ARICA Y PARINACOTA

APRUEBA MANUAL DE PROCEDIMIENTOS DE PUESTA EN OPERACION Y EXPLOTACION DE EQUIPOS DE COMUNICACIONES Y SEGURIDAD DE RED, GOBIERNO REGIONAL DE ARICA Y PARINACOTA

RESOLUCION EXENTA N° 2321

ARICA, 31 DIC 2013

VISTOS:

1. El Memorándum N° 29, de fecha 31 de diciembre de 2013, de la Jefa(s) de la Administración y Finanzas al Departamento Jurídico del Gobierno Regional de Arica y Parinacota.
2. El Decreto con Fuerza de Ley N° 1 de 2000, de la Secretaria General de la Presidencia, que fijó el texto refundido, coordinado y sistematizado de la ley N° 18.575, Orgánica Constitucional de Bases Generales de Administración del Estado; el Decreto con Fuerza de Ley N° 1 de 2005, que fijó el texto refundido, coordinado, sistematizado y actualizado de la ley N° 19.175, Orgánica Constitucional sobre Gobierno y Administración Regional; lo dispuesto en el artículo 61 de la Ley N° 19.880, que establece Bases de los Procedimientos Administrativos que rigen los Actos de los Órganos de la Administración del Estado; el Decreto Ley N° 1.263, de 1975, Orgánico de Administración Financiera del Estado; lo dispuesto en la Resolución N° 1.600, de 2008, de la Contraloría General de la República, que establece normas sobre la exención del trámite de toma de razón; y las facultades que invisto como Intendente(S) del Gobierno Regional de Arica y Parinacota.

CONSIDERANDO:

La petición planteada por la Jefa(S) de la Administración y Finanzas del Gobierno Regional de Arica y Parinacota, señalada en el numeral 1 del presente instrumento.

RESUELVO:

1. **APRUÉBASE** Manual de Procedimientos de Puesta en Operación y Explotación de Equipos de Comunicaciones y Seguridad de Red del Gobierno Regional de Arica y Parinacota.

2. En cumplimiento de lo señalado en el Artículo 6 de la Resolución N° 1600 de 2008, de la Contraloría General de la República, se inserta el Manual de Procedimientos, que por medio de este acto se aprueban, cuyo texto, es el siguiente:

Gobierno Regional Arica y Parinacota: Manual de Procedimientos de Puesta en Operación y Explotación de Equipos de Comunicaciones y Seguridad de Red

HISTORIAL DE CAMBIOS

NOMBRE DEL FICHERO	VERSIÓN	RESUMEN DE CAMBIOS PRODUCIDOS	FECHA
GORE - Manual de procedimientos Equipamiento Comunicaciones y Seguridad Red v1.00.doc	1.00	Primera versión.	03/12/2013

CONTROL DE DIFUSIÓN

RESPONSABLE:

DISTRIBUCION:

INDICE

1. FIREWALL: PROCEDIMIENTO PARA LA CREACION DE REGLAS Y EXCEPCIONES

Responsable

Responsable	Encargado de la Unidad Informática

1.1. Objeto

- Establecer los procedimientos necesarios para la implementación de reglas y excepciones en el firewall con el fin de habilitar / deshabilitar accesos a usuarios y servicios.

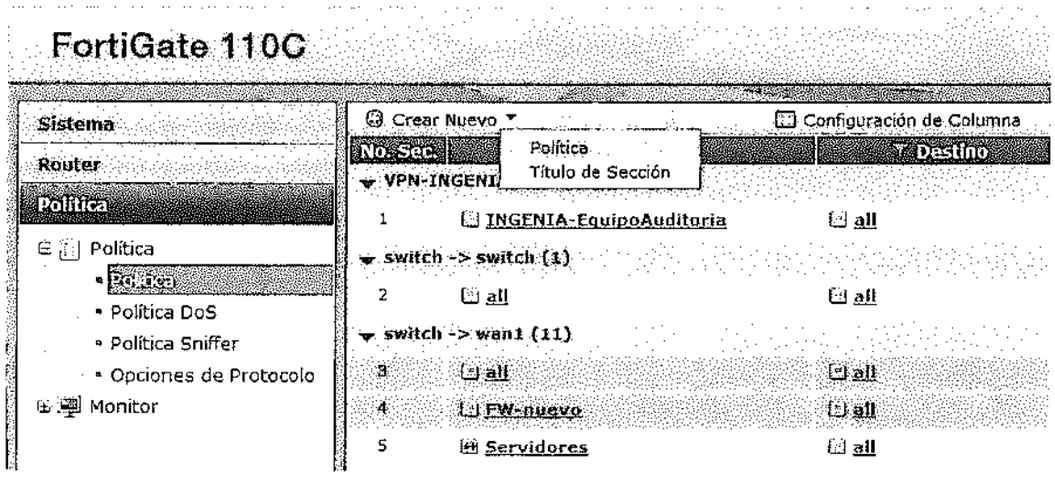
1.2. Requisitos previos

- Para poder cambiar reglas y excepciones en el Firewall será necesario tener un conocimiento del escenario de partida, es decir, de las reglas ya implementadas en el firewall.

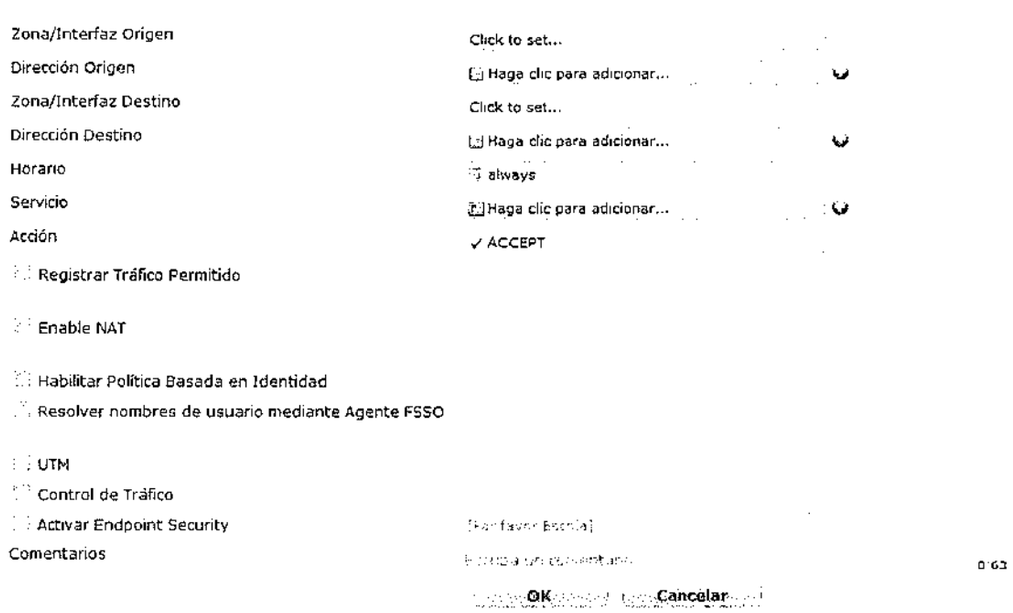
- Las reglas y excepciones se realizarán en base a dirección IP origen y destino, no usuario. Es posible que el firewall aplique políticas en base a usuarios, pero mediante la instalación del cliente FSSO (The Fortinet Single Sign On) para la interacción entre el directorio activo y el Firewall. Sin el cliente instalado y configurado, no es posible la aplicación de políticas en base a usuarios.

1.3. Procedimiento

En el menú izquierdo del firewall, seleccionar Política → Política. Aparecerán en el recuadro derecho todas las políticas implementadas. La zona "Switch" pertenece a la zona segura (LAN) y la zona "Wan1" pertenece al acceso a Internet.

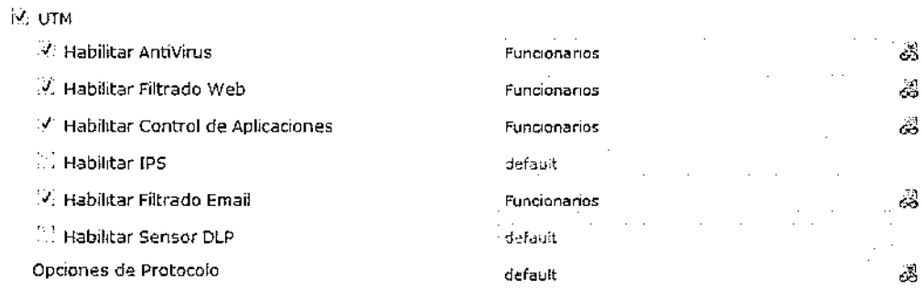


1. En el recuadro superior, seleccionar Crear Nuevo → Política. Aparecerá el menú correspondiente para crear la política:



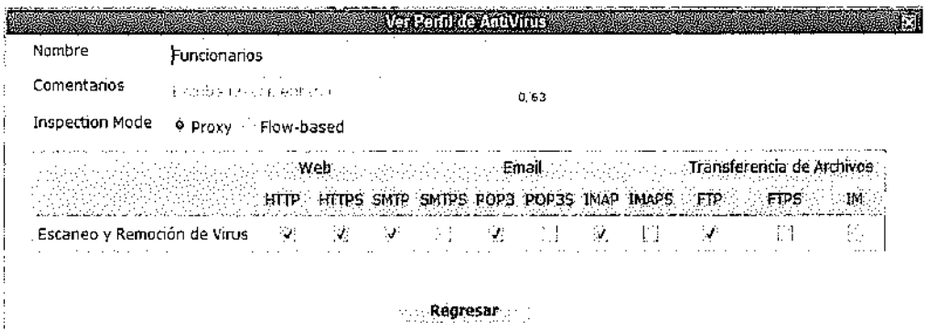
2. Seleccionar *Zona/Interfaz Origen (Switch o wan1)* y *Zona/Interfaz Destino*. Se tendrán que elegir las direcciones origen y destino previamente creadas en el menú principal *Objetos del Firewall→Dirección*. Si se desea, se puede seleccionar un horario previamente creado para que aplique en la regla. También se deberá seleccionar el tipo de servicio de entre los predefinidos (si se trata de alguno nuevo se deberá crear en *Objetos del firewall→ Servicio → Personalizado previamente*).

3. Elegir entre las opciones (se enumeran las más importantes):
   - Registrar el tráfico permitido: posibilita ver los logs de esa política
   - Enable NAT: hace una traducción de direcciones, en este caso particular se aplica desde la zona switch a la wan1 un NAT utilizando la dirección del interfaz de destino para la traducción (las direcciones internas privadas se traducen a una externa pública para la navegación)
   - UTM: Para habilitar la inspección del tráfico, antivirus, filtrado web, etc.



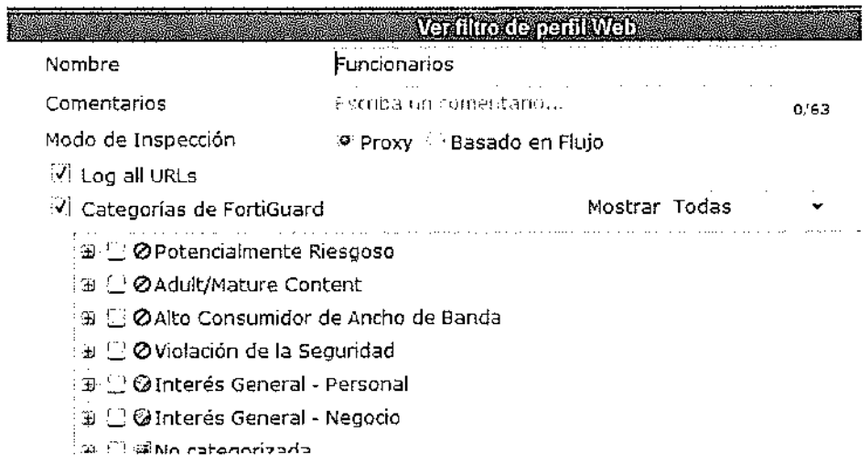
En esta opción, al ser marcada, aparecerá un menú desplegable donde se podrá elegir si la política tendrá habilitada el antivirus, filtrado web, control de aplicaciones, IPS, Filtrado de Email, etc.

- Habilitar antivirus:



Facilita la opción de que se active el antivirus para distintos protocolos (Web, Email, Ftp, etc)

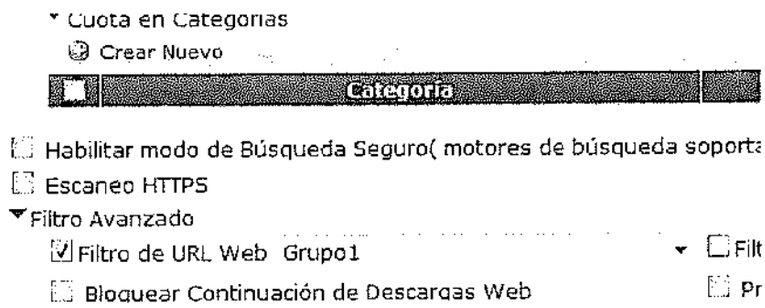
- Habilitar Filtrado Web:



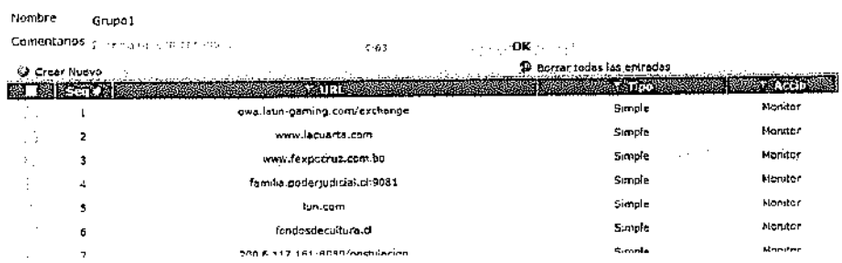
En esta categoría se puede elegir el modo de inspección (Proxy / Basado en flujo), y también si se emiten los logs de las URLs (webs). Normalmente el modo de inspección a elegir será el modo Proxy.

Por otro lado, en el menú desplegable de Categorías de FortiGuard, podremos elegir para las categorías predefinidas, cual estará prohibida o cual permitida.

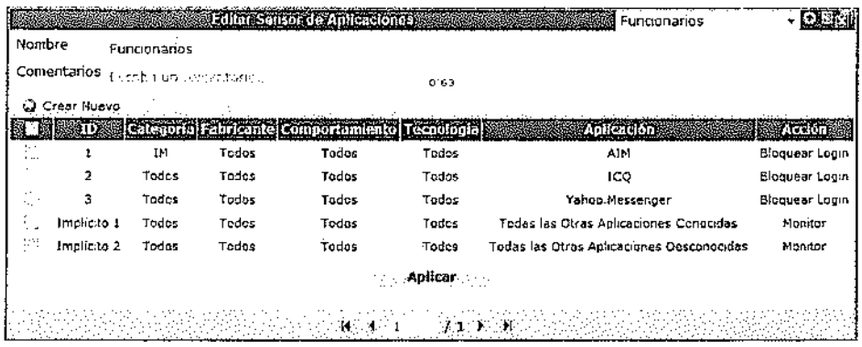
Si se quiere ser un poco más específico y cortar, por ejemplo, el acceso a la URL www.youtube.com, se puede seleccionar un grupo de URLs para su filtrado declaradas previamente en la opción "Filtro Avanzado", marcando "Filtro de URL Web" y eligiendo un grupo de URL previamente creado.



Para crear un grupo de URLs, serán en el menú *Perfiles de UTM→Filtro Web→Filtro de URL*. Allí se pueden incluir las direcciones web que se quieran monitorizar o filtrar.

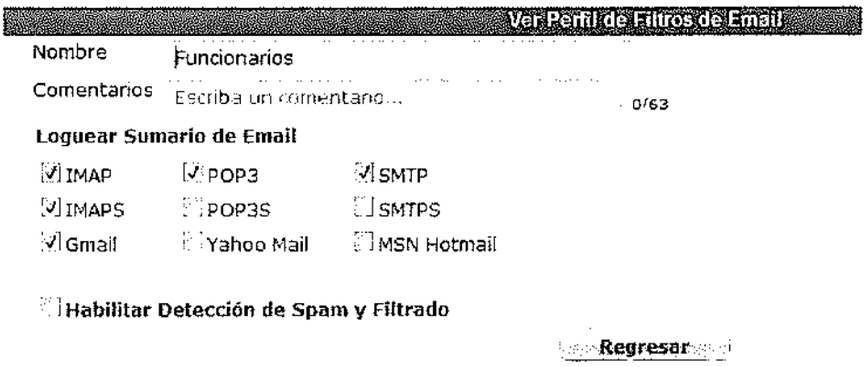


- Habilitar control de aplicaciones:



Permite realizar un control sobre las aplicaciones utilizadas, ya sea para bloquearlas o para monitorizarlas. Si se pulsa "Crear Nuevo" en la edición del sensor de aplicaciones, podremos elegir entre las categorías ya predefinidas de aplicaciones de Fortigate, que están declaradas en el menú *Perfiles de UTM→Control de aplicaciones→Lista de aplicaciones.*

- Habilitar Filtrado Email:



Permite obtener logs sumarizados de distintos tipos de Email, y detectar / filtrar spam.

- Habilitar sensor IPS: para la detección y prevención de intrusos. Se recomienda marcar esta opción en las políticas de entrada (de wan1 hacia switch) únicamente.
- Habilitar sensor DLP: para almacenar logs de email y tráfico web.

- Control de tráfico: si se quiere priorizar algún tipo de tráfico sobre otro, o garantizar caudales, se puede realizar con esta opción. Tan sólo habrá que declarar un tipo de caudales que se quieren tener en el menú Objetos del Firewall→ Calidad de servicio→ Compartido. Al crear los tipos de caudales, se especificará el caudal máximo, el garantizado y su prioridad.

1.4. Verificación de evidencias

Evidencias	**Cumplimiento y observaciones**
Se aplica una metodología creación de políticas de firewall	
Antes de crear la política	
a. Saber previamente las zonas origen y destino	
b. Conocer si la política a crear debe estar permitida o no	
c. Investigar si la política debería llevar implantada algún tipo de filtro Web, antivirus, antispam, etc	

Evidencias	Cumplimiento y observaciones
d. Antes de configurar la política, estudiar previamente la posición que debe tener entre el resto de políticas existentes.	
Las pruebas de verificación	
a. Comprobación de la conexión permitida o rechazada b. Verificación de las características de la política implementada (Filtro web, antivirus, etc)	

2. FIREWALL: PROCEDIMIENTO DE CREACION DE ZONAS EN EL FIREWALL FORTIGATE 110C

Responsable

Responsable	Encargado de la Unidad Informática

2.1. Objeto

- Explicación de los pasos necesarios para la configuración de zonas como la DMZ (Zona Perimetral), necesarias para la publicación de servicios de una forma segura sin que se ponga en riesgo la LAN. Con la utilización de zonas, se evitan accesos directos de Internet a la zona más segura (LAN). También se pueden utilizar nuevas zonas para protección sobre zonas no seguras distintas de internet.

2.2. Requisitos previos

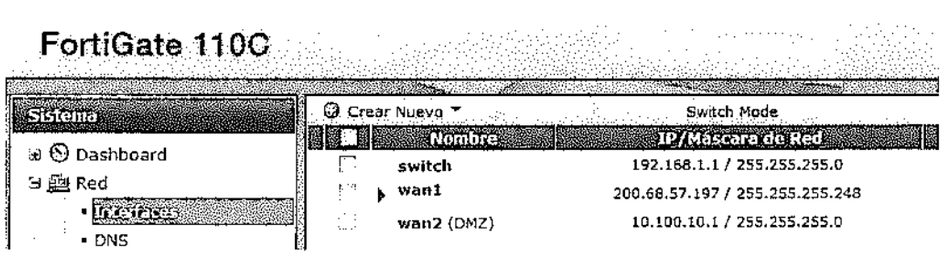
- Se requiere que físicamente se pueda conectar la nueva zona físicamente al firewall, mediante conectorización Ethernet.

2.3. Procedimiento

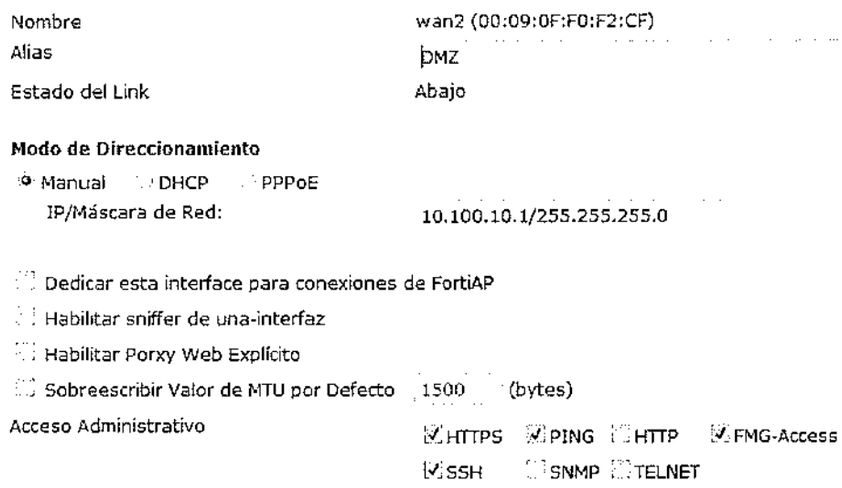
Cada vez que se quiera dar de alta una nueva zona, se deberán realizar las siguientes tareas:

1. Configuración de la zona en el firewall. Para la creación de la zona, se realizará mediante los siguientes pasos:

   - Creación de la nueva zona: en el menú *Sistema → Red → Interfaces* se encuentran listadas las distintas zonas e interfaces.

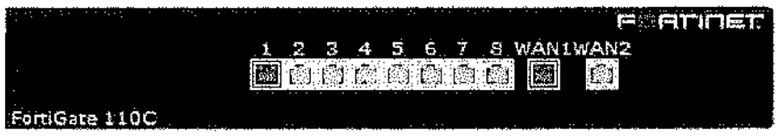


- Seleccionar *Crear Nuevo → Interfaz* para crear la zona. En este caso sólo es posible la creación de una zona DMZ (Interfaz físico wan2). Actualmente este interfaz se encuentra configurado pero no conectado



  - En esta opción se puede seleccionar el nombre, alias y direccionamiento IP de la nueva zona, así como las opciones de administración del firewall en ese interfaz. El resto de opciones no son esenciales para la creación de la zona.

2. Conexión física de la nueva zona al interfaz correspondiente. En el caso del firewall Fortigate 110c, sólo tiene uno disponible: el interfaz wan2



3. Implementación de políticas para dar conectividad a la nueva zona. Se deberá seguir el *Procedimiento Para la Creación de Reglas y Excepciones* descrito anteriormente para crear conectividad entre la nueva zona e internet, o hacia / desde la zona segura (LAN)

2.4. Verificación de evidencias

Evidencias	**Cumplimiento y observaciones**
Se aplica una metodología de	
Los siguientes elementos serán parte de la creación de la zona	
a. Verificación de que existen puertos físicos libres para la creación de la nueva zona	
b. Verificación del nuevo rango de direccionamiento IP de IP zona	
c. Implementación de políticas de comunicación entre zonas	
d. Pruebas de comunicación entre zonas para verificar la correcta conectividad	

3. FIREWALL: PROCEDIMIENTOS PARA LA ACTIVACION DE LA PROTECCIÓN CONTRA ATAQUES: IPS/DoS

Responsable

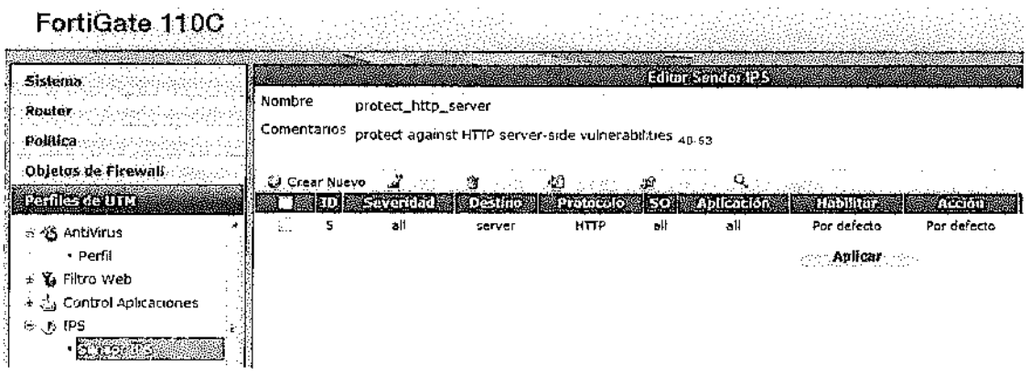
Responsable	Encargado de la Unidad Informática

3.1. Objeto

- Establecer los procedimientos para la activación de los mecanismos del firewall correspondientes a la prevención de intrusos y protección frente a ataques de denegación de servicio (DoS)

3.2. Requisitos previos

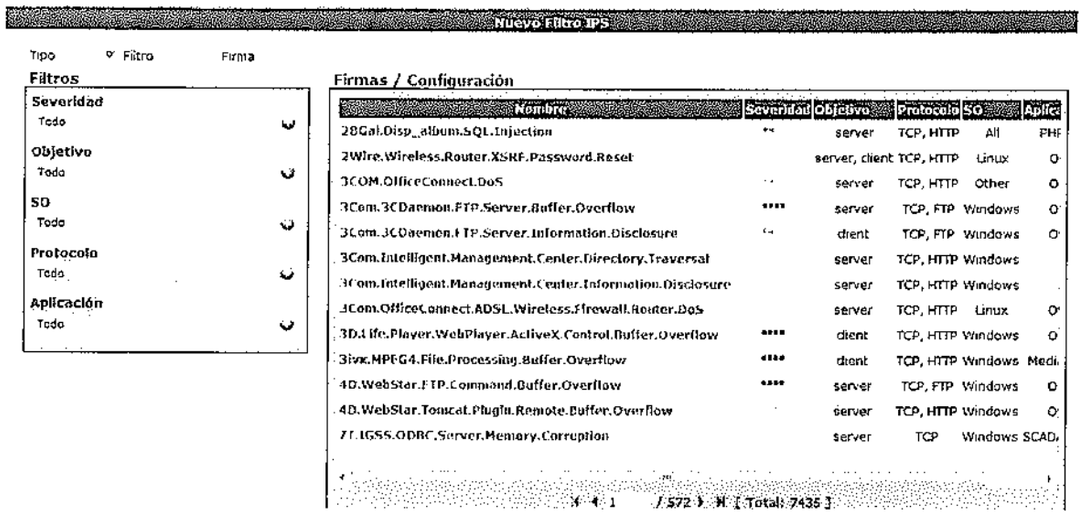
- La aplicación de medidas de protección frente a intrusos y denegación de servicio implica la posibilidad de que existan falsos positivos. Por ello, se recomienda comenzar a implementar estas medidas de la manera más ligera posible, incluyendo las amenazas más críticas en un principio. A partir de ahí se podrá ir subiendo en el tipo de amenazas e ir observando si existen falsos positivos. Todo ello para que el tráfico deseado no se vea comprometido.



3.3. Procedimiento

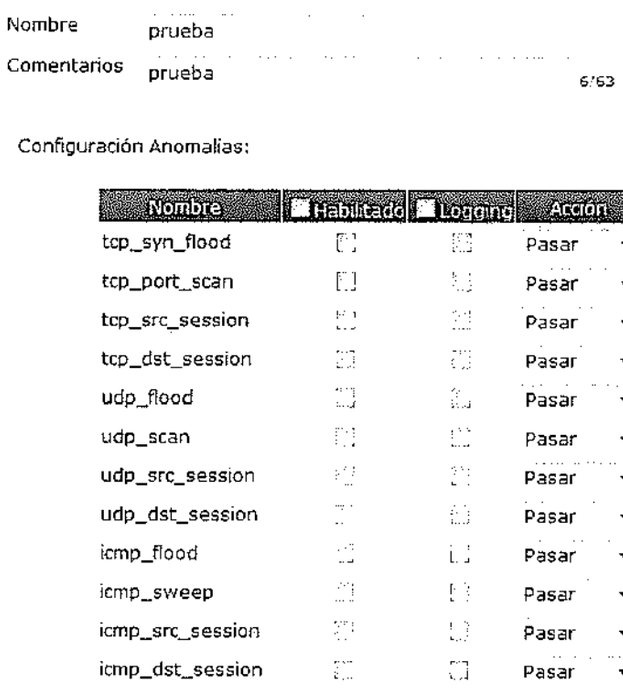
Para aplicar las políticas de detección de intrusos, y denegación de servicio, se procederá como se describe a continuación. Se recomienda aplicar estas políticas en la dirección de zonas menos seguras a más seguras.

1. Creación del sensor IPS: Para poder aplicar el sensor IPS a una política determinada, se deberá primero crear el sensor con la sensibilidad que se desee. Para ello se debe seleccionar la opción Perfiles de *UTM→IPS→Sensor IPS*. Dentro de esta opción, pulsar "Crear Nuevo"



En el menú se podrá elegir el tipo de IPS (normalmente es Filtro), y una serie de características del mismo (severidad, objetivo, Sistema Operativo, protocolo y aplicación). Con estas opciones se puede precisar con exactitud qué tipos de tráfico se van a controlar.

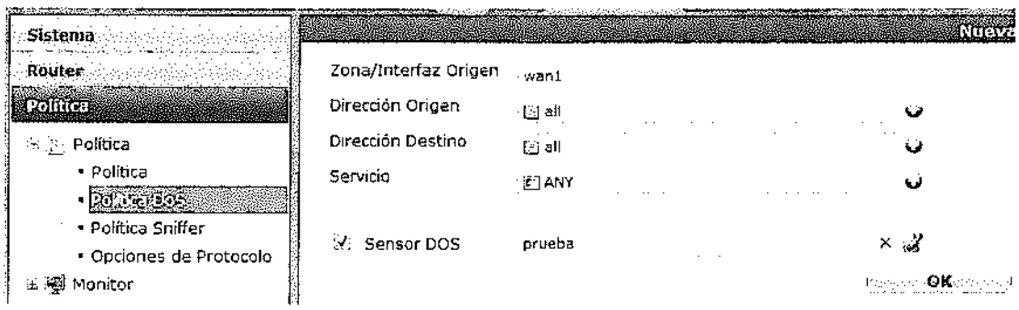
2. Creación del sensor DoS: Para poder aplicar el sensor DoS a una política determinada, se deberá primero crear el sensor con la sensibilidad que se desee. Para ello se debe seleccionar la opción *Perfiles de UTM→IPS→Sensor DoS*. Dentro de esta opción, pulsar "Crear Nuevo"



En el sensor podremos configurar si se dejan pasar o no cierto tipo de anomalías de DoS predefinidas ya en el firewall y además si se almacenan los logs cada vez que se detecte alguna. Además de todo eso, se podrá modificar el umbral de accesos por el cual se considera un ataque o no.

3. Aplicar el sensor IPS a las políticas: En la opción de UTM de cada política explicada en el procedimiento 1, se puede seleccionar si se desea activar el sensor IDS y seleccionar el que se ha creado previamente

4. Creación de políticas de DoS: Para el caso del sensor de DoS, se tendrá que crear una política específica. En el menú *Política→Política DoS*, se puede crear la política precisando interfaz origen (normalmente, el de la zona no segura), direcciones origen y destino y aplicación.



3.4. Verificación de evidencias

Evidencias	**Cumplimiento y observaciones**
Realizar las siguientes comprobaciones	
a. Sentido en el que se está aplicando el sensor IPS o DoS	
b. Verificación de que no se está impidiendo el tráfico deseado (Falsos positivos)	

4. FIREWALL: PROCEDIMIENTOS PARA LA MONITORIZACION DEL TRAFICO Y LOGS EN EL FIREWALL

Responsable

Responsable	Encargado de la Unidad Informática

4.1. Objeto

- Documentación de toda la metodología para la obtención de logs y monitorización del tráfico en el Firewall

4.2. Procedimiento

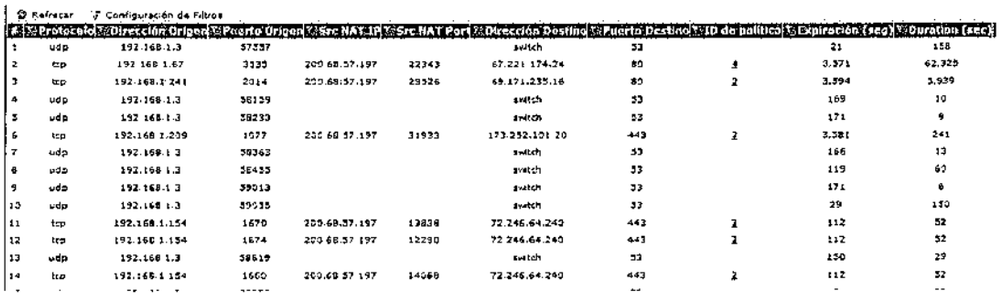
Existen varios tipos de monitorización en el Firewall. Cada tipo proporciona datos sobre el tráfico, accesos prohibidos, etc. Se desglosan a continuación:

1. Monitorización de políticas y sesiones

a) En el menú *Políticas → Monitor de Políticas*, se puede observar las sesiones abiertas y el tráfico cursado por política:

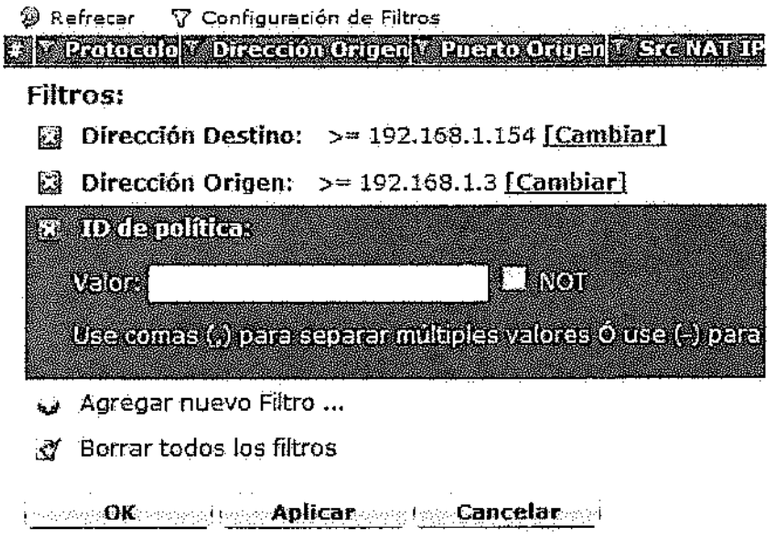
ID de Política	Interfaz/Zona de Origen	Interfaz/Zona de Destino	Acción	Sesiones Activas	Bytes	Paquetes
2	switch	wan1	✓	521	144.58 GB	235.746.220
7	switch	wan1	✓	106	42.35 GB	69.762.374
4	switch	wan1	✓	101	53.22 GB	74.686.314
10	switch	wan1	✓	63	10.07 GB	16.207.512
5	wan1	switch	✓	41	40.22 GB	59.028.980
6	wan1	switch	✓	12	11.44 GB	16.872.293
3	switch	wan1	✓	4	8.30 GB	11.336.754

b) En el menú Políticas→ Monitor de Sesiones, se puede analizar el tráfico cursado en base a direccionamiento IP origen o destino, NAT o puerto utilizado. También se pueden observar datos como la duración de la sesión así como el tráfico cursado.


Refrescar Configuración de Filtros

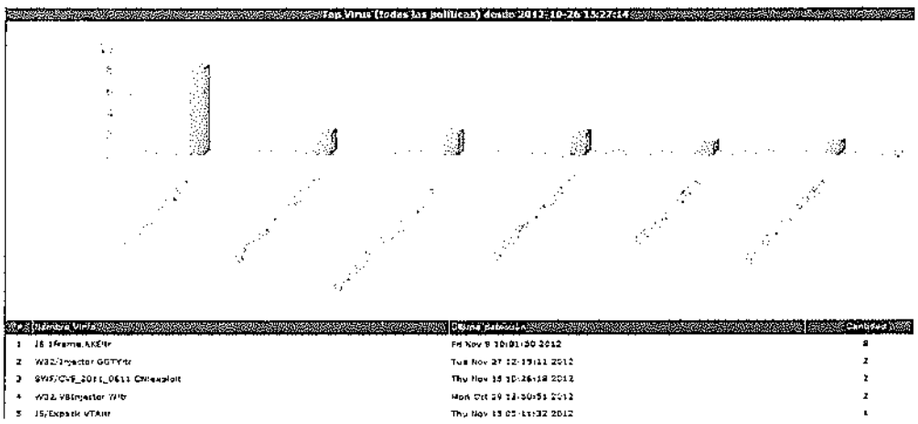
#	Protocolo	Dirección Origen	Puerto Origen	Src NAT IP	Src NAT Port	Dirección Destino	Puerto Destino	ID de política	Expiración (seg)	Duración (seg)
1	udp	192.168.1.3	57537			switch	53		21	158
2	tcp	192.168.1.67	3135	200.68.57.197	32343	67.221.174.24	80	4	3.371	62.325
3	tcp	192.168.1.241	2014	200.68.57.197	29526	69.171.235.16	80	2	3.594	3.939
4	udp	192.168.1.3	58139			switch	53		169	10
5	udp	192.168.1.3	58233			switch	53		171	9
6	tcp	192.168.1.209	1577	200.68.57.197	31933	173.252.101.20	443	2	3.581	241
7	udp	192.168.1.3	59363			switch	53		166	13
8	udp	192.168.1.3	58435			switch	53		119	60
9	udp	192.168.1.3	59013			switch	53		171	0
10	udp	192.168.1.3	59135			switch	53		29	150
11	tcp	192.168.1.154	1670	200.68.57.197	13838	72.246.64.240	443	2	112	52
12	tcp	192.168.1.154	1674	200.68.57.197	12290	72.246.64.240	443	2	112	52
13	udp	192.168.1.3	58619			switch	53		150	29
14	tcp	192.168.1.154	1660	200.68.57.197	14068	72.246.64.240	443	2	112	52

Si se quiere analizar un tipo de tráfico concreto o hacia un origen / destino en particular, se podrá seleccionar en "Configuración de Filtros". En esta opción podremos filtrar las sesiones para que se vean sólo las que se están buscando.

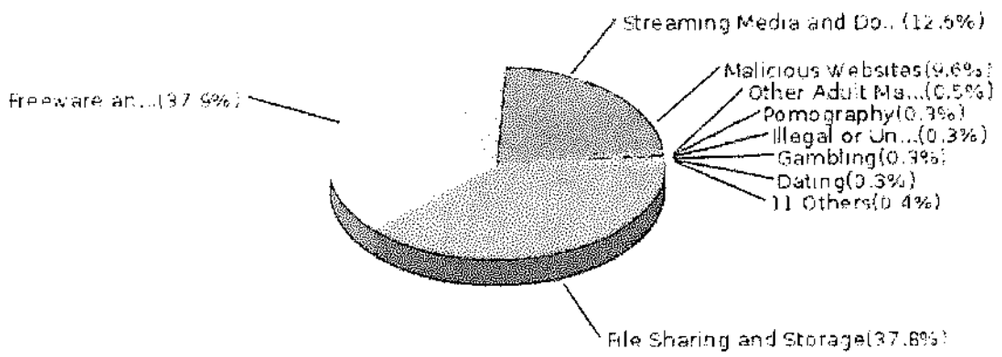


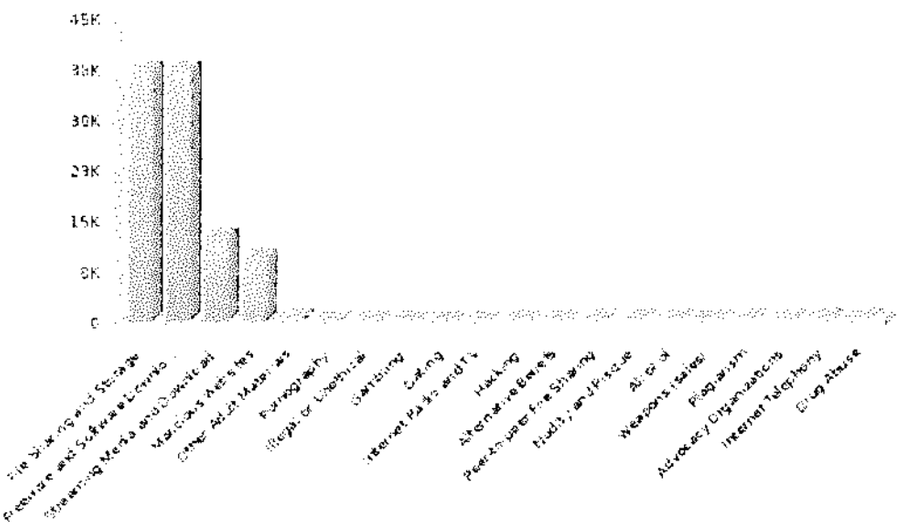
2. Monitor de características UTM

a) Monitor AV (antivirus): En el menú *Perfiles de UTM→Monitor→ Monitor de AV*, se obtienen estadísticas de los virus detectados.

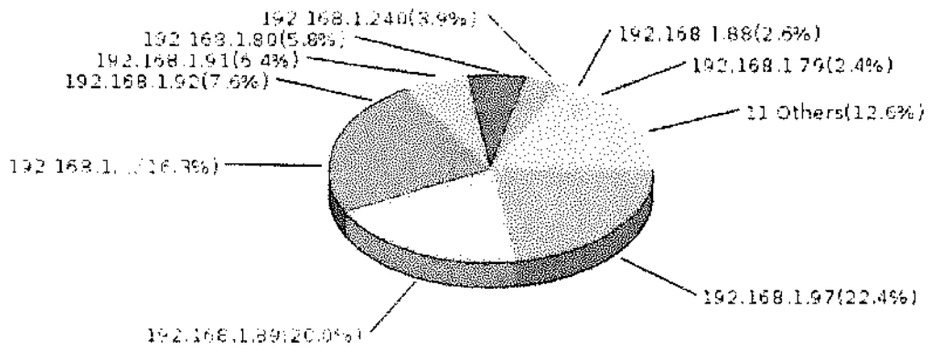


b) Monitor Web: Se trata de una de las más interesantes monitorizaciones del aparato, ya que de esta se obtienen datos de páginas bloqueadas por el filtrado web del firewall.





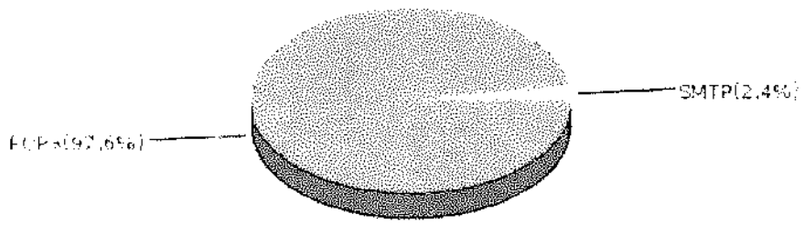
Si se selecciona alguna de las categorías del gráfico de barras, se obtiene un listado de usuarios que más han intentado acceder a este tipo de sitios denegados.



c) Monitor de Aplicaciones: Para aplicaciones predefinidas y utilizadas en políticas, presenta las que tienen una mayor utilización de ancho de banda, sesiones y usuarios.

d) Monitor de Intrusiones: Monitoriza las intrusiones detectadas por el sensor de IPS

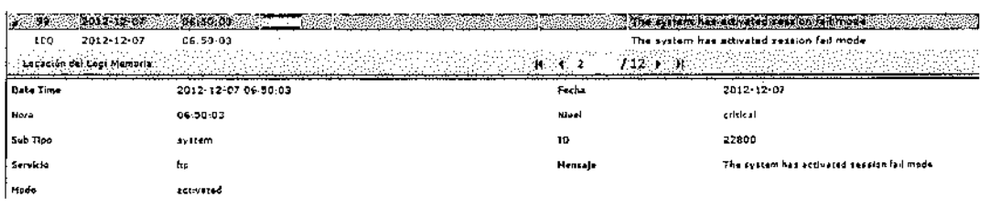
e) Monitor de Correo Electrónico: Se monitorizan los correos totales y los correos bloqueados.



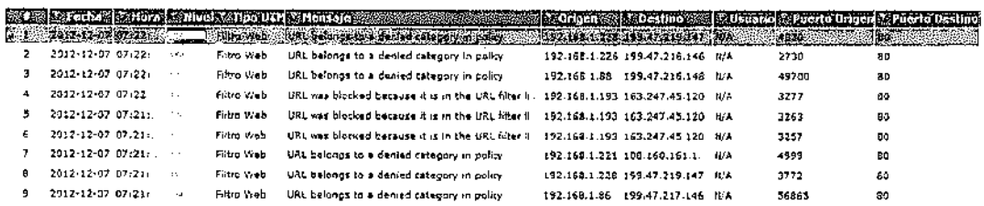
3. Monitorización de Logs

En el menú Logs&Reporte se detallan todos los tipos de logs generados por el aparato.

a) Logs de eventos *(Menú Acceso a logs→ Eventos).* Se proporcionan los logs de eventos generados por la máquina, en función de su gravedad. Se pueden utilizar filtros para seleccionar en función del nivel de la gravedad (Emergency, alert, critic, error, warning, notice, information, debug) y la fecha entre otros parámetros.

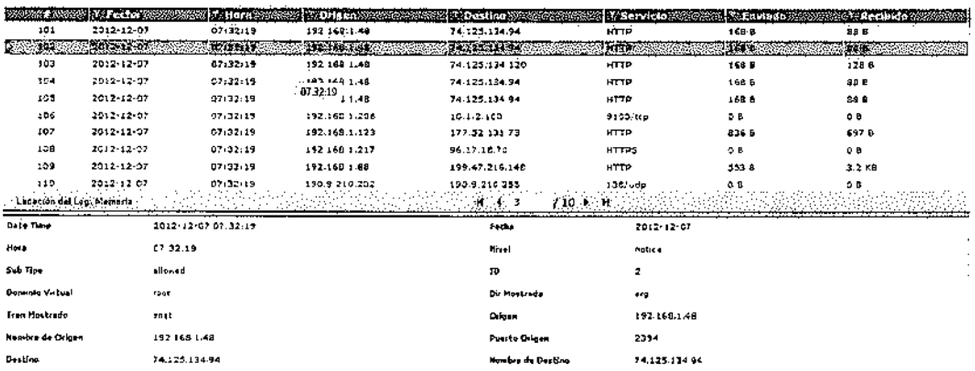


b) Logs de UTM: Muestra los logs de UTM, pudiendo filtrar por el tipo de UTM utilizado (Web Filtering, Antivirus, etc), direcciones IP origen y destino entre otros datos.



#	Fecha	Hora	Nivel	Tipo Log	Mensaje	Origen	Destino	Usuario	Puerto Origen	Puerto Destino
1	2012-12-07 07:22:			Filtro Web	URL belongs to a denied category in policy	192.168.1.226	199.47.216.146	N/A	2730	80
2	2012-12-07 07:22:			Filtro Web	URL belongs to a denied category in policy	192.168.1.226	199.47.216.146	N/A	2730	80
3	2012-12-07 07:22:			Filtro Web	URL belongs to a denied category in policy	192.168.1.88	199.47.216.146	N/A	49700	80
4	2012-12-07 07:22			Filtro Web	URL was blocked because it is in the URL filter li	192.168.1.193	163.247.45.120	N/A	3277	80
5	2012-12-07 07:21:			Filtro Web	URL was blocked because it is in the URL filter li	192.168.1.193	163.247.45.120	N/A	3263	80
6	2012-12-07 07:21:			Filtro Web	URL was blocked because it is in the URL filter li	192.168.1.193	163.247.45.120	N/A	3257	80
7	2012-12-07 07:21:			Filtro Web	URL belongs to a denied category in policy	192.168.1.221	108.160.161.1	N/A	4599	80
8	2012-12-07 07:21:			Filtro Web	URL belongs to a denied category in policy	192.168.1.238	199.47.219.147	N/A	3772	80
9	2012-12-07 07:21:			Filtro Web	URL belongs to a denied category in policy	192.168.1.86	199.47.217.146	N/A	56863	80

c) Logs de tráfico: Para cada política que tiene habilitada la opción "log", se muestra cada conexión realizada



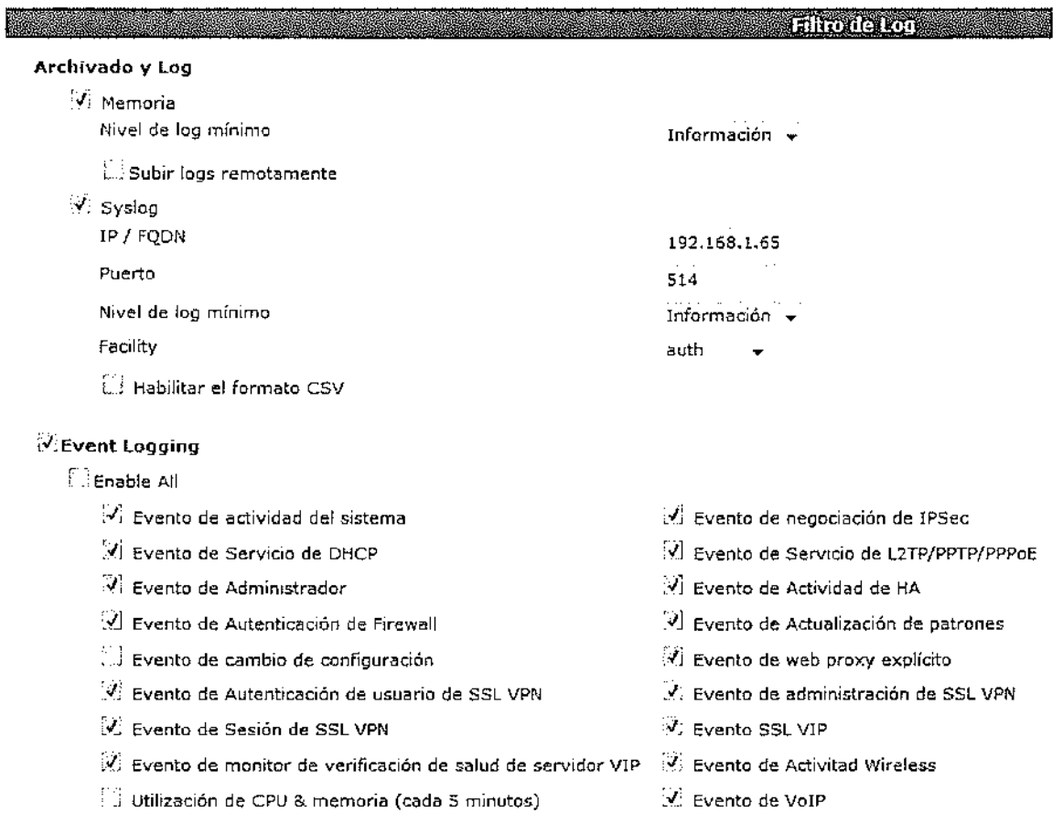
#	Fecha	Hora	Origen	Destino	Servicio	Enviado	Recibido
101	2012-12-07	07:32:19	192.168.1.48	74.125.134.94	HTTP	168 B	88 B
102	2012-12-07	07:32:19	192.168.1.48	74.125.134.94	HTTP	168 B	88 B
103	2012-12-07	07:32:19	192.168.1.48	74.125.134.120	HTTP	168 B	128 B
104	2012-12-07	07:32:19	192.168.1.48	74.125.134.94	HTTP	168 B	88 B
105	2012-12-07	07:32:19	192.168.1.48	74.125.134.94	HTTP	168 B	88 B
106	2012-12-07	07:32:19	192.168.1.206	10.1.2.10	9100/tcp	0 B	0 B
107	2012-12-07	07:32:19	192.168.1.123	173.32.131.73	HTTP	836 B	697 B
108	2012-12-07	07:32:19	192.168.1.217	96.17.16.70	HTTPS	0 B	0 B
109	2012-12-07	07:32:19	192.168.1.88	199.47.216.146	HTTP	353 B	3.2 KB
110	2012-12-07	07:32:19	190.9.210.202	190.9.210.255	138/udp	0 B	0 B

Locación del Log: Memoria — 1 / 10

Date Time	2012-12-07 07:32:19	Fecha	2012-12-07
Hora	07:32:19	Nivel	notice
Sub Tipo	allowed	ID	2
Dominio Virtual	root	Dir Mostrado	org
Fran Mostrado	mnt	Origen	192.168.1.48
Nombre de Origen	192.168.1.48	Puerto Origen	2394
Destino	74.125.134.94	Nombre de Destino	74.125.134.94

4. Configuración de los Logs

En el menú *Logs&Reporte→Configurar Logs→ Configurar Logs*, se pueden configurar los tipos de logs que se quieren presentar. Además, se puede seleccionar si los logs se almacenan en memoria (opción por defecto) o si desea además enviarlos a un servidor de syslog.



Filtro de Log

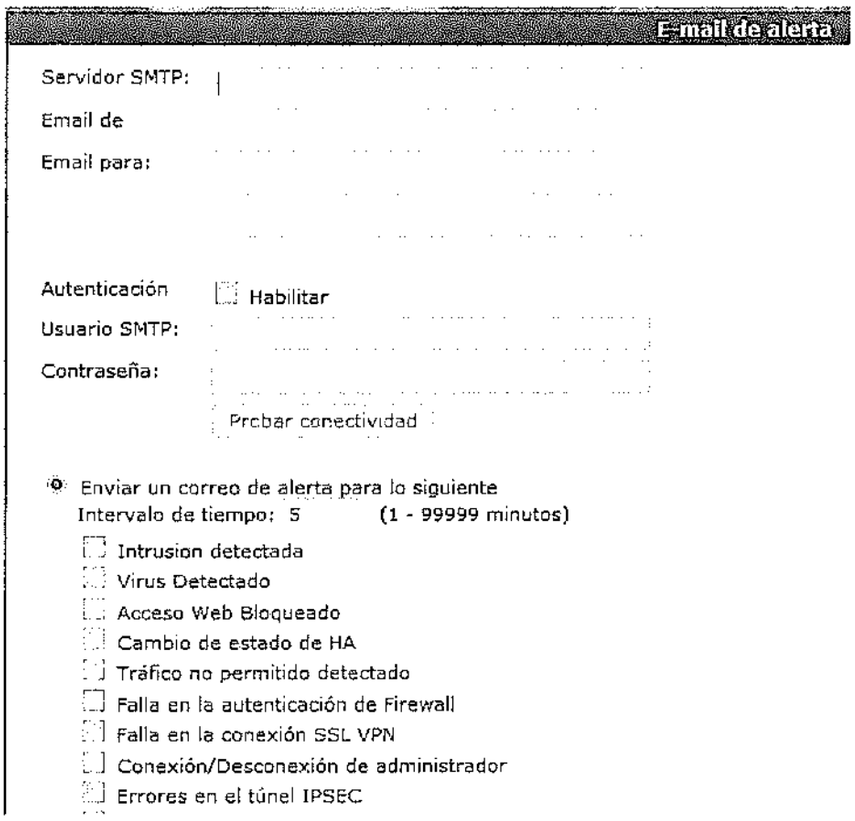
Archivado y Log

- [x] Memoria
  - Nivel de log mínimo: Información
  - [ ] Subir logs remotamente
- [x] Syslog
  - IP / FQDN: 192.168.1.65
  - Puerto: 514
  - Nivel de log mínimo: Información
  - Facility: auth
  - [ ] Habilitar el formato CSV

[x] Event Logging

- [ ] Enable All
- [x] Evento de actividad del sistema
- [x] Evento de Servicio de DHCP
- [x] Evento de Administrador
- [x] Evento de Autenticación de Firewall
- [ ] Evento de cambio de configuración
- [x] Evento de Autenticación de usuario de SSL VPN
- [x] Evento de Sesión de SSL VPN
- [x] Evento de monitor de verificación de salud de servidor VIP
- [ ] Utilización de CPU & memoria (cada 5 minutos)
- [x] Evento de negociación de IPSec
- [x] Evento de Servicio de L2TP/PPTP/PPPoE
- [x] Evento de Actividad de HA
- [x] Evento de Actualización de patrones
- [x] Evento de web proxy explícito
- [x] Evento de administración de SSL VPN
- [x] Evento SSL VIP
- [x] Evento de Activitad Wireless
- [x] Evento de VoIP

a) Alertas por Email: En el menú Logs&Reporte→Configurar Logs→Alertas por Email, se pueden configurar las alertas por email basadas en eventos log. Cada vez que se produzca un log determinado que se preconfigure, este generará que se envíe un correo de aviso. Para que los correos se envíen, se debe disponer de un servidor SMTP.



4.3. Verificación de evidencias

Evidencias	**Cumplimiento y observaciones**
Se realizarán las siguientes pruebas para la verificación de los logs	
a. Verificación visual en la web del firewall	
b. Verificación en servidor de syslog	
b. Verificación de alertas por email	

5. FIREWALL: PROCEDIMIENTO PARA LA REALIZACION DE LA COPIA DE SEGURIDAD DEL FIREWALL

Responsable

Responsable	Encargado de la Unidad Informática

5.1. Objeto

- Establecer los procedimientos necesarios para la realización de una copia de seguridad del Firewall para que pueda ser restaurada en caso de avería o necesidad de llevar al sistema a una configuración anterior.

5.2. Requisitos previos

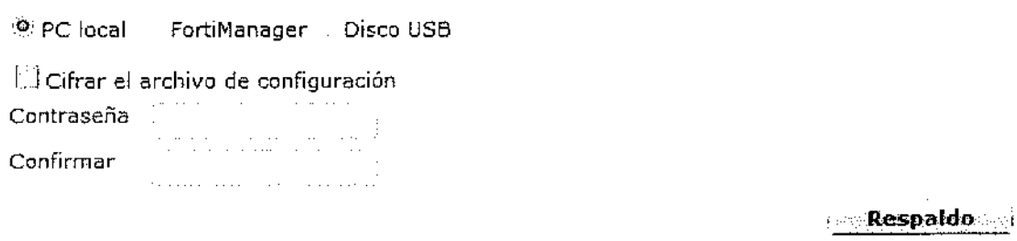
- La existencia de un PC que se conecte a la administración del firewall.
- Alternativamente a la opción anterior, el uso de una memoria USB directamente conectada al firewall.

5.3. Procedimiento

Para la realización de un **backup** de la configuración del dispositivo, se realizará lo siguiente:

1. Seleccionar el menú Sistema→Dashboard→ Status. Dentro del recuadro de Configuración del Sistema, seleccionar "Respaldo"

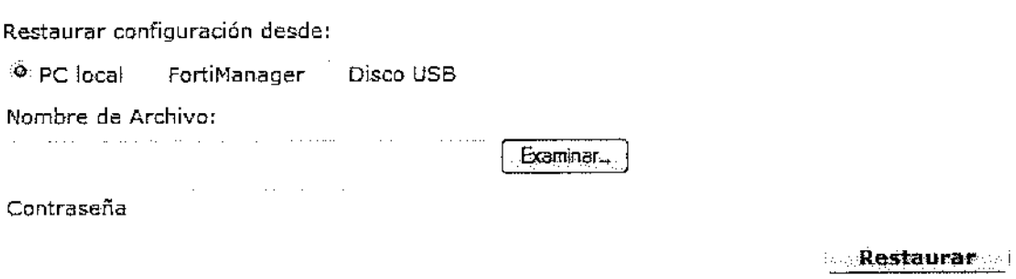
   En esta opción se podrá elegir entre hacer la copia en un PC Local o en la memoria usb. La configuración será almacenada en un fichero .conf que podrá ser utilizado para una restauración futura. Para hacer la copia, pulsar "Respaldo".



Para la realización de la **restauración** de la configuración del dispositivo, se realizará lo siguiente:

2. Seleccionar el menú Sistema→Dashboard→ Status. Dentro del recuadro de Configuración del Sistema, seleccionar "Restaurar"

   Al igual que en la opción del respaldo, se podrá seleccionar entre la fuente del PC o de un disco USB conectado al Firewall. Se tendrá que seleccionar el fichero con la configuración deseada y pulsar "Restaurar"



5.4. Verificación de evidencias

Evidencias	Cumplimiento y observaciones
Verificación de que la copia de seguridad se ha realizado correctamente:	
a. Verificación de la existencia del fichero de copia de seguridad en el PC	
b. Verificación de la existencia del fichero de copia de seguridad en el USB	

6. FIREWALL: PROCEDIMIENTO PARA LA REALIZACION DE UNA VPN SSL PARA EL ACCESO DESDE EL EXTERIOR

Responsable

Responsable	Encargado de la Unidad Informática

6.1. Objeto

- Establecer los procedimientos necesarios para la realización de una VPN a través de SSL para el acceso remoto a equipos internos o a la DMZ.

6.2. Requisitos previos

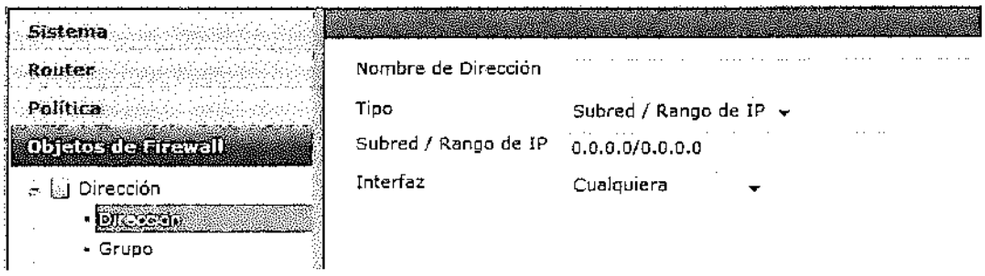
- Se ha detectado que existe un problema con la versión de software actual del firewall y la VPN SSL. Será necesario actualizar previamente el firewall a la última versión para que funcione correctamente la VPN. La versión actual es la v4.0,build0496,111108 (MR3 Patch 3), y la última la V5.0GA. El firewall se puede actualizar directamente el menú *Sistema→Dashboard→Información del sistema→ Versión de Firmware → Actualizar*. Desde ahí elegir la opción "Bajar desde Fortiguard Network" con las opciones por defecto y pulsar "ok". La actualización de Firmware provoca la desconexión del aparato durante varios minutos y no se puede interrumpir el proceso, de lo contrario se puede estropear el aparato.

- Se recomienda utilizar otros navegadores distintos del Internet Explorer por si no funcionara con este (Firefox, Chrome)

6.3. Procedimiento

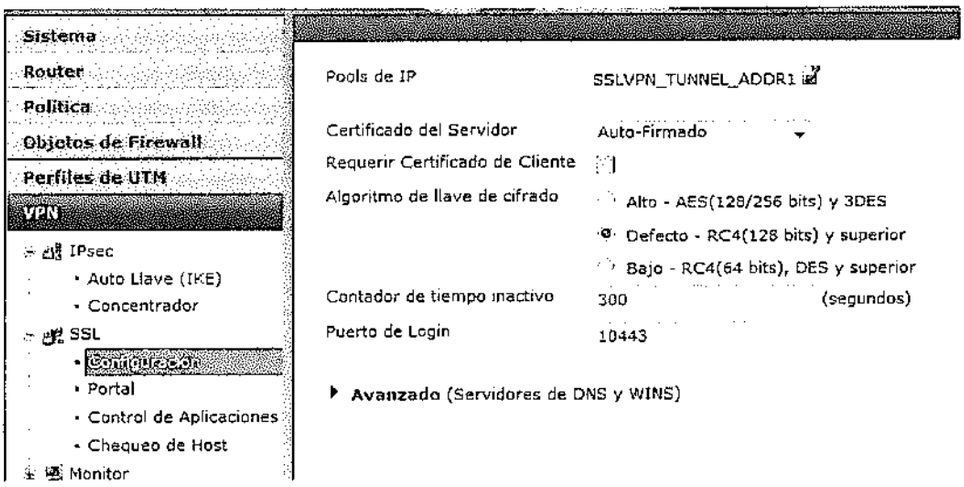
Para realizar la configuración de una VPN SSL en el dispositivo, se realizará lo siguiente:

1. Lo primero que se debe realizar es la creación de un pool de direcciones IP para asignar a los usuarios que se conecten a la VPN. Se deberá ir al menú Objetos del Firewall→Dirección→Dirección. En el recuadro interior, pulsar "Crear Nuevo" y seleccionar "Dirección/FQDN".

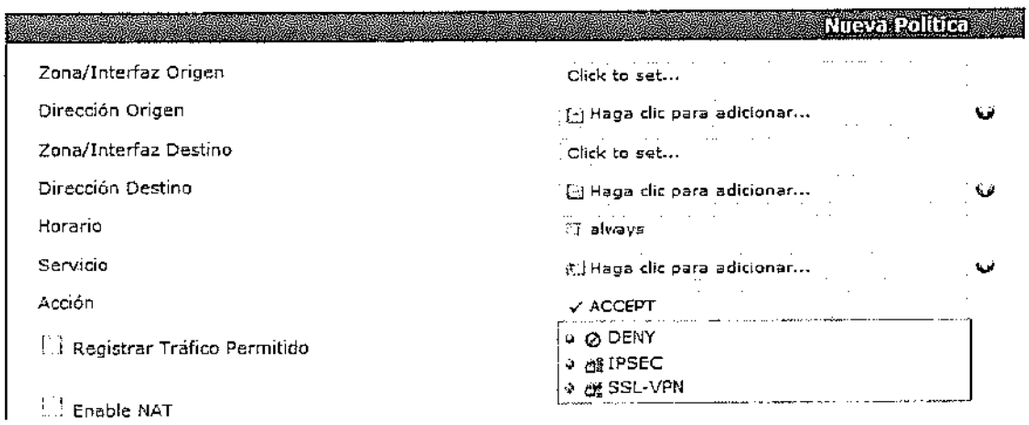


Posteriormente se deberá incluir el nombre del rango que se va a crear y el direccionamiento IP que van a recibir los clientes VPN

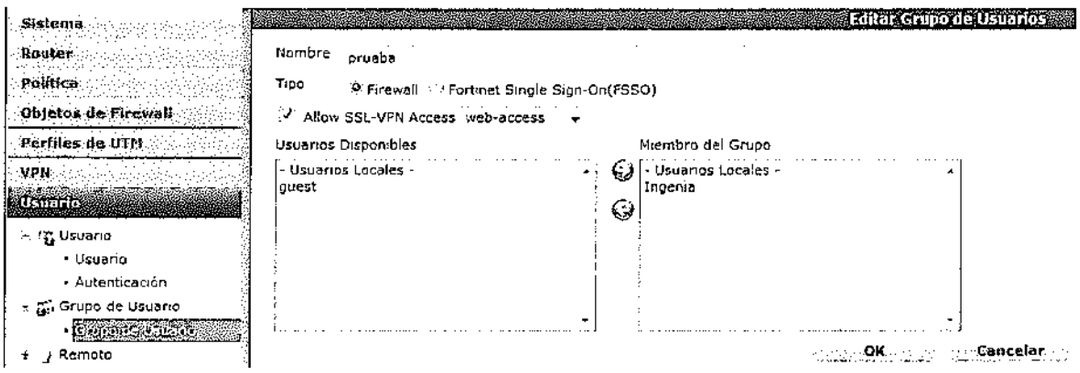
2. En el menú VPN→SSL→Configuración, seleccionar el pool de direcciones que se ha creado previamente, y mantener el resto de opciones por defecto. Pulsar "aplicar"



3. Se deberá crear una política asociada desde el interfaz wan1 hacia la zona switch (LAN) o la DMZ si la hubiere para el acceso desde el exterior. La manera de crear la política es similar a la que se describió en el *Procedimiento para la Creacion de Reglas y Excepciones*. Tan sólo se deberá seleccionar en el apartado "Acción" la opción "SSL-VPN"



4. Por último, se deberán crear los usuarios y grupo de usuarios que accederán a la VPN SSL. En la opción Usuario→Usuario, se podrán crear los usuarios junto con sus password de acceso. Posteriormente, en Usuario→Grupos de usuarios→Grupos de usuario, se crea un grupo con los usuarios que se han creado previamente. Al crear el grupo, se marcará la opción de SSL-VPN. Dentro de esta, marcar "tunnel-access" para especificar ese modo de tunelización.



5. Por último, el cliente VPN deberá acceder a la VPN SSL mediante el siguiente enlace: http://Dirección IP Publica Firewall:10443/remote Deberá tener activado ActiveX para que pueda funcionar correctamente.

6.4. Verificación de evidencias

Evidencias	Cumplimiento y observaciones
Verificación de que un usuario pueda conectar a la VPN:	
a. Conexión al portal especificado	
b. Verificación de conectividad una vez introducidos usuarios y contraseña	

7. REDES INALAMBRICAS: MEJORES PRÁCTICAS EN LA PLANIFICACION DE FRECUENCIAS DE LOS PUNTOS DE ACCESO

Responsable

Responsable	Encargado de la Unidad Informática

7.1. Objeto

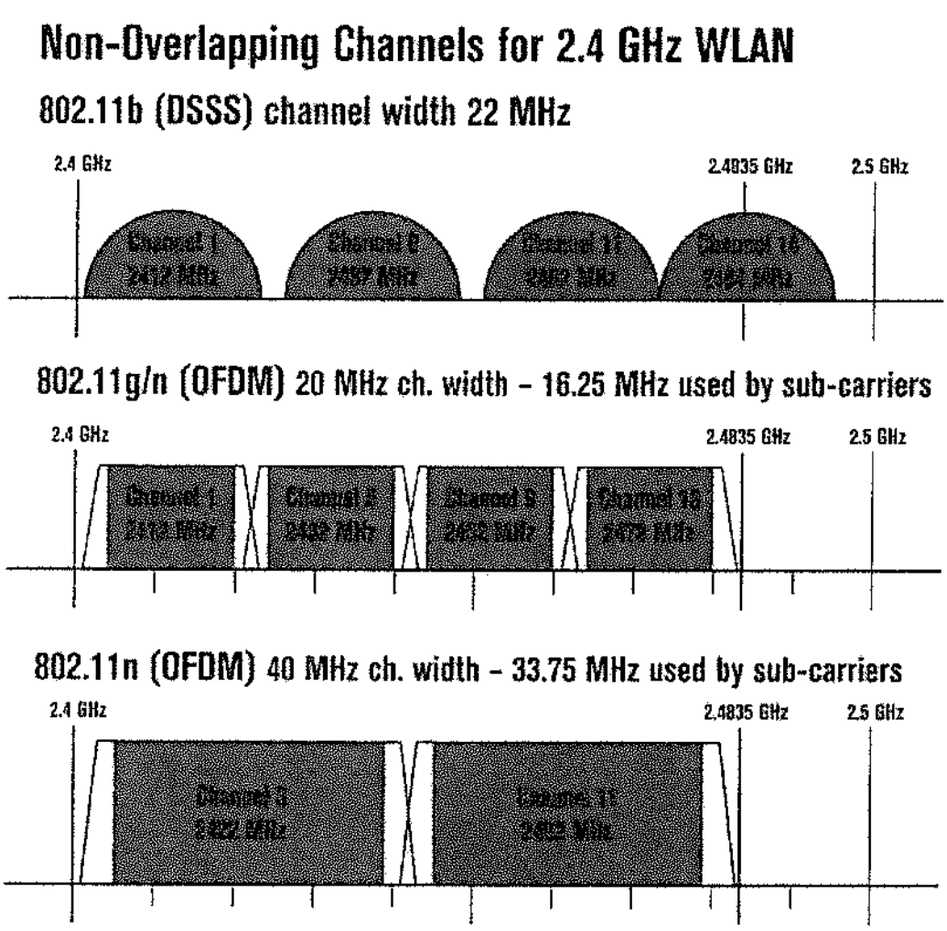
- Realizar una planificación de frecuencias de los puntos de acceso que no se solape con los adyacentes ni los existentes alrededor. Con ello se consiguen un mejor rendimiento global de la red al no haber solape.

7.2. Requisitos previos

- Realizar un análisis de las frecuencias asignadas a los puntos de acceso.
- Realizar un estudio de cobertura y frecuencias en la zona que puedan interferir en la red inalámbrica propia (utilizando aplicaciones como NetStumbler)

7.3. Procedimiento

En puntos de acceso adyacentes, se deberán elegir frecuencias no solapables:



Es decir, para la WIFI más común que sigue el estándar 802.11g, las frecuencias (canales) no solapables son el 1, 5, 9 y 13 (1, 4, 8 y 11 en el caso de no existir el canal 13).

Si se está utilizando el estándar 802.11n a 2.4GHz, la problemática es mayor ya que suele utilizar un ancho de banda de 40MHz, por lo que sólo hay dos canales disponibles (canales 3 y 11)

7.4. Verificación de evidencias

Evidencias	Cumplimiento y observaciones
Verificación de frecuencias una vez realizada la planificación	
a. Estudio de cobertura con aplicaciones como Netstumbler	
b. Verificación de frecuencias adyacentes de puntos de acceso ajenos a la organización no están solapadas.	

8. REDES INALÁMBRICAS: MEJORES PRÁCTICAS PARA LA SEGURIDAD Y AUTENTICACION

Responsable

Responsable	Encargado de la Unidad Informática

8.1. Objeto

- Hacer que los usuarios se autentiquen de una manera segura en el sistema mediante el acceso inalámbrico y no existan agujeros de seguridad en la red.

8.2. Requisitos previos

- Comprobar que los puntos de acceso y los clientes pueden configurar el modo de autenticación que se va a sugerir.

8.3. Procedimiento

WPA2 Personal (AES) es actualmente la forma de seguridad más potente que ofrecen los productos inalámbricos, y es la que se recomienda para todos los usuarios. Cuando se habilite WPA2, se deberá seleccionar una contraseña segura, una que ninguna otra persona pueda adivinar.

Si se utilizan dispositivos Wi-Fi antiguos en la red que no sean compatibles con WPA2 Personal (AES), una buena alternativa es el Modo WPA/WPA2 (a menudo denominado Modo WPA mixto). Este modo permitirá a los dispositivos más modernos utilizar la encriptación WPA2 AES, más potente, mientras que los dispositivos antiguos podrán emplear la encriptación WPA TKIP, también más antigua. Si el punto de acceso inalámbrico no es compatible con el Modo WPA/WPA2, la siguiente mejor opción es el modo WPA Personal (TKIP).

Debido a graves deficiencias de seguridad, los métodos de encriptación WEP y WPA TKIP se consideran obsoletos y se recomienda encarecidamente no utilizarlos. Estos modos solo deberían emplearse si fuera necesario ofrecer soporte para dispositivos inalámbricos antiguos que no sean compatibles con WPA2 AES y no puedan actualizarse para aceptar WPA2 AES. Los dispositivos que utilicen estos métodos de encriptación obsoletos no podrán aprovechar totalmente el rendimiento 802.11n ni otras prestaciones. Debido a estos problemas, la Wi-Fi Alliance ha ordenado a la industria Wi-Fi que retire el WEP y el WPA TKIP.

Igualmente, se recomienda el uso de un servidor radius para la autenticación de usuarios, ya que con este método se unifica y centraliza la gestión de passwords. No obstante, requeriría de hardware adicional y métodos de autenticación distintos.

Verificación de evidencias

Evidencias	Cumplimiento y observaciones
Verificación de que los clientes se autentican con el nuevo método WPA2/AES	

9. SWITCHES Y ROUTERS CISCO: MEJORES PRACTICAS EN CUANTO A LA SEGURIDAD

Responsable

Responsable	Encargado de la Unidad Informática

9.1. Objeto

- Realizar una plantilla de configuración en routers y switches Cisco que no sea vulnerable a ataques y sea segura.

9.2. Requisitos previos

- Realizar un análisis de las necesidades de configuración en base a las recomendaciones de seguridad, ya que no todas ellas son aplicables en cada caso y dependen en gran medida de la aplicación de las comunicaciones.

- De ahora en adelante nos referiremos a switches y routers indistintamente, los procesos son aplicables a ambos salvo que se especifique lo contrario.

9.3. Procedimiento de securización de switches y routers: Passwords

Los switches de Cisco tienen dos niveles de acceso por defecto: User (Nivel 1) y Privileged (Nivel 15). El nivel de usuario es accedido normalmente por conexiones Telnet o SSH o por consola a un switch. El nivel privilegiado se usa después de establecer el nivel de usuario. El nivel "Privileged" puede configurarse con una password de "enable" o con una password "enable secret". Esta última está protegida con más seguridad ya que usa una función en hash MD5. (la otra puede verse en texto plano).

Las contramedidas en este sentido para mitigar vulnerabilidades en las passwords en switches de Cisco son las siguientes:

- Se puede hacer que las password de enable, username password, password de consola y vty figuren encriptadas y no en texto plano con el comando:

  Service password-encryption

- Configurar una password de "enable secret" en cada Switch. No configurar "enable" passwords a menos que se necesiten para generar más niveles de acceso que los que figuran por defecto. Se recomienda igualmente que la password de "enable secret" sea diferente a la del usuario.

  Enable secret xxxxxx

9.4. Procedimiento de securización de switches y routers: Puerto de Management

Los switches(y routers) de Cisco tienen un puerto de Management, la línea de consola (line con 0), que suministra un acceso directo a la administración del switch. Si la configuración del puerto de Management es muy permisiva, es susceptible de ataque.

1.1.1. Vulnerabilidades

Las vulnerabilidades específicas relativas al puerto de Management son las siguientes:

- Un switch con el puerto de consola usando una cuenta de usuario por defecto permite a un atacante intentar realizar conexiones utilizando una o más cuentas bien conocidas (por ejemplo, administrator, root, security,etc)

- Si un switch tiene un puerto de consola sin password, con una password por defecto o con una password débil, entonces un atacante puede adivinarla o romperla mediante ataques de diccionario.

- Si las conexiones a un puerto de consola no tienen un tiempo de "timeout" o tienen un gran periodo de tiempo de expiración, las conexiones estarán más tiempo disponibles a un atacante para obtenerlas.

- Un banner advierte a cualquiera que se conecte al switch de que su acceso está sólo autorizado

1.1.2. Contramedidas

El método más seguro para administra un switch es hacerlo "fuera de banda". Este método no mezcla el tráfico de gestión con el operacional y no consume ancho de banda operacional. La gestión fuera de banda usa sistemas dedicados en exclusiva.

Las siguientes contramedidas mitigan las vulnerabilidades de la línea de consola disponible en cada switch:

- Establecer una única cuenta para cada administrador para acceder a la línea de consola. Los comandos presentados en el ejemplo crean una cuenta con nivel de privilegio y establece un nivel de privilegio por defecto para la línea de consola. El nivel de privilegio 0 es el más bajo en los switches Cisco y permite un número muy bajo de comandos. El administrador puede ir a un nivel más alto (por ejemplo 15) desde el nivel 0 usando el comando enable.

```
Username xxxx privilege 0

Line con 0

Privilege level 0
```

- Usar las recomendaciones generales siguientes para crear una password: tiene que ser como mínimo de 8 caracteres de longitud, no basado en palabras, y que incluya caracteres que no sean letras y números. También Cisco recomienda que el primer carácter de la password no sea un número. Se recomienda cambiar las passwords cada 90 días, y usar una password única de consola para cada switch. No se debería utilizar la misma password de consola para otros servicios (por ejemplo Telnet) en el mismo switch. Los comandos siguientes presentan un ejemplo y establecen una cuenta con password que se encriptará con MD5 y habilita una cuenta local chequeando el login en la línea de consola:

```
Username xxxx secret xxxxx

Line con 0

Login local
```

- El tiempo de timeout de la consola se establecerá en 9 minutos o menos para desconectar las conexiones inactivas en consola. No es recomendable establecer este tiempo a 0 porque en los switches de Cisco se deshabilitará el timeout. Ejemplo:

```
Line con 0

Exec-timeout 9 0
```

- Crear un banner legal para el proceso de login en la línea de consola para cada switch. El siguiente ejemplo muestra cómo hacer esto con el comando "banner motd" usando "$" como carácter delimitador. Este banner aparecerá también en las virtual lines.

```
Banner motd $

**************************

EJEMPLO  DE BANNER

**************************

$
```

9.5. Procedimiento de securización de switches y routers: Servicios de red

Los switches de Cisco pueden tener muchos servicios de red habilitados. Muchos de estos servicios no son necesarios para una operación normal del switch. Aún así, si estos servicios están habilitados en el switch pueden ser susceptibles a obtención de información o ataques de red. Muchos de los servicios usan uno de los siguientes protocolos de transporte de capa 4: TCP (Transmission Control Protocol) o UDP (User Datagram Protocol). Las vulnerabilidades específicas asociadas con los servicios de red son las siguientes:

- Las conexiones a muchos servicios de un switch no están encriptadas, por lo que un atacante puede ser capaz de coleccionar tráfico relativo a estos servicios usando un analizador de red. El tráfico puede obtener nombres de usuario, password, y otra información de configuración relativa al switch.

- Un switch con un servicio establecido sin clave, o con clave por defecto o débil como comentamos anteriormente es susceptible de un ataque

- El acceso externo a un servicio de red en un switch hace que este sea vulnerable a un ataque. Como acceso externo se entiende que un número grande de sistemas puede conectar al switch

- Se recomienda que las conexiones a un servicio de red tengan un tiempo de expiración (timeout, por ejemplo de 9 minutos) para que las conexiones no estén disponibles a un atacante.

1.1.1. Contramedidas

Si es posible, en lugar de usar un servicio de red, por ejemplo el Telnet, para realizar una gestión del switch, utilizar el puerto de consola de cada switch. Esto reduce la exposición de la información de configuración y passwords ya que la gestión es local. Las siguientes contramedidas mitigarán las vulnerabilidades de servicios de red:

- Servicios Innecesarios de Red: Si es posible, es recomendable deshabilitar cada servicio de red no necesario en los switches. En algunos casos, el comando afecta al switch globalmente, mientras que en otros casos el comando afecta sólo a un interfaz del switch. Para aplicar los cambios en varios interfaces, utilizar el comando "range" para especificar los interfaces a configurar:

  Interface range gigabitethernet 6/1 – 3

- TCP y UDP Small Servers (puertos 7,9,13,19): Cisco proporciona soporte para pequeños servidores (por ejemplo: echo, discard, daytime y chargen). Dos de esos servidores, echo y chargen) pueden usarse para ataques de denegación de servicio contra uno o más switches. Estos servicios pueden ser deshabilitados con los siguientes comandos:

  No service tcp-small-servers

  No service udp-small-servers

- Bootp Server (puerto UDP 67):los switches de Cisco pueden actuar como un servidor de bootp para distribuir las imágenes de sistema a otros sistemas de Cisco. A menos que sea un requerimiento operacional, es mejor deshabilitarlo para minimizar el acceso no autorizado a la imagen del sistema:

  No ip bootp Server

- Finger (puerto TCP 79): los switches de cisco soportan el servicio finger que puede suministrar información de los usuarios que están actualmente conectados al switch. El servicio se deshabilita con uno de los siguientes comandos (dependiendo de la versión de IOS)

  No ip finger

  No service finger

- Configuration Autoload: un switch Cisco puede obtener su configuración de un servidor de red mediante varios métodos. Estos métodos no son recomendables porque la información de configuración se pasa en texto plano durante el proceso de arranque y puede ser obtenida por usuarios no autorizados. Usar los siguientes comandos para deshabilitar esto métodos:

  No service config

  No boot host

  No boot network

  No boot system

- Packet Assembler / Disassembler (PAD)

- PAD habilita conexiones X.25 entre los sistemas de red. A menos que la red requiera esta capacidad, debería ser deshabilitada:

  No service pad

- Address Resolution Protocol (ARP): Normalmente los mensajes de ARP están confinados en un único dominio de Broadcast, pero un switch puede enviar mensajes Proxy ARP de un dominio a otro. A menos que se requiera que un switch sea intermediario para peticiones de ARP, esta característica debería estar deshabilitada:

  No ip Proxy-arp

- Mensajes ICMP (Internet Control Message Protocol): un switch Cisco puede generar automáticamente 3 tipos de mensajes ICMP: Host Unreachable, Redirect y Mask Reply. El mensaje Mask Reply suministra la máscara de subred para una red en particular al demandante. Un atacante puede usar estos mensajes para intentar mapear la red. Se recomienda deshabilitar estos mensajes con los siguientes comandos en cada interfaz (incluso el Null 0):

  No ip unreachables

  No ip redirects

  No ip mask-reply

- El interfaz Null 0 merece una particular atención. Este interfaz es un sumidero de paquetes. A veces se utiliza para prevenir ataques de denegación de servicio todos los paquetes bloqueados son entregados en este interfaz. Este generará mensajes de Host Unreachable que podrían inundar la red a menos que esa facilidad esté deshabilitada. Los atacantes pueden también ser capaces de usar estos mensajes para determinar la configuración de listas de acceso identificando los paquetes bloqueados.

  Los broadcast dirigidos permiten mensajes de broadcast iniciados desde distintos dominios de broadcast que están localmente vinculados al switch. Por ejemplo, un atacante que use broadcast dirigidos ICMP para este propósito. Es recomendable que esta capacidad del switch sea deshabilitada, usando el comando siguiente en cada interfaz:

  No ip directed-broadcast

- Servicios de red potencialmente necesarios: Algunos servicios de red pueden ser necesarios para la administración del switch. Si es necesaria la gestión remota o un servicio de red específico, entonces se debería considerar establecer una única cuenta de cada administrador para el acceso a un servicio de red necesario.

- Domain Name Server (DNS): Puertos TCP y UDP 53. Para especificar un servidor DNS para la resolución de nombres, se usa el comando "ip name Server". Este comando se usa para establecer hasta 6 servidores DNS. Para habilitar la traducción de hostname a dirección IP, se utiliza el comando

"ip domain-lookup". Esto permite a peticiones de broadcast de DNS desde el switch ser resueltas por un servidor de DNS.

En algunos casos, el administrador no desea la capacidad de realizar peticiones DNS:

No ip domain-lookup

- SSH Secure Shell (TCP Puerto 22): si es necesario acceder a un switch de manera remota, entonces es mejor considerar utilizar SSH en vez de Telnet. SSH proporciona conexiones encriptadas remotas. Para incluir SSH en el switch, el administrador debe configurar el switch con los siguientes comandos:

Hostname xxxx

Ip domain-name xxxx

Crypto key generate rsa

Una vez ejecutado el último comando se preguntará sobre el número de bits que utilizará la clave.

Para restringir el acceso por SSH al switch, se configuran listas de acceso extendidas (ej: 101) que permitan solo al administrador del sistema hacer esas conexiones y aplicar estas listas de acceso a las virtual terminal lines. Permitir sólo conexiones SSH a esas líneas usando el comando "transport input ssh". Establecer el nivel de privilegio a 0 y el periodo de timeout a 9 minutos (exec-timeout). Finalmente, usar el comando login local para habilitar la comprobación de cuenta local para pedir usuario y password. Ejemplo:

no access-list 101

access-list 101 remark Permit SSH access

access-list 101 permit tcp host 10.1.6.1 any eq 22 log

access-list 101 permit tcp host 10.1.6.2 any eq 22 log

access-list 101 deny ip any any log

line vty 0 4

access-class 101 in

transport input ssh

privilege level 0

exec-timeout 9 0

login local

El comando "login local" no puede usarse con AAA. En lugar de eso se usa el comando "login authentication".

- Servidor Telnet (TCP 23): si el administrador no puede hacer un upgrade a una versión de IOS con SSH, entonces se debe restringir el acceso a Telnet al switch. Configurar una lista extendida (por ejemplo, la 102) que permita a los sistemas de administración hacer conexiones y estar incluidos en esta lista de acceso a los virtual terminal lines. Para permitir conexiones Telnet en estas líneas, se usa el comando "transport input telnet". Como en la ocasión anterior, se recomienda poner el nivel de privilegio a 0, establecer un tiempo de timeout a 9 minutos y usar el comando "login local".

no access-list 102

access-list 102 remark Permit telnet

```
access-list 102 permit tcp host 10.1.6.1 any eq 23 log
access-list 102 permit tcp host 10.1.6.2 any eq 23 log
access-list 102 deny ip any any log
line vty 0 4
  access-class 102 in
  transport input telnet
  privilege level 0
  exec-timeout 9 0
  login local
```

- HTTP Puerto 80 (Hyper Text transfer protocol): en la IOS se incluye un servidor de http para permitir la administración remota del switch a través de un interfaz web. Si no es necesario, deshabilitar el servidor http usando el comando:

```
No ip http Server
```

Si fuera necesario, se recomienda utilizar una lista de acceso estándar que permita sólo a los sistemas de administración el acceso. Finalmente, utilizar "ip http authentication local" para habilitar la comprobación de la cuenta en local.

```
no access-list 11
access-list 11 remark Permit HTTP
access-list 11 permit host 10.1.6.1 log
access-list 11 permit host 10.1.6.2 log
access-list 11 deny any log
ip http server
ip http access-class 11
ip http authentication local
```

- SNMP Simple Network Management Protocol (puertos UDP 161 y 162): SNMP es un servicio que se usa para establecer funciones de gestión usando una estructura de datos llamada Management Information Base (MIB). Desgraciadamente, SNMP Version 1 está ampliamente implementada pero no es muy segura, ya que usa solo comunidades en texto plano para acceder a la información del switch, incluyendo su fichero de configuración.

Si no se usa SNMP, los siguientes comandos deshabilitarán el servicio:

```
no snmp-server community
no snmp-server enable traps
no snmp-server system-shutdown
no snmp-server
```

Si se requiere SNMP en el switch, entonces es mejor utilizar SNMP versión 3. Esta versión es más segura que la versión 1 porque usa hash criptográfico para autenticación que protege el string de la comunidad. Se recomienda utilizar los comandos anteriores para deshabilitar SNMP antes de configurar la versión 3 de SNMP para eliminar cualquier posible comunidad por defecto.

Los siguientes comandos muestran un ejemplo de SNMP versión 3 para el switch. El modelo empieza creando unas listas de acceso estándar (ejemplo:12) que permiten sólo a esos sistemas permitidos acceder al switch. Después, define un grupo (admins) que tiene lectura y escritura de la MIBs (adminview). Entonces se añade cada usuario (ej root) al grupo con una password que puede ser encriptada (md5) antes de ser enviada a la red. También la lista de acceso estándar se aplica a los usuarios. Finalmente, la vista de la MIB en los ejemplos siguientes da acceso desde el exterior a la MIB excepto los ítems que muestran la dirección IP y la información de routing:

```
no access-list 12

access-list 12 permit 10.1.6.1

access-list 12 permit 10.1.6.2

snmp-server group admins v3 auth read adminview write    adminview

snmp-server user root admins v3 auth md5 5ecret-5TR1N access 12

snmp-server view adminview internet included

snmp-server view adminview ipAddrEntry excluded


snmp-server view adminview ipRouteEntry excluded
```

Si se requiere SNMP en un switch y sólo se permite la versión 1, los siguientes comandos del ejemplo muestran cómo configurar el switch con un string de comunidad que tiene sólo permisos de lectura y lista de acceso estándar:

```
no access-list 12

access-list 12 permit 10.1.6.1

access-list 12 permit 10.1.6.2

snmp-server community g00d-5tr1n9 ro 12
```

Además de configurar el servicio de SNMP, la información de Trap de SNMP puede enviarse a los sistemas que gestionan los switches. Los siguientes comandos muestran la configuración:

```
snmp-server host 10.1.6.1 traps g00d-5tr1n9-2

snmp-server host 10.1.6.2 traps g00d-5tr1n9-2

snmp-server trap-source Loopback0

snmp-server enable traps
```

- CDP (Cisco Discovery Protocol): CDP proporciona una capacidad de compartir información de sistema entre los routers de Cisco, switches y otros productos. Alguna de esta información incluye el nombre de dominio de VLAN Trunking Protocol (VTP), VLAN Nativa y duplex. Si esta información no se requiere para necesidades operacionales, entonces debería deshabilitarse globalmente y para cada interfaz. Para deshabilitar CDP globalmente en un switch, usar el comando "no cdp run". Para deshabilitar CDP en un interfaz en un switch, usar el comando "no cdp enable".

```
no cdp run

no cdp advertise-v2

interface range fastethernet 0/1 - 24

no cdp enable
```

Si es necesario usar CDP, necesita ser habilitado globalmente y sólo en los interfaces donde es necesario. El siguiente ejemplo suministra un ejemplo de deshabilitación / habilitación de CDP en un interfaz:

```
cdp run
interface VLAN10
  no cdp enable
interface VLAN101
  cdp enable
```

Nota: una red de voz puede necesitar CDP para tener un rendimiento adecuado, dependiendo del diseño de la red de voz y de la política de seguridad. Si los teléfonos IP son desplegados usando Auto Discovery o DHCP, entonces se necesita CDP habilitado globalmente y deshabilitado en todos los puertos no conectados a un teléfono IP. No obstante, estos servicios proporcionan avenidas para la obtención de información ataques. Las opciones de Auto Discovery y DHCP no están recomendadas para implementaciones de Voz sobre IP seguras.

9.6. Procedimiento de securización de switches y routers Seguridad de puertos

1.1.1. Vulnerabilidades

Los interfaces de nivel 2 en un switch Cisco son denominados como puertos. Un switch que no proporciona seguridad de puerto permite a un atacante conectar un sistema a un puerto no usado y habilitado, y recopilar información o realizar ataques. Un switch puede ser configurado como un hub, lo que significa que cada sistema conectado al switch puede potencialmente ver todo el tráfico de red pasando por el switch a todos los sistemas conectados al switch. Por tanto, un atacante podría recopilar tráfico que contenga nombres de usuario, claves o información de configuración de los sistemas de la red.

1.1.2. Contramedidas

La seguridad de puerto limita el número de MACs válidas permitidas en un puerto. Todos los puertos del switch o interfaces deberían estar securizados antes que el switch sea puesto en producción. En este sentido las características de seguridad son establecidas o quitadas según requerimientos en lugar de añadir y reforzar al azar como resultado de un incidente de seguridad. Notar que la seguridad de los puertos no puede ser usada para puertos de acceso dinámico o puertos destino para un analizador de puerto. Aún así, utilizar seguridad de puerto para puertos activos en el switch cuanto sea posible.

Los siguientes ejemplos muestran los comandos para apagar un puerto o un rango de ellos:

```
interface fastethernet 0/1
      shutdown
interface range fastethernet 0/2 - 8
   shutdown
```

Las capacidades de seguridad en puerto pueden variar dependiendo en el modelo del switch y de la IOS. Cada puerto activo puede ser restringido por un máximo de direcciones MAC con una acción seleccionada para cualquier violación de la restricción. Estas acciones pueden ser tirar el paquete (violation Protect), tirar el paquete y enviar un mensaje (violation restrict or action trap) o apagar el puerto (violation shutdown o action shutdown). Shutdown es la opción por defecto y es la más segura. Las opciones Protect y Restrict ambas requieren hacer un track de direcciones MAC, por lo que consumen más recursos de CPU del switch.

Las direcciones MAC son adquiridas dinámicamente, con algunos switches que soportan entradas estáticas y entradas sticky. Las entradas estáticas son manualmente introducidas para cada puerto y salvadas en la configuración (switchport port-security mac-address mac-adress). Las entradas Sticky son similares a las entradas estáticas excepto por que son aprendidas dinámicamente (switchport port-security mac-adress sticky). Estas entradas dinámicas son salvadas en la running configuration, y si esta es salvada a la startup configuration, las direcciones MAC no necesitan ser reaprendidas en un restart del switch.

También, se puede establecer el número máximo de direcciones MAC en un puerto (switchport port-security maximum value)

El administrador puede habilitar la expiración de las entradas estáticas de MAC configuradas en un puerto (switchport port-security aging static). También, la expiración puede ser establecida por inactividad (switchport port-security aging type inactivity)

Un ejemplo de restricción de un puerto estáticamente:

switchport port-security
switchport port-security violation shutdown
switchport port-security maximum 1
switchport port-security mac-address 0000.0200.0088
switchport port-security aging time 10
switchport port-security aging type inactivity

Para restringir un Puerto dinámicamente, se usan los siguientes comandos:

switchport port-security
switchport port-security violation shutdown
switchport port-security maximum 1
switchport port-security mac-address sticky

Si una violación de seguridad ocurre, el Puerto inmediatamente se pone en error-disabled y su LED se apagará. El switch enviará un trap de SNMP, y mensajes de log y syslog e incrementa el contador de violación. Cuando un puerto está en estado de error-disabled, el administrador puede recuperarlo de ese estado usando el comando "errdisable recovery cause psecure-violation" o haciendo un "shutdown" y "no shutdown" en el puerto.

9.7. Procedimiento de securización de switches y routers Disponibilidad del sistema

1.1.1. Vulnerabilidades

Existen muchos ataques que pueden causar Denegación de Servicio, parcialmente o completamente, a sistemas o redes. Los switches son susceptibles a estos ataques. Los ataques DoS se centran en hacer que los recursos no estén disponibles (procesador, ancho de banda, etc). Las vulnerabilidades específicas con las siguientes:

- Algunos ataques de Fast Flooding pueden causar que el procesador del switch no esté disponible para acceso de gestión.

- El control de flujo 802.3X permite a los puertos que reciben pausar la transmisión de paquetes desde el transmisor durante periodos de congestión. Si esta característica está habilitada, se puede recibir una pausa, parando la transmisión de paquetes de datos. Las tramas de control de flujo podrían usarse en un ataque de denegación de servicio.

- Algunos ataques activos y ciertos errores pueden causar una inundación de paquetes en los puertos de un switch.

- Switches conectados directamente corriendo el protocolo UDLD (Unidirectional Link Detection) pueden determinar si existe un enlace unidireccional entre ellos. Los mensajes UDLD pueden ser usados en un ataque de denegación de servicio.

- El ataque SYN Flood envía petición de conexiones repetidas sin enviar la aceptación (ACK) a la petición de conexión. Este ataque puede sobrecargar el buffer del switch de conexiones incompletas llegando a deshabilitarlo.

- Las redes convergentes envían tanto datos como voz. Si no están configuradas correctamente, estas redes pueden permitir que el tráfico de voz se convierta en un ataque de inundación contra el tráfico de datos.

1.1.2. Contramedidas

Las siguientes contramedidas mitigarán las vulnerabilidades de disponibilidad del sistema en cada switch.

- Para prevenir los ataques de inundación (Fast flooding) y garantizar que tanto los procesos de más baja prioridad pueden tener tiempo de proceso usar el comando "Scheduler interval". El siguiente ejemplo establece un tiempo máximo antes de correr los procesos menos prioritarios a 500ms:

  scheduler interval 500

  Otra manera de garantizar tiempo de procesador para procesos es usar el comando "scheduler allocate". Este comando establece el tiempo de interrupción y el tiempo de proceso. El tiempo de interrupción es el número máximo de microsegundos para gastar en Fast switching en un contexto de cualquier interrupción de red. El tiempo de proceso es el número mínimo de microsegundos para gastar a nivel de proceso cuando las interrupciones de red están deshabilitadas. El siguiente ejemplo hace el 10 por ciento del procesador disponible para tareas de proceso, con un tiempo interrupción de 4000 microsegundos y tiempo de proceso de 400 microsegundos:

  scheduler allocate 4000 400

  Para deshabilitar el control de flujo en cada interfaz se utiliza el siguiente comando:

  flowcontrol receive off

  Para deshabilitar UDLD en cada interfaz, existen dos comandos que dependen del modelo de switch y la versión de IOS.

  no udld port

  udld disabled

  Para prevenir ataques de SYN Flood el administrador puede establecer la cantidad de tiempo que el switch puede esperar intentando establecer una conexión TCP. El siguiente comando establece una espera de 10 segundos:

  ip tcp synwait-time 10

  Para establecer que el tráfico de Voz tenga más prioridad sobre la red, debe ser sencillo determinar cuáles son los paquetes de voz, incluso si la señalización de voz y datos están encriptadas. Este riesgo adicional debe ser considerado para decidir si los parámetros de QoS (Calidad de Servicio) se configurarán para tráfico de voz. La clasificación de los paquetes es el primer paso en establecer su prioridad a través de la red y debería ser realizado en el primer punto disponible. Algunos switches pueden clasificar paquetes con propósito de QoS. Los siguientes ejemplos muestran lo que se puede hacer en un switch capaz de implementar QoS:

  El siguiente comando activa las características de QoS

  mls qos

El siguiente comando fuerza la prioridad "best effort" para un sistema no confiable:

mls qos cos 0

mls qos cos override

El siguiente commando aceptará la prioridad asignada por un sistema confiable (ej voice Gateway)

El siguiente comando aceptará la prioridad asignada por un teléfono IP pero forzará la prioridad best effort para cualquier PC conectado al Teléfono):

mls qos trust dscp

mls qos trust device cisco-phone

switchport priority extend cos 0

- Aislar el tráfico de voz en subredes separadas usando VLANs y controlar la interacción entre voz y datos. Será necesaria la aplicación de listas de acceso.

9.8. Procedimiento de securización de switches: VLANs

1.1.1. Introducción

Una VLAN (Virtual Local Area Network) es un dominio de broadcast. Todos los miembros de una VLAN reciben paquetes de broadcast enviados por los miembros de la misma VLAN, pero no reciben paquetes enviados por miembros de VLANs diferentes. Todos los miembros de una VLAN están lógicamente agrupados en un mismo dominio de broadcast independientemente de su localización física. Añadir, mover o cambiar los miembros se consigue vía software en un switch. Se requiere routing para la comunicación entre miembros de distintas VLANs.

Las siguientes subsecciones describen las vulnerabilidades y correspondientes contramedidas para las áreas siguientes: VLAN 1, VLAN Privada, VTP, Autonegociación de Trunk, VLAN Hopping y asignación dinámica de VLAN.

1.1.2. VLAN 1

1.1.2.1. Vulnerabilidades

Los switches de Cisco usan la vlan 1 como VLAN por defecto para asignar sus puertos, incluyendo sus puertos de gestión. Además, los protocolos de nivel 2 como CDP y VTP necesitan enviarse por una VLAN específica en enlaces trunk, por lo que se elige la VLAN 1. En algunos casos, la VLAN 1 puede abarcar toda la red si no es convenientemente cortada. También da a los atacantes a un acceso más fácil y alcance extendido para sus ataques

1.1.2.2. Contramedidas

No usar la VLAN 1 tanto para accesos locales como para exteriores. Dedicar un puerto físico del switch y VLAN en cada switch para Gestión. Crear un interfaz virtual de switch (SVI) o interfaz de nivel 3 para esa VLAN y conectarla a un switch dedicado con un camino hacia los host de gestión. No se debe permitir a las VLANs operacionales acceder a la VLAN de gestión. También, no introducir la VLAN de gestión en el switch.

Para obtener una gestión externa que separe el tráfico de usuario del propio de gestión, usar los siguientes comandos:

Crear la VLAN de gestión fuera de banda:

```
Vlan 6
Name Administration-VLAN
```

Crear una dirección IP de gestión y restringir el acceso a ella. También habilitar el interfaz:

```
no access-list 10
access-list 10 permit 10.1.6.1
access-list 10 permit 10.1.6.2
interface vlan 6
description ADMIN-VLAN
ip address 10.1.6.121 255.255.255.0
ip access-group 10 in
no shutdown
```

Asignar la VLAN de gestión a un interfaz dedicado:

```
interface fastethernet 4/1
description Out-Of-Band Admin
switchport mode access
switchport access vlan 6
no shutdown
```

Asegurar que los puertos de trunk no llevan la VLAN de Gestión:

```
interface range gigabitethernet 6/15 – 16
switchport trunk allowed vlan remove 6
```

Asignar los interfaces no usados a otra VLAN distinta a la VLAN 1:

```
vlan 999
name *** BIT BUCKET for unused ports ***
shutdown
exit
interface range fastethernet 5/45 - 48
switchport mode access
switchport access vlan 999
shutdown
```

1.1.3. VLANs Privadas

1.1.3.1. Vulnerabilidades

En ciertas circunstancias donde sistemas similares no necesitan interactuar directamente, PVLANs suministran protección adicional. Una PVLAN primaria define un dominio de broadcast en el cual se asocian PVLANs secundarias. Las PVLANs secundarias pueden ser PVLANs aisladas o comunitarias. Los host de las PVLANs aisladas pueden comunicar sólo con puertos promiscuos, y hosts en PVLANs comunitarias pueden comunicar sólo entre ellos y con los puertos promiscuos asociados. La configuración suministra un preciso de aislamiento para cada sistema.

Un uso adecuado de las PVLANs protege a los sistemas de que otros pueden compartir un segmento de VLAN común implementando la separación a nivel 2. Esta configuración se encuentra comúnmente en esquemas con múltiples servidores, en zonas como la subred DMZ (De-Militarized Zone) fuera de un firewall. Si un servidor está comprometido, entonces el servidor puede ser la fuente de un ataque en otros servidores a su vez. PVLANs mitigan el riesgo deshabilitando la comunicación entres servidores que no deberían contactarse entre ellos.

Las PVLANs tienen una limitación: deben ser direccionadas por un sistema para ser seguras. Un router puede retornar tráfico, en la misma subred donde fue originado. Una PVLAN sólo aísla tráfico de nivel 2. Un router el cual es un sistema de Nivel 3 y es vinculado a un puerto promiscuo, podría encaminar tráfico para todos los puertos en la PVLAN. Dos hosts en una PVLAN aislada fallarán para comunicar a nivel 2 pero pueden tener éxito a nivel 3, lo que evita la protección de nivel 2.

1.1.3.2. Contramedidas

Una configuración con múltiples servidores en una sola VLAN debería usar PVLANs para la separación a nivel 2 entre servidores. Los routers deberían tener puertos y servidores promiscuos en una PVLAN aislada. Sólo los servidores que necesiten comunicar directamente con otros servidores deberían estar en una PVLAN comunitaria.

Es recomendable implementar VACLs en la PVLAN para filtrar el tráfico originado por y encaminado el mismo segmento.

En ciertas circunstancias donde sistemas similares no necesitan interactuar directamente, las PVLANs mitigan los ataques. En las redes de voz esto puede ser el caso de que ciertos proxys sirviendo al mismo juego de usuarios pero usando diferentes protocolos.

En el siguiente ejemplo, se crea una PVLAN con un servidor NTP en un puerto promiscuo y dos servidores aislados:

```
vlan 200
        name SERVERS-PRIVATE
        private-vlan primary
        private-vlan association 201

vlan 201
        name SERVERS-ISOLATED
        private-vlan isolated

interface GigabitEthernet6/1
        description SERVER 1
        switchport private-vlan host-association 200 201
        switchport mode private-vlan host
```

```
        no shutdown

interface GigabitEthernet6/2
        description SERVER 2
        switchport private-vlan host-association 200 201
        switchport mode private-vlan host
        no shutdown

interface GigabitEthernet6/6
        description SERVER NTP Server
        switchport mode private-vlan promiscuous
        switchport private-vlan mapping 200 201
        no shutdown
```

1.1.4. VTP

1.1.4.1. Vulnerabilidades

VTP es un protocolo de nivel 2 propietario de Cisco que se usa para distribuir la configuración de VLANs por trunks. VTP permite añadir, borrar y cambiar el nombre de las VLANs en una red, lo que permite a los switches tener una configuración consistente en un dominio de gestión de VTP.

Todos los switches en el mismo dominio de gestión comparten su información de VLAN y un switch puede participar sólo en un dominio VTP.

Un switch puede estar en uno de los tres siguientes modos VTP: servidor, transparente y cliente. Un switch en modo servidor origina configuraciones de VTP para que los otros switches lo usen. En el modo servidor los administradores pueden crear, modificar, y borrar VLANs de todo el dominio VTP. Los servidores de VTP anuncian su configuración de VLANs a otros switches en el mismo dominio de VTP y sincronizan sus bases de datos. Un switch en modo transparente recibe y retransmite paquetes VTP, pero no los crea ni usa los que recibe para modificar su base de datos de VLAN. Un switch en modo cliente recibe, usa y pasa paquetes VTP pero no los origina. Un switch puede funcionar en modo VTP pruning, en el cual se abstiene de retransmitir paquetes VTP en los puertos elegidos.

Por defecto, los switches comparten información de VLAN sin ninguna autenticación. Así, las configuraciones de VLAN no precisas pueden propagarse en un dominio VTP. Por este motivo, los switches por defecto están configurados como servidor de VTP. Es posible que para un solo switch, que haya efectuado el número suficiente de reconfiguraciones VTP, haga una sobreescritura o eliminación de todas las asignaciones de VLAN de una red operacional tan sólo conectándola a la red. Tal ataque no tendría que ser necesariamente malicioso, simplemente moviendo un switch de laboratorio a un entorno operacional podría tener este efecto.

Por defecto, la gestión de dominios VTP están configurados en un modo inseguro sin password. Es posible mitigar el daño de sobreescritura accidental con la protección de password. Un cliente chequea la password antes de implementar la configuración de VLAN que recibe vía VTP. La password, no obstante, no encripta la información de VTP. VTP configurado con password sólo asegura la autenticidad del mensaje. Un atacante con un analizador de red puede fácilmente ganar conocimiento de la estructura de la red local. A pesar de esto, la password está codificada con otra información, y es difícil determinar la password de otra información recopilada en la red.

1.1.4.2. Contramedidas

Está claro que VTP simplifica la administración, particularmente con un número largo de VLANs desplegados. Aun así, VTP es lo suficientemente peligroso para que su uso pueda ser descartado. Si es posible, apagar VTP usando el siguiente comando:

no vtp mode
no vtp password

no vtp pruning

Si VTP es necesario, entonces considerar la siguiente configuración. Establecer dominios de gestión de VTP adecuadamente. Todos los switches en el mismo dominio de gestión comparten la misma información de VLAN. Un switch únicamente puede participar en un dominio de gestión de VTP. Usar el comando siguiente para establecer el dominio VTP:

vtp domain test.lab

Asignar una password fuerte de VTP al dominio de VTP. Ejemplo:

vtp password g00d-P5WD

Habilitar VTP pruning y usarlo en los puertos apropiados. Por defecto, las VLANs numeradas del 2 a la 1000 son elegibles:

vtp pruning

Asignar VTP a modo transparente con el siguiente comando:

vtp transparent

1.1.5. Auto negociación de Trunk

1.1.5.1. Vulnerabilidades

Un puerto de trunk es un enlace punto a punto entre dos puertos, típicamente en distintos sistemas de red, y agrega paquetes desde múltiples VLANs. Cisco implementa dos tipos de trunks: 802.1q (estándar abierto) e ISL (propietario de Cisco).

Un puerto puede usar el protocolo DTP (Dynamic Trunking Protocol) para negociar automáticamente qué protocolo de trunk puede usar, y cómo operará el protocolo de trunk. Por defecto, los puertos Ethernet de Cisco tienen como configuración "dynamic desirable", lo que permite al puerto activamente intentar convertir el enlace en un trunk. Aún peor, las VLANs que componen un trunk son todas las disponibles en un switch. Si el modo DTP un puerto de un switch vecino está en "trunk", "dynamic auto" o "dynamic desirable", y si dos switches soportan un protocolo común de trunk, entonces la línea se convertirá automáticamente en un trunk, dando a ambos un acceso total a todas las VLANs en el switch vecino.

Un atacante que pueda explotar DTP puede tener acceso a información útil de estas VLANs.

1.1.5.2. Contramedidas

No usar DTP si es posible. Asignar puertos de trunk a VLANs nativas distintas de la VLAN 1:

```
interface fastethernet 0/1
  switchport mode trunk
  switchport trunk native vlan 998
```

Poner interfaces de no trunk en modo no trunking permanente sin negociación:

```
interface fastethernet 0/1
   switchport mode access
   switchport nonegotiate
```

Poner los interfaces de trunk en modo trunk permanente, sin negociación:

```
interface fastethernet 0/1
  switchport mode trunk
  switchport nonegotiate
```

Específicamente listar todas las vlans que forman parte del trunk:

```
interface fastethernet 0/1
   switchport trunk allowed vlan 6, 10, 20, 101
```

Usar una única VLAN native para cada trunk en un switch:

```
interface fastethernet 0/1
  switchport trunk native vlan 998
interface fastethernet 0/2
  switchport trunk native vlan 997
```

1.1.6. VLAN Hoping

1.1.6.1. Vulnerabilidades

En ciertas situaciones, es posible enviar un paquete de cierta manera que un Puerto en modo de trunk es capaz de interpretar un paquete de la VLAN nativa como si fuera de otra VLAN, permitiendo al paquete ser miembro de esa VLAN. Esta técnica se llama VLAN Hopping. Usando esta técnica un intruso malicioso puede ganar acceso a una red local y podría inyectar paquetes en otra red local en la red para atacar máquinas en la red destino.

1.1.6.2. Contramedidas

Deshabilitar CDP, VTP y DTP en cada switch si es posible. Asignar una VLAN en shutdown como VLAN nativa de cada trunk, y no usar estas VLANs para ningún propósito.

```
interface fastethernet 0/1

switchport trunk native vlan 998

no cdp enable
```

Restringir las VLANS en un trunk a sólo las que son necesarias (como ha sido descrito anteriormente).

1.1.7. Listas de acceso (ACLs)

1.1.7.1. Vulnerabilidades

Un switch sin listas de acceso permite accesos exteriores para conexiones TCP/IP, al switch para cualquier sistema (por ejemplo, un servidor crítico) en una red protegida. Esta situación resulta en una mayor probabilidad de ataques.

1.1.7.2. Contramedidas

En la preparación de implementación de listas de acceso, categorizar sistemas vinculados a los switches en grupos que usan los mismos servicios de red. Agrupando los sistemas de esta manera ayuda a reducir el tamaño y complejidad de las ACLs asociadas. En redes de voz, usar VLANs separadas para Callmanagers, teléfonos SCCP, SIP, Proxys, Gateways MGCP y H323 es un buen ejemplo de ello. Considerar también los

servicios de red utilizados por sistemas similares de distintos fabricantes para mejorar la precisión de las ACLs puede tener sentido como política de seguridad de red.

Las listas de acceso pueden permitir o denegar cada paquete basado en la primera entrada de control de acceso en la que el paquete hace match.

ANÓTESE Y COMUNÍQUESE.

PATRICIO LOPEZ BERRIOS
INTENDENTE (S)
GOBIERNO REGIONAL DE ARICA Y PARINACOTA

MPS/jmg
DISTRIBUCION:
1. DAF
2. Unidad de Informática
3. Depto. Jurídico.
4. Oficina de Partes