayer ActivaLC Control Buller D	man	(Art)	Estamated	Witten	TO/HTTP	40 secula	O multite	
	The Proceeding of the Automatic Sciences Budley Convertion	reduct	det	Extended	Wittines	1CRNITTP	(Chinale	C intuitity	0/5-2034-4580
	35-Smart (CODESV5-Gateway Server Directory Tra-	high	were in the second	Industrial	Windows	TEP	(3 tearly	C and the	Cy6.0013-4701
	38-Smart (CODI/SYS/Catenyoy Remark Direl)	Net	serves plant	Induitrial	Winters	TOP	() much	O codim.	CVI 2012-470
	35-Smart (DOD) WILLIAMMAY Server Have Buffer 1	math	807905	traductorial	Westweet	TEP	O much	O chudae	CV0-2023-4444
	20-Smart COOKSYS Gamman Semant Integer Unant	THE .	807907	Regular, Extended	Windows	104	AVAID BY	O oute	CVE 0013-0001
	In Smart COOLYYS, Gammay Server Memory Acro	official li	ALL REAL PROPERTY.	minerar	Windows	TOP	(Claroch)	O much	03-0014/0-
	IS-board COOLIVIS-Damoury Servert Records House	- interest	server, cherk	industrial	Weekser	TOP	(Blanch	O stuble	1010-0022-4708
	ID-Inset CODE/VE-Gammas In-sec Itals, Buffer-C	075.0	and set officers.	industrial in	Westmen	NP 0	C tribell	O window	CVE 2012-4708
	28 Investig0001211.Web Server Buffer Overflow	- mail		Industrial	Windows	tON/THE .	C true	O roda	COLUMN AND
	IN Inset CODEWE Web Issue UR: Italia Bufful I	high	441140	and solved that	Westman	tD/yeft#	(3 then it	O make	Cv8.001+040.*

Warning 14.622 (DB Repairs Educated, Industrial, Table 1270).

 IPS Filters: hacer click en Add Filter. Las firmas están incluidas en los filtros, de forma que en función del filtro que elijamos, se aplicarán unas firmas u otras. Se recomienda perfilar bien los filtros de forma que no se consulten firmas innecesarias. En este ejemplo hemos elegido como filtro que el OS sea Windows y el protocolo DNS, aplicándose 97 firmas.

Agregar Filten								
100 Wester Ultrace Dill Apro	# 7 m t							0.6
Configuration de Columnus +								G.
Nortire	Severidad .	Olymme	00	01	Sarvitio	Appine	Endor	CVE40
AACH Bound	1.99.4	10.000	Repairs Extension	40	UDP(2H)	C 1644	C -marks	
Radolase Canad Strike Stream	140	amendant	Repta Estended	Withinst	TOHITINESLO	O jam	C-reate	
Belland Berer	Tradit .	processory.	Replice Lybrowicz	44	TCP:rTTPL/DPDN	(Cales)	C-inatite	
Wardshife (Antional)	100.4	1844	Reprine Lateration	18	TEPHTTPUERON	Saber	Q-reality	
DC12bdu Extension	itee .	part and it.	Extension	48	ICHINGROWS	(Crees	@ inate	
DML Availe and Delection	iter .	persecularit	Pegala Estavore	10	LIDRONS	O pert	O realty	
Direct Butterininel Domain Attach	in the second se	-	Extension	With Street of Concession, Name	LIDP2H9	(China)	Q-marks	CVC-DIDE 1447
DN5/MITES	lon .	adaptity .	Pepalat Extended	.40	UDFDH8	(Chiefe	G enable	
19ME Availed Labor Longer	540	-	Extension		TCEDHS	Ø-1000	C rule	
TPM: Provided CPProvide	100	10140	Extension	48	TCRONG	Ó.,	O duale	
This involted Parameters	low.	wheel	Economic	44	TERONS.	Ø	C-fuith	
DMD/muliid Polemer	hter.	and the second	Estendet	.44	TOPONS	C pers	Cout	
DND Label Compression Recordsee Daily	high-	del marri i	Repairs Tatantini	Weinersteinen	1CPONSLOP	O pare	Girelable	CV8-0007-5000
1955 Name Doctions	low	inner.	Extended	Ad.	1070%5	© parts	(C-builde	
1945 Ownerstand Mercanger	Apr .	antuir .	Extension .	48	TCP:0HS	O pers	C river	
1345 Panter Long	Aug.	server.	Replic Extension	A8	TCFONS	Q parts	C enable	CVE 2011 Med
DND Reverse Assistent Linebug Samulting	reduce	cherti .	Extension	Birging .	UDRONE .	(C shund	Genate	CVE-200+-0872
DMS.Server Response Spectrag	mediant.	server.class)	Reputer, Extensive	Window.	UDROND	(Dates)	O-math.	EVE-3007-3896
DML Speaking Attenuet	high-	class	Reprise Extension	(Add	LIDP2NS	(States)	6 craite	OVERIGE (AL)

wrene an are the means browned without 1968 (7)

telecable

Por último, tenemos una lista de firmas en las que hay que especificar un umbral de tiempo y una duración. De esta forma se bloqueará solo en caso de cumplir estos campos.

telecable

laiste	Signature	Threathe	λė.	DurationEls	econdul .	Irack By	Action	Hock Outston
	Ogrum Asterinia Rile Descriptor Delli	-70		3.	×	Ax. I	(144)	form.
1	(lighum-Antoniae AAA2 Call Nomine Dark	278	1	1		Av 1	1044 B	Tere
0	Delferfiske Pailing Duele Allach	100		5		Avy -	1 100 E	how
2	FTPLogitudisation for car	78	÷	10	- 2	Av 1		how
3	Freedblc/TCF Researchly Dell	30		2		Av 1	and [Anne
3	MANPLogin. Brute Force	40	1	10	. 8	14	(int)	here
3	MS-Active Directory (2047 Parket Handling Doll	18967	1	1		Are 3	(1848) (tion .
0	HS-OWA Bruie Fund	16	1	1	3	(Aw)	1.000	i line .
0	MS.RQP.Convention Bruns France	296	1	10.1		No. 1	1000	(Non)
0	MS Windows Group Policy Security Proteins Bepare	1		31		1964011	(internal	line !

5. Para terminar, hacer click en OK.

euskaltel 🔇

1.13. Configuración perfiles antivirus para navegación

La protección Antivirus se encarga de detectar, desinfectar y/o eliminar códigos maliciosos, con actualizaciones en tiempo real para proteger contra nuevos ataques. Está certificado por ICSA Network Antivirus y es capaz de analizar los siguientes protocolos: HTTP, SMTP, POP3, IMAP, MAPI, FTP y IM.

 Para acceder a la configuración del Antivirus, dentro de "Policy & Objects" "Object Configurations" y en el panel izquierdo seleccionamos "Security Profiles" "Antivirus".



En esta pantalla podemos ver todos los perfiles de seguridad, si queremos editar alguno, hacemos click encima del perfil y seleccionamos el botón "Edit". Para crear un perfil nuevo, seleccionamos el botón "Create New".

Manual Fortimanager

Em pre sas.

telecable

- 2. Una vez dentro de la configuración inicial, distinguimos los campos siguientes:
- Name: nombre identificativo del perfil que estamos creando.
- Inspection Mode: por defecto "Proxy".
- Detect Viruses: tenemos dos opciones, "Block" o "Monitor".
- Seleccionamos los protocolos que queremos analizar.

Policy & Objects v	Policy	Packages Object Configurations				
ADOM Revisions ADOM Revisions Additional Control Security Profiles Addition DNG Filter Web Application Firmual Web Filter Application Control Intrusion Prevention Security Fabric User & Device	3 3 3 3		Penny Block De De De De De De De De De De De De De	Flow-based Monitur	C None Subcious Fles Only Al Supported Files	0.253

1.14. Configuración VPN SSL

euskaltel 🔇

Una VPN SSL permitirá a usuarios remotos acceder a la red de la empresa. Esta conexión se hará vía web o mediante un túnel utilizando FortiClient.

El modo web permitirá a los usuarios acceder a los recursos de la red sin necesidad de un cliente pesado, solo con un navegador web.

Para los usuarios que se conecten mediante el modo túnel, será necesario instalar un cliente pesado llamado Forticlient para poder realizar esta conexión. Se podrá configurar Split – tunnel para evitar el paso de la navegación a internet del usuario por el FW, de modo que no sobrecargue la red.

1. Para configurar una VPN SSL en primer lugar, nos dirigimos al menú principal y seleccionamos "VPN Manager", en el menú superior pulsamos el botón "SSL VPN" y hacemos click en Portal Profiles y luego en CreateNew.

telecable

	VPN Manage	r~	IPsec VPN		Monitor	Мар	View	5SL	VPN	
+ /	dd SSL VPN	±	Install Wizard	1						
SSL	VPN				+ Create	New	E 6	dit	自 Delete	6
Ell Port	al Profiles				Name					
I Mon	itor			0	Portal_E	what	<i>8</i>			

- 2. Si habilitamos Tunnel Mode:
- Split Tunneling. Permitimos que las conexiones a internet del usuario vayan por fuera del túnel de modo que puedes configurar un proxy para la navegación.
- Routing Address: aquí indicamos routing que se nos asignará una vez conectados a la VPN
- Source IP Pools: Aquí se indica el rango de direccionamiento que se asignará a los clientes conectados a la VPN.



Si habilitamos Web Mode:

- Portal Message: Breve descripción del portal al que se conectan los usuarios.
- Show Session information: marcar si queremos que se muestre información de la sesión al usuario remoto
- Show connection launcher: marcar si queremos añadir la herramienta de conexión a los usuarios remotos
- Show login history: marcar si queremos mostrar el historial a los usuarios remotos
- User bookmarks: Se indican los accesos rápidos a determinados recursos para cada portal de VPN creado. Para crear los marcadores pincharemos sobre "Create New"

telecable

Create New Bookmark

(42/192	BOOMTER.	
Type	HTTP/HTTPS +	
URL		
Description		
Single Sign-On	Disabled Automatic Static	

- Enable FortiClient Download: marcar si queremos mostrar el link de descarga del software FortiClient.
- 3. Nos dirigimos al menú principal y seleccionamos "VPN Manager", en el menú superior pulsamos el botón "SSL VPN" y hacemos click en SSL VPN y luego en Create New.

VPN Manager 🗸 IPsec VP	N Monitor Map View SSL VPN
+ Add SSL VPN Install Wizard	
SSL VPN	🕂 Create New 🗹 Edit 📋 Delete
Portal Profiles	Device
Monitor	No entry found.

4. Para realizar la configuración inicial tenemos que indicar la siguiente información:

- Device: seleccionar un dispositivo manejado por el FortiManager.
- Listen on Interface: definir la interfaz que Fortigate va a usar para escuchar las peticiones SSL VPN. Generalmente es la propia interfazexterna.
- Listen on Port: añadir el número de puerto para el acceso HTTPS.
- Restrict Access: limitar el acceso a hosts específicos en caso de así quererlo.
- Idle Logout: si seleccionamos la opción "on", debemos indicar la cantidad de tiempo que la conexión puede estar inactiva antes de realizar el logout del usuario.

En cuanto a la configuración del "Modo túnel", tenemos que especificar la información de los siguientes campos:

• Address Range: podemos escoger el rango automático o personalizado.

euskaltel 🔇

 DNS Server: podemos seleccionar el mismo DNS que el sistema del cliente o uno específico.

telecable

- Specify WINS Servers: si seleccionamos la opción "on", podemos especificar los servidores WINS.
- Authentication/Portal Mapping: aquí indicamos los usuarios que tendrán acceso a dicha VPN, y el portal al que tendrán acceso.

+ AMELINA & I	with Write-II					
BRANKS.	Creater New 331, VPN: Settings					
E Partol Problem	Dente		Personal del trabaci	6 ⁷		
CE Hunter	Committee Larger D		() with an exclusion			
	Connection Designed O		1.0		_	
	Common and Address of		12			
			A HOC'IDHULD	1 Avera Balancian	-	
	Lines in Ref.		(sheet			
	Broaded Broad		Concession of the local division of the	A loss and the strength boots of		
27	and the second second	ally second		State of the state		
R	the Light.	the Light				
	tractive For	Provide Par		DMD0 Description		
	Server Certificate		1008030308			
	Reading Client Centrifulate	Resulte Diret Centrule		34		
	Turent Mode Cland Settings O	Toreal Mode Clant Settings O				
	Address Range		Accordingly as ign addr	Toront Strendy sustain Prompty		
	DNS between	DMB between		Santa Santa		
	Specific WING Servers	Specific WIND Income		245		
	Alters Distanced Report street		-			
	Automatication Participation (
	+ Constant Both B	And a local second s	in the second			
		Uar	Realm	Portal		
	1	NUM	1	Area Scenar		
	-	And a	-	*		
	7	and the second s		And Description		
		All Other United Groups				
	Advanced Options 2	and the second se				

5. Por Último, debemos crear una regla de seguridad para el acceso remoto. Para ello vamos a Policy & Objects y hacemos click en Create New:

	a discontinuation de partir de la contra de	Calapar Al II Object Selector V		
Sen h	Q Could New IPv4 Policy			
PW10941 30.004.00 IP4198V	Name	VPN-55L		
Prony Policy	burning blantaur	EN ROUDENPD		0
Protatution targets	Outgoing Interface	Determ		0
hel will	Source Internet Service	1977		
	Source Address	Eventsi, Senara as		0
	Source User	Advanta Advan		00
	Source User Group	AGont group		0
	P550			
	RSSD	D		
	Source Device	+		
	Destination Internet Service	144		
	Destination Address	0.4		0
	Service	OALL		0
	Schedule	O sharps		0
	Action	Deny Accept IPSEC		
	Ling Trutte	Ono Log @Log Security Events	OLig Al Sestors	
	2010 818029	Generate Logs when Session 96a	154	
		Canne Poceni		
	NAT			
		Che Destrution Interfaier Address	EFred Prt	
		ODsnamic IP Pool		

- Name: nombre de la regla de la VPN.
- Incoming interface: interfaz virtual SSL.
- Outgoing interface: interfaz local a la que acceden los usuarios remotos.
- Source Addres: objeto con el pool de usuarios remotos.
- Source user: usuarios que queremos que accedan a la red.
- Source user group: grupo de usuarios que queremos que accedan a la red.
- Destination address: dirección de la red local a la que acceden los usuarios remotos.
- NAT: si se habilita se usará la dirección IP de la interfaz de salida.

En esta regla se puede filtrar los accesos por usuario si se quiere restringir para determinados usuarios.

1.15. Configuración VPN IPSEC

IPsec es un protocolo de VPN que se usa para proteger la comunicación por internet a través de una red IP. Se establece un túnel en un sitio remoto que permite el acceso a tu sitio central. Una IPsec funciona protegiendo la comunicación del protocolo de internet verificando cada sesión y codificando individualmente los paquetes de datos durante la conexión.

1. Antes de pasar a la configuración de la VPN, tenemos que dirigirnos a "System Settings" y en el menú izquierdo seleccionar el apartado "All ADOMs". Activamos la opción "VPN" en "Central Management".

Edit ADOM					
Name	root				
Type	FortiGate		5.2 5.4	5.6 6.0	
Devices					Q
	A Name		IP Address	Platform	
	CD Pre-shiPrein	- 28	Lanuth?k	Family to 1000	
	4 0030UA			VDOM	
	d blinelast			VDOM	
	o thi burnai			VDOM	
	o blikere			VDOM	
	d thistes			VDOM	
	o colutions			VDOM	
	0.05,08m/1	1		VDOM	
	d lightplant			VDOM	
	ið root			VDOM	
2					
Central Management	VPN C	FortiA	P □SD	-WAN	
Default Device Selection for Install	 Select All 	Unsele	set All		
				OK	Car





2. Paraconfigurar una VPN IPSEC en primer lugar, nos dirigimos al menúprincipal y seleccionamos "VPN Manager", en el menú superior pulsamos el botón "IPsec VPN".

VPN Manager 🗸 IPse	c VPN M	onitor Map V	New SS	L VPN	
Service VPN Community - Inst	all Wizard				
All VPN Communities	+	Create New	🗹 Edit	自 Delete	Column Settings
- 🛛 Default - 🗖 Dial Up 5	0	# Na	me		
- 🗱 IPsec DCM	0 :	1 🖾	Default		
— 🗱 Star 1	0 2	2 🖬	Dial Up 5	5	
	0	3 *	IPsec DC	M	
	0	4 *	Star 1		

3. En este menú podemos ver las distintas VPNs ya creadas, las cuales podemos editar pinchando encima y pinchando en el botón "Edit".También podemos crear una seleccionando el botón "Create New".

VPN Mar	ager 🗸 🛛 IP:	sec VPN	Monito	r Map	View SS	IL VPN	
S VPN Comm	unity 🗸 In	stall Wizard	i)				
a 🖾 All VPN Cor	nmunities		+ Crea	te New	🗹 Edit	自 Delete	Column Settings
Default	5			N	ame		
- NIPsec DO	M	D	1	12	Default		
Star 1		D	2		Dial Up	5	
		D	3	*	IPsec D	CM	
		D	4	*	Star 1		

4. En estaprimeraventana tenemos que indicar el nombre, opcionalmente una descripción y escogemos la topología de la VPN. Tenemos tres opciones:

- Full Meshed: cada puerta tiene un túnel para todas las demás puertas.
- Star: cada puerta tiene un túnel hacía un hub central.
- Dial Up: algunas puertas, a menudo usuarios móviles, tienen direcciones IP dinámicas y se ponen en contacto con la puerta para establecer el túnel.

Una vez escogida esta configuración, le damos a next.





VPN	Topology	Setup	Wizard

hoose VPN topol	ogy	-	
×	*	~	
Full Meshed	Sar	Dial up	



telecable

5. Ahora tenemos que configurar la información de la autenticación y encriptación para la topología escogida, para ello se hace uso del protocolo IKE. Una vez escogida, seleccionamos next.

/PN Topology Setu	p Wizard			
Authentication & En	cryption Settings:			
Authentication	Pre-shared Key	Contricators		
	Generatrikandom			
	OSpecify			
Encryption				
IKE Security (Ph	ase 1) Properties			
IKE Version	1 2			
	Encryption	Authentication		
Click here to a	6d a mew entry.		+ 🗈	
UPsec Security (F	huse 21 Properties			
	Encryption	Authentication		
		+ Back	Next + Cons	1

6. Por último, tenemos que configurar la Zona VPN, escogiendo entre crear una zona predeterminada o personalizada.También hay que personalizar las Propiedades avanzadas de IKE Security Phase 1 y 2.Volvemos a seleccionar el botón next.

PN Topology Setup Wiza	rd							
VPN Zone	04							ł
	() Create	Default Zone						
	O Use Cu	ntom Zone						
IKE Security Phase 1 Advance	d Properties							
Diffie-Heltman Group(s)	□1 □17 □28	02 018 029	25 219 230	20 20 21	□15 □25	□16 □27		
Exchange Mode	OAgeres	sive @Main	ID Protection					
Key Life	28800		(120	-172800 seco	inds.)			
Dead Peer Detection	ODisable		On Demand	r.				
IPsec Security Phase 2 Advan	ced Properties	E.						
Diffie-Hellman Group(s)	01 017 0m	22 218 77mi	25 019	■ 14 □ 20	D15 D11	□16 □27		
				< Back		Next •	Canad	

7. Nos aparecerá una última ventana con toda la información que hemos ido personalizando, revisamos que este todo correcto y para terminar seleccionamos el botón OK.

6 55			
Summary			
Name	Pruetta		
Topology	Star		
Authentication	Pre-shared Key (Geneciste)		
Encryption	IKE Security (Phase 1) Proporties		
	Diffie-Heliman Groupist : 2,5		
	Rey Life : 28800 (seconds.)		
	B Dead Peer Detection : On Demand		
	Psec Security (Pruse 2) Properties		
	Elthe Helman Groups) : 2.5		
	Replay Detection		
	Perfect Forward Secrecy(PFS)		
	Key Life: 1800(seconds)		
	< Back	OK	Center







8. Ahora tenemos que crear una Gateway para la VPN IPSec. Para ello en el menú principal seleccionamos"VPN Manager"y seleccionamos la VPN creada. Pinchamos en"Create New"y en el desplegable"Managed Gateway".

=	VPN Manager 🗸	IPsec VPN	Monitor Map View	SSL VPN	
- 54	VPN Community 🗸	Install Wizar	d		
<u>ن</u> ا	All VPN Communities				Name :
	Default Dial Line 5		Star		Number of VPN ;
	* IPsec DCM				Authentication:
1	🛠 Star 1		+ Create New 🗸 🛛	Edit 🖻 Delete	🙃 Column Settings -
		C	Managed Gateway	Role	e
		N	External Gateway		

9. En primer lugar, seleccionamos la subnet.

rotected Network	Device	Default VPN Interface	Local Gateway	Advanced	
Press, Ins. Juli Per	1	OE ABROWOL, DE IOR 3 WILLIE ERBERT POPULATI Y ENTRy Selecte	erenas 💌		
			< Back	Next +	Cancel





10. En este ejemplo se va a crear el Hub, también tenemos que crearlo con el rol Spoke, para ello se siguen los pasos siguientes de la misma forma, con la diferencia de seleccionar el rol en la primera pantalla. Una vez tenemos el rol seleccionado, indicamos el dispositivo.

VPN Gateway Setup	Wizard - 🗱 Prue	bal			
	••••	m		6	
Protected Network	Device	Default VPN Interface	Local Gateway	Advanced	
Role	OHub () Spole			
Device	Proskill	salpat, admitta			
			(Back	Next >	Canal

11. En el apartado "Default VPN Interface" seleccionamos la interfaz por defecto (normalmente es la interfaz que da a internet) y hub-to-hub (únicamente requerida para múltiples hubs).

VPN Gateway Setup Wizar	d - ♣ Prueba1		
	D, 💼		
Protected Network Dev	Ice Default VPN Interface	Local Gateway	Advanced
Default VPN Interface	8-00.10400	*	
Hub-to-Hub Interface	# 15 NG DIMENSION		(Required for multiple Hubs)
		+ Rack	Next + Carcel







12. Indicamos la dirección IP para la Local Gateway.

VPN Gateway Setup	Wizard - 🕸	Prueba1			
	•				
Protected Network	Device	Default VPN Interface	Local Gateway	Advanced	
Local Gateway	10.0	ddress			
			(Bach	Next >	Generi

13. Porúltimo, podemos escoger el routing de formamanualo automática. Por defecto se deja como está.

Ci laxo					
outing	Manual (via	Device Manager) (OAutor	with:		
ummary Network(s)	Seq#	Network	Prior	ity	
	1		• 1	+	
dvanced Options >					





14. Para realizar la instalación, en la misma pantalla de antes hacemos click en "Install Wizard".

VPN Manager 🗸 IPsec VP	N Monitor Map View SSL VPN	
VPN Community Insta All VPN Communities	I Wizard	Name :
Default Dial Up 5 * IPsec DCM	Star	Number of VPN : Authentication:
# Prueba1 - ₩ Star 1	+ Create New V 🗹 Edit 🛱 Delete	ති Column Settings -

15. Seleccionamos la política creada en el anteriorapartado.

Install Wizard		
Install Policy Package & Dev Install a selected policy p	rice Settings ackage. Any device specific settings for devices asso	ciated with the package will also be installed.
Policy Package	mandematic and (relationed)	
Convert	Write a commerit	
Create ADOM Revisio		
Schedule Install		
O Install Device Settings (only)		
		Next + Canini

16. Confirmamos que está seleccionada.

Install Wizard - Policy Pac	kage and Device Setting	(FW:10000_3	IS_CEAL	ITTC)
Please select one or more devices to install	Use checkbax or Ctrl or Shift key for mu	(tiple selections)	Seconda .	
 A Device Name 	IP Address	Platform		







telecable

17. Una vez se realice la carga seleccionamos el botón"Install"

Install Wizard - Policy Package (FW3509163_96_C/EAUTC)

NOCK	Name		Status
	Personal Inc. of a	80	Copy to device done
2	17% minute		Init ups context done
3	New connections		Write preview done
r kree	rface Validation		
Polic	cy and Object Validation		
< Read	ty to install		
	115-50-	222	
-	vice Name	Status	Action
De		C Consection Lin	Instant Devices Define Devices (DB)

1.16. Configuración Política DLP

euskaltel 🔇

Esta política es una estrategia que sirve para asegurarse de que los usuarios finales no envíen información sensible o crítica fuera de la red corporativa. Para ello, se utilizan reglas que examinan el contenido de los archivos y etiquetan la información de confidencial o crítica, para que los usuarios no puedan divulgarla.

1. El primer paso es habilitar el DLP (Data Leak Prevention). Para ellos nos dirigimos a "Policy & Objects" y hacemos click en la opción "Display options" de la pestaña "Tools".

Policy & Objects V Policy	Packages	Object	Confi	gurations			
🛎 Policy Package 🗸 🛆 Install 🗸	AD	OM Revis	ions	$\mathbf{\Phi}$ Tools \sim	🖍 Collapse /	AJI 3≣ C	Object Sele
11 Search Q	Create	New 🗸	ß	Display Op	ptions	ion 🗸	to Colu
S: A default IPv4 Policy			P	Find Unused Objects		То	
Installation Targets		Implicit (1	-1/1	Find Duplicate Objects			
	1		h	nplicit Deny	♦ any	⊕ ar	τý

telecable

2. Ahora habilitamos la opción"Data Leak Prevention".

M C Preman Copicts	Multicast Addresses Services Victual IPx Traffic Shapers Health Check	Wildcard PODN Althresses Schedules If Posts Virtual Servers Web Proxy Forwarding Server	
C Security Profiles	AntiVirus Web Application Finewall Auto-Spam VolP Prove Outlons Provile Group Web URL, Fiber Web Fiber Local Category ICAP Servers Application Group	DNS Filter With Filter Duta Lask Prevention Data Lask Prevention CAP SSL/SSH Inspection Web Rating Overrides Web Content Filter File Filter Application Signatures DIPS Custom Signature	

3. En la barra superior nos dirigimos a "Object Configurations".

Policy & Objects 🗸	Policy P	clages Object	Configurations			
A Policy Package 🗸 🔥	install 🛩	ADOM Revis	ions 🗘 Tools 🗸	/ Coll	açıse All 🛛 🗄 Ob	iect Selector 🗸
11 Search.	٩	Create New 🗸	Ø Edit → 🔒	Delete 1	Section 🗸	G Column Settings -
D default IPv4 Policy			Name	From	To	Source
 Installation Targets 		= - Implicit (1	-1 / Total:1)			
		0 1	Implicit Deny		O any	O all

4. En"Security Profiles" seleccionamos"Data Leak Prevention" y hacemosclicken "Create New".



5. Para la creación de un nuevo perfil DLP tendremos que rellenar los siguientes campos:

€ ADOM Revisions © 1:	-	e				
2 Zone Americane	+	Create New DUP Profile				
A Frend Objects	1	Name				
Security Polities AntiVisia DNE Filter	-	Carrowst				8/25
Web Application Firewall Web Filter		Ingestion Made Advanced Options 3	Prox Plot Land	1		
Application Cantral Intruster Prevention		CLP Filter + Create New 28 ILLT @ Drive	& Column Settings w			٩
Cale (and Press) for		D Filter By	Aution	Service	Anthie	
illi Security Fateric A Univ & Device	1	No entry found.				

- Name: nombre del perfil DLP.
- Inspection mode: por defecto se deja en modo proxy. En Flow-based, el Fortimanager examina los archivos sin ningún almacenamiento, a medida que llega cada paquete de tráfico, se procesa y reenvía sin esperar el archivo completo o la página web, esto permite respuestas más rápidas para peticiones http, con la desventaja de que pueden darse con mayor facilidad falsos positivos o negativos en el análisis de la información, además de que varias características que pueden ser usadas en el modo proxy no pueden ser usadas aquí.
- Por el contrario el modo Proxy almacena en el buffer y lo examina todo como un conjunto antes de determinar una acción. Esto permite una inspección más completa que en otros métodos, obteniendo menos falsos positivos o negativos en los análisis de datos.
- DLP filter: para crear un filtro DLP debemos hacer click en Create New y sete abrirá una pestaña así, donde deberemos indicar que queremos aplicar al perfil DLP para evitar que salga de nuestra red.





telecable

Filter	Manages Film		
	Containing Credit Card #		
	O Containing SSN		
	O'File Size larger than	9	KB
	O File Type included in		
	Offile Finger Print		
	O'Watemark Sensitivity		
	O Regular Expression		
	CEncrypted		
Examine the F	allowing Services		
Web Access	CHITP_POST CHITP_GE	ET	
Email	DISMTP DPOPS DIMA	P DIMARI	
Others	DETP DINTP		
Action	Allow		
	[Transa		

Tenemos diversas opciones para filtrar, que son las siguientes:

- Lo primero es elegir si queremos filtrar sobre el contenido de cierto mensaje o sobre archivos.
- Filtrar cuando contenga números de tarjetas de crédito.
- Filtrar archivos que contengan SSN.
- Filtrar archivos mayores de cierto tamaño.
- Filtrar archivos ejecutables.
- Filtrar archivos en función de la huella digital.
- Filtrar archivos que contengan ciertas marcas de agua.
- Filtrar archivos en función de expresiones regulares.
- Filtrar archivos encriptados.

- También tenemos la opción de filtrar en función del servicio (web access, email, FTP y NNTP).
- Deberemos establecer también la acción a aplicar sobre estos filtros, pudiendo permitirlo, bloquearlo, hacer que quede registrado en un log o poner en cuarentena la dirección ip de la que proviene.

1.17. Políticas de navegación por grupo de usuarios

1. Seleccionar en el menú principal la opción de "Policy & Objects".



2. Aparecemos directamente en el menú de las políticas, por lo que hacemos click en "Createnew".



3. Los campos de esta configuración vienen explicados en el apartado 2.5 "Configuración política básica de navegación". A continuación, para crear una política de usuarios de FSSO seleccionamos el grupo de usuarios correspondiente.

Name		
Incoming Interface	Dany	0
Outgoing Interface	Dany	0
Source Address	🐸 IP_10,148. Mill with	0
Source User	+	
Source User Group	SFSSO_Acc	0
FSSO	8	
RSSO		
Source Device	+	
Destination Internet Service	CHF	
Destination Address	🖾 all	ø
Service	C HTTP C HTTPS	0
Schedule	to always	0
Application	+	





1.18. Proxy Web

1. En primer lugar, nos dirigimos en el menú principal al apartado "Device Manager".



2. En la pestaña"Tools" seleccionamos la opción" Global Display Options".







3. En la ventana nos aparecerán varias opciones para activar o desactivar, en nuestro caso activamos la casilla" Explicit Proxy".

C System	Dashboard Port Pair Global Resources Modern HA DNS DNS Service on Interface Management Administrators Local Host ID Replacement Message FortGuard Automation Setch Alert Email NAT64 Prefix	interface Victual Diamain DHCP Server Snitter Interface Policy Snitter Interface Policy SNItt ONS Database Exalicit Prove Admin Settings Admin Settings Admin Profile CA Centificates Replacement Message Group Security Fabric Log Setting Threat Weight FortSandbox	
C Router	Gateway Detection	Policy Route CSPF	

4. En el menú principal seleccionamos el apartado "Policy & Objects" y dentro de "Policy Packages" (por defecto entramos en este menú), hacemos click en la pestaña "Tools" y en el menú desplegable la opción "Display Options".







5. En la ventana activamos la opción" Proxy Policy".

C Policy	IPv6 Policy IPv6 Policy NAT64 Policy IPv4 DoS Policy IPv4 Interface Policy Multicast Policy IPv6 Local In Policy Intedation Targets	Pv4 Victual Wire Pair Policy NAT46 Policy Proxy Policy Pv6 Do5 Policy Pv6 Interface Policy Pv6 Interface Policy Pv6 Interface Policy Traffic Shaping Policy
ZO Zone/Interface		
C Firewall Objects	Addresses Multicast Addresses Services Victual IPs Truttic Shapors Health Check	Internet Service Whitcard FQDN Addresses Schedules Foods Virtual Servers Web Ptoxy Forwarding Server

6. Una vez habilitadas las opciones anteriores, nos dirigimos a"Device Manager" • "Device & Groups".

EE Device Manager - Device	& Groups	Firmware License Pr	exhiming Temple	ten Scripto SD-WAN		
B Abi Device B Device Group	w install	Weat X Task v			1	
Hamped For Carts	88	9 Causes Text	-8-	O Denime .	Contraction Contraction	. ·
	B to	i 🛱 Delete. 🕫 Import I	Nicy Abdal-	More 🗸 😘 Column	Settings +	
		rvice Name	Config Status	Policy Package Status	Firmware Version	Host Name
	0 40	w/minet	&.Modified		Fertiliste 6.0.4,5u8/0231 (SA)	PW2HTMC
	0 11	100/1010-01011	whenty and	A Never installed	Fart/Gate 6.0 Abult/0231 (GA)	
	0 =	SPACE AND	- Synchroniand	A Never Installed	FertiGate 6.0 Altuili0231 (GA)	
	0 =	Print (percention)	- Synchronized	A Never installed	FartiGete 6.0.4,5-vik(0231 (GA)	
	0 =	Chinese and	- Synchronized	A Never Installed	FurtiGete 6.0.4.build0231 (GA)	
	0 =	Stat webber	- Synchronized	A Never installed	Fort/Gabr 6.0-4.5u8/0231 IGAU	
fearth. Q	0 =	Contractor State (- Synchronized	A Never installed	FortiGate 6.0.4,build0231 (GA)	
x di Pwenthio	0 -	CALCULATE AND INCOME.	& Modified	✓ //w180mid3	FortiGate 6.0 Admitt0231 (GA)	
	0 =	Chillippide (Suff)	- Senthronized	A Never Installed	FortiGate 6.0.4.3wikt0231 (GA)	
	0 =	and the P. Schemerter B.	- bentreriard	A Never installed	FurthGate 6.0.4 build(0251 IGA)	





7. Seleccionamos el dispositivo sobre el que queremos configurar el Proxy. A continuación nos posicionamos encima de "System: Interface" y hacemos click en "ExplicitProxy".

E Device Manager -	Device & Groups Firmwa	re License	Provisioning Templates Scrip	ts SD-WAN	
a Add Device 書 Device	e Group 🤟 Install Wizard	× Tools ~			
Managed FortiGate	FW180953 :		System (Interface Router III)	Display Options	
	+ Create New ~	25 Edit	Interface	re~ 6 Col	lumn Settings -
	A Name		Explicit Proxy	olicy Interface	Addressing Mode
	Turmei (1)		Replacement Message Group		
	D 0000,0800	70.55.475	and the Plannel \$150		Manual
	- Zane (0)				
Search.	Q				
* IL FW180960					

8. Una vez en la ventana de configuración activamos el Proxy y seleccionamos las interfaces. Indicamos el puerto en el que escuchará el proxy web, por defecto es el 8080.

Explicit Web Proxy	
Enable Explicit Web Proxy	HTTP / HTTPS FTP PAC
Listen on Interfaces	Q
	port7 x 1 Entry Selected
HTTP Port	8080
HTTPS Port	Use Http Port Specify
PAC File Content	* 🗵
Unknown HTTP version	Best Effort Reject
Proxy FQDN	default.fqdn
Max HTTP request length (2-64)	4
Max HTTP message length (16- 256)	32
Realm	default
Default Firewall Policy Action	Deny Accept
Web Proxy Forwarding Servers	



euskaltel 🔇



Apply

telecable

9. Finalmente en FortiManager, la política la rellenamos al igual que en el apartado 1.5.

A Policy Pockage - A Install -	ADOM Revisions & Tools -	Expand All 18 Object Selector v		
i feasth. Q	Create New Prory Policy			
 Pv4 Palicy 	Explicit Proxy Type	Explicit Web Transparent Web FTP WANT	Dotinies	
Prog Roley Installation Tangets	Outgoing Interface	Owny	0	
E defeat	Souna	+		
	Destination	+		
	Service	+		
	Schedule	©always	0	
	Action	Accept Dony #Redirect		
	Log Violation Traffic			
	Web Proxy Tensanting Server			
	Comments			

1.19. Balanceadores de carga

1.19.1 Definición del servicio balanceado

Lo primero que debemos hacer es habilitar una opción que encontraremos en el apartado "Policy & Objects", en Tools.

Policy & Objects 🗸	Policy P	ackages Object	Configuratio	m,			
♣ Policy Package ~ &	install 🗸	+ ADOM Revis	ions 🗘 Too	ls 🗸 🦯 Ex	pand All BE Obje	ct Selector 🗸	
It Search	Q	Create New 🗸	🛿 Edit 🗸	B Delete	Section v 1	G Column Settings -	
B default IPv4 Policy			Proxy	Dest	nation Inte Source	Destination	Serv
Proxy Policy Installation Targets							

Aquí deberemos habilitar "Virtual Servers" y "Health Check".

euskaltel 🔇

C Firewall Objects	Addresses	Internet Service
	Multicast Addresses	Wildcard FQDN Addresses
	Services	Schedules
	S Virtual IPs	IP Pools
	Traffic Shapers	Virtual Servers
	Health Check	Web Proxy Forwarding Server

Una vez hemos habilitado esta opción nos dirigimos a Virtual Servers, dentro de "Policy & Objects", en la sección de "Object Configurations" y hacemos click en "Create New".

telecable



Ahora tenemos que crear un nuevo servidor virtual.

reate New Virtual Server				
Name				
Convents				0/255
Colur				- ° .
interface	O ans			
Type	HTTP	10718		
Virtual Server IP	0.0.0	0000		
Virtual Street Port	80			
Lost Balance Method	South #	Soute IP Hast		
Porsistema	Givere	@Nere OHITPCaske OSS.Socie:0		
HTTP Multiplexing	Ohen	is HTTP requests/requiries over a single - Clause IP	TCP covertion	
Health Direck		CHI	here to select	
Advanced Options >		11.00		
Per-Device Mapping	300			
A Court New 25 Lat. 10	Dates & Dates Service y			0
D IP Address	Put	Weight	Max Connections	
No entry found.				

Para ello debemos de rellenar los siguientes campos:

• Name: nombre del servicio balanceado.

euskaltel

 Interface: Interfaz por la que el firewall correspondiente recibirá las conexiones.

telecable

- Type: protocolo que va a ser balanceado.
- Virtual Server IP: IP del servicio a la que se van a conectar los clientes.
- Virtual Server Port: Puerto en la que va a estar el servicio y por lo tanto al que se van a conectar los clientes al servicio.
- Load Balance Method: Forma en la que se van a repartir (balancear) las conexiones a los nodos de servicio reales.
- Persistence: Asegura que un usuario se conecta al mismo nodo real durante una sesión para los protocolos HTTP, HTTPS.
- Health Check: Métodos para determinar la salud de los nodos. Existen tres posibilidades, mediante ping, mediante conexión TCP o mediante un GET HTTP.

1.19.2. Creación de la granja de servidores

En esta parte debemos dar de alta los nodos que constituyen la granja de servidores. Para ello hacemos click en "Create New".

		C Reserve Client #			
Insuth Check Advanced Options 3 Per-Device Mapping		Cick here to select			
		(and			
ReafServers					
+ Create New 25 tax	13 Delater & Column Settle	5×		9	
D IF Address	Port	Weight	Max Connections		
No orby found.					

IP Address	0.0.0		
Port	0		
Weight	1		
Max Connections	0		
HTTP Host			
Mode	Active	+	
Client IP	0.0.00		
	(e.g.x.x.x.x.x.x.x.y.y.y.y)		
Advanced Options >			

Create New Real Servers

Debemos rellenar entonces los siguientes campos:

• IP Address: IP del servidor real.

- Port: puerto de servicio en el servidor real.
- Max Connections: número de conexiones máximas establecidas para el nodo del servicio.
- Mode: Active o disable por defecto. En caso de estar desactivado no daría servicio.

1.19.3. Utilización en la política

El objeto virtual server se utilizará en la política como destino en la regla, para permitir el acceso desde todo Internet o las redes que se quiera limitar el acceso.

Name	2	
Incoming Interface	Dany	0
Outgoing Interface	Dany	٥
Source Internet Service	OFF	
Source Address	15 all	0
Source User	+	
Source User Group	+	
Source Device	+	
Destination Internet Service	OFF	
Destination Address	S Virtual_server	0
Service	@ ALL	0
Schedule	to always	0
Action	Deny Accept IPSEC	



