ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"DISEÑO E IMPLEMENTACIÓN DE UNA TOPOLOGÍA DE RED DE DATOS CON ESQUEMA DE SEGURIDAD PERIMETRAL Y ACCESO A INTERNET DE ALTA DISPONIBILIDAD"

EXAMEN DE GRADO (COMPLEXIVO)

Previo a la obtención del título de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

SONIA ELIZABETH ÁLVAREZ BECERRA

GUAYAQUIL- ECUADOR

AÑO 2015

AGRADECIMIENTO

A Dios por darme la oportunidad de ejercer mi profesión y a mi familia por su apoyo incondicional.

DEDICATORIA

A mi esposo por su amor y su apoyo constante.

TRIBUNAL DE SUSTENTACIÓN

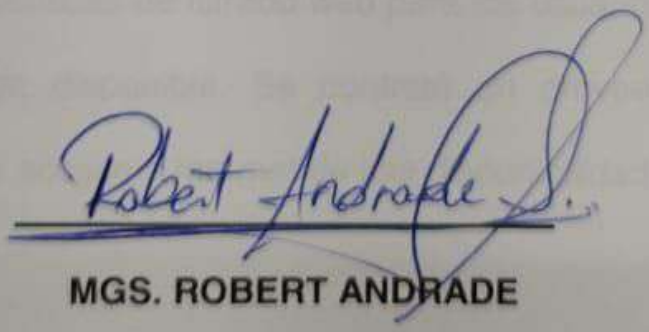
ING. LENIN FREIRE

DIRECTOR MSIA

MGS. NÉSTOR ARREAGA

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA



MGS. ROBERT ANDRADE

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

RESUMEN

Este trabajo tiene como fin diseñar una topología de red con la seguridad básica necesaria para el funcionamiento de una empresa mediana.

Se realizó la instalación de un UTM comercial de marca Fortinet como plataforma de seguridad perimetral. Se segmentó las redes para poder tener un mejor control de los accesos a cada una de ellas creando una red LAN, una red DMZ de FRONTEND y una red de BACKEND

Se configuraron las políticas de filtrado web para los usuarios optimizando el uso ancho de banda disponible. Se contrató un proveedor de Internet adicional para brindar acceso a Internet de alta disponibilidad en la matriz.

Se configuró una red VPN para el acceso seguro desde el exterior de los administradores de red.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

DLP	Data Leak Prevention (Prevención de fuga de datos)
DMZ	Demilitarized zone (Zona desmilitarizada)
ECMP	Equal-costmulti-path
FortiOS	Sistema operativo de Fortinet
IPS	Sistema de prevención de intrusos
ISP	Internet Service Provider (Proveedor de servicios de Internet)
LAN	Local Area Network (Red de Área Local)
Mbps	Megabits por segundo
UTM	Unified Threat Management (Gestión Unificada de Amenazas)
VPN	Virtual Private Network (Red privada virtual)

ÍNDICE DE FIGURAS

INTRODUCCIÓN

El crecimiento acelerado y la necesidad de contar con servicios de comunicación eficientes han hecho que las empresas adquieran soluciones de tecnología para atender problemas específicos que muchas veces dejan brechas de seguridad de las cuales el proveedor de la solución no es consciente.

Es imprescindible que las empresas cuenten con un esquema de seguridad perimetral básico para poder crecer de forma ordenada y considerando los riesgos de seguridad informática.

El presente documento muestra la implementación de una topología de red segura para una empresa mediana, la implementación no se ha realizado en su totalidad por la complejidad de las diferentes aplicaciones usadas, sin embargo, es posible ir migrando poco a poco los diferentes servicios a cada una de las redes implementadas y cada vez que se vaya a instalar un nuevo

equipo o servicio éste deberá ser instalado considerando las nuevas políticas de seguridad de red establecidas.

CAPÍTULO 1

GENERALIDADES

1.1 DESCRIPCIÓN DEL PROBLEMA

La corporación perteneciente al sector bananero tiene como actividad principal la exportación de banano, su matriz está ubicada en la ciudad de Machala y dispone de oficinas en El Guabo, Puerto Bolívar, Machala, Naranjal y Guayaquil.

El acceso a Internet en la matriz es de vital importancia para las operaciones de la empresa exportadora, sin embargo la calidad del servicio de Internet no es la esperada debido a que el sistema usado para optimizar el consumo de Internet no permite controlar el uso de aplicaciones con un alto consumo de ancho de banda, además se requiere que el administrador se encuentre actualizando

permanentemente la lista de páginas bloqueadas y permitidas en el sistema.

La empresa ha ido creciendo considerablemente en los últimos años, debido a las exigencias del mercado. La necesidad de cumplir con los requerimientos legales y tributarios ha hecho que su parque tecnológico haya crecido a la par de las necesidades sin que se haya considerado la seguridad de la información que circula a través de la red. La importancia de la confiabilidad y la disponibilidad inmediata de la información para el funcionamiento del negocio hizo que se requiera un rediseño de la topología de la red con un esquema de seguridad que sea la base para el crecimiento tecnológico posterior.

1.2 SOLUCIÓN PROPUESTA

Se realizará el reemplazo el actual servidor proxy por una solución comercial, un equipo UTM que permite el filtrado web de forma eficiente así como la restricción del uso de aplicaciones no deseadas y la limitación del consumo del ancho de banda, esto le permitirá a los administradores de red hacer los cambios necesarios de forma inmediata, llevando un registro de los cambios de configuración realizados por cada usuario administrador.

Se contratará otro proveedor de Internet balanceando la carga mientras ambos entreguen el servicio y brindando alta disponibilidad en caso de que un proveedor no brinde conexión a Internet.

Se diseñará la topología de red segmentando en tres redes:

- Una red para los servidores de FRONTEND expuestos al exterior.
- Un segmento para los servidores de los cuales la DMZ consume información y que son los que manejan la información crítica de la empresa.
- Un segmento para la red LAN que contiene a todas las estaciones de trabajo y servidores que solo son accedidos desde la red interna.

Se implementará un servidor VPN en el UTM para permitir el acceso de los sitios más remotos como Naranjal y Guayaquil de forma segura, así como para permitir el acceso a la administración de los dispositivos de forma remota evitando dejar abiertos los puertos de administración de servidores hacia el exterior.

CAPÍTULO 2

DESARROLLO DE LA SOLUCIÓN

2.1 ANÁLISIS DE SITUACIÓN ACTUAL

La topología de red actual es muy simple, se cuenta con un servidor proxy con dos tarjetas de red a través del cual pasa todo el tráfico desde y hacia Internet. Este proxy hace las veces de firewall y es a su vez un servidor de correo.

Se cuenta con un servidor de aplicaciones móviles, un servidor web para facturación electrónica y servidores de base de datos todos instalados en el mismo segmento de red que los usuarios.

La red se conecta a Internet a través del servicios proporcionado por Telconet con un ancho de banda de 5 Mbps el cual es administrado por el servidor proxy, sin embargo, el ancho de banda no es suficiente

porque los usuarios pueden usar libremente aplicaciones que tienen un alto consumo de ancho de banda. No existe un control para evitar que los usuarios puedan acceder desde sus hogares a sus computadores del trabajo usando cualquier software de gestión remota. Además no existen restricciones para el departamento de Sistemas, permitiendo que alguno de los usuarios de este grupo pueda saturar el ancho de banda si lo desea.

La administración de este servidor es complicada, las políticas de firewall y de navegación no se cambian por temor a que se pueda causar una caída del servicio.

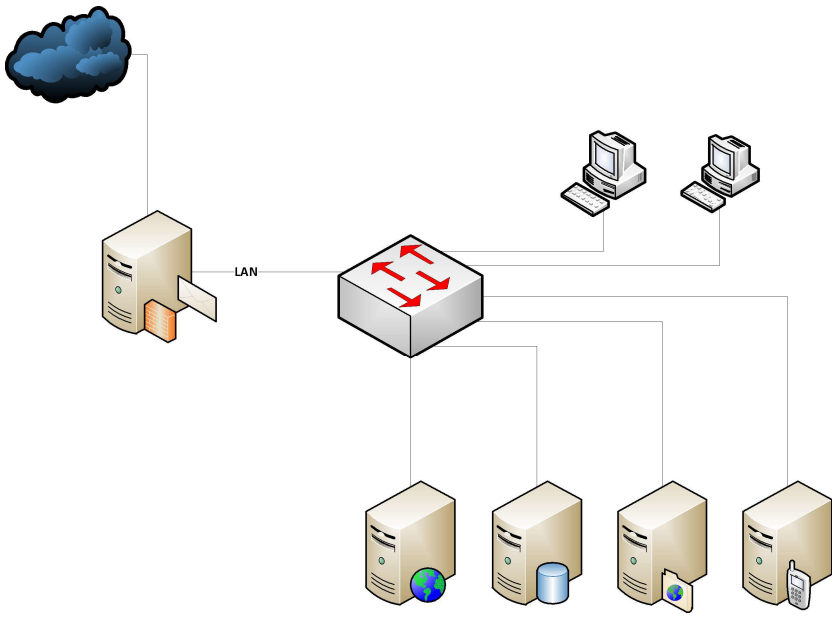


Figura 2.1 Topología de red actual

La empresa cuenta con dispositivos grabadores de video, los cuales tienen una dirección IP pública asociada para poder visualizar desde exterior las cámaras de forma ocasional, asimismo se tiene abiertos los puertos de administración del servidor de correo y web desde el exterior en caso de requerir la asistencia de un proveedor o de requerir la gestión remota por parte del personal del sistemas.

Se han dado problemas de caída del servicio de Internet en varias ocasiones por problemas administrativos con el proveedor y en alguna ocasión un problema técnico tardó más de tres horas en resolverse, sin embargo es muy importante para las operaciones de la compañía exportadora disponer de conexión a Internet permanente debido a la importancia de las operaciones en línea realizadas en el exterior.

La empresa cuenta con 80 usuarios en la matriz, 20 usuarios en la sucursal principal en El Guabo, 1 usuario en la ciudad de Arenillas, 1 usuario en Guayaquil y 18 usuarios distribuidos en cada una de las haciendas.

2.2 PLATAFORMA DE SEGURIDAD

Se eligió una solución de seguridad unificada comercial de la empresa Fortinet, que permite la segmentación de la red y contiene las funcionalidades de Firewall, Antivirus, Antispam, Filtrado Web, IP SEC/SSL VPN, IPS y DLP.

El equipo elegido es un Fortigate 200B, el cual reemplazará a servidor proxy utilizado actualmente, este equipo posee 16 interfaces de red y permite configurar las políticas de comunicación entre cada una de las interfaces aplicando en cada política controles de antivirus, filtrado web, antispam, IPS y DLP en caso ser necesario.

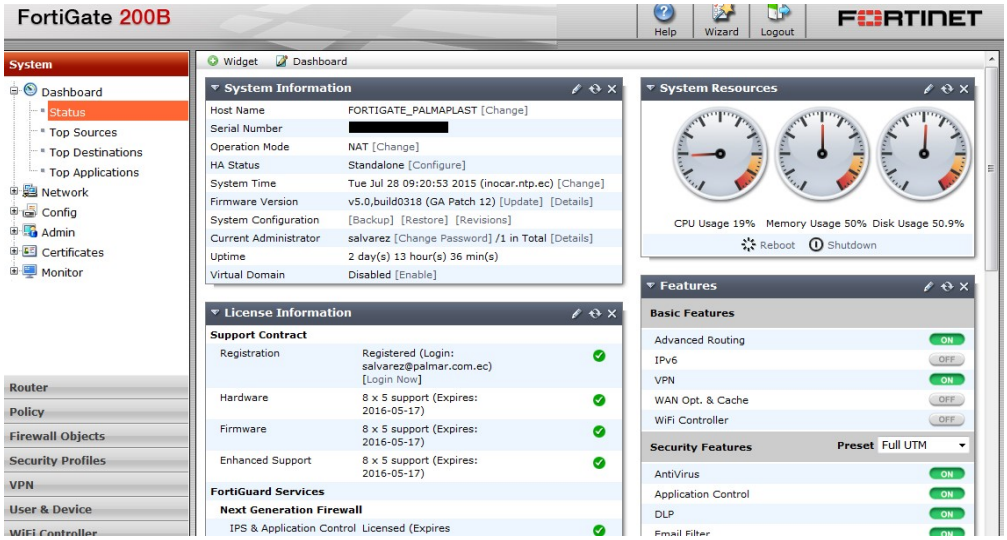


Figura 2.2 Panel del control Fortigate

Se realizaron las siguientes configuraciones básicas de seguridad recomendadas por Fortinet para la fortificación del dispositivo [1]:

- Actualización de versión de firmware a la recomendada por el fabricante.
- Creación de cuentas de administrador adicionales con acceso permitido solo desde la red local y VPN.

Name	Trusted Hosts	Profile	Type
admin	128.128.0.0/16	super_admin	Local
operador	128.128.0.0/16	Mantenimiento	Local
ppalacios	10.212.134.192/28, 128.128.0.0/16	super_admin	Local
salvarez	10.212.134.192/28, 128.128.0.0/16	super_admin	Local

Figura 2.3 Lista de usuarios administradores

- Bloqueo de los puertos de administración desde el exterior
- Cambio de puertos de administración
- Cambio de tiempo de inactividad a 5 minutos
- Sincronización de hora automática con servidor NTP
- Deshabilitar auto instalación por USB
- Configuración de Log y auditoría para notificar eventos vía email al administrador del dispositivo.

2.3 FILTRADO WEB

El equipo funciona con un servicio llamado Fortiguard, el cual requiere una renovación anual de la licencia para la actualización de las firmas de antivirus, antispam, IPS y filtrado web. El servicio Fortiguard hace uso de la categorización de sitios web de tal manera que no es necesario especificar cada página que se desee bloquear o activar porque esto se hace automáticamente se acuerdo a la categoría en la que se encuentre

la página. Lo mismo hace con las aplicaciones que se conectan a Internet, las cuales se pueden bloquear de forma individual o por categoría.

En la figura 2.4 se muestra el perfil de filtrado web WF_CONTABILIDAD, el cual está habilitado en la política de acceso de las IP asignadas a los asistentes contables. En la parte inferior se muestra un listado de páginas permitidas las cuales son excepciones dentro de alguna categoría bloqueada.

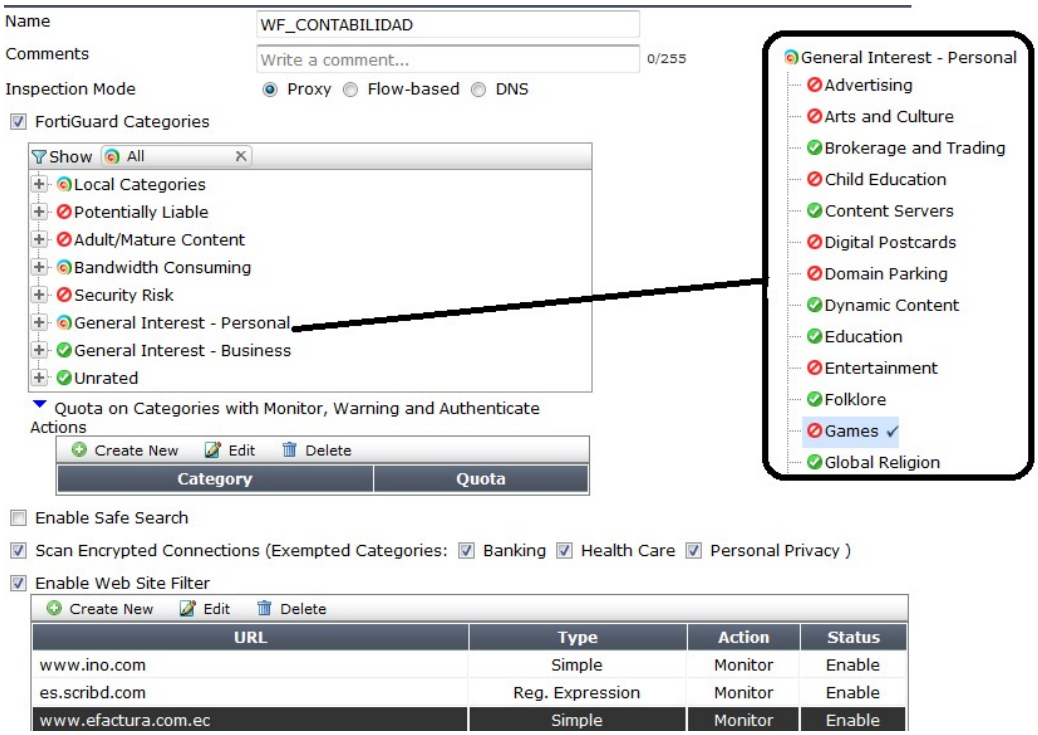


Figura 2.4 Ejemplo de filtrado web

La aplicación de esta política evita la navegación a sitios no permitidos a través de los navegadores de Internet, sin embargo este filtrado puede saltarse usando otras aplicaciones para la navegación web, además se requiere bloquear aplicaciones peer to peer las cuales no se conectan a un sitio específico ni utilizan un puerto fijo. Esto se consiguió haciendo uso de sensores de aplicaciones, dentro de los cuales se establece las restricciones de acceso a las aplicaciones ya sea de forma individual o por categorías. En la figura 2.5 podemos ver que se ha permitido la aplicación Skype pero sin embargo el resto de aplicaciones peer to peer se encuentran bloqueadas, en la parte final podemos apreciar que dentro de este sensor también está bloqueado el uso de aplicaciones de control remoto a través de Internet

Category	Popularity	Technolo...	Ri...	Action	Application
P2P				Monitor	Skype
				Monitor	30197
				Monitor	MS.Office.Communicator
General.Interest	1 2 3 4 5	All	All	Monitor	9gag, AOL.Search, AOL.Search_Member ... [Show all 250]
				Block	YouTube
				Block	YouTube_Video.Access
				Block	YouTube_Video.Upload
IM	1 2 3 4 5	All	All	Traffic Shaping	AIM, ICQ, MSN.Messenger ... [Show all 4]
P2P	1 2 3 4 5	All	All	Block	ABC, ANts.P2P, Apollon ... [Show all 87]
				Block	Download.Accelerator.Plus
				Block	Facebook
Game	1 2 3 4 5	All	All	Block	51.Com_Games, AIM.Game, Addicting.Games ... [Show all 131]
Update	1 2 3 4 5	All	All	Traffic Shaping	360safeguard.Update, ALTools.Update, ALYac.Update ... [Show
Video/Audio	1 2 3 4 5	All	All	Block	1kxun, 6cn_Search.Music, 8tracks ... [Show all 235]
				Block	Free.Download.Manager
				Block	HTTP.Download.Accelerator
Remote.Access	1 2 3 4 5	All	All	Block	Access.Remote.PC, Airdroid, Alpemix ... [Show all 90]
				Monitor	All Other Known Applications
				Monitor	All Other Unknown Applications

Figura 2.5 Sensor de aplicaciones

La organización aún no dispone de un servidor de dominio por lo que todas las políticas se están aplicando en base a la IP del dispositivo de red asignado, se crearon los diferentes grupos de IP y a cada uno de los grupos se le asignó una o varias políticas de comunicación entre cada interfaz de red.

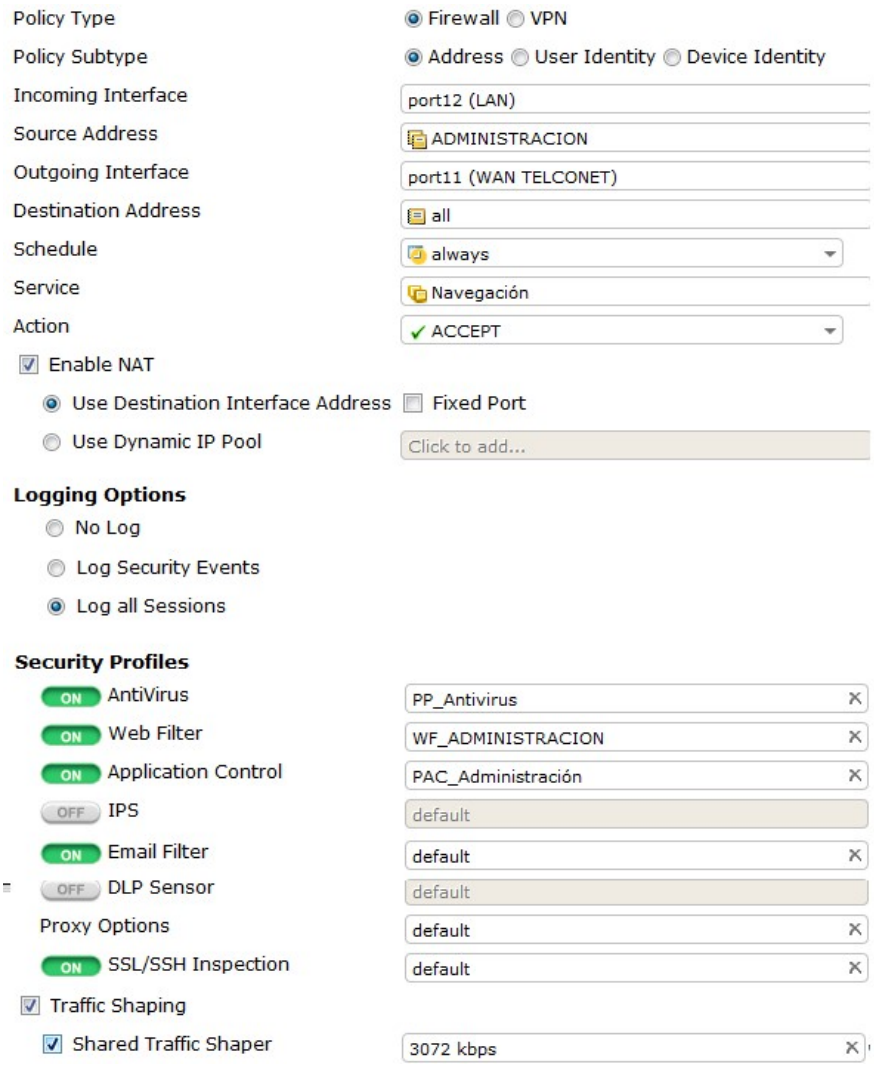


Figura 2.6 Política de salida para el grupo ADMINISTRACIÓN

En la figura 2.6 se puede apreciar una de las políticas de acceso a Internet configuradas. En esta se permite la salida a Internet del grupo ADMINISTRACIÓN, a través de los puertos habilitados en el grupo Navegación y sin restricción de horario. Se puede observar que para esta política se están aplicando un perfil de seguridad web, un sensor de aplicaciones, un filtro de correo, además se limita el tráfico a 3 Mbps entre todos los miembros del grupo que usan esta política.

2.4 SEGMENTACIÓN DE RED

Para planificar la segmentación de redes que existirán en una organización, se deben identificar los diferentes servidores y servicios para decidir su distribución. Aquellos que necesiten tener una puerta por la que entre tráfico desde Internet, deberán ir en una DMZ de servicios públicos o FRONTEND. La ubicación de los servidores que nutren estas aplicaciones públicas deben ir en una red diferente y protegida, o de BACKEND. El tráfico a permitir entre todas estas redes habrá de ser el justo y necesario para evitar exposiciones de servicios/máquinas por error. [2]

La red de la empresa no se encontraba debidamente segmentada, de tal manera que si un atacante lograba vulnerar un servidor expuesto al exterior podía tener los mismos permisos de acceso a la red que un

usuario interno, pudiendo extender su ataque a los servidores críticos de la organización.

Se dividió la red en los siguientes segmentos:

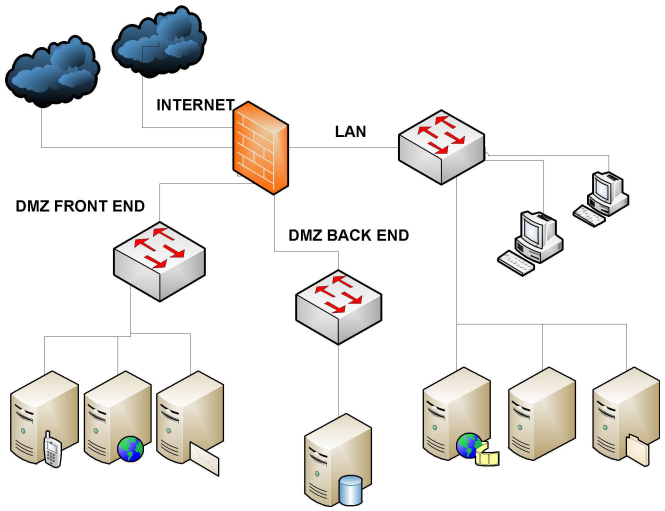


Figura 2.7 Topología de red final

INTERNET. Contiene los equipos proporcionados por los ISP para el acceso a Internet, los rangos de IP usados son los proporcionados por el proveedor.

DMZ. En esta red se ubican todos los equipos que brindan servicios a través de Internet. Esta red es accesible desde el exterior a través de los puertos permitidos, tiene acceso a ciertos servicios de la red de BACKEND pero no tiene acceso a la red interna.

BACKEND. En esta red se ubican los servidores críticos a los que aceden los usuarios internos y de los cuales consumen información los servidores ubicados en la DMZ.

LAN. En esa red se ubican los usuarios internos y los servidores que solo son de uso interno como los servidores de video vigilancia, telefonía IP, DNS, NTP entre otros.

Para establecer esta segmentación de red se crearon las siguientes políticas de acceso entre interfaces:

Red DMZ

Source	Destination	Schedule	Service	Action
port11 (WAN TELCONET) - port10 (DMZ)				
all	VIP_MAIL_PRETTYLIZA	always	Correo Prettyliza	✓ Accept
all	VIP_MAIL_PALMAR	always	Correo Zimbra	✓ Accept
all	VIP_WEBAPP	always	WEB_8080 HTTP	✓ Accept
all	VIP_FACTELECTRONICA	always	HTTP	✓ Accept
all	VIP_EST_METEREOLOGICAS_FUMIPALMA	always	HTTP WEB_8080	✓ Accept
all	VIP_OPENFIRE	always	OPENFIRE5222	✓ Accept

Figura 2.8 Políticas de red DMZ

Las IP públicas de los servidores públicos se configuraron como IP virtuales en las interfaces externas, de tal manera que al llamar la IP pública se realiza el redireccionamiento a la IP privada ubicada en al DMZ, se habilitaron solo los puertos necesarios para el funcionamiento de cada uno de los servicios.

Red BACKEND

Source	Destination	Schedule	Service	Action
port10 (DMZ) - port13 (BACK END)				
Servidor Facturacion Electronica Corporativo	Servidor Jenny Servidor Oasys	always	MS-SQL VNC	✓ Accept
SERVERAPP	Servidor Jenny	always	MS-SQL VNC	✓ Accept

Figura 2.9 Políticas de red BACK END

Se habilitó la conexión entre la red DMZ de FRONT END y la red de BACK END permitiendo solo el acceso a los puertos utilizados por el motor de base de datos SQL para obtener los datos que necesita los sitios web de facturación electrónica y de aplicaciones móviles. En esta red no se incluyó a todos los servidores de base de datos conectados a la red debido a la complejidad de cada caso.

Red LAN

La red LAN se conecta la red de DMZ para hacer uso de las aplicaciones web y de correo electrónico de forma local para esto se aplicaron las siguientes políticas:

Source	Destination	Schedule	Service	Action
port12 (LAN) - port10 (DMZ)				
all	Servidor correo pretyliza.com	always	Correo Prettyliza	✓ Accept
all	Servidor de Correo Zimbra	always	Correo Zimbra	✓ Accept
all	Servidor Mensajeria Openfire	always	OPENFIRE5222	✓ Accept
all	Servidor Facturacion Electronica	always	HTTP	✓ Accept
all	Servidor APP	always	HTTP WEB_8080	✓ Accept

Figura 2.10 Políticas de la red DMZ desde la LAN

La red LAN se conecta a Internet haciendo uso de diferentes políticas de acuerdo a los grupos de acceso a Internet a los que pertenece cada IP

Source	Destination	Schedule	Service	Action
port12 (LAN) - port11 (WAN TELCONET)				
GERENCIA	all	always	ALL	✓ Accept
SERVIDORES_LAN	all	FUERA JORNADA	ALL	✓ Accept
SERVIDORES_LAN	all	JORNADA LABORAL	ALL	✓ Accept
SISTEMAS_BLOQUEADOS	all	JORNADA LABORAL	ALL	✓ Accept
SISTEMAS	all	FUERA JORNADA	ALL	✓ Accept
SISTEMAS	all	JORNADA LABORAL	ALL	✓ Accept
DESARROLLO	all	always	Navegación	✓ Accept
ADMINISTRACION_CHAT_FB	all	always	ALL	✓ Accept
ADMINISTRACION_VIDEOS	all	always	Navegación	✓ Accept
DISEÑO	all	always	Navegación	✓ Accept
RASTREO_VEHICULAR	all	always	Navegación	✓ Accept
ADMINISTRACION_ACCESO_REMOTO	all	always	ALL	✓ Accept
ADMINISTRACION	all	always	Navegación	✓ Accept
Usuarios moviles	all	always	ALL	✓ Accept
CONTABILIDAD_ACCESO_REMOTO	all	always	Navegación	✓ Accept
CONTABILIDAD	all	always	Navegación	✓ Accept
TEMPORALES	all	SALIDA TEMPORALES	Navegación	✓ Accept
INTERNO	all	always	Navegación	✓ Accept

Figura 2.11 Políticas de acceso a Internet desde la LAN

Cada grupo tiene sus propios permisos de acceso a Internet, se han definido limitaciones de ancho de banda, filtrado de sitios web, puertos y horarios de acceso a Internet. Por ejemplo:

El grupo TEMPORALES solo puede navegar en Internet una hora al día.

El grupo SERVIDORES_LAN no tiene permisos de navegación, y solo puede actualizar el sistema operativo fuera de la jornada laboral.

El grupo SISTEMAS tiene una restricción de uso de ancho de banda dentro de la jornada laboral.

En el grupo INTERNO solo permite acceso a los sitios web empresariales o de uso interno.

La red LAN también se conecta a la red de BACK END debido a que las aplicaciones deben consultar las base de datos que está en esta red para esto usa las siguientes políticas:

Source	Destination	Schedule	Service	Action
port12 (LAN) - port13 (DMZ BACK END)				
all	Servidor Jenny Servidor Oasys	always	MS-SQL VNC	✓ Accept

Figura 2.12 Políticas de acceso a la red de BACK END desde la LAN

2.5 ALTA DISPONIBILIDAD INTERNET

FortiOS usa ECMP (equal-costmulti-path) para distribuir el tráfico a un mismo destino como Internet o a otra red. Usando ECMP se puede agregar múltiples rutas al destino y dar a cada una de estas rutas la distancia y la prioridad. Se incluyen tres opciones de configuración para rutas de failover y balanceo de carga: Source IP based (basada en la IP de origen), Weighted Load Balance, (basada en el peso) y Spillover (basada en el uso) [3]

La empresa contaba con el servicio de Internet con un ancho de banda de 5 Mbps, adicionalmente se contrató 5 Mbps con otro proveedor como respaldo. Para usar todos el ancho de banda de modo eficiente y

considerando que ambas tienen el mismo ancho de banda se consideró la configuración de Spillover, mediante la cual el UTM distribuye las sesiones en rutas ECMP basada en cuán ocupadas están las interfaces añadidas a las rutas.

Al seleccionar Spillover se agrega límite a las interfaces de las rutas ECMP. Fortigate envía todas las sesiones a la interfaz con el número menor hasta que el ancho de banda procesado por esta interfaz alcance el límite de Spillover establecido. Fortigate envía las sesiones adicionales a la siguiente interfaz con el número de interfaz más bajo. [4] Se configuraron las rutas por defecto para cada una de las interfaces:

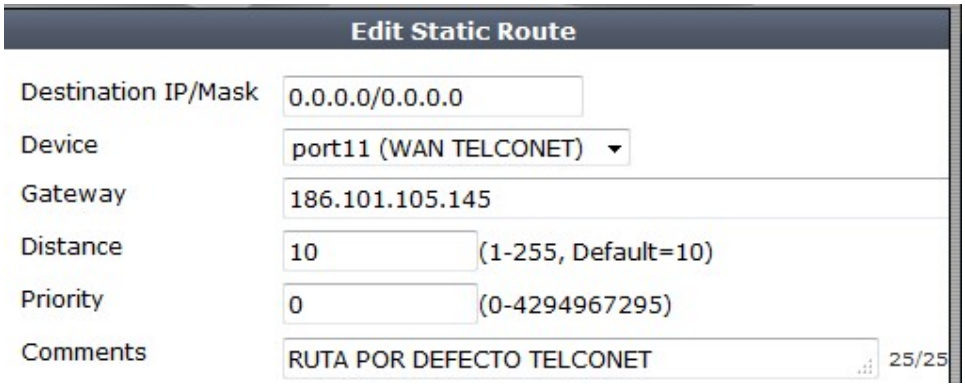


Figura 2.13 Interfaz ISP Telconet

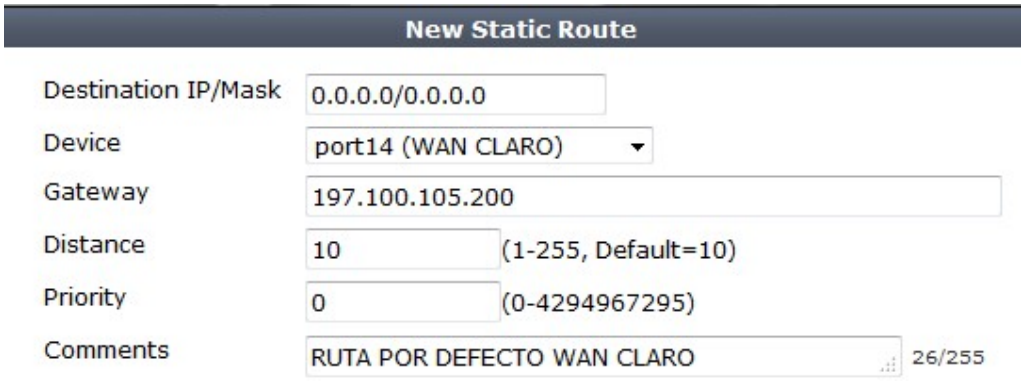


Figura 2.14 Interfaz ISP CLARO

Se duplicaron todas las políticas de acceso para la salida a Internet, para que todas puedan salir a través de la interfaz de proveedor de respaldo.

A continuación se muestra la configuración establecida para el balanceo de carga, la interfaz port10 se configuró como interfaz principal con un threshold de 3000, lo que significa que atenderá todas las peticiones recibidas pero cuando llegue a un consumo aproximado de 3 Mbps, las nuevas sesiones serán direccionadas a la interfaz port14 del ISP de respaldo. Es posible que las interfaz principal siga recibiendo y atendido nuevas sesiones debido a que se queda grabado en la caché la interfaz con la que está siendo atendida una IP. Una vez que la interfaz principal haya disminuido su consumo de ancho de banda hasta alcanzar un nivel inferior al límite, volverá a atender nuevas sesiones, balanceando de esta manera la carga de forma equitativa y aprovechando de forma eficiente el ancho de banda contratado.

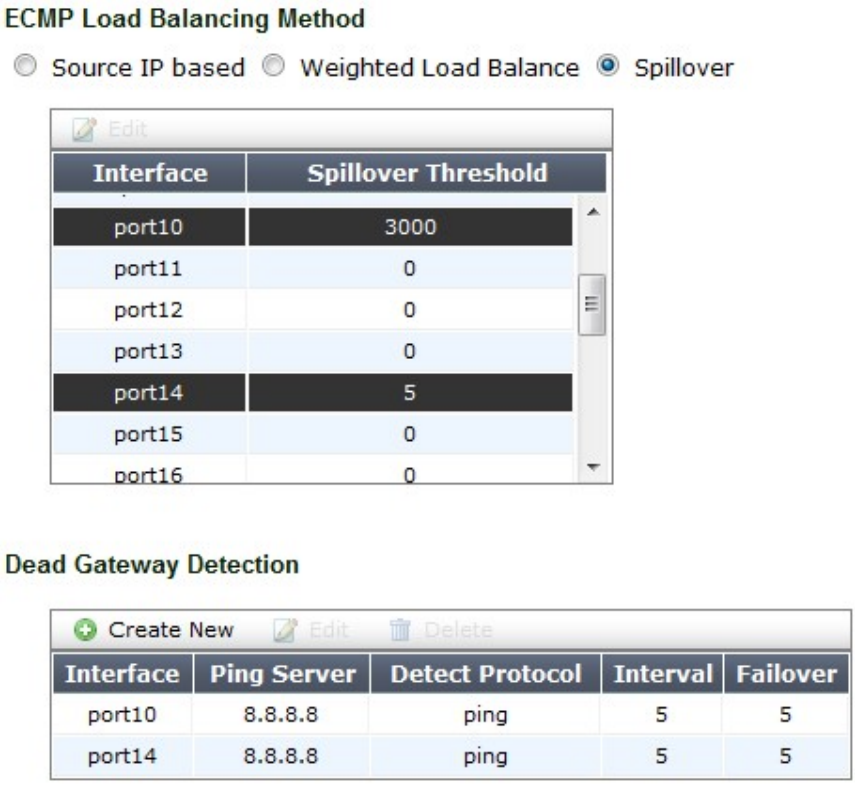


Figura 2.15 Configuración de ECMP fail - over

2.6 CONFIGURACIÓN DE VPN

Una red VPN (red privada virtual) es una red privada construida dentro de una infraestructura de red pública, como por ejemplo Internet. Las empresas pueden usar una red VPN para conectar de manera segura oficinas y usuarios remotos por medio de un acceso a Internet económico suministrado por un tercero, en lugar de a través de enlaces WAN dedicados o enlaces de acceso telefónico de larga distancia. Existe dos

tipo de VPN cifradas: VPN IPSec de sitio a sitio y VPN de acceso remoto.[5]

Se realizó la configuración de un servidor VPN para la conexión remota de los usuarios administradores de sistemas evitando tener que poner IP públicas o publicar puertos de administración en Internet. La sucursal de Naranjal se conectaba a la red local a través de un túnel VPN establecido entre el servidor proxy y el router del ISP de Naranjal. No se pudo establecer la conexión entre ruteadores optando por hacer la conexión VPN mediante software.

Se usó el protocolo IPSec con clave compartida a través de una de las interfaces WAN, habilitando los controles de filtrado web en la política de comunicación hacia Internet. Las políticas habilitadas para al VPN son las siguientes:

Source	Destination	Schedule	Service	Action
VPN_IPSEC - port10 (DMZ) (1)				
VPN_IPSEC_RANGE	RED_DMZ_PALMAPLAST	always	SSH5025 PING Correo Prettyliza Correo Zimbra	✓ Accept
VPN_IPSEC - port11 (WAN TELCONET) (1)				
VPN_IPSEC_RANGE	all	always	Navegación	✓ Accept
VPN_IPSEC - port12 (LAN) (1)				
VPN_IPSEC_RANGE	all	always	ALL	✓ Accept
VPN_IPSEC - port13 (BACK END) (1)				
VPN_IPSEC_RANGE	Servidor Jenny Servidor Oasys	always	MS-SQL VNC	✓ Accept

Figura 2.16 Políticas de acceso a la VPN

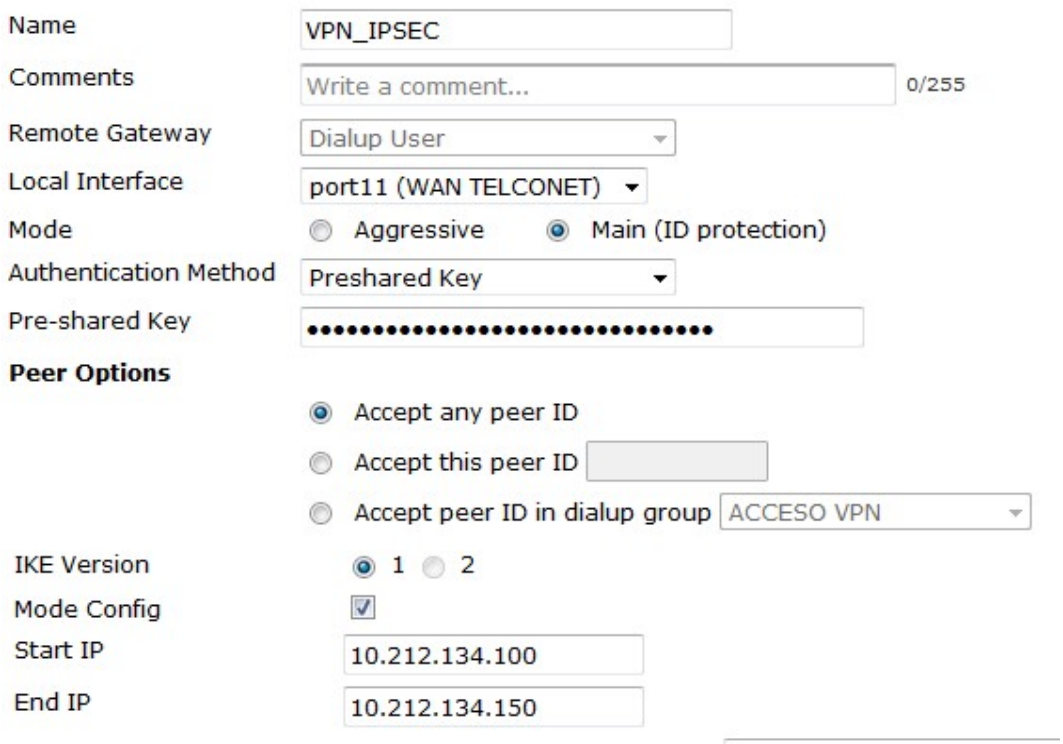


Figura 2.17 Configuración de VPN IPSEC

Para conectarse a la red VNP se utiliza el software gratuito FortiClient, un usuario necesita conocer la IP del servidor de VPN y puerto, la clave precompartida, además de su nombre de usuario y clave para poder conectarse a la VPN

CAPÍTULO 3

ANÁLISIS DE RESULTADOS

3.1 PRUEBAS DE FILTRADO WEB

Se comprobó la aplicación de los distintos filtros de navegación. En la figura 3.1 se muestra que no es posible acceder al sitio proxyweb.com.es debido a que pertenece a la categoría Proxy Avoidance y esta categoría se encuentra bloqueada en la política de filtrado web de este grupo. Al bloquear esta categoría se evita que los usuarios con conocimiento de redireccionamiento web se salten las políticas de seguridad establecidas.

En la Figura 3.2 se muestra que hay 0.87 Mbps disponibles en ese momento para una IP del grupo SISTEMAS, este grupo al tener acceso con menos restricciones era el que más ancho de banda consumía y limitaba el ancho de banda disponible para el personal administrativo. Debido a que se aplicó un control de ancho de banda dentro de la

jornada laboral, los usuarios planifican las descargas de software para un horario fuera de la jornada.

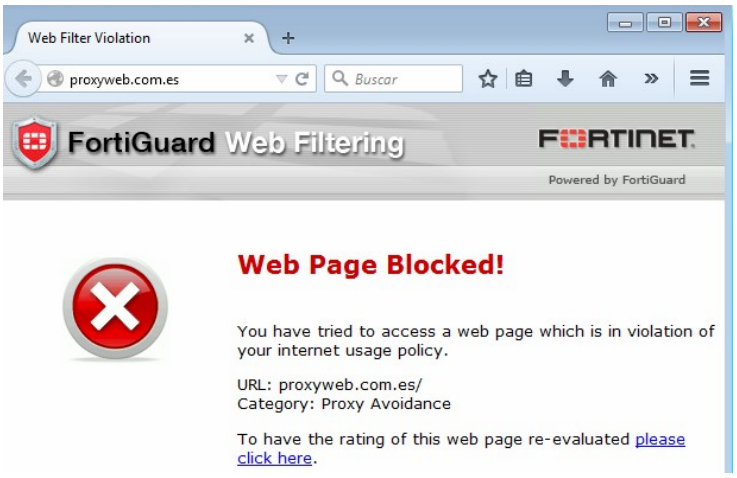


Figura 9.1 Acceso a sitio no permitido grupo SISTEMAS

Figura 9.2 Ancho de banda disponible grupo SISTEMAS

El bloqueo de aplicaciones funcionó como se esperaba, en la figura 3.3 se puede apreciar la aplicación Teamviewer en el escritorio de un usuario del grupo ADMINISTRACIÓN. Los usuarios de este grupo no tienen permiso de usar aplicaciones de control remoto a través de Internet. De esta forma aunque use la versión portable de la aplicación no podrá acceder remotamente si no se ha autorizado el uso de esta aplicación.

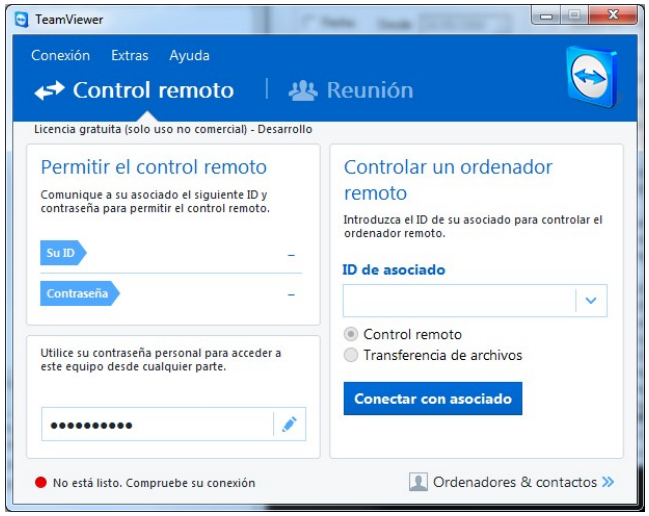


Figura 9.3 Bloqueo de aplicación de control remoto

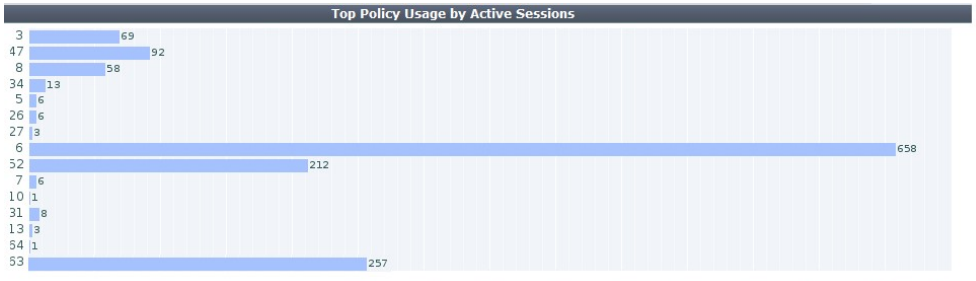
3.2 PRUEBAS DE BALANCEO DE CARGA

Se realizaron pruebas de navegación y al revisar los log de tráfico se encontró que se estaba haciendo uso de los dos proveedores de Internet, en la figura se puede apreciar el uso tanto de la interfaz del puerto 12 (Telconet) como de la interfaz del proveedor de respaldo (puerto 14)

#	Date/Ti...	Source	Destination	Src Interfa...	Dst Interfa...	Sent / Receiv
1	17:41:41	128.128.11.104 (v-128-128-11-104.whoi.edu)	31.13.73.52 (scontent-mia1-1.cdninstagram.com)	port12	port11	3.82 KB / 5.42 KB
2	17:41:41	128.128.11.104 (v-128-128-11-104.whoi.edu)	port14 l3.73.1 (star.c10r.facebook.com)	port12	port11	2.38 KB / 4.38 KB
3	17:41:41	128.128.11.47	91.228.165.59 (ts.eset.com)	port12	port11	2.79 KB / 751 B
4	17:41:41	128.127.1.7 (host-128-127-1-7.italprovider.it)	186.101.105.206 (palmar.com.ec)	port10	port10	133.12 KB / 5.20 K
5	17:41:41	128.128.12.31	37.252.227.51 (ping3.teamviewer.com)	port12	port11	120 B / 52 B
6	17:41:41	128.128.21.15	128.127.1.7 (host-128-127-1-7.italprovider.it)	port12	port10	2.01 KB / 42.02 KB
7	17:41:41	128.128.11.40	193.163.252.179 (my.maerskline.com)	port12	port11	52 B / 40 B
8	17:41:41	128.128.11.100 (v-128-128-11-100.whoi.edu)	193.163.252.179 (my.maerskline.com)	port12	port11	432 B / 3.04 KB
9	17:41:41	128.128.41.6 (u-128-128-41-6.xr.usgs.gov)	193.163.252.179 (my.maerskline.com)	port12	port11	71 B / 125 B
10	17:41:41	128.128.12.59	193.163.252.179 (my.maerskline.com)	port12	port11	62 B / 102 B
11	17:41:41	128.128.12.19	193.163.252.179 (my.maerskline.com)	port12	port14	2.10 KB / 41.62 KB
12	17:41:40	45.114.11.24	31.13.73.1 (star.c10r.facebook.com)	port11	port12	2.11 KB / 2.89 KB
13	17:41:40	128.128.12.19	72.247.9.145 (fbcdn-vthumb-a.akamaihd.net)	port12	port14	1.89 KB / 17.88 KB
14	17:41:40	128.128.41.20 (u-128-128-41-20.xr.usgs.gov)	23.210.109.178 (s-static.ak.facebook.com)	port12	port11	933 B / 557 B

Figura 9.4 Log de tráfico

Se realizó el monitoreo de uso de las políticas de navegación encontrando que las políticas que tenían mayor tráfico eran dos políticas de acceso a Internet de los usuarios del grupo ADMINISTRACIÓN, tanto la política de salida de la interfaz principal (ID 6) como política de salida de la interfaz de respaldo (ID 63) estaban siendo usadas para la salida a Internet. En la siguiente figura se puede apreciar que la interfaz principal tiene 658 sesiones activas mientras que la interfaz de respaldo tiene 257 sesiones activas. Ambas interfaces se encuentran respondiendo a las peticiones de los usuarios ya que se ha alcanzado el límite que puede atender por sí sola la interfaz principal.

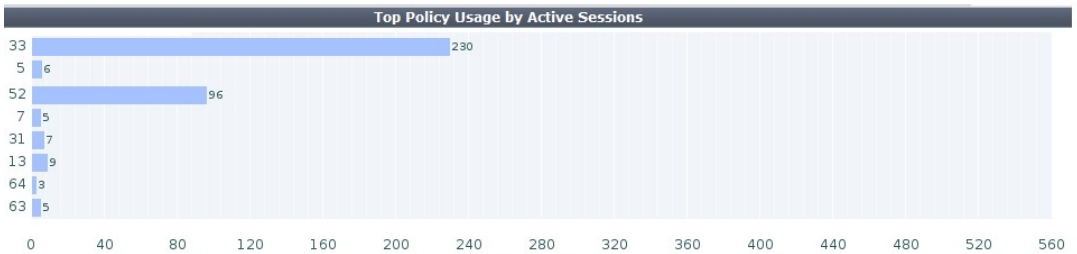


Policy ID	Source Interface/Zone	Destination Interface/Zone	Action	Active Sessions	Bytes	Packets
3	port10	port11	✓	69	2.30 GB	3,333,486
47	port12	port11	✓	92	1.14 GB	2,784,377
8	port12	port11	✓	58	23.12 GB	30,847,201
34	port11	port10	✓	13	13.89 GB	14,538,377
63	port12	port14	✓	257	16.97 GB	27,683,246
5	port12	port11	✓	6	24.95 GB	36,850,038
26	port12	port11	✓	6	2.31 GB	3,164,540

Figura 9.5 Monitoreo de uso de interfaces WAN

3.3 PRUEBAS DE ALTA DISPONIBILIDAD DE SERVICIO DE INTERNET

Se realizó una simulación de corte del servicio de Internet en la interfaz principal dejando habilitado solo el tráfico a través de la interfaz de respaldo, se encontró el siguiente resultado mostrado en la figura 3.6, donde puede ver que solo se aplican se activan las políticas que utilizan la interfaz de respaldo ubicada en el puerto 14



Policy ID	Source Interface/Zone	Destination Interface/Zone	Action	Active Sessions	Bytes	Packets
33	port12	port14	✓	230	17.02 GB	27,753,251
5	port12	port14	✓	6	24.95 GB	36,850,038
52	port12	port14	✓	96	7.50 GB	11,707,307
7	port12	port14	✓	5	2.90 GB	5,229,233
31	port14	port12	✓	7	719.89 MB	1,362,392
13	ssl.root	port12	✓	9	465.65 MB	2,094,845
64	port12	port10	✓	3	1.29 GB	1,668,861
63	port12	port10	✓	5	22.59 MB	30,312

Figura 9.6 Monitoreo de interfaces WAN en failover

3.4 FUNCIONAMIENTO DE LA VPN

Se configuró la red VPN Palmar en un equipo conectado a Internet fuera de la empresa usando el software FortiClient.

Desde la VPN se accedió a la consola de administración del UTM, en la figura 3.7 se puede apreciar, el log con las conexiones realizadas por el administrador.

#	Date/Ti...	Source	Destination	Application Name	Sent / Received
1	16:32:03	salvarez (10.212.134.200)	128.128.11.254 (vpninside.whoi.edu)	Web Management(HTTPS)	937 B / 453 B
2	16:32:02	salvarez (10.212.134.200)	128.128.11.254 (vpninside.whoi.edu)	Web Management(HTTPS)	937 B / 453 B
3	16:31:51	salvarez (10.212.134.200)	128.128.11.254 (vpninside.whoi.edu)	Web Management(HTTPS)	3.12 KB / 1.64 KB
4	16:31:51	salvarez (10.212.134.200)	128.128.11.254 (vpninside.whoi.edu)	Web Management(HTTPS)	1.93 KB / 990 B
5	16:31:51	salvarez (10.212.134.200)	128.128.11.254 (vpninside.whoi.edu)	Web Management(HTTPS)	1.93 KB / 990 B

Figura 9.7 Log de conexiones por VPN

En la figura 3.9 se muestran la configuración de la red y las pruebas de conexión a la LAN.

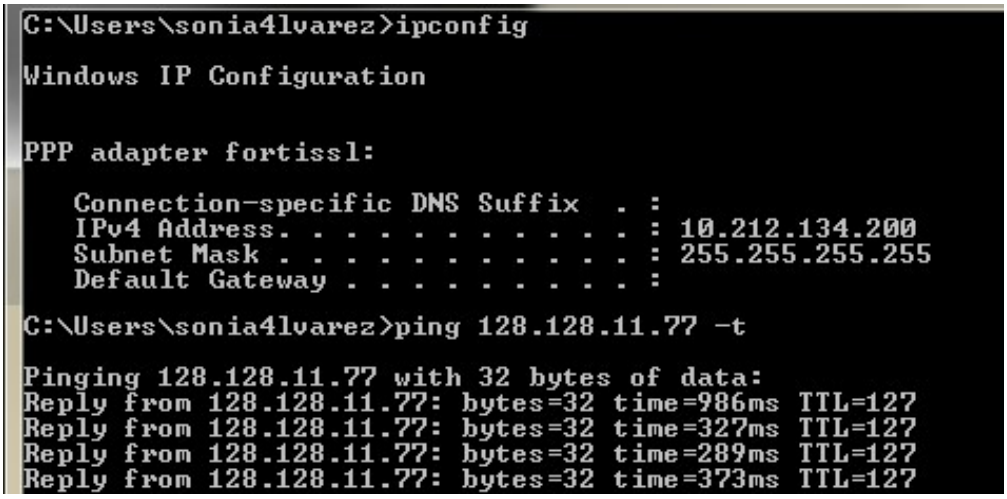


Figura 9.8 Comprobación de conexión a IP privada

A través de la VPN se pudo acceder a visualizar las cámaras de CCTV. La conexión VPN también funcionó exitosamente desde varios dispositivos móviles con sistema operativo Android. De esta manera se evitó tener que poner IP públicas a los dispositivos de grabación de video.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. La plataforma utilizada para el filtrado web y de aplicaciones es muy eficiente, ahora es posible controlar todo el tráfico de entrada y salida hacia Internet y hacer cambios en las políticas sin temor a dañar la configuración.

2. Se encontraron dificultades al momento de implementar la topología de red en su totalidad. Se deben planificar la migración de los servidores de forma progresiva para disminuir el impacto causado en el operación de los sistemas especialmente en los sistemas que requieren el soporte de un proveedor externo.

3. La inversión en tecnología solo fue necesaria en la adquisición del appliance de seguridad. La segmentación de la red no tuvo ningún

costo adicional para la empresa debido a que ya se contaba con la infraestructura necesaria.

RECOMENDACIONES

1. Los administradores deben hacer respaldos antes y después de hacer cambios en las políticas de seguridad y configuración del equipo.

2. Es posible implementar un firewall adicional para gestionar el tráfico interno, dejando que el UTM solo gestione el tráfico que debe pasar hacia el exterior con el objetivo de incrementar la seguridad y disminuir el tráfico de red que pasa a través del UTM

3. Las sucursales se conectan directamente a la red LAN de la empresa, se recomienda segmentar estas redes tanto para disminuir el tráfico en cada sucursal como para incrementar la seguridad permitiendo que solo se accedan a los servicios y equipos autorizados por el firewall.

4. Se recomienda el uso de políticas de DLP e IPS para aprovechar las funcionalidades del dispositivo.

BIBLIOGRAFÍA

[1]Fortinet, HardeningyourFortiGate, http://docs.fortinet.com/d/fortigate-hardening-your-fortigate, fecha de publicación abril del 2015

[2]Martinez,L., Securizando un entorno de máquinas virtuales con Virtualbox, http://www.securitybydefault.com/2012/07/securizando-un-entorno-de-maquinas.html, fecha de consulta julio del 2015

[3]Fortinet, FortiOSHandbook (forFortiOS 5.2), http://help.fortinet.com/fos50hlp/52data/index.htm, fecha de consulta de junio del 2015, página 262

[4]Fortinet, FortiOSHandbook (forFortiOS 5.2), http://help.fortinet.com/fos50hlp/52data/index.htm, fecha de consulta junio del 2015, página 263

[5]Cisco, Seguridad VPN, http://www.cisco.com/web/ES/solutions/es/vpn/index.html, fecha de consulta julio del 2015