IMPLEMENTACIÓN Y ACTUALIZACIÓN EN LA INFRAESTRUCTURA DE SEGURIDAD DE UNA RED INFORMÁTICA

DEPLOYMENT AND UPDATE OF A NETWORK'S SECURITY INFRASTRUCTURE

ABSTRACT
This article stresses the importance of security for computer networks within organizations and shows the results obtained from a security infrastructure update at a particular company. The updating process included improvements to the initial design (in terms of both hardware and software) for various company branches around the country. A new firewall is implemented at the company's industrial facilities and a site-to-site VPN is created for communication with the main headquarters. Due to the malfunction of the addressing scheme and also to the change of ISP, full firewall integration is deployed together with static route reconfiguration.
The academic value of the present work is to offer key guidelines for any implementation as well a providing the reader with information-security and firewall-associated concepts.

Keywords: Computer Network, VPN, fw, firewall, Checkpoint, Information Security.

RESUMEN
En éste artículo se evidencia la importancia de la seguridad en las redes informáticas dentro de cualquier organización y muestra los resultados encontrados al actualizar la infraestructura de seguridad de una organización e incluir mejoras de diseño (desde el punto de vista del hardware y software) que cuenta con varias sucursales en el País. Será implementado un nuevo cortafuegos en la sucursal de zona franca así como la creación de una VPN site to site con la sede principal. Se realizará la integración de todos los firewalls con la sede principal y la reconfiguración de rutas estáticas por mala configuración y por cambio de proveedor ISP.
El aporte académico del proyecto consiste en brindar lineamientos clave en cualquier implementación así como conceptos en seguridad de la información y firewalls.

Palabras clave: Red de computadoras, VPN, fw, firewall, Checkpoint, Seguridad de la información.

Nancy Yaneth Gelvez García
Ingeniera de Sistemas, MSc. en Ciencias de la información y las Telecomunicaciones, Docente de tiempo completo en Ingeniería de Sistemas de la Escuela Colombiana de Carreras Industriales (ECCI).
nayag24@hotmail.com

Miguel Andrés Flórez Vianchá
Ingeniero electrónico egresado de la Universidad Distrital "Francisco José de Caldas" y actualmente labora en la empresa de seguridad de la Información Digiware de Colombia S.A, como Especialista en infraestructuras de seguridad de Redes.
andresf5222@hotmail.com

Victor Daniel Angulo Morales
Ingeniero electrónico egresado de la Universidad Distrital "Francisco José de Caldas" y actualmente se desempeña como Ingeniero de gestión de la red CECAD de la Universidad Distrital.
vdangulom@correo.udistrital.edu.co

Tipo: Artículo reporte de caso

Fecha de Recepción: Agosto 25 de 2011
Fecha de Aceptación: Diciembre 10 de 2011

1. INTRODUCCIÓN

Debido a la creciente cantidad de amenazas y riesgos sobre la red, es necesaria una "infraestructura de seguridad" que proteja el activo más preciado de las empresas como lo es la información y datos sensibles que en caso de robo o pérdida pueden generar millonarios costos para la organización.

Gracias al avance exponencial de la tecnología, a las amenazas emergentes sobre Internet y al crecimiento de las empresas, son necesarias actualizaciones a los esquemas de seguridad y a los dispositivos encargados de la protección de la red para ofrecer mayor seguridad, incrementar el performance, proteger y agregar nuevas tecnologías. Por ésta razón se pone a consideración de la comunidad académica y científica los resultados obtenidos de un proyecto que buscaba actualizar la infraestructura de seguridad de una Multinacional de productos farmacéuticos para garantizar la protección de su información de acuerdo a las demandas del cliente con el fin de que sea un referente a ser tenido en cuenta cuando se pretendan realizar este tipo de implementaciones.

El artículo se compone de varias etapas. En la sección Antecedentes, se evalúan las tecnologías existentes, las empresas y el mercado actual en Colombia en seguridad de la información, en el Marco teórico se brindan algunas definiciones claves en el desarrollo del artículo, la Metodología y Desarrollo muestra el plan de trabajo y las actividades realizadas, listando los lineamientos y mejores prácticas que se pueden seguir en proyectos de éste tipo. Por último se presentan los Resultados, las Conclusiones y la Bibliografía del proyecto.

2. ANTECEDENTES

Entidades gubernamentales, financieras y todo tipo de organizaciones tienen información crítica, valiosa y sensible sobre clientes, productos, empleados, que generalmente reposa en equipos informáticos y a la que se accede de manera remota; todo ello ha hecho que los delitos en el ámbito de TI hayan incrementado, lo que implica riesgos informáticos más latentes [1].

No obstante, a nivel regional existen algunas empresas dedicadas a la seguridad de la información que brindan servicios de seguridad cubriendo las necesidades de pequeñas y grandes compañías entra las que se destacan las mostradas en [2]. Para brindar protección en la red existen herramientas que se han desarrollado desde la aparición de los sistemas de telecomunicaciones debido a la infinidad de vulnerabilidades existentes en los sistemas operativos y protocolos de comunicación. Según ISACA (organización global encargada de elaboración, adopción y prácticas en seguridad de la información) [3] algunas herramientas tecnológicas disponibles actualmente para el aseguramiento de la red son los firewalls [8]. En este sentido GARTNER (Líder en investigación en tecnologías de información) realizó un análisis comparativo entre diferentes marcas de cortafuegos de los mejores productos en ambientes empresariales tal como se muestra en la Fig. 1 teniendo en cuenta características como la visión (eje horizontal), la capacidad de ejecución (eje horizontal), el servicio al cliente y la trayectoria en el mercado y los precios.

Destaca notoriamente checkpoint quien se encuentra en el cuadrante "Leaders" (en rojo).

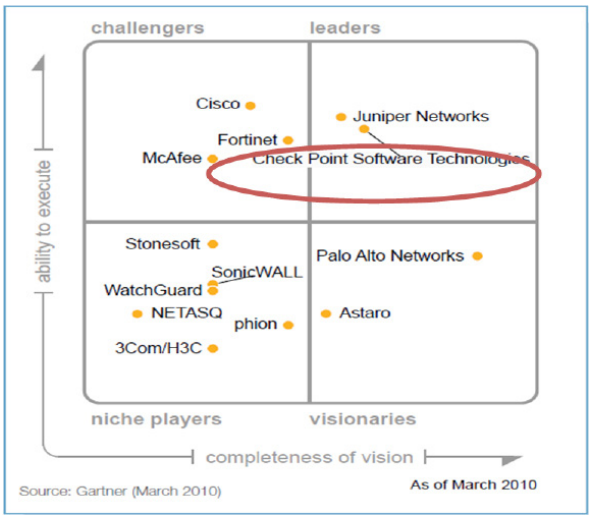


Fig. 1. Cuadrante entre la visión del fabricante y la facilidad para implementar de cada producto en ambientes empresariales [5].

Otras herramientas importantes son los relacionados con la administración de cuentas de usuario, los IDS (sistemas de detección de intrusos), el encriptamiento de los datos, los IPS (sistemas de protección de intrusos) que además de detectar ataques como los IDS, definen acciones sobre las firmas para bloquear patrones de intrusiones o generar alarmas. Adicionalmente existen los antivirus, los PKI (que son las infraestructuras de clave pública [4], los certificados SSL (Secure sockets layer) y las VPN [6] y [7].

3. MARCO TEÓRICO

Las VPN (redes privadas virtuales) buscan transmitir información entre diferentes lugares a través de Internet creando túneles encriptados en donde se mantiene la confidencialidad, la autenticidad y la integridad de la información [6], en la Fig. 2 se ilustra el proceso para la creación y envio de datos a través de una VPN.

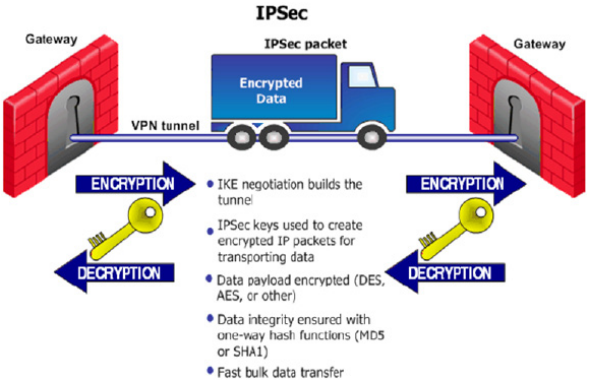


Fig. 2. Creación y envío de datos por VPN [7]

El proceso se desarrolla en dos fases; en la primera fase se utiliza encripción asimétrica (mucho más lenta) para intercambiar un SA o Security Asociation que consta de una llave pública, algoritmos de encripción, métodos de autenticación y algoritmos hash. El SA será utilizado para establecer la segunda fase, en la cual se utilizará encripción simétrica (mucho más rápida) y se negociará otro SA estableciendo el túnel y garantizando la codificación del tráfico mediante el protocolo IPSEC entre los pares.

Los firewall inspeccionan y controlan el flujo de tráfico entre diferentes redes. Por ejemplo entre Internet y la LAN como se puede apreciar en la Fig. 3.

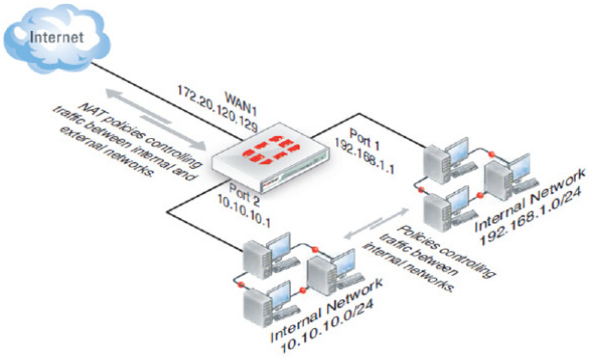


Fig. 3. Firewall perimetral entre Internet y dos redes internas (LANs) [8].

Generalmente los dispositivos se ubican en el perímetro de la red para brindar seguridad entre las redes externas (inseguras) como Internet y las redes internas (seguridad perimetral), o dentro de las redes internas para brindar diferentes niveles de seguridad.

La arquitectura utilizada mostrada en la Fig. 4 tiene 3 componentes básicos:

- La interface de administración
- El repositorio de logs, políticas, reglas y objetos
- El gateway o firewall

A veces se opta por unir el punto 2 y 3 (en recuadro rojo) llamado opcionalmente como "ambiente o arquitectura StandAlone".

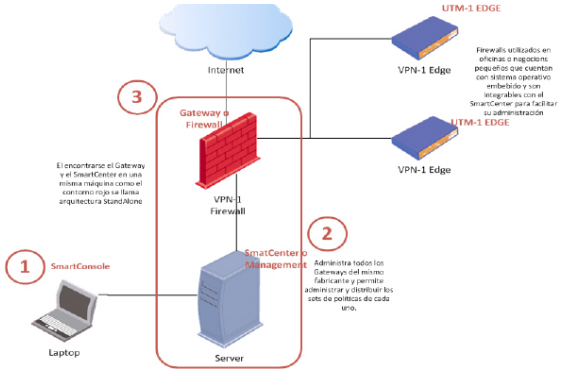


Fig. 4. Arquitectura de Firewalls Checkpoint.

4. METODOLOGÍA Y DESARROLLO

El proyecto fue desarrollado de acuerdo a etapas que presentan de una manera sencilla y detallada los pasos a seguir para la consecución de los objetivos propuestos para la topología de red avaluada:

4.1. Recolección de información

Se relaciona con el levantamiento de información acerca de las instalaciones físicas, la infraestructura de red (topología de red suministrada, topología de red corregida y topología de red futura), los equipos instalados actualmente, sus interfaces, rutas, memoria, CPU, versión de S.O, etc. También se recolecto información acerca de las VPNs existentes (ubicación, IPs, parámetros de encripción, entre otros).

En la Fig. 5 se observa la topología de red existente la cual fue complementada de acuerdo al análisis aplicado en este ítem.

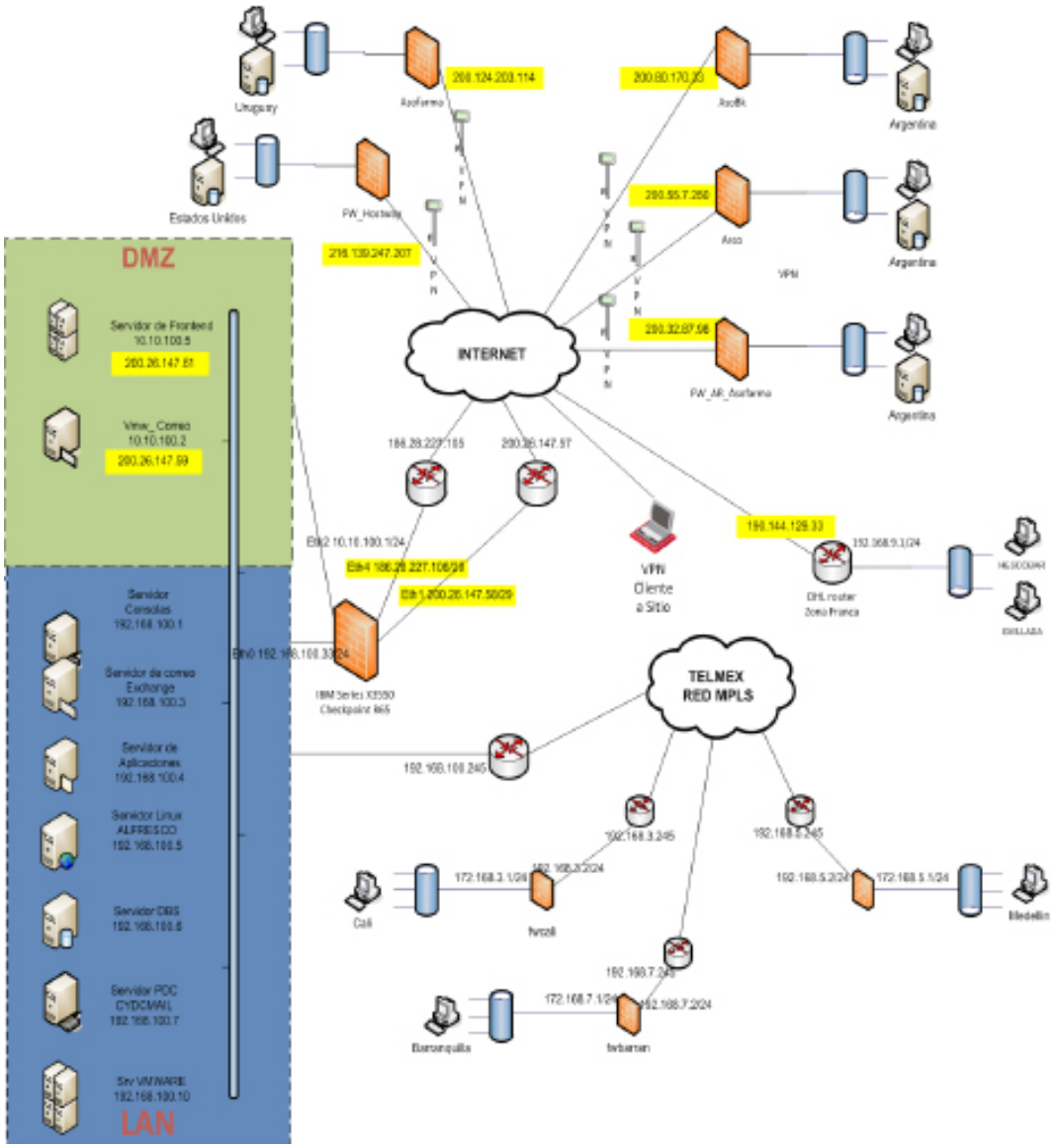


Fig. 5. Topología de red actual corregida.

La topología de red planteada incluye la interconexión de la sede principal con 3 sucursales por canal MPLS y 1 por Internet, además de 5 VPNs site to site fuera de Colombia y una VPN cliente a sitio.

Dentro de los principales problemas detectados están:

- No hay protección perimetral en zona franca
- La transmisión de datos desde la sucursal hacia la sede principal se realiza a través de Internet sin ningún tipo de seguridad.
- No es posible la administración de políticas de seguridad en Medellín ni en zona franca.
- La tabla de enrutamiento del fw principal es extensa y no está adaptada a la topología de red.
- Hay dos routers para internet que deberían ser utilizados para VPNs en uno de ellos y tráfico de internet en el otro.
- El proveedor del canal MPLS será reemplazado por lo que el direccionamiento en el router de borde cambiará.

En la tabla 1 se muestra un resumen del estado actual y lógico de los dispositivos existentes cuya imagen física se observa en la Fig. 6.

Tabla 1. Resumen del estado actual del Firewall de la sede principal y los firewalls de las sucursales.

FIREWALL SEDE PRINCIPAL (TROYA)				
UBICACIÓN	BOGOTÁ D.C.			
HARDWARE	Open server IBM SYSTEM X3550			
SOFTWARE	Checkpoint Secure Platform R65			
ESTADO DE LA MÁQUINA	CPU (top)	4%		
	Memoria (free –m)	Total: 2.7 Gb		Usada: 433 Mb
	Disco Duro (df –k)	/var	719M used	0.7%
		/sysimg	577M used	4.1%
		/opt	458M used	1.4%
		/boot	11M used	0.8%
		/	281M used	3%
FIREWALL SEDE MEDELLIN (FWMEDELLIN)				
UBICACIÓN	ANTIOQUIA - MEDELLÍN			
HARDWARE	UTM-1 EDGE X			
SOFTWARE	Checkpoint Firmware 6.047X			
ADMINISTRACIÓN	No hay administración			
FIREWALL SEDE CALI (FWCALI)				
UBICACIÓN	VALLE DEL CAUCA – CALI			
HARDWARE	UTM-1 EDGE X			
SOFTWARE	Checkpoint Firmware 6.047X			
ADMINISTRACIÓN	192.168.100.33			
FIREWALL SEDE BARRANQUILLA (FWBARRANQUILLA)				
UBICACIÓN	ATLANTICO – BARRANQUILLA			
HARDWARE	UTM-1 EDGE X			
SOFTWARE	Checkpoint Firmware 6.047X			
ADMINISTRACIÓN	192.168.100.33			

4.2. Estado del sistema y copias de respaldo

Como mejor práctica, antes de comenzar cualquier actualización de una infraestructura de seguridad es importante tomar backups de configuración de los dispositivos afectados, se debe tener un punto de retorno antes de modificar, añadir o borrar algo en la configuración en caso de aparecer contratiempos. Fueron tomados 2 backups como se observa en la tabla 2, el primero de la configuración del S.O y de la configuración general de checkpoint [9] y el segundo solamente de la configuración de checkpoint.

Fig. 6. Ubicación en el rack del Open Server X3550 de IBM (firewall sede principal izquierda) y vista frontal del firewall UTM-1 EDGE (firewall sucursales derecha).

Tabla 2. Copias de respaldo de la configuración del firewall de la sede principal

UTILIDAD	NOMBRE	TAMAÑO
Backup	backup_troya_2_7_2011_18_26.tgz	89Mb
Upgrade export	bkp_troya_2jul2011.tgz	55Mb

4.3. Depuración

En el set de políticas de un firewall generalmente hay bastantes reglas u objetos obsoletos que pudieron tener vigencia en su momento, pero debido a cambios en la red, en el direccionamiento o en las necesidades de la organización, éstas/os ya no son usados y sólo incrementan el tamaño del set de políticas, dificultando su administración.

Fueron depurados 2 objetos duplicados y 19 objetos sin uso. Ninguna regla fue eliminada

debido a que la nueva migración no las exigía.

4.4. Actualización del S.O (sistema operativo) del módulo de seguridad (firewall) IBM X3 550

Las actualizaciones son hechas con el fin de conservar la configuración de los productos instalados como políticas de seguridad y objetos así como las configuraciones de red y otros parámetros del S.O. La actualización se realiza de la versión R65 a la versión R71 de checkpoint [10] [11] que se observa en rojo en la Fig. 7. En el Release Notes de la versión R71 [8] se pueden encontrar las mejoras obtenidas con la actualización.

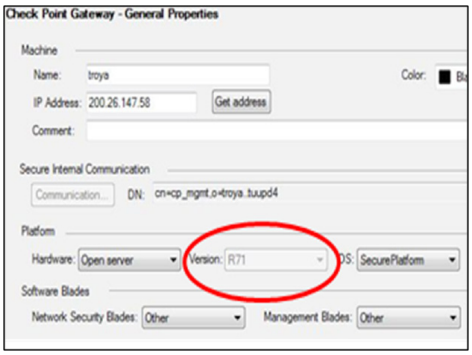


Fig. 7. Propiedades del Firewall StandAlone de la sede principal.

4.5. Pruebas de servicios y conectividad sobre la red

Estas son necesarias ya que garantizan que la actualización haya sido trasparente para toda la infraestructura de red y que nada resultase afectado. Se comprueba conectividad con las puertas de enlace, salida a Internet, acceso a las sucursales por el canal dedicado y a través de las VPNs que se observan en la topología de red.

4.6. Actualización de firmware sobre los firewall de Medellín, Cali y Barranquilla e integración con la central de administración principal

La librería sobre el SmartCenter es actualizada para soportar integración con el firmware a actualizar (8.0.37X), se migraron los firewall de manera remota de la versión 6.5.48x a la versión 8.0.37X, éstos fueron integrados con el fw principal a fin de instalar políticas y realizar la administración desde un único lugar.

Se verifican y crean los sets de políticas de cada sucursal, en la Fig. 8 se observa uno de ellos.

SOURCE	DESTINATION	VPN	SERVICE	ACTION
* Any	fwbarran	Any Traffic	* Any	drop
Red_Interna_Bar	* Any	Any Traffic	TCP http TCP https	accept
Red_Tecnofarma	Red_Interna_Bar	Any Traffic	* Any	accept
Servidores	Red_Interna_Bar	Any Traffic	* Any	accept
* Any	* Any	Any Traffic	* Any	drop

Fig. 8. Set de políticas de Barranquilla luego de la integración.

4.7. Implementación del firewall UTM-1 EDGE en zona franca

Debido a que la sucursal de zona franca se encuentra desprotegida y de frente a una red pública, se implementa un fw con la configuración mostrada en la tabla 3.

Tabla 3. Configuración de las interfaces del fw de zona franca.

INTERFACE	DIRECCION IP	MASCARA	DEFAULT GATEWAY
WAN (Internet)	192.168.9.6	255.255.255.0	192.168.9.1
lan (Red Local)	10.92.0.1	255.255.255.0	N/A

INTERFACE	DHCP SERVER	DNS
WAN (Internet)	N/A	200.14.207.210 200.26.137.100
lan (Red Local)	10.92.0.1 10.92.0.100	N/A

El fw es actualizado a la versión 8.037X y se integró satisfactoriamente con el SmartCenter para ser administrado desde la sede principal,

en donde se crea un set de reglas (Fig. 9) de acuerdo a las políticas de seguridad de la sucursal.

NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION
Regla Ping	Red_Tecnofarma	fwDHL	Any Traffic	icmp-requests https	accept
Stealth Rule	Any	fwDHL	Any Traffic	Any	drop
Navegacion	Red_Interna_DHL	Any	Any Traffic	https http FW1_topo IKE IKE_NAT_TRAVEL IKE_tcp IPSEC VPN1_IPSEC_enc	accept
Clean-up Rule	Any	Any	Any Traffic	Any	drop

Fig. 9. Set de políticas del fw implementado en zona franca.

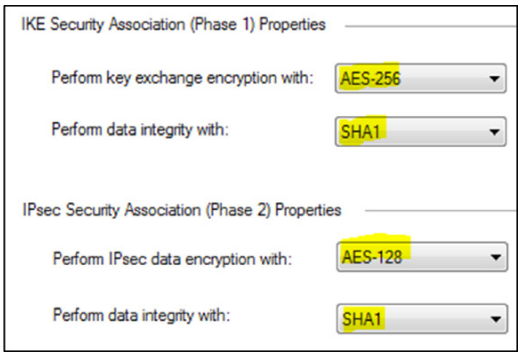


Fig. 10. Parámetros de encripción de la VPN con zona franca

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION
14	VPN DHL	Red_Tecnofarma Red_Interna_DHL	Red_Interna_DHL Red_Tecnofarma	vpnDHL	Any	accept
15	VPN DHL Servidores	Servidores Red_Interna_DHL	Red_Interna_DHL Servidores	vpnDHL	Any	accept

Fig. 11. Reglas de tráfico de la VPN.

4.8. VPN site-to-site entre el firewall de zona franca y el firewall de la sede central de la empresa

Es creada una comunidad de VPN cuyos miembros son "troya" y "fwDHL" con el fin de cifrar el tráfico entre zona franca y la sede principal. Se observan los parámetros de encripción de la fase I y II en la Fig. 10 y las reglas de tráfico en la Fig. 11.

4.9. Reconfiguración de firewalls de acuerdo al cambio de proveedor ISP

El cambio del proveedor del canal MPLS de TELMEX a ETB impacta las rutas que se ubican en el firewall de la sede principal, así que se procede a modificar la tabla de enrutamiento para cambiar las rutas asociadas con la IP 192.168.100.245 (Fig. 12 Izquierda) por la IP 192.168.100.2 (Fig. 12 Derecha).

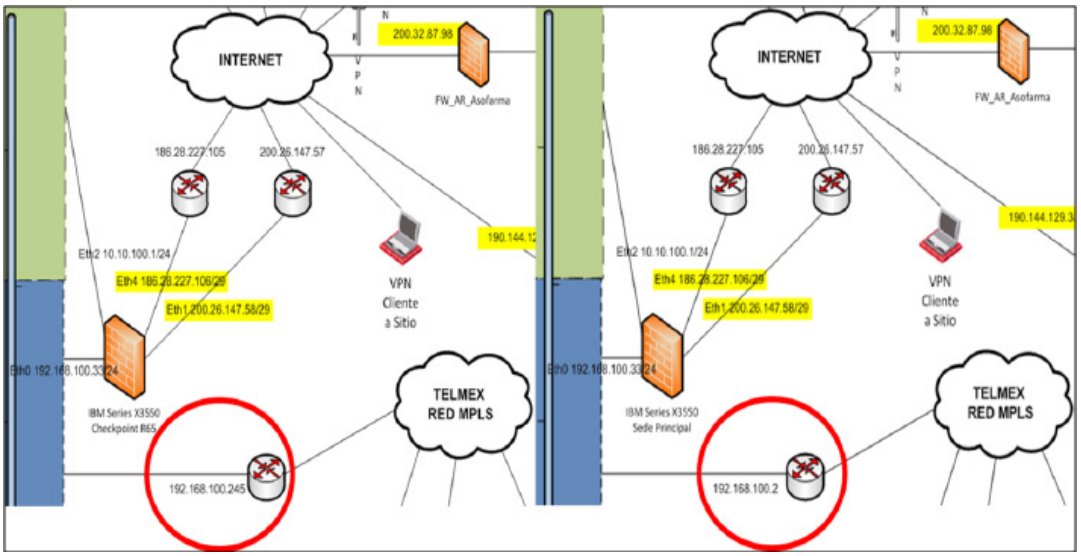


Fig. 12. Zoom de la topología actual (Izquierda) y futura (Derecha) respectivamente mostrando los cambios a realizar.

En la Fig. 13 se observa la tabla de enrutamiento resultante; y subrayado en rojo las rutas que se modifican.

192.168.7.0	192.168.100.2	255.255.255.0
192.168.100.0	0.0.0.0	255.255.255.0
72.246.25.0	186.28.227.105	255.255.255.0
10.10.100.0	0.0.0.0	255.255.255.0
192.168.5.0	192.168.100.2	255.255.255.0
204.2.241.0	186.28.227.105	255.255.255.0
96.16.98.0	186.28.227.105	255.255.255.0
96.17.106.0	186.28.227.105	255.255.255.0
192.168.3.0	192.168.100.2	255.255.255.0
74.125.67.0	186.28.227.105	255.255.255.0
12.148.220.0	186.28.227.105	255.255.255.0
200.41.9.0	186.28.227.105	255.255.255.0
10.10.200.0	192.168.100.13	255.255.255.0
172.168.3.0	192.168.100.2	255.255.255.0
172.168.5.0	192.168.100.2	255.255.255.0
72.14.253.0	186.28.227.105	255.255.255.0
172.168.7.0	192.168.100.2	255.255.255.0

Fig. 13. Rutas con la nueva puerta de enlace.

4.10. Balanceo de tráfico por los dos canales de ISP

Cuando es implementado un segundo canal WAN para la salida a Internet el administrador no cambia el default gateway del firewall si no que comienza a añadir rutas hacia segmentos de IPs públicas causando un detrimento en el performance del gateway por la tabla de enrutamiento. Por tal motivo se implementan resúmenes y se pasa de tener 44 rutas a tan sólo 18 y se utilizan los tres canales WAN para tráfico por Internet, hacia las VPNs y hacia las sucursales respectivamente.

En la Fig. 14 se observan las rutas finales sobre el firewall.

```
[Expert@troya]# netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask
200.124.203.114 200.26.147.57   255.255.255.255
200.80.170.133  200.26.147.57   255.255.255.255
200.32.87.98    200.26.147.57   255.255.255.255
216.139.247.207 200.26.147.57   255.255.255.255
200.55.7.250    200.26.147.57   255.255.255.255
186.28.227.104  0.0.0.0         255.255.255.248
200.26.147.56   0.0.0.0         255.255.255.248
192.168.7.0     192.168.100.2   255.255.255.0
192.168.100.0   0.0.0.0         255.255.255.0
10.10.100.0     0.0.0.0         255.255.255.0
192.168.5.0     192.168.100.2   255.255.255.0
192.168.3.0     192.168.100.2   255.255.255.0
10.10.200.0     192.168.100.13  255.255.255.0
172.168.3.0     192.168.100.2   255.255.255.0
172.168.5.0     192.168.100.2   255.255.255.0
172.168.7.0     192.168.100.2   255.255.255.0
127.0.0.0       0.0.0.0         255.0.0.0
0.0.0.0         186.28.227.105  0.0.0.0
```

Fig. 14. Rutas finales sobre el firewall.

5. ANALISIS DE MEJORAS Y RESULTADOS

5.1. Actualización de los firewalls de la sede principal y de las sucursales

La actualización del firewall principal presenta nuevas características o mejoras como se observa en el release notes [9] de la versión R71 comparado con la versión R65.

Como se puede observar (Fig. 15) las barras más extensas corresponden a 3 características que fueron mejoradas en la versión R71.

- El motor de IPS cambió de SmartDefense a IPS-1 permitiendo 10Gbps de throughput e incluso cuando todos los blades están activos, el throughput permanece sobre 2.2Gbps.
- Se mejora hasta 3 veces el rendimiento de fw y 4 veces el de IPS.
- La nueva arquitectura de antivirus mejora hasta 15 veces el throughput de éste blade.

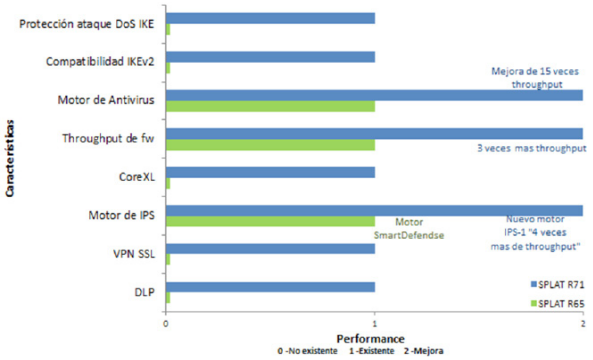


Fig. 15. Comparación de algunas características de la versión R65 y R71.

La actualización del firmware para los firewalls de las sucursales mejoraría en los siguientes aspectos según el Embedded NGX[10] de la versión 8.1.

- Mejora en el throughput de firewall
- Incrementa cantidad de conexiones (60000), túneles VPN (hasta 400), entre otros.

La escala evalúa tres niveles, la no existencia, la existencia o la mejora de las características

entre las dos versiones como se muestra en la Fig. 16.

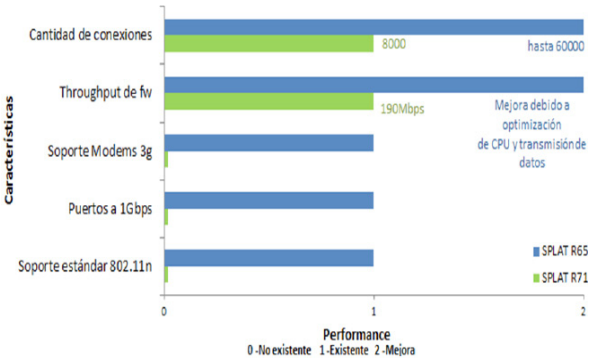


Fig. 16. Comparación de algunas características entre el firmware 6.5.47X y el 8.0.37X.

5.2. Implementación del nuevo fw en zona franca

Luego de ser implementado el firewall de zona franca y por la imposibilidad de realizar algún sniffer sobre el tráfico, sobre el Smartcenter (el cual es el que recibe los logs provenientes del firewall mencionado), se ubicó un script ejecutado con la utilidad "cron" de Linux para que se ejecutase cada 15 minutos durante 3 días y extrajera estadísticas de tráfico aceptado, perdido y total (tabla 4), obteniendo como resultado el gráfico de la Fig. 17.

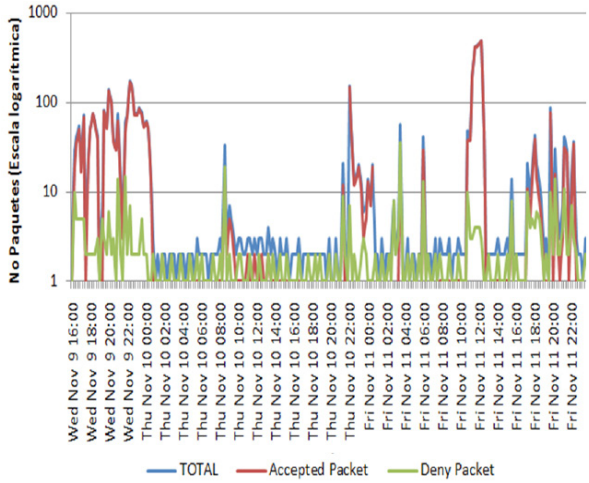


Fig. 17. Número de paquetes aceptados, dropeados y totales en escala logarítmica y en función del tiempo (cada 15 min).

Tabla 4. Estadísticas de tráfico.

Color	Nombre	Promedio	Mínimo	Máximo	Eje Y (Log10)	Unidades
	Total Packet	23,775785	1	488	1 - 1000	Packets/15 min
	Accepted Packet	21,26009	0	485	1 - 1000	Packets/15 min
	Deny Packet	2,5156951	1	36	1 - 1000	Packets/15 min

Relacionando el grafico 17 y la tabla 4, se concluye que el firewall efectivamente está brindando una protección a la sede y se está rigiendo por políticas de seguridad adecuadas.

5.3. Integración

La integración del SmartCenter con los firewall de Medellín, Cali, Barranquilla y la sede principal, simplificará significativamente las labores de administración del cliente ya que puede tener control sobre todos los corta fuegos en una sola interface y desde su computadora.

La Fig. 18 muestra el porcentaje de administración de la plataforma antes y después del proyecto, la cual se obtuvo en base a porcentajes que se establecieron según la importancia de la administración y configuración de políticas mostradas en la tabla 5.

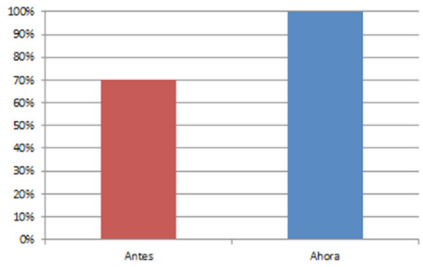


Fig. 18. Porcentaje de administración de los fw, antes y después de la actualización.

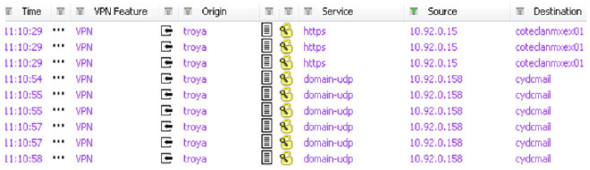
Tabla 5. Porcentaje asignado según la importancia de administración y configuración de políticas.

Firewall	%
Firewall Sede Principal	40%
Firewall Medellín	15%
Firewall Cali	15%
Firewall Barranquilla	15%
Firewall Zona Franca	15%

De acuerdo con los datos anteriormente mostrados existe una mejora del 30% en la administración de la infraestructura de seguridad de la red garantizando seguimiento e implementación de las políticas de seguridad que tiene la empresa.

5.4. VPN site to site

Con la creación de la VPN entre zona franca y la sede principal se garantizó la confidencialidad, integridad y autenticación de la comunicación gracias a los túneles VPN entre los firewalls logrando que difícilmente la información pueda ser leída sobre Internet. En la Fig. 19 se observan los registros de tráfico encriptado entre las dos sedes identificados por el "candado con llave".



Time	VPN Feature	Origin	Service	Source	Destination
11:10:29	VPN	troya	https	10.92.0.15	cotecdanmxex01
11:10:29	VPN	troya	https	10.92.0.15	cotecdanmxex01
11:10:29	VPN	troya	https	10.92.0.15	cotecdanmxex01
11:10:54	VPN	troya	domain-udp	10.92.0.158	cydcmail
11:10:55	VPN	troya	domain-udp	10.92.0.158	cydcmail
11:10:55	VPN	troya	domain-udp	10.92.0.158	cydcmail
11:10:57	VPN	troya	domain-udp	10.92.0.158	cydcmail
11:10:57	VPN	troya	domain-udp	10.92.0.158	cydcmail
11:10:58	VPN	troya	domain-udp	10.92.0.158	cydcmail

Fig. 19. Registro de tráfico encriptado desde la sede de zona franca hacia la sede principal.

6. CONCLUSIONES

- Se realizó una recopilación de lineamientos y mejores prácticas para implementar y/o actualizar infraestructuras de seguridad perimetral de cualquier característica.
- La actualización de los firewall permitió añadir algunas características y mejorar otras que en el futuro pueden ser utilizadas por el cliente.
- El UTM-1 Edge implementado en zona franca brindó protección perimetral a la sucursal por medio de políticas de seguridad instaladas desde la sede principal y un registro de eventos para el tráfico desde o hacia zona franca reduciendo así los riesgos y amenazas de seguridad.
- La integración de los firewalls garantizó una herramienta única de gestión para la infraestructura de seguridad perimetral ayudando al administrador de red a mejorar y simplificar su trabajo.
- Debido al alto precio de los canales dedicados, cada vez más se adopta el modelo de VPNs para la transmisión segura entre redes internas de la organización.
- Se redujo el número de rutas de 44 a tan sólo 18 aumentando el performance de la máquina.
- Se diseñó una topología de red antes y después de culminar el proyecto basándose en los datos obtenidos en el proceso de recolección de información y de la topología de red suministrada para plasmar así la red física de manera adecuada.
- Un proceso adecuado de recolección de información garantizó el éxito del proyecto. La información acerca de las interfaces, rutas, políticas de seguridad instaladas, VPNs y otras configuraciones de red fueron importantes para diseñar la topología de red, el plan de trabajo y la metodología del proyecto.

Referencias Bibliográficas

[1] C. Segura, La crisis y la administración de riesgos, [En línea], consultado en Febrero 13 de 2011, disponible en: http://seguraarmand.org/wordpress/?tag=administracion-de-riesgos.

[2] ACIS, Lista de empresas de seguridad informática, [En línea], consultado en Mayo 30 de 2011, disponible en: http://www.acis.org.co/index.php?id=778.

[3] ISACA, CISM Review manual 2008. Spanish edition: Isaca, ISBN: 193328496X, pp. 2, 2008.

[4] Wikipedia, Infraestructura de clave pública, [En línea], consultado en Junio 20, disponible en: http://es.wikipedia.org/wiki/Infraestructura_de_clave_p%C3%BAblica.

[5] GARTNER RAS Core research note

G00174908, Magic quadrant for enterprise network firewalls, Ed R71. USA, 2010.

[6] Check point software technologies LTDA, virtual private networks", Ed R71. USA, 2009, Caps 5-14-15, pp. 64, 303.

[7] Check point Software technologies LTD, "check coint security administrator R70/R71 – training manual, Ed R71. USA: checkpoint LTD, Cap 1-12, Pag 4-8, 379, 2010.

[8] Fortinet, fortios handbook V2 for fortiOS 4.0MR2, version 2. USA: Fortinet, pp. 184, 2010.

[9] Check point software technologies LTD, Releases notes R71, Ed R71, USA: Checkpoint LTD, pp. 23 2011,

[10] Check point software technologies LTD, "NGX embedded NGX 8.1, Releases notes general availability version, 2010.

[11] Checkpoint support center, performance analysis for security gateway NGX R65 / R7x [En línea], consultado en Julio 17 de 2010, disponible en: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk33781&js_peid=P-114a7bc3b09-10006&partition=General&product=Security