UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

INFORME

Informe sobre las actividades desempeñadas en el área de seguridad perimetral del Fondo de Información y Documentación para la Industria.

QUE PARA OBTENER EL TÍTULO DE
INGENIERO EN TELECOMUNICACIONES

PRESENTA:

JOSÉ FERNANDO FLORES MEDINA

DIRECTOR DE INFORME
ING. JESUS REYES GARCIA
CIUDAD UNIVERSITARIA

Índice.

Índice de figuras.

Informe sobre las actividades desempeñadas en el área de seguridad perimetral del Fondo de Información y Documentación para la Industria.

1. Objetivo.

El presente informe describirá las actividades que se realizan en el Área de Seguridad perimetral, en el Fondo de Información y Documentación para la Industria (INFOTEC), el cual dentro de sus principales funciones, brinda servicios de consultoría y desarrollo de soluciones tecnológicas para el sector público y privado.

Se abordan las siguientes temáticas:

- Los esquemas básicos que se utilizan para proporcionar seguridad en una red de datos.
- Las principales amenazas que se presentan a los recursos informáticos internos.
- Las mejores prácticas para lograr tener un nivel adecuado de seguridad.
- Las principales tecnologías que se pueden emplear para robustecer una red de datos.
- Una descripción de cómo administrar la seguridad perimetral, de acuerdo con las actividades que desempeñé.

Para la operación, administración y mantenimiento de los equipos perimetrales mencionados, se requiere tener conocimientos sólidos en cuanto al funcionamiento de las redes de datos, lo más importante es conocer cómo se transmite la información de un sitio a otro, los protocolos involucrados y las funciones que realiza cada uno de los dispositivos. Adicionalmente, se requieren conocimientos específicos, en este caso, de administración de seguridad perimetral, conocimiento sobre mejores prácticas, esquemas de defensa, tecnologías disponibles, vulnerabilidades, amenazas y explotaciones.

2. Introducción.

En 1990 se presentó una expansión considerable del acceso público a las redes de datos y de la comunicación circulante en las mismas. Debido a que facilitaron y agilizaron el intercambio de información entre múltiples usuarios, paralelamente también creció la dependencia en dichas redes, en la tecnología de cómputo y la necesidad de proteger los datos desde donde fuesen originados hasta sus destinos.

Actualmente diversas tecnologías realizan funciones que ayudan en la tarea de mitigar los riesgos de seguridad informática. El presente informe, aborda esta

cuestión desde una perspectiva de seguridad perimetral y muestra algunos de los dispositivos y procedimientos empleados en un ambiente real, los cuales son los más comúnmente empleados y pueden ser dados a conocer de manera pública.

La importancia de los dispositivos descritos en este informe, radica en su contribución a la protección de los datos y de los equipos de las infraestructuras ubicadas en el interior del perímetro que abarcan.

3. Marco teórico.

3.1 Clasificación de las redes de datos:

3.1.1 Redes públicas.

Llevan una gran cantidad de datos de manera insegura, los controles de seguridad son débiles, tal es el caso de redes que sólo requieren una contraseña para su acceso.

3.1.2 Redes semi-privadas (o zonas desmilitarizadas).

Son las redes que se ubican entre las redes públicas y las privadas, también conocidas como zonas desmilitarizadas (DMZ). Estas redes pueden llevar información confidencial bajo ciertas regulaciones.

3.1.3 Redes privadas.

Redes de organizaciones que llevan contenido confidencial y datos pertenecientes a algún propietario. Las redes privadas comúnmente tienen un direccionamiento exclusivo y no son compatibles con las redes públicas como Internet, por lo que se requiere una traducción de dirección para su interpretación.

3.2 Defensa del perímetro.

Las redes internas o privadas se componen de los siguientes bloques: servidores de aplicación, servidores proxy, servidores de datos, servidores de impresoras, servidores de correo, entre otros.

Para proteger estas unidades de procesamiento de datos, se requieren soluciones de seguridad a nivel de red (Figura 1. Defensa del perímetro), en conjunto con sistemas de seguridad basados en servidores. A nivel de red se pueden colocar firewalls en la terminal final de cada segmento de red, opcionalmente combinado con enrutadores que también implementen seguridad, lo anterior en defensa del perímetro.

Las zonas desmilitarizadas pueden ser colocadas alrededor de la periferia, mientras que en las fronteras de los ambientes de red, se pueden colocar aplicaciones proxy que también funcionarían como sistemas de defensa del perímetro.

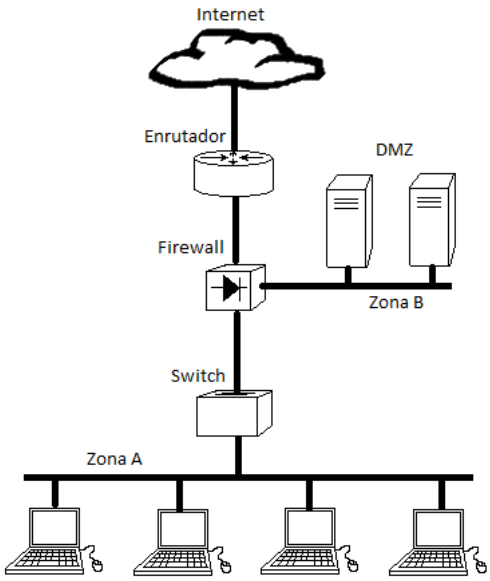

Figura 1. Defensa del perímetro

3.2.1 Diseño de sistemas y arquitecturas contra amenazas internas.

Se estima que los incidentes internos son más del 50% de los ataques, para mitigar estos se toman medidas de prevención y detección, tales como: métodos del menor privilegio y control de acceso, endurecimiento de los sistemas, redes anti-sniffing (resistentes al escaneo indebido de tráfico) y fuerte autenticación (en el primer caso); monitoreo de usuarios, redes y sistemas de detección de intrusos basados en red y en host (para el segundo caso).

3.2.2 Arquitectura y diseño.

Un sistema de monitoreo recolecta datos a través de sniffers, sistemas de detección y sistemas de prevención de intrusos, logs, además de recolectores dedicados para áreas específicas como web, correo electrónico y bases de datos.

3.2.3 Dispositivos de defensa.

- Firewalls.

“Pieza de software o hardware que actúa como barrera entre una red interna y una red externa”[1], por ejemplo Internet. Refuerzan el control de acceso por medio de políticas.

- Firewall de filtrado de paquetes.

Dispositivo que examina datos entrantes y salientes, comparándolos contra un conjunto de reglas que dependiendo de la acción que tengan configurada, los dejaran pasar o no a la red interna. Su operación es en las capas tres y cuatro del modelo OSI.

La información del protocolo que el paquete lleva, puede emplearse para aplicar un filtrado, o bien puede utilizarse la dirección origen y/o la dirección destino.

Su principal ventaja es la velocidad a la que se ejecutan las operaciones, en comparación con los otros tipos de firewall.

- Firewall de filtrado de paquetes stateful.

Estos equipos emplean técnicas de inspección de estado, utilizando una memoria dinámica que almacena las tablas de estado de las conexiones entrantes y las ya establecidas. Las técnicas usan control de datos de capas superiores y el protocolo TCP para el proceso de filtrado. Posterior a la validación de la conexión, los paquetes se envían con base en un conjunto de reglas definidas para la conexión particular.

- Firewall Proxy.

Trabajan en la capa siete del modelo OSI para su operación. La función proxy sustituye las conexiones terminales en un servicio orientado a conexión. Es decir, tanto los clientes como los servidores no se ven entre sí, sino que ven al proxy, lo cual da seguridad al dispositivo de la red local.

La principal desventaja es la velocidad de sus operaciones.

- Firewall personal.

Son firewalls basados en software, que son instalados en equipos de cómputo. Filtran ciertos paquetes para prevenir que éstos salgan o ingresen al sistema.

Son un complemento esencial de una solución de seguridad, pues los otros tipos de firewalls no previenen ataques generados en la red interna, mientras que éstos sí tienen capacidad de mitigarlos.

[1] Watkins, Michael; Wallace Kevin; CCNA Security; CISCO Press; USA, 2008. Page 323

- Sistema de Prevención de Intrusos (IPS).

Es una herramienta de seguridad encargada de monitorear los eventos que ocurren en una red. Busca intentos de intrusión, que tienen el objetivo de comprometer la confidencialidad, la integridad o disponibilidad de algún sistema informático, o bien de eludir los mecanismos de seguridad de éste.

El Sistema de Prevención de Intrusos, que funciona por medio de módulos, establece políticas de seguridad para proteger al equipo o la red de un ataque; protege reactivamente.

El IPS tiene la habilidad de bloquear inmediatamente las intrusiones, sin importar el protocolo de transporte utilizado y sin reconfigurar un dispositivo externo. Esto significa que el IPS puede filtrar y bloquear paquetes en modo nativo (al utilizar técnicas como la caída de una conexión, la caída de paquetes ofensivos, el bloqueo de un intruso, etc.).

Cabe mencionar que el tráfico inspeccionado por lo general es unidireccional, es decir, únicamente se analiza tráfico desde el exterior (Internet) a la red interna (Red de Área Local).

Básicamente el dispositivo IPS funciona de dos formas: comparando el tráfico circulante contra firmas de ataques conocidos y comparando el patrón de comportamiento del tráfico contra patrones configurados por los administradores como tráfico normal.

En el primer caso, las firmas o vacunas (término que depende del fabricante) son continuamente proporcionadas por el proveedor del equipo, siendo tarea de los administradores y del comité de gestión de seguridad de la información[2], el seleccionar las adecuadas para proteger la red de datos.

En el caso del fabricante FORTINET, las firmas son agrupadas dentro de un sensor, que posteriormente se agrupa junto con otros sensores en un perfil. El perfil se ubicará en las políticas que así lo requieran.

En el caso del fabricante HP, las firmas son agrupadas directamente en un perfil de protección. El perfil se aplicará sobre los segmentos que correspondan. Adicionalmente, pueden configurarse políticas de respuesta.

Genéricamente, el IPS proveerá: protección a aplicaciones, protección a la infraestructura, protección al desempeño de la red, al desempeño de sistemas y gestión del tráfico.

[2] De acuerdo con las recomendaciones del estándar ISO/IEC 17799:2005 Information technology. Code of practice for information security management

- Solución de seguridad UTM.

Unified Threat Management es la solución más moderna para enfrentar amenazas contra los dispositivos y aplicaciones.

Anteriormente la integración de todos los elementos para proporcionar seguridad en una red de datos aumentaba el costo y la complejidad de la misma. Ya que todos los dispositivos debían contener configuraciones acordes entre sí, el hecho de no cumplir este punto, creaba inevitablemente puntos ciegos.

En otras palabras, la aproximación tradicional no podía enfrentar las más recientes amenazas, dejando a las organizaciones vulnerables.

Con la proliferación de dispositivos capaces de conectarse a la red de datos prácticamente en cualquier lugar y momento, tales como las nuevas tabletas electrónicas y los teléfonos inteligentes, surge una nueva necesidad de poder dar acceso a estos de una manera segura y controlada. Anteriormente simplemente se les negaba el acceso a estos relativamente nuevos equipos, pero considerando la cantidad actual, la demanda que representan en cuanto al uso de recursos y el hecho de que pueden agilizar operaciones y eficientar procesos de las empresas, sencillamente ya no podía emplearse el viejo método prohibitivo.

UTM es la nueva aproximación de seguridad que hace posible conectarse en cualquier lugar y en cualquier momento, garantizando seguridad tanto para los dispositivos que se conectan, como para todos los recursos dentro de la red local.
UTM está diseñado para lidiar mejor contra las nuevas amenazas, tales como:

- El acceso indebido a sitios web por parte de los usuarios internos, ya sea porque son seducidos al presentárseles motivaciones como premios o porque quieren consultar un tema de moda en algún sitio. La amenaza consiste en que el usuario puede ser redirigido a un sitio maligno en el que el código HTTP que descargue sea malicioso.
- Ser víctima del software malintencionado “Rasomware”, el cual cifrará archivos esenciales para la operación del sistema, pudiendo descifrarlos únicamente pagándole a los atacantes una suma de dinero, para obtener las llaves correspondientes.
- Amenaza “form injection”, que consiste en la inyección de preguntas y campos en una sesión de navegación, las cuales parecen ser parte de un formulario de preguntas reales del sitio al que accedieron.

UTM logra proteger contra todas las amenazas listadas, al contar con una capacidad de inspección a contenidos de paquetes más eficiente que las tecnologías precedentes “stand-alone”.

UTM implementa algoritmos especializados, encargados de identificar el tipo de tráfico que circula en la red, independientemente del puerto en capa 4 por el que se establece la comunicación.

El dispositivo basado en la tecnología UTM puede actuar como un servidor "proxy", para revisar que los paquetes cumplan con las políticas aplicables, antes de ser reenviados.
UTM al proveer una solución de seguridad integral, permite tener una visibilidad holística sobre el perímetro, una gestión más rápida, un impacto de la latencia menor y adicionalmente reduce los gastos de operación de las empresas.

Los equipos del fabricante líder en el mercado de la seguridad, FORTINET, dan una defensa efectiva multi-capas combinada en un solo dispositivo. Gracias a su procesador de red que trabaja a nivel de interfaz, se revisan patrones contenidos en el tráfico a una alta velocidad; gracias a su procesador de seguridad, se combaten las múltiples amenazas; el procesador de propósito general, entre otras funciones hace el análisis posterior del grupo de datos, puede elegir entre enviarlos al destino correspondiente o hacer que los paquetes pasen a través del procesador de contenido; ya que dicho procesador de contenido no está en línea, éste solamente funcionará en aquel tráfico que realmente lo necesite, analizando los objetos contenidos en el flujo de datos por medio de un reconocimiento de protocolos contra las amenazas conocidas.

Los equipos del fabricante FORTINET, proporcionan lo siguiente:

1. Control de aplicación.

   Identifican y controlan aplicaciones, programas, servicios de red y protocolos. Adicionalmente pueden proporcionar prioridades a algunas aplicaciones haciendo uso de la funcionalidad "trafic shaping". Las aplicaciones son permitidas, monitoreadas o bloqueadas en la puerta de enlace.

2. Sistema de prevención de intrusos.

   Como se describe en párrafos anteriores, se emplean técnicas de comparación del tráfico contra firmas y de acuerdo con comportamiento que presentan.
   Una funcionalidad extra muy útil, es el hecho de poder configurar un brazo del dispositivo (interface física o lógica) como detector de intrusos.

3. Filtrado de contenido Web.

   Restringen la visibilidad del usuario hacia el exterior, reduciendo la exposición a spyware, phishing, pharming, sitios inapropiados y sitios que redirigen a otros que son inseguros.

4. Antispam.

   Detección de amenazas empleando técnicas como listas de direcciones IP, URL, funciones hash sobre los mensajes para su posterior comparación, revisión del nombre de dominio (DNS lookup), revisión en relación a si contienen palabras prohibidas (banned) o patrones prohibidos.

5. Prevención de pérdida de datos.

   Previene que los datos sensibles para una organización sean transferidos intencional o inintencionalmente, comparando lo que se envíe desde el interior con cadenas de texto y patrones definidos por el administrador de la red, de tal manera que si se localizan dichas cadenas o patrones, el equipo los bloquea.

6. Antivirus.

   Emplean bases de datos con firmas de virus y patrones de archivos, en caso de que una infección se detecte, los archivos son borrados o puestos en cuarentena según se ha configurado el equipo, además de que notificara al usuario.

7. Firewall.

   También se incluye la funcionalidad de un firewall en la solución de seguridad.

8. VPN.

   El dispositivo es compatible para implementar redes privadas virtuales.

- VPN IPsec

IPsec es un conjunto de protocolos y servicios usados para cifrar datos, proporciona autentificación, confidencialidad e integridad. Trabaja en la capa tres del modelo OSI.

Los paquetes son encapsulados dentro de paquetes IPsec.

La arquitectura, usa asociaciones de seguridad como la base para la construcción de funciones de seguridad dentro del protocolo de Internet. La asociación de seguridad es un conjunto de algoritmos y parámetros usados para separar y autenticar los datos circulantes. Dentro de ésta última dos equipos acuerdan la manera en que los datos serán intercambiados y protegidos.

La técnica de intercambio de llaves (IKE), permite a dos partes envueltas en una transacción, establecer la asociación de seguridad. Esta técnica posee dos fases:

Fase 1. Auténtica a las partes involucradas y establece un canal seguro para el intercambio de la llave.
Fase 2. Negocia los parámetros para definir el túnel IPsec.

La fase 1, desarrolla un intercambio de llave Diffie- Hellamn. Esta llave es la utilizada para negociar los parámetros de la fase 2.
Existen dos modos de funcionamiento de la fase 1:

Main mode. Desarrolla tres intercambios de dos vías entre la parte que inicia la comunicación y el receptor.

Aggressive mode. Desarrolla tres intercambios de una vía, siendo en uno de éstos en donde se comparten parámetros para la fase 1, es un intercambio de información no cifrada.

Se recomienda el modo “Aggressive” cuando la dirección IP de alguna de las partes y sólo en alguna de ellas, se le asigna de manera dinámica.

La fase 2, realiza la negociación de los parámetros IPsec a través del túnel de la fase uno. Los parámetros son renegociados regularmente, pudiendo configurarse para mayor protección un intercambio Diffie-Hellman.

La fase dos opera solamente con el modo “Quick mode”. Éste se encarga de renovar las variables que utiliza el algoritmo Diffie-Hellman en la fase 1.

Tipos de VPN por protocolo IPsec.

1. VPN basada en rutas.

Se crea de manera local una interface virtual IPsec, la cual aplica cifrado y descifrado al tráfico que la atraviesa. Funciona a través de dos políticas entre la interface virtual IPsec y la interface física o virtual de la subred.

2. VPN basada en políticas.

Funciona con una sola política que soporta tráfico bidireccional.

Topologías de VPN en uso del protocolo IPsec.

1. Sitio a sitio (gateway a gateway).

Dos unidades compatibles, crean un túnel VPN entre dos subredes con segmento privado.

2. Dialup-Client.

A diferencia de la topología sitio a sitio, ésta no depende de la dirección IP del Gateway para establecer el túnel de la fase 1.

El cliente de VPN es un software empleado en el host para el establecimiento de comunicaciones privadas de forma virtual. El cliente cifra el tráfico IP y direcciona los paquetes a la interface pública del Gateway.

4. Definición del problema o contexto de la participación profesional.

Administrar, operar y mantener las arquitecturas de redes de datos, de los diversos clientes de la organización y de la propia organización, a los cuales se les provee de seguridad a nivel perimetral.

Con el objetivo de proteger el perímetro de las redes internas, se emplean dispositivos de propósito específico, tales como IPS y firewalls, cuyas configuraciones deben ser coordinadas con las de otros equipos como conmutadores, enrutadores y computadoras, de tal forma que en conjunto construyan una arquitectura acorde a la estrategia de defensa a profundidad.

5. Análisis y metodología empleada.

Como primer paso para proporcionar la administración, operación y mantenimiento adecuados de una solución de seguridad perimetral, realicé en conjunto con mis compañeros de área, el análisis correspondiente para conocer la red y el tráfico que en ésta fluye, posibilitando el mantener un estrecho control sobre los dispositivos de control de acceso.

Una vez contando con la información sobre la arquitectura y diseño, trabajé en equipo con mis compañeros de área, para establecer una línea base de operación normal, de la cual se acordó qué tipo de desviaciones serían sometidas a investigación, ya que dichas desviaciones pudiesen ser indicios de un intento de explotación, o bien indicar sistemas comprometidos.

Con el sistema de monitoreo con servidores de logs, analicé la utilización de protocolos, la actividad web, la actividad de correo electrónico, el uso de los datos en las bases de datos, así como también la actividad de los equipos como computadoras de escritorio y portátiles (Figura 2. Diagrama genérico de solución de seguridad).

Lo anterior se aplicó a nivel de organización y a nivel de usuarios de manera individual.

Para garantizar el acceso físico no autorizado a equipos, aproveché el apoyo del personal del centro de datos, el cual se encarga del monitoreo de las cámaras de seguridad, logrando con lo anterior, que los dispositivos y datos importantes no salgan de la organización sin autorización.

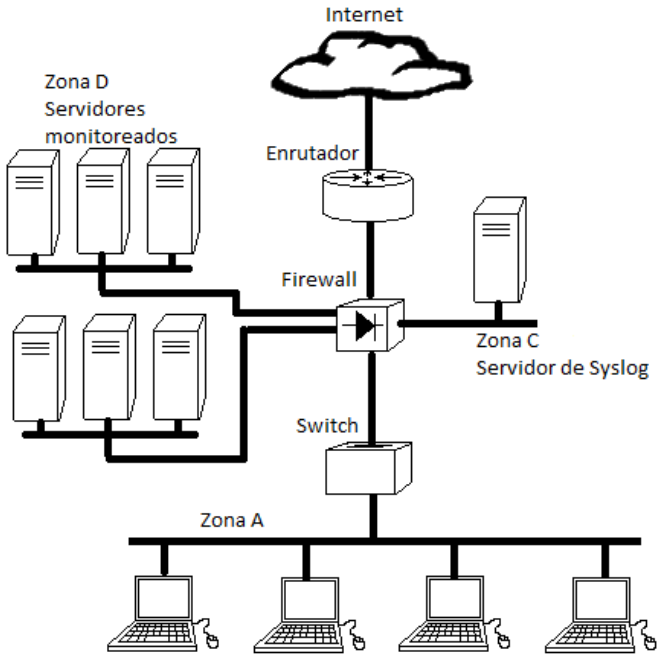

Figura 2. Diagrama genérico de solución de seguridad.

Ya que se tuvo que analizar una gran cantidad de datos, empleé programas de cómputo especializados para correlacionar eventos y generar reportes, estos últimos siendo componentes importantes de la administración.

El sistema de prevención de intrusos (IPS), proporcionó seguridad a ataques comunes como el análisis de vulnerabilidades, denegación de servicio, spam y escaneo de la red interna.

Ya que estos sistemas modifican el control de acceso de los conjuntos de reglas de manera automática, continuamente monitoreé la consistencia de permisos entre todos los equipos de seguridad perimetral, evitando así generación de falsos positivos.

Los conjuntos de reglas fueron evaluados constantemente, para la verificación de su equiparabilidad entre sí, errores y la plena integridad de los dispositivos. Además de que también apoyé en mantener documentada la configuración de los equipos, los cambios que se les realizaron y sus respaldos.

5.1 Sobre la implementación.

Como práctica para la correcta operación, analicé y comprendí el por qué los diseñadores eligieron dentro de la gama de tecnologías disponibles con sus

respectivas variantes, los dispositivos que finalmente fueron implementados. A continuación se detalla dicho análisis:

5.1.1 Firewalls.

Ya que la mayoría del software a la venta y gratuito, no tiene características optimizadas para la seguridad, se presentan vulnerabilidades inevitablemente en la mayoría de las redes. Es por ello que la organización optó por el empleo de firewalls.

Con estos equipos es posible evitar por ejemplo: ataques de spoofing, en los cuales se falsifica una dirección IP; además de ataques de escaneo y crackers en los que se encuentran vulnerabilidades y datos sensibles, para posteriormente romper contraseñas.

También son útiles cuando se manejan aplicaciones con pobre autentificación, es decir, aplicaciones que por sí mismas no pueden distinguir entre usuarios legítimos e ilegítimos.

Los anteriores son problemas comunes en casi todas las redes de datos, ya que son imputables a los fabricantes.

Al comienzo, la red implementada operaba con firewalls “stateful- packet filter” del fabricante CISCO, ya que éstos eran fáciles de desplegar como solución integral de seguridad para “firewall, comunicaciones unificadas (voz y video) seguras, redes privadas virtuales (SSL e IPsec) y sistemas de prevención de intrusos.[3]
Aprovechando las ventajas que ofrece al operar en las capas 3, 4 y 5 del modelo OSI, mantiene un rastreo de las conexiones, supervisando códigos SYN, RST, ACK y FIN en los encabezados.

Por otra parte, no todos los protocolos son stateful, por lo que no pueden ser monitoreados por ejemplo UDP e ICMP.
Las mayores desventajas de esta generación de equipos, son el contar con un filtrado de contenido muy simple, no proporcionando protección adecuada contra la mayoría de los componentes maliciosos de ciertos programas y el no contar con un escáner de virus.

Las limitaciones de estos firewalls respecto a las tecnologías de nueva generación, convirtieron en una necesidad la migración de los dispositivos en operación por sus contrapartes más modernas.

En el caso de los firewall CISCO 5520, se utiliza la característica de inspección de protocolos de aplicaciones.

[3] Watkins, Michael; Wallace Kevin.CCNA Security. CISCO Press.USA, 2008. Page 326

Se recomienda usar dicha característica en las siguientes circunstancias:

1. Cuando existen aplicaciones que abren puertos secundarios TCP y/o UDP. Es decir, la sesión inicial se establece en un puerto conocido y posteriormente se abren otros de manera dinámica como parte de ésta.

2. Cuando existen aplicaciones que incrustan una dirección IP dentro de un paquete, con el objetivo de que el equipo al que el paquete está dirigido, pueda comunicarse con el que tiene la dirección incrustada. Sin embargo, la dirección es de un segmento interno e inaccesible desde la red pública si no hay una traducción.

5.1.2 Intrusion Prevention System.

Principalmente se emplearon los IPS para prevenir el lanzamiento de ataques exitosos, siendo útiles los métodos de detección de anomalías y el del mal uso de los recursos de red. Evitan la realización de comunicaciones a través de puertos estandarizados por la IANA que no corresponden, es decir, que tratan de llevar tráfico sobre un determinado puerto que debería transportarse en otro, la mayor parte de las veces se presentan estos casos cuando el tráfico es malintencionado. Gracias al nivel de generación de logs en estos equipos, se puede realizar un análisis para prevenir futuros ataques, ya que se pueden detectar vulnerabilidades pasadas desapercibidas al momento de la implementación, o bien, llevar un estudio estadístico.

Otra de las razones por las que se implementaron estos dispositivos, fue para el desarrollo de casos forenses.

Como parte del esquema de defensa profundidad, cada una de las implementaciones consideran un enrutador capaz de descartar paquetes del exterior, un firewall que controlará el estado de las sesiones, redundancia en la topología para alta disponibilidad, el firewall personal de cada equipo y su software antivirus. Siendo todo lo anterior actualizado constantemente, dependiendo de las indicaciones de los fabricantes.

5.1.3 UTM.

Se realizó una migración de dispositivos tradicionales, a aquellos que implementan las tecnologías unificadas (UTM).

Estos nuevos equipos se emplearon como una solución integral de seguridad, complementados con los IPS anteriormente descritos, con la finalidad de robustecer aún más el perímetro.

Gracias a su versatilidad, se mejoró la administración en lo que respecta a seguridad perimetral, debido a que al estar integradas todas las funcionalidades mencionadas en un sólo equipo, no se realiza un reproceso innecesario de los paquetes, ya que todos los módulos tienen conocimiento sobre lo que realizaron los demás.

Se emplearon los dos tipos de redes privadas virtuales compatibles: SSL e IPsec. En el primer caso, se aprovechó la ventaja de poder accesar a los mismos recursos de la red, en comparación a si la conexión fuera bajo el protocolo IPsec, sin embargo evitando la necesidad de tener que hacer configuraciones muy extensas; para el segundo caso, empleándolas únicamente para comunicaciones de red local a red local (Site-to-Site).

5.1.4 Control de acceso.

Empleando una topología de control de acceso a la red como la mostrada a continuación (Figura 3. Control de acceso), los diversos dispositivos como conmutadores, routers y firewalls, mantienen una comunicación directa con el servidor de autenticación ACS (Access Control Server), el cual trabaja con el protocolo TACACS+ (Terminal Access Controller Access Control System). Gracias a este servidor, todas las peticiones para ingresar a todos los equipos con fines administrativos, deben ser analizadas y aceptadas únicamente por éste.

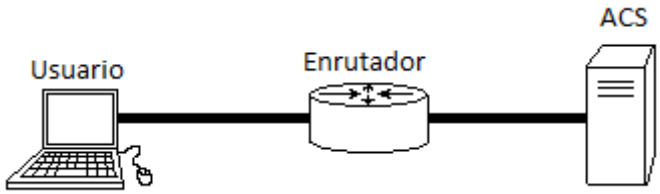

Figura 3. Control de acceso

Además de seguridad, se garantiza una administración más simple, ya que el servidor contiene una base de datos general y centralizada para todos los administradores y sus privilegios, en lugar de que en cada dispositivo se deban guardar en memoria a todos los administradores.

Por otra parte, el servidor puede guardar todos los comandos ejecutados por un usuario durante una sesión, lo cual robustece la seguridad de la red al poder saber los cambios hechos en las configuraciones de los diversos dispositivos, conociendo quién los realizó y cuándo.

En una solución de seguridad que cuenta con múltiples capas de control de acceso, es complicado el mantener consistente la configuración de los equipos involucrados. Teniendo sólo una, se tiene un mejor control sobre la infraestructura y se eliminan agujeros de seguridad.

VPN.

Con la finalidad de tener acceso remoto a los diversos recursos internos de la red de datos, siendo éste de manera segura y confiable, se configuraron redes privadas virtuales (VPN).

Realicé las configuraciones sitio a sitio para ciertos clientes, entre su infraestructura y la de los administradores.

Por otra parte, configuré las conexiones VPN entre los administradores y las infraestructuras, empleando un concentrador de VPN al cual se conectan los clientes para autenticarse en el servidor TACACS+, pudiendo entonces ser enrutados con una dirección IP virtual hacia dichas infraestructuras.

En esta situación, la topología operante entre los clientes de VPN y el concentrador es “dialup-client”.

6. Participación profesional

Administré, operé y brindé mantenimiento a la infraestructura implementada de firewalls basada en zonas, manteniendo un control estricto sobre la comunicación entre éstas, monitoreando el tráfico UDP, ICMP y las sesiones TCP. Apliqué inspección de paquetes en protocolos de capa tres y capa siete. Proporcioné seguimiento y cumplimiento a las políticas de la organización y clientes, las cuales competen a la seguridad perimetral, asegurando los siguientes puntos:

- Denegación de todo el tráfico excepto lo absolutamente indispensable para el funcionamiento de las organizaciones.
- Uso del principio de menor privilegio, garantizando que los usuarios contarán solamente con los privilegios necesarios para realizar sus actividades.
- Obtención de listas de protocolos requeridos para la operación de las organizaciones.
- Cumplimiento de la estrategia de registro de actividades (“logging”) en el nivel y tipo adecuados.
- Establecimiento de límites de conexión de acuerdo con las necesidades de cada organización.

Realicé configuraciones de acceso en firewalls, con el objetivo de filtrar paquetes de los protocolos IP, TCP y/o UDP. Lo anterior de acuerdo con los requerimientos del cliente y su política de seguridad de la información.
De manera frecuente, llevé a cabo las configuraciones que a continuación se ejemplifican.

6.1 Configuraciones básicas en equipos firewall.

6.1.1 Procedimiento de creación de una política en el firewall Juniper con Firmware versión 6.1.0r4.0 para sistemas operativos ScreenOS.

- Creación de los objetos que requerirá la política, éstos pueden ser de servicios o de direcciones IP. En caso de ser más de un servicio o dirección, deberá crearse también un grupo.

La manera más sencilla (ejemplificada) para hacerlo, es empleando la interface web que proporcionan los dispositivos mismos.

Para un objeto simple de dirección IP, se seleccionan en el panel de navegación las siguientes opciones: Policy > Policy Elements > Addresses > List

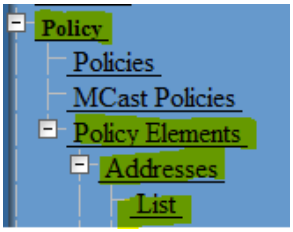

Figura 4. Menú para la creación de un objeto de dirección IP.

En el listado de objetos presentado, se elige la opción New en la esquina superior derecha, lo cual desplegará lo siguiente:

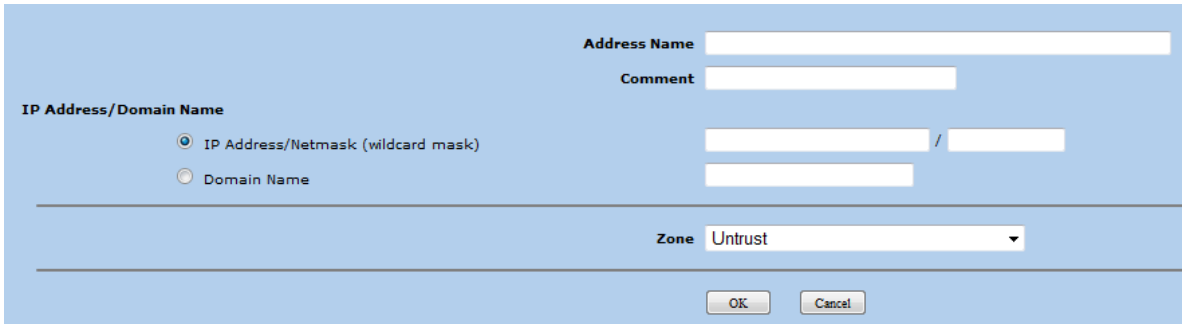

Figura 5. Creación de un objeto de dirección IP.

El llenado de los campos se describe a continuación:

- Se coloca el nombre del objeto.
- Se coloca de manera opcional un comentario referente al objeto.
- Se colocan los octetos de la dirección IP.
- Se selecciona si es una dirección o bien un nombre de dominio.
  - En el primer caso se coloca la dirección y máscara en formato abreviado, o se coloca un rango por wildcard.
  - En el segundo caso se coloca el nombre de dominio.

- Se elige la Zona correspondiente.
- Se presiona la opción “OK” o “Cancel”.

Para un objeto simple de servicios, se seleccionan en el panel de navegación las siguientes opciones: Policy > Policy Elements > Services > Predefined o Custom.

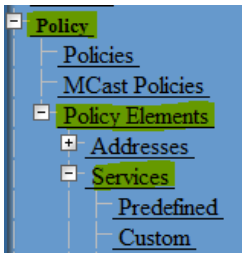

Figura 6. Menú para la creación de un objeto de servicio.

Si es elegida la opción “Predefined”, se pueden editar los objetos de servicios que el firmware contiene por default (los más comúnmente utilizados). Para lo anterior se presiona “Edit”.

Si se selecciona la opción “Custom”, se pueden crear objetos de servicios completamente nuevos. Para esta actividad, se presiona “New”.

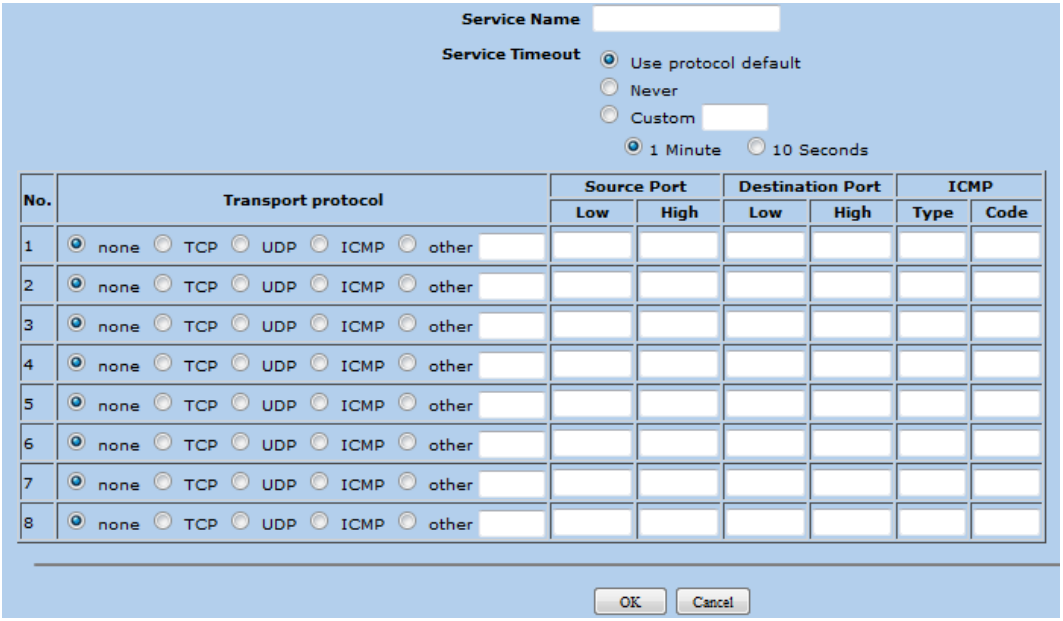

Figura 7. Creación de un objeto de servicio.

Los campos se llenan de la siguiente manera:

- Se coloca un nombre para el objeto.
- Se elige el tiempo que se mantendrá la sesión o conexión.
  - Usar el predeterminado de acuerdo al protocolo, TCP 30 minutos y UDP 1 minuto.
  - Sin tiempo límite.

- Personalizado en minutos o segundos (la cantidad colocada se multiplica por 1 o 10 dependiendo).

- Se selecciona el o los protocolos de transporte, así como también los rangos de puertos de origen y destino.
  - None, ignora el renglón de campos; TCP; UDP; other para aplicaciones especiales hechas a la medida para ciertas empresas.
- Se presiona la opción “OK” o “Cancel”.

- Agrupación de objetos.

Teniendo listos los objetos, se pueden agrupar en caso de ser necesarios. Es común agruparlos para una mejor administración de las políticas, pues un nombre adecuado puede identificar a varios objetos, incluso es posible hacer grupos que contengan grupos y/o objetos.

Para agrupar objetos de direcciones IP, es necesario seguir los siguientes pasos:
Elegir del panel de navegación: Policy > Policy Elements > Groups

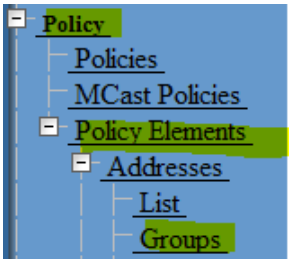

Figura 8. Menú para la creación de un grupo de direcciones IP.

Seleccionar la opción “New”.

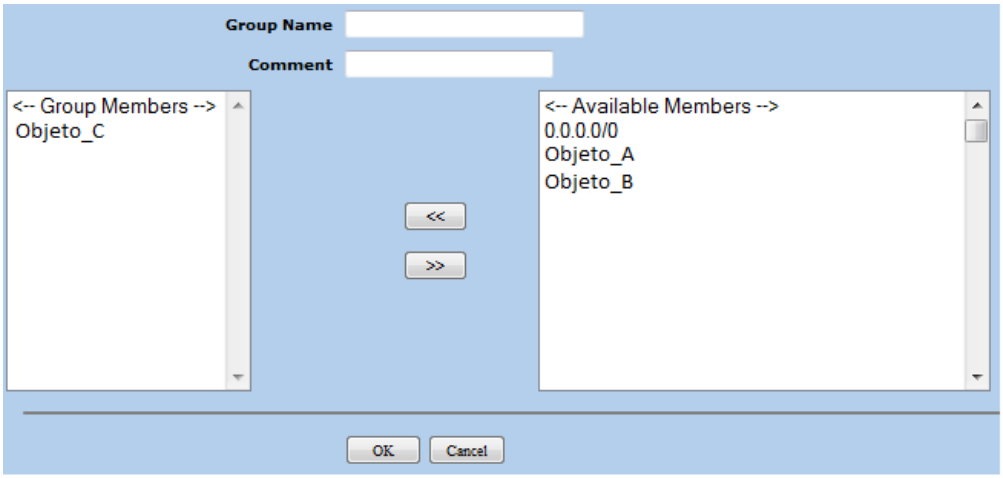

Figura 9. Creación de un grupo de direcciones IP.

- En el primer campo se coloca un nombre referente a los objetos que se agruparán.

- En el segundo campo, opcionalmente se coloca un comentario.
- De la lista derecha de objetos disponibles, se seleccionan los adecuados y presionando el botón virtual “<<” se mueven a la lista de objetos en el grupo.
- Se presiona la opción “OK” o “Cancel”.

El proceso para hacer un grupo de servicios es muy similar, solamente que los Objeto_A, Objeto_B y Objeto_C son servicios y no direcciones o rangos de direcciones.
Finalizando lo anterior, es posible crear la política.

- Políticas de acceso.

En Policy > Policies:

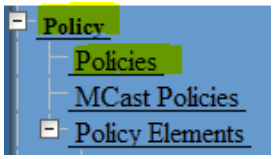

Figura 10. Menú para la creación de una política de acceso.

Se eligen las zonas correspondientes entre las que se requiere una comunicación controlada. Se selecciona “New” en la esquina superior derecha.

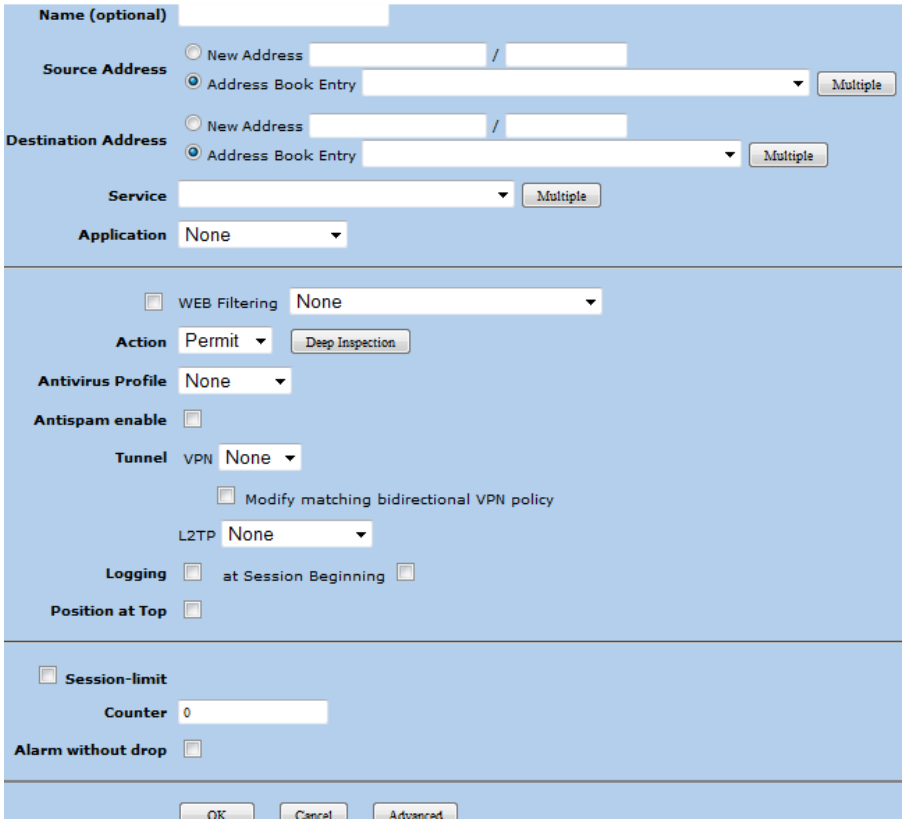

Figura 11. Creación de una política de acceso.

- En el primer campo se coloca un nombre referente a la política.
- Se elige si el origen será una nueva dirección IP, alguna de las existentes o un grupo existente.

    Para el primer caso sería notación abreviada.

    Para el segundo se presiona “Multiple”.

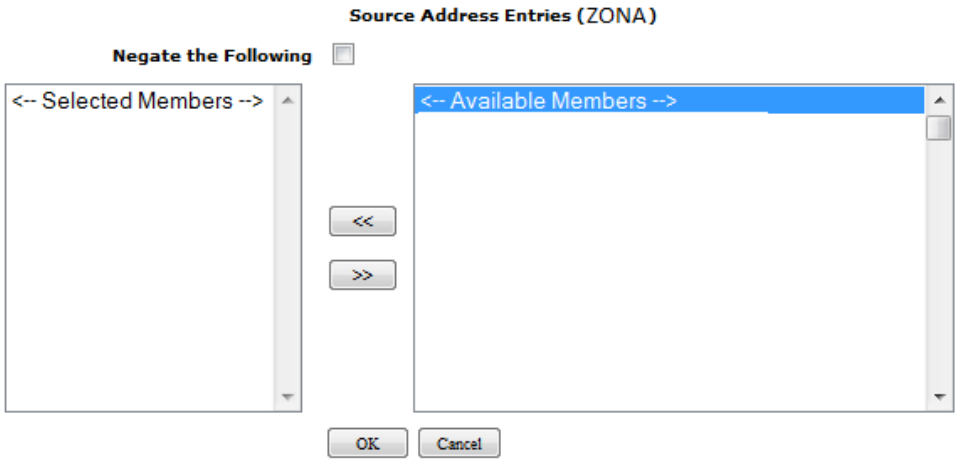

Figura 12. Elección de direcciones IP para una política de acceso.

- Se pueden agregar objetos seleccionándolos y moviéndolos, o si se palomea el “ckeckbox” “Negate the Following”, se agregan todos los objetos excepto los explícitamente seleccionados de la lista.
- Para el destino, se realiza exactamente lo mismo, se agrega una dirección nueva o se usan las ya existentes presionando la opción “Multiple” en “Destination Address”.
- En “Service”, se eligen los objetos de servicios.
- En “Aplication”, opcionalmente se puede elegir alguna de las aplicaciones más comúnmente utilizadas como SQLNET.
- Posteriormente se puede aplicar algún tipo de filtrado web por URL.
- La Acción puede ser “Permit” o “Deny”.
- Se puede aplicar opcionalmente un perfil de antivirus, dicho perfil contiene modos de escaneo para FTP, HTTP, IMAP, POP3, SMTP e IM.

    Permite hacer un escaneo a todo el tráfico, a una parte del tráfico que contenga archivos de un tipo específico o escaneo inteligente (analizando la carga de los paquetes).
- Se puede seleccionar la opción “Antispam”, cuyo perfil contiene una lista blanca con dominios seguros y una lista negra con dominios inseguros.
- Se puede indicar si la comunicación será realizada a través de un túnel VPN, o túnel L2TP.
- La opción “Logging”, permite tener un histórico del tráfico recibido por el firewall.

- Se puede escoger un límite en tiempo para las sesiones y/o un límite en cantidad de sesiones por dirección origen. Puede elegirse que el equipo envíe una alarma, pero no termine la sesión en “Alarm without drop”.
- Se presiona la opción “OK” o “Cancel”.

La parte de opciones Avanzadas, es para la aplicación de una traducción de dirección (NAT), pudiendo ser de manera una a una, o una a varias con un pool de direcciones. También es para aplicar autenticación de usuarios o grupos de usuarios; aplicar prioridades y un ancho de banda máximo y/o garantizado; entre otras opciones.

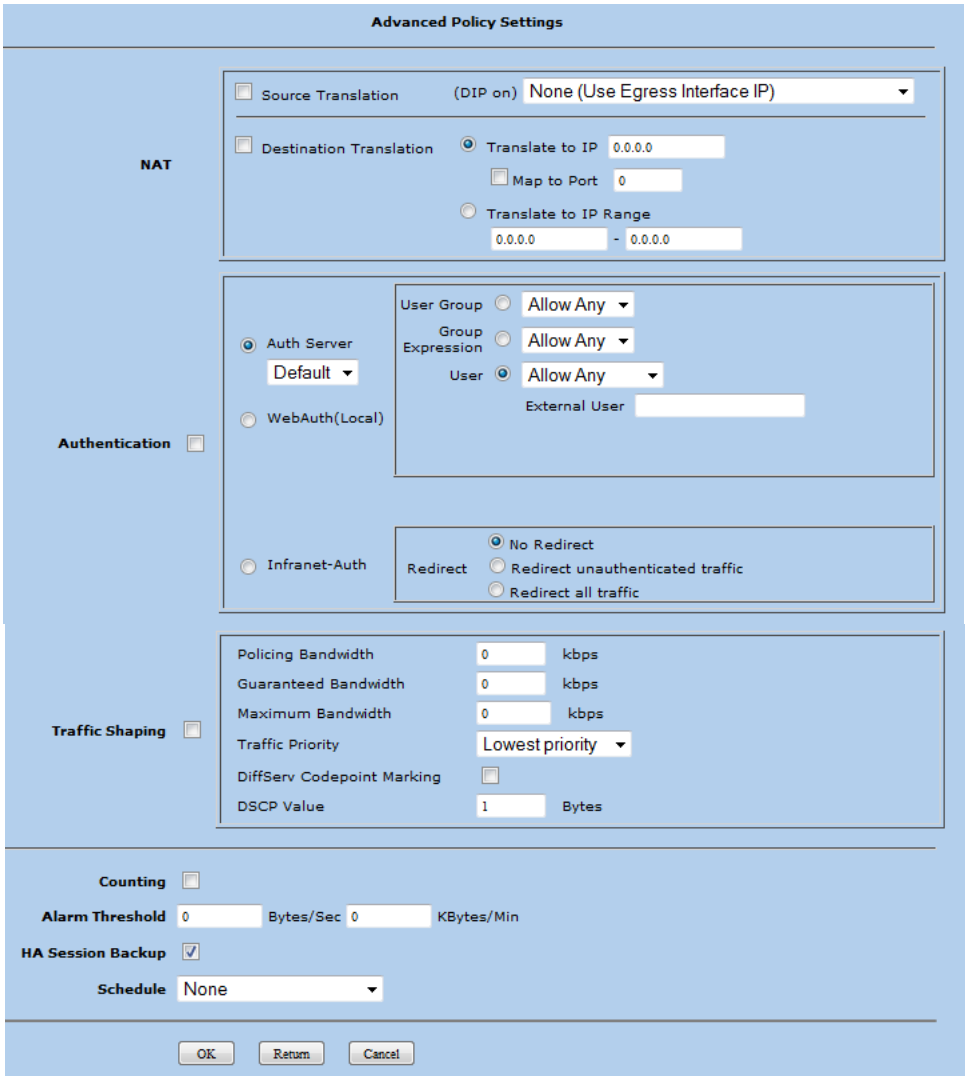

Figura 13. Configuraciones avanzadas para una política de acceso.

6.1.2 Procedimiento de creación de una política en el firewall CISCO ASA 5520 con Firmware Cisco Adaptive Security Appliance Software Version 8.0(4)28.

La forma más secilla de configuración de listas de acceso, es empleando la aplicación Java Cisco Adaptive Security Device Manager proporcionada por CISCO. El procedimiento es descrito a continuación.

- Lista de control de acceso (ACL).

  Seleccionando en el Menú superior “Configuration”, en el panel de navegación “Access Rules” y en seguida “firewall”, se presentará un listado de las listas de acceso ACL.

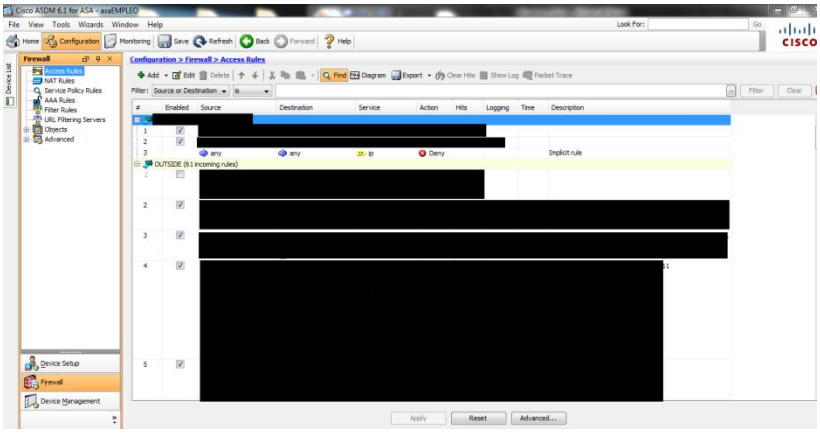

Figura 14. Configuraciones de una lista de acceso.

- Se selecciona la opción “Add” en el submenú.

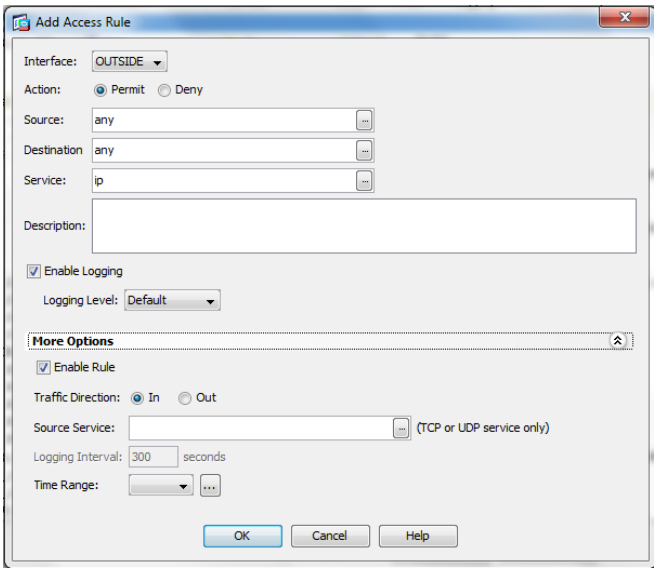

Figura 15. Elección de direcciones IP y servicios para una lista de acceso.

- Primeramente se elige la interface origen, es decir, por donde el firewall recibirá el tráfico.
- Se selecciona la acción “Permit” o “Deny”.
- Se elige la dirección o grupo de direcciones fuente.

  En caso de no tener ya creado el o los objetos de dirección, se permite colocarlos en su forma abreviada separados por comas, lo que los creará automáticamente.
- De igual manera, se coloca el o los objetos destino.
- En “Service” se indica el servicio, en caso de no existir, puede crearse automáticamente con la siguiente notación:
  - ip, tcp/número de puerto o nombre de protocolo, udp/número de puerto o nombre de protocolo.
  - Ejemplo: tcp/80 es equivalente a tcp/HTTP.
- Opcionalmente se puede agregar una descripción.
- Se puede habilitar la opción “Enable Logging” para tener un registro histórico, además de poder elegir el nivel de Log que se necesite.
- Al seleccionar “More Options”, puede habilitarse o deshabilitarse la lista de acceso; indicar si el tráfico será entrante o saliente; indicar un servicio origen; un límite de tiempo en la política, posterior al cual se detendrá la generación de logs por paquete; además de un límite de tiempo de sesiones y conexiones.
- Se presiona la opción “OK”, “Cancel” o “Help”.

Con la finalidad de proporcionar un control más granular, configuré listas de acceso extendidas, posibilitando el filtrado de paquetes por protocolo dirección fuente y dirección destino. Cabe destacar que siempre se sigue la recomendación de colocar en la configuración, primero las listas de acceso más específicas.
Realicé bloqueos por dirección IP de equipos que presentaban actividad sospechosa y de aquellos rangos identificados por fabricantes y comunidades como peligrosos.

Llevé a cabo la revisión del comportamiento de la red, verificando que no hubiera una desviación considerable respecto a la actividad normal de operación por cliente.

6.2 Configuraciones básicas en dispositivo IPS TippingPoint 2500N HP.

6.2.1 Procedimiento para crear segmentos.

Inicialmente se asignan segmentos (físicos o virtuales) para la protección de un cliente, cada segmento está compuesto de dos interfaces, una de entrada y una de salida, que hacen posible la implementación “In-line”.

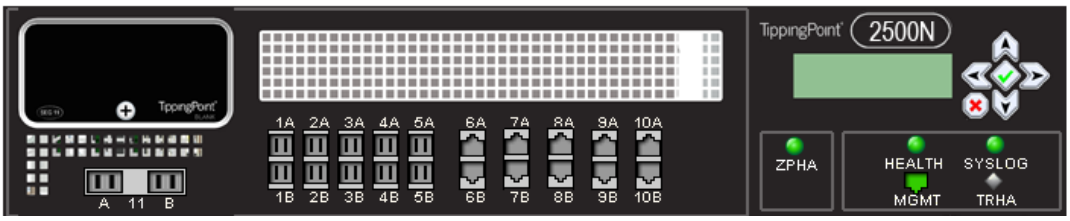

Figura 16. TippingPoint 2500N.

En la imagen se distinguen los segmentos del 6 al 10, siendo conectada la interface A hacia la parte menos segura de la subred (un firewall o un enrutador) y la interface B hacia la más segura (un conmutador o un servidor).

Para la asignación de segmentos se realizan los siguientes pasos:

En la barra de herramientas se selecciona “Devices”, en el panel izquierdo se elige “Virtual Segment” y se presiona el botón “New” en la esquina inferior derecha.

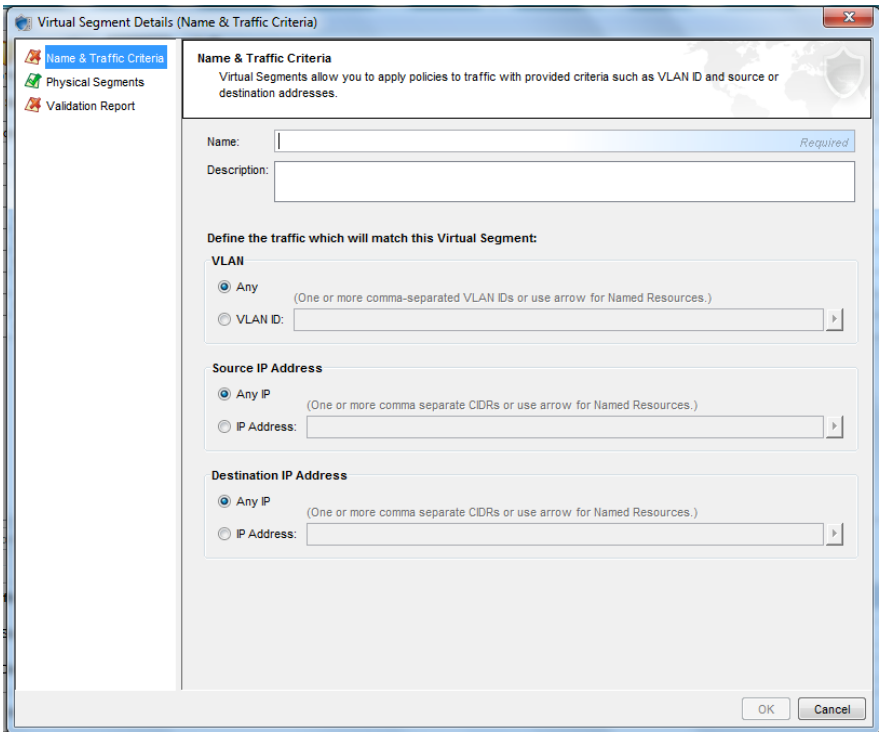

Figura 17. Asignación de un segmento virtual en un equipo TippingPoint 2500N.

- Se designa un nombre en referencia a la infraestructura o entidad que se protegerá.
- Opcionalmente se puede proporcionar una descripción.
- Se especifica el tráfico al que aplicará el segmento virtual:

  Se especifica una o varias VLAN, se especifica una o varias direcciones IP fuente y se especifica una o varias direcciones IP

destino. Puede especificarse cualquier combinación de los anteriores.

- Seguidamente se especifican los segmentos físicos.

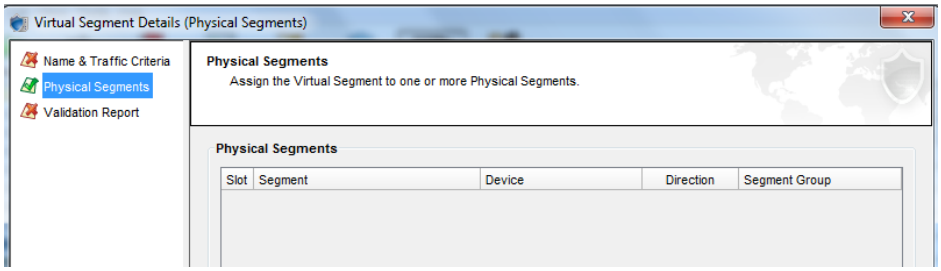

Figura 18. Elección de segmentos físicos en un equipo TippingPoint 2500N.

- Finalmente se selecciona “Validation Report”, en cuyo proceso el IPS ejecutará una serie de algoritmos para identificación de posibles errores en la configuración.

6.2.2 Procedimiento para agrupar segmentos.

Para la agrupación de segmentos se debe proceder de la siguiente manera:

En la barra de herramientas se selecciona “Devices”, en el panel izquierdo se elige “Segment Groups” y se presiona el botón “New” en la esquina inferior derecha.

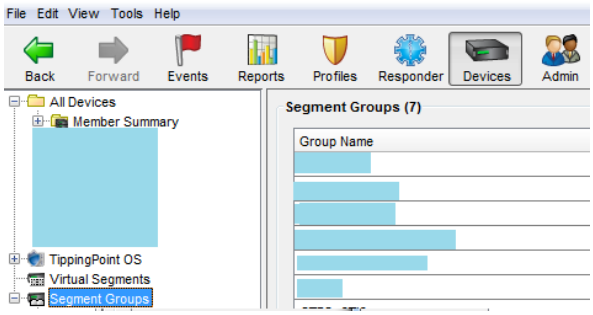

Figura 19. Asignación de un segmento virtual en un equipo TippingPoint 2500N.

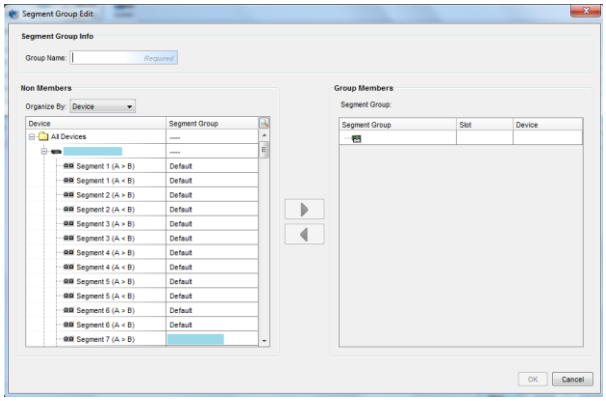

Figura 20. Elección de un segmento en un equipo TippingPoint 2500N.

- Se designa un nombre referente a la infraestructura o entidad que se protegerá.
- Se selecciona si se quiere un despliegue de información por dispositivo, o por grupo de segmentos.

    El objetivo es crear un grupo virtual de segmentos que podría contener segmentos físicos o virtuales de más de un equipo IPS.

6.2.3 Procedimiento para la creación de perfiles de protección.

Se configuraron perfiles con vacunas de acuerdo con las necesidades de cada cliente, las cuales mitigan ataques en base a patrones ya conocidos.
Procedimiento para la creación de un perfil en el sistema de prevención de intrusos.
En la barra de herramientas se selecciona “Profiles” y posteriormente “IPS Profiles”.

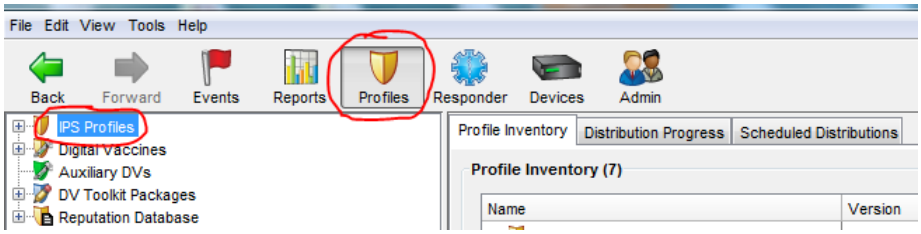

Figura 21. Menú para la creación de un perfil en un equipo TippingPoint 2500N.

Se selecciona la opción New en la esquina inferior derecha.

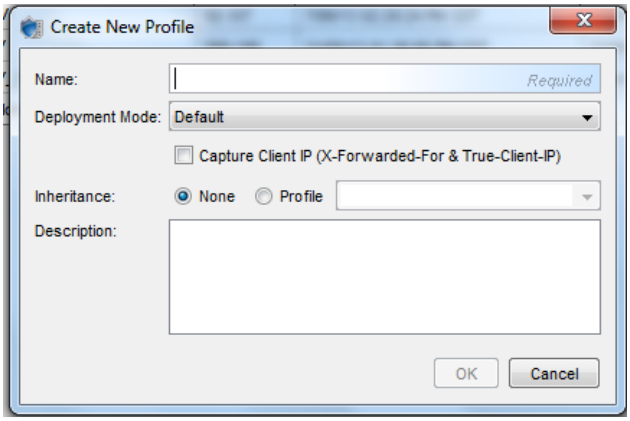

Figura 22. Creación de un perfil en un equipo TippingPoint 2500N.

- En el primer campo se coloca un nombre descriptivo del perfil.
- En “Deployment Mode”, se puede seleccionar alguna de las siguientes opciones, dependiendo de la ubicación física del IPS en la red de datos:

1. Aggressive. Provee mayor seguridad, a cabio de un desempeño más pobre de la red. Es recomendable para combatir iniciativas de día cero.
2. Core. Ofrece desempeño mejorado para una ubicación en el interior de la red (no en el perímetro). Considera que los dispositivos perimetrales han bloqueado la mayor parte de las amenazas.
3. Default. Hace un balance entre seguridad de alta calidad y desempeño del dispositivo. Es genérico en cuanto a ubicación.
4. Edge. Ideal para granjas Web y zonas DMZ que exponen contenido a la red pública.
5. Perimeter. Ofrece óptimo desempeño en el perímetro de la red, protege contra tráfico en general.

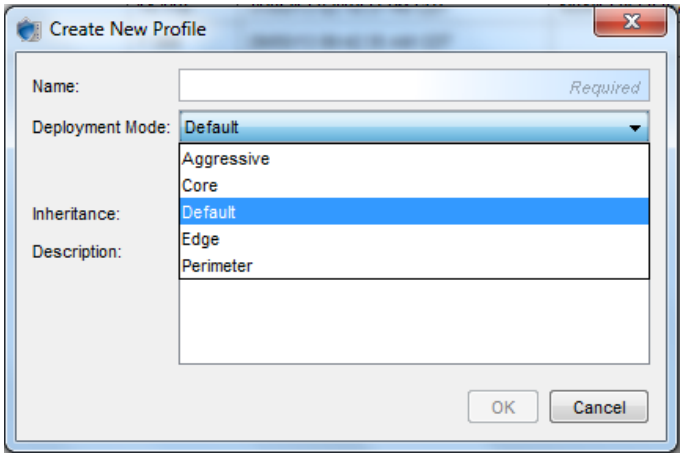

Figura 23. Elección de un modo de despliegue en un equipo TippingPoint 2500N.

Por la naturaleza de la red y características de los clientes, comúnmente el despliegue del dispositivo se elige “Edge”.

Al confirmar la creación del perfil, se cargan en automático los filtros que la versión de Firmware contenga en la versión “Digital Vaccine”. Los filtros se agrupan por protección de aplicación, protección de infraestructura y protección al desempeño.

En cada una de las agrupaciones de filtros, el administrador y el comité tienen que elegir (de acuerdo con la política de seguridad de la información) cuáles de las disponibles son de utilidad para la protección de la red de datos. Para facilitar la elección, cada una de las vacunas proporciona una descripción sobre su funcionalidad.

Por ejemplo, uno de los ataques más comunes es “1125: HTTP: ../.. Directory Traversal”. Consultando la descripción en “Profiles”, “IPS Profiles”, el perfil correspondiente, “Aplication Protection” y en el listado de vacunas como el mostrado a continuación, se presiona dos veces la que es menester revisar.

✓	1414: Telnet: Sun Solaris Login Bypass Vulnerability	Category	Block / Notify	Vulnerabilities	DV
✓	1420: IMAP: BODY Buffer Overflow - 1	Category	Block / Notify	Exploits	DV

Figura 24. Ejemplo de firmas en un equipo TippingPoint 2500N.

La descripción es la siguiente:

“Este filtro detecta intentos de secuencias “.. \ ..” o secuencias “../..” de recorrido de directorio en un servidor web. Varios servidores web son vulnerables a ataques transversales de directorio. Un atacante podría aprovechar esto en una solicitud, como un esfuerzo para ver los archivos o ejecutar código arbitrario en el sistema con los privilegios administrativos del servidor web”.[4]

Para la configuración del perfil de protección, es necesario tomar en cuenta aspectos relevantes, tales como el pleno conocimiento de los recursos que se van a proteger, lo que implica tener información sobre el sistema operativo con el que operarán, de forma general el software instalado y por ende las vulnerabilidades que tendrán. De esta manera, es posible tener una aproximación sobre las vulnerabilidades que estarán presentes y por lo tanto saber cuál es la manera más conveniente de asegurar los recursos, después de haber identificado y documentado los riesgos de la infraestructura[5].

Cuando el perfil ha sido personalizado por el administrador, se distribuye en los grupos de segmentos anteriormente configurados. Para distribuir, se presiona el botón “Distribute…”, en la ventana principal del perfil, después de elegir los grupos de segmentos, se presiona “OK”.

6.2.4 Procedimiento para la creación de una política de respuesta.

En el Menú de navegación, se selecciona “Respoder”, “Response History”, “Policies” y “New” en la parte inferior derecha.

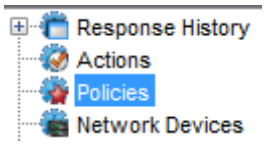

Figura 25. Creación de una política de respuesta en un equipo TippingPoint 2500N.

En “Initiation and Timeout”, que contiene la lista, se despliega lo siguiente:

[4] Dispositivo TippingPoint HP 2500N. Base de datos de vacunas.

[5] De acuerdo a las recomendaciones documentadas en el Estándar ISO/IEC 17799 17799:2005 Information technology. Code of practice for information security management

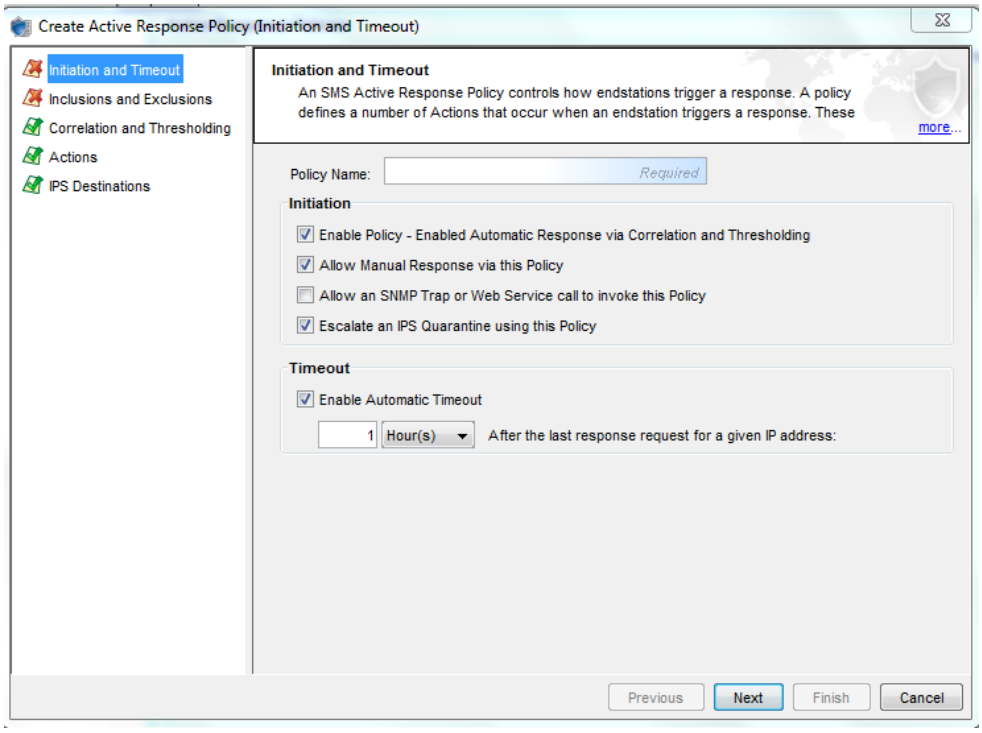

Figura 26. Elección de parámetros iniciales en una política de respuesta en un equipo TippingPoint 2500N.

A continuación se describe el llenado de la plantilla.

- Se da un nombramiento referente al bloqueo que establecerá la política.
- En “Initiation”, para activar la respuesta se pueden seleccionar opciones como:
    1. Enable Policy – Enabled Automatic Response via Correlation and Thresholding. Correlaciona la cadena de eventos originada en el dispositivo administrado, responde cuando se cumplen los criterios de los umbrales.
    2. Allow Manual Response via this Policy. Activa la respuesta de la política de manera manual.
    3. Allow an SNMP Trap or Web Service call to invoke this policy. Activación vía externa, desde un sistema de gestión de red.
    4. Escalate an IPS Quarantine using this Policy. Hace una escalación desde una cuarentena hasta una respuesta SMS de red.
- Sobre “Timeout”, se puede habilitar la opción “Enable Automatic Timeout”, lo cual terminará la aplicación continua de acciones de respuesta (estas acciones constituyen la respuesta configurada en la política), una vez que concluya el tiempo límite, aún si no se mitigó el problema.

En “Inclusion and Exclusions”, el llenado es como el descrito en seguida:

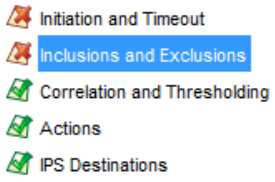

Figura 27. Especificación de inclusiones o exclusiones en una política de respuesta en un equipo TippingPoint 2500N (parte 1).

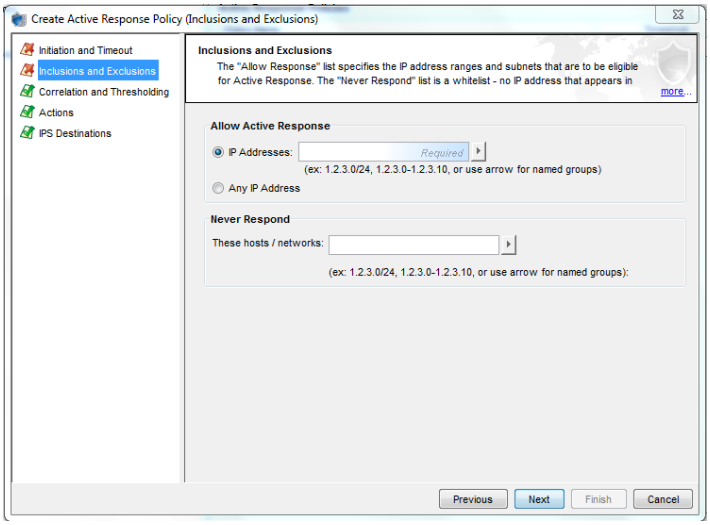

Figura 28. Especificación de inclusiones o exclusiones en una política de respuesta en un equipo TippingPoint 2500N (parte 2).

- Allow Active Response. Permite especificar las direcciones IP o rangos de éstas, a las que la política de respuesta será aplicada.
- Never Respond. Permite colocar las direcciones IP o rangos de direcciones, las cuales serán excepciones a la política de respuesta.

En “Correlation and Thresholding”.

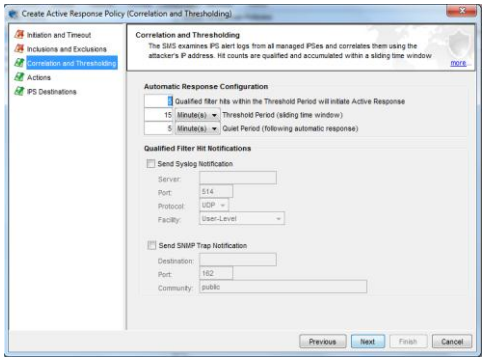

Figura 29. Especificación de parámetros para correlación y umbrales en una política de respuesta en un equipo TippingPoint 2500N.

- “Automatic Response Configuration”.
  - Se brinda un umbral de empates (“hits”), dentro de un periodo de tiempo en el que se deberá activar la respuesta.
  - Se especifica el tiempo de duración del periodo.
  - Se especifica un tiempo “Quiet Period”, éste se inicia después de comenzada la acción de respuesta, no podrá empezar un nuevo periodo de tiempo hasta que concluya el “Quiet Period”.
- “Qualified Filter Hit Notifications”
  - Se pueden marcar las opciones “Send Syslog Notification”, para generar registros de eventos y enviarlos a un servidor para su almacenamiento.
  - Se elegir “Send SNMP Trap Notification”, para enviar avisos de activación de la política de respuesta a un equipo de administración de red.

En acciones.

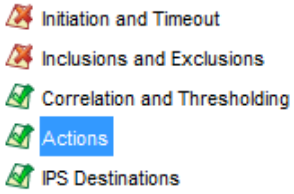

Figura 30. Menú para la especificación de parámetros de acción en una política de respuesta en un equipo TippingPoint 2500N.

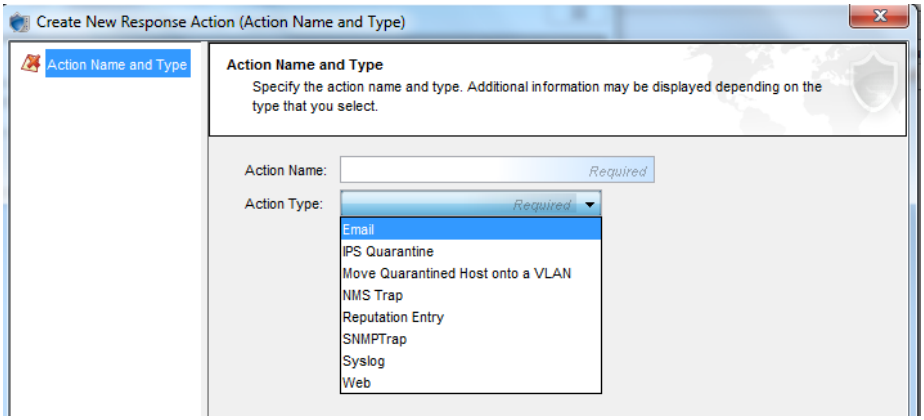

Figura 31. Especificación de parámetros de acción en una política de respuesta en un equipo TippingPoint 2500N.

- Se especifica un nombre y se elige alguna de las siguientes:
  - Email. Enviar un correo informativo sobre la activación de la política de respuesta.

- IPS Quarantine. Enviar a cuarentena la dirección IP que activó la política.
- NMS Trap. Enviar información a un equipo de administración de red.
- Reputation Entry. Agregar la dirección IP a una lista de reputación.
- SNMPTrap. Enviar información a un equipo de administración de red.
- Syslog. Enviar el evento a un servidor almacén de logs.
- Web. Manda una petición Web. Desarrolla un HTTP GET en una URL.

Apoyé en dar respuesta a algunas intrusiones efectuando las siguientes acciones:

Bloqueo de dirección IP.
Interrupción de la sesión o conexión correspondiente.
Observando el patrón de la intrusión para su análisis.
Robusteciendo la configuración de seguridad de los equipos involucrados.

En apoyo con los dispositivos IPS, mitigué ataques conocidos como por ejemplo: inyecciones de código SQL, en donde se inyectan comandos PHP a una base de datos; o el ya mencionado en párrafos anteriores, “Directory Traversal” en el protocolo HTTP.

Brindé seguimiento y revisión a los falsos positivos presentados, para realizar posteriormente las configuraciones necesarias sobre el equipo, con el objetivo de corregir las malas detecciones de éste.

Por otra parte, mitigué actividades sospechosas que fueron detectadas por el equipo IPS, las cuales presentaron un comportamiento anómalo y previamente se corroboró que no se trataban de falsos positivos.

6.3 Configuración de zonas en el dispositivo Fortigate 3950 B 4.0MR3.

Se ejemplificará la creación de dos pares de interfaces VLAN, que posteriormente se agregarán a las zonas hipotéticas “inside” y “outside”.

Para crear una interface VLAN se efectúa lo siguiente:

6.3.1 Creación de interfaces.

Se accede a “System”, “Network”, “Interface” y “Create New”.

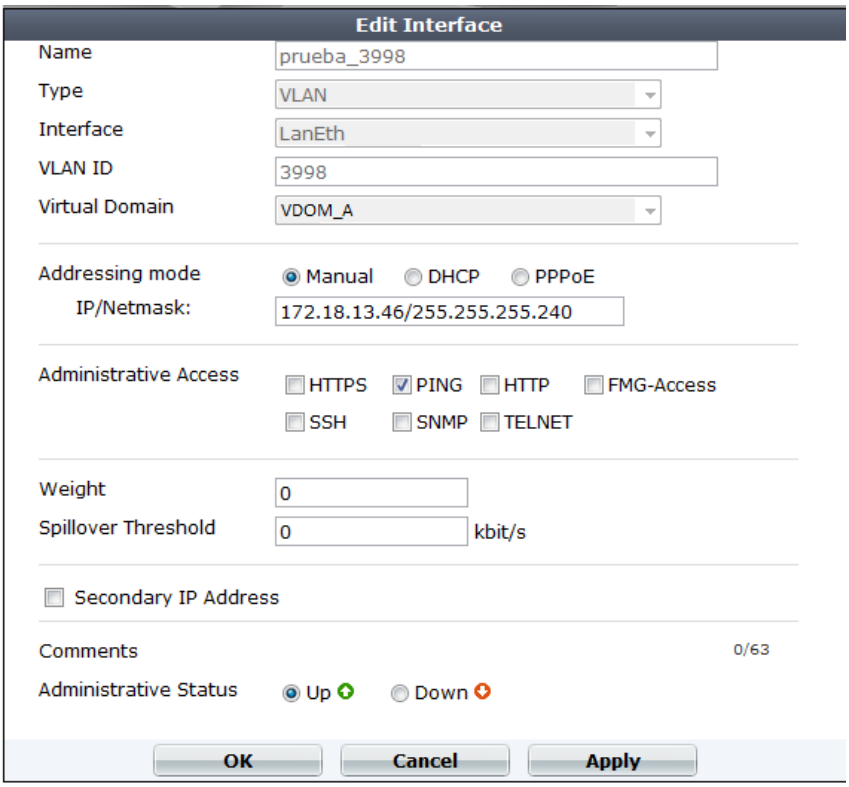

Figura 32. Creación de una interface en un equipo Fortigate 3950B.

En este caso se los campos se llenan de la siguiente manera:

- Name: La interface VLAN de ejemplo nombrada prueba_3998.
- Type. Tipo VLAN.
- Interface: Se asocia a la interface agregada física LanEth.
- VLAN ID.Se indica el “tag” 3998.
- Virtual Domain: Se asigna al dominio virtual VDOM_A.
- Addressing mode: Se asigna un direccionamiento manual (“Manual”).
- Administrative Access: Para fines administrativos puede elegirse algún protocolo de los disponibles, para ejemplificar se palomea “PING”, que permite hacer pruebas de conectividad en la capa 3 del modelo OSI.
- Weight :No se asigna un “Weight”, ya que no se requieren prioridades de reenvío de paquetes.
- Spillover Threshold: De igual manera, no se asigna un límite de ancho de banda disponible en la interafce con “Spillover”.
- Secundary IP Address: No se requiere una dirección IP secundaria.
- Se selecciona “OK”.

Con un procedimiento similar se crean las otras interfaces VLAN: prueba_3999 y VLAN_1601.

6.3.2 Generación de zonas.

A continuación se generan las zonas que agruparán las interfaces anteriores.

Ya en el dominio virtual correspondiente, se crea la zona “inside”.

Se accede a “System”, “Network”, “Interface” y “Zone”.

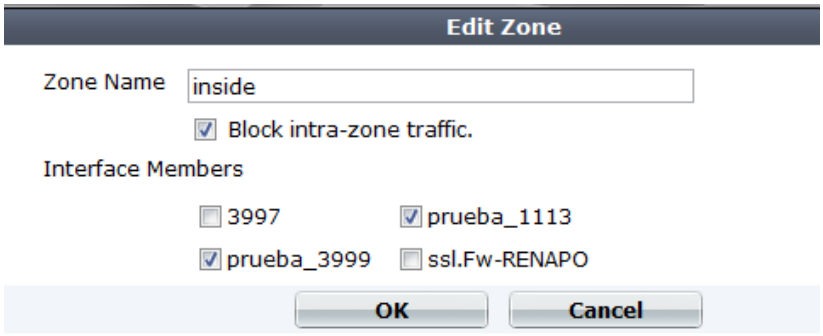

Figura 33. Creación de una zona en un equipo Fortigate 3950B.

- Zone Name: Se coloca el nombre correspondiente.
- Block intra-zone traffic: Opcionalmente se puede bloquear el tráfico intrazona.
- Se agregarán las interfaces VLAN prueba_1113 y prueba_3999.
- Se presiona “OK”.

Similarmente se crea la zona “outside”, la cual contendrá a la interface VLAN_1601, que hipotéticamente se conectará al enrutador que da salida a la red pública.

6.4 Configuración de políticas de seguridad perimetral en el equipo Fortigate 3950 B 4.0MR3.

Una vez contando con las zonas de seguridad, se pueden configurar las políticas correspondientes.

En este caso se establecerá una política para que todos los equipos en la zona “inside” puedan comunicarse con equipos en Internet, los protocolos permitidos serán HTTP, HTTPS y DNS.

Para la configuración se accede a “Policy”, “Policy” y se elige “New Policy”:

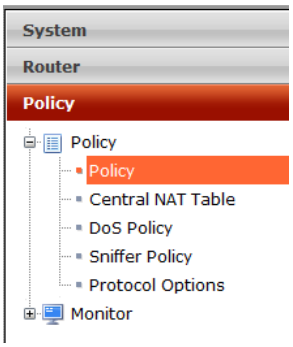

Figura 34. Menú para la creación de una política de acceso en un equipo Fortigate 3950B.

En la primera parte de los campos, se indican las interfaces fuente y destino (“inside” y “outside” respecitvamente).

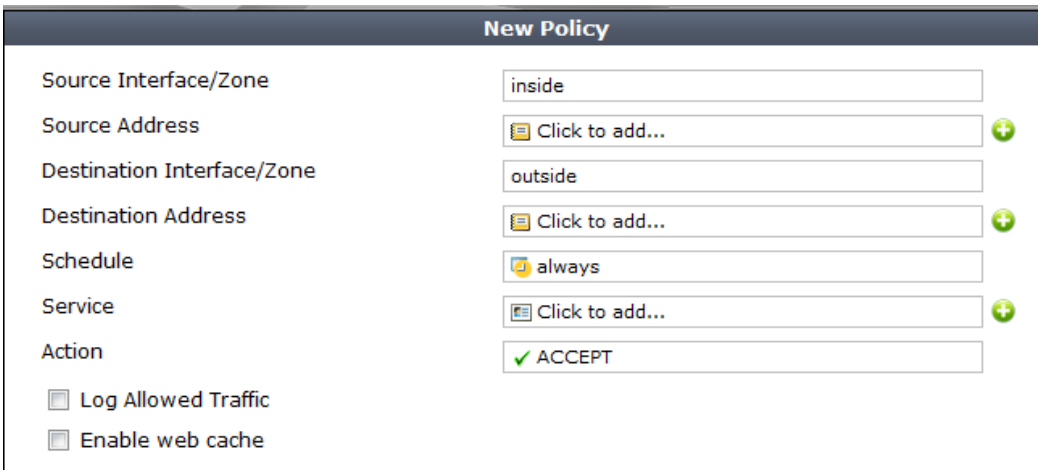

Figura 35. Especificación de parámetros para la creación de una política de acceso en un equipo Fortigate 3950B.

Como direcciones fuente, se requiere crear los objetos. En el símbolo “+” se habilita la opción de creación.

Ya que todos los equipos tendrán salida a Internet, se generará un objeto “any” que los contenga enteramente.

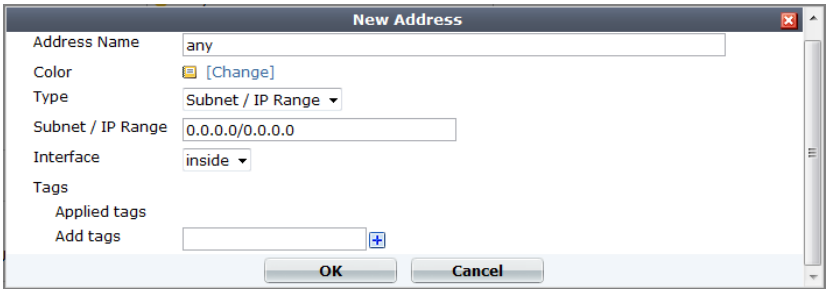

Figura 36. Especificación de direcciones para la creación de una política de acceso en un equipo Fortigate 3950B.

- Address Name: Se asigna un nombre.
- Color: Opcionalmente se puede elegir un color.
- Type: El tipo se selecciona entre Subnet / IP Range para direcciones específicas, FQDN para dominios y Geography para indicar países.
- Subnet / IP Range: Especificando la dirección como 0.0.0.0/0.0.0.0, se aplicará para todos.
- Interface: Como interface se coloca “inside”, para incluir todas las interfaces agrupadas por dicha zona.
- Add tags: Opcionalmente puede etiquetarse el objeto.

De la misma forma se crea el objeto “any” en la zona “outside”.

Se seleccionan los servicios que ya se encuentran previamente configurados como HTTP, o se crean si es que no existen.

Se ejemplificará la creación de un objeto DNS1.

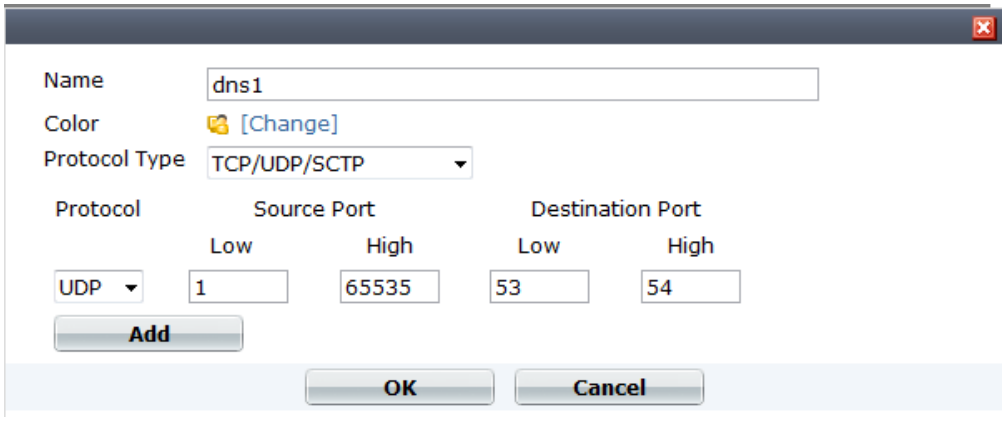

Figura 37. Especificación de servicios para la creación de una política de acceso en un equipo Fortigate 3950B.

- Name: El nombre es dns1.
- Color: Puede elegirse un color de la paleta disponible.
- Protocol Type: Como protocolos se puede elegir TCP/UDP/SCTP, IP o ICMP. Ya que los algoritmos de DNS operan en TCP y/o UDP, se selecciona el primero.
- Protocol: Como protocolo se especifica UDP, se permiten todos los puertos del equipo origen, pero solamente los puertos 53 y 54 de destino. Para fines demostrativos, se coloca también el 54 para no tener un conflicto con el servicio “DNS” predeterminado.

Se establece la acción como “ACCEPT”.

En las siguientes opciones (mostradas en la siguiente imagen), se pueden configurar:

- Generación de Logs.
- Web cache. Para optimización de sesiones.
- Habilitar una traducción de direcciones IP.
- Configurar la política para que aplique solamente a un grupo de usuarios.
- Usar autenticación FSSO.
- Aplicar características de UTM, Traffic Shaping, Seguridad en el punto final y etiquetas.

  De las anteriores, solamente se elegirá Enable NAT, ya que los equipos internos requieren una dirección homologada para atravesar la red pública.

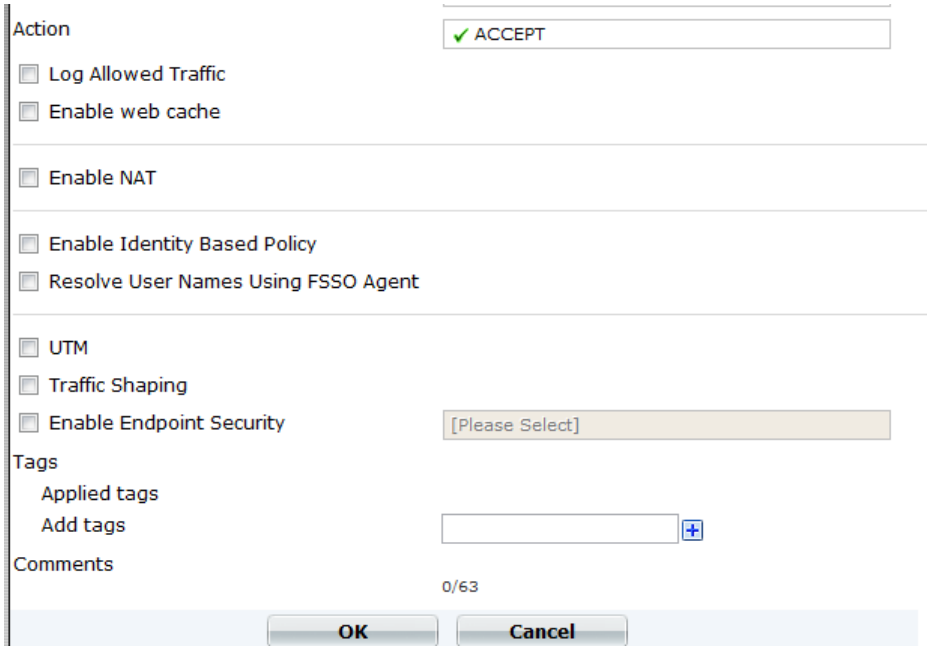

Figura 38. Continuación de la especificación de parámetros para la creación de una política de acceso en un equipo Fortigate 3950B.

6.5 Configuración de un túnel de VPN IPsec en el equipo Fortigate 3950 B 4.0MR3.

A continuación se muestra el procedimiento de configuración de una red privada virtual a través del protocolo IPsec.

En VPN> IPsec> Auto Key (IKE) y haciendo click sobre Create New.

6.5.1 Fase 1.

Se establecen los parámetros de la fase 1, con los cuales los pares negociarán el levantamiento del túnel ISAKMP.

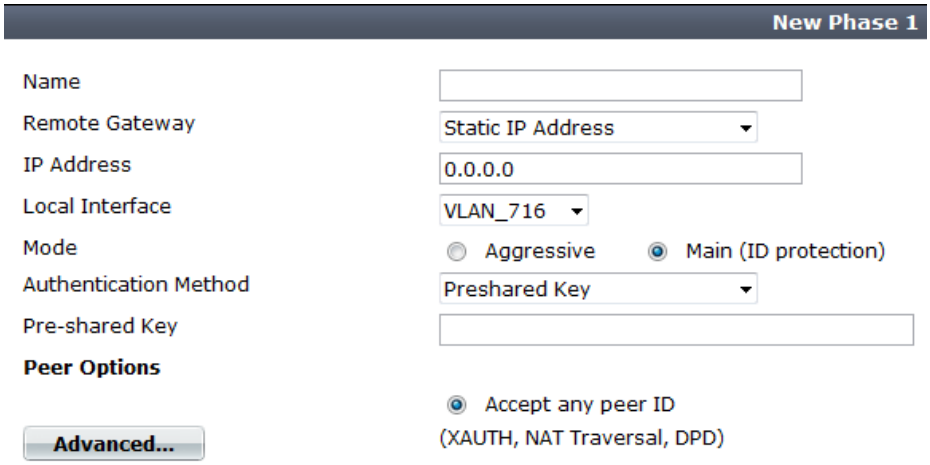

Figura 39. Especificación de parámetros de fase 1 para la configuración de una VPN en un equipo Fortigate 3950B.

- Name: Se asigna un nombre.
- Remote Gateway: Se especifica si el Gateway remoto será:
  - Static IP Address. Si el par será estático.
  - Dialup User. Si el par recibe dinámicamente una dirección IP.
  - Dynamic DNS. Si el par se identificará por un nombre de dominio.
- Local interface: Se selecciona la interface local.
- Mode: Se puede elegir entre dos modos de establecimiento de túnel.
  - Aggressive. Para el levantamiento del túnel en solo 3 intercambios de paquetes.
  - Main(ID protection). Para el levantamiento del túnel en 6 intercambios de paquetes.
- Authentication Method: Se pueden elegir como métodos de autenticación:
  - Preshared Key. Para autenticarse con una llave acordada previamente.
  - Con una firma RSA. Para autenticación en base a certificados.
- Accept any peer ID. Si se escogió la opción “Preshared Key”, ésta se incluye predeterminadamente. Si se escogió la opción por certificado, se puede indicar que se acepte cualquier identificador, o bien, un identificador único.

Para las opciones avanzadas:

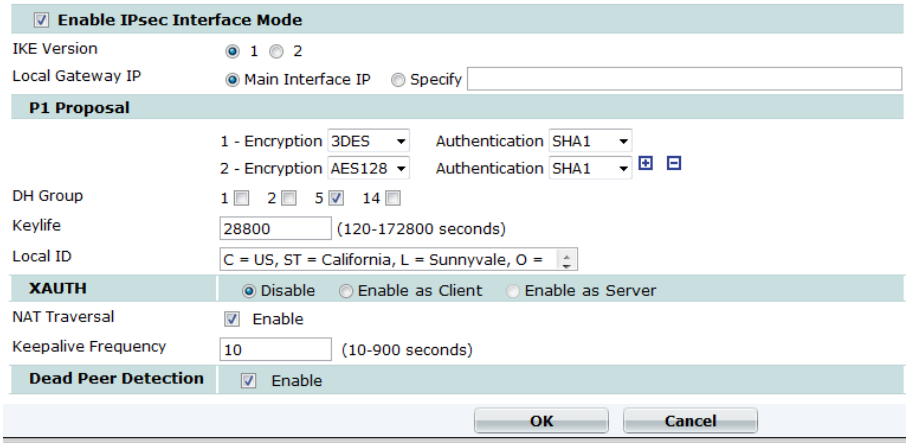

Figura 40. Continuación de la especificación de parámetros de fase 1 para la configuración de una VPN en un equipo Fortigate 3950B.

- La primera opción para habilitar “IPsec Interface Mode”, permite configurar una VPN basada en rutas. Si no se selecciona, se creará una VPN basada en políticas.

  Para una VPN basada en rutas, se crea una interface virtual para la terminación local de la red.

- IKE Version: Seleccionando la opción anterior, puede elegirse entre usar la versión IKE 1 o 2, la segunda es más reciente y por tanto más segura.
- Local Gateway IP: La terminación del túnel se puede establecer con la IP de la interface principal, o se puede especificar otra.
- P1 Proposal: Se configuran las propuestas con las que negociarán los pares.
  - Por ejemplo, usar Cifrado 3DES y autenticación SHA1.
  - Se pueden establecer como máximo 3 propuestas.
- DH Group: Se indica el o los grupos Diffie-Hellman.
- Keylife: Se especifica la duración de la llave. Cada vez que caduca, debe ser regenerada.
- Local ID: Si se eligió en la terminación opuesta, aceptar a un solo identificador (en modo “Aggressive”), en la terminación local debe asignarse dicho identificador.
- XAUTH. Solamente es requerida en la versión IKEv1 y para clientes Dialup. Es el parámetro con el que el equipo se autenticará con el servidor remoto.

  El equipo puede usarse como servidor de autenticación.

- NAT Traversal. Utilizada en caso de que entre los pares se encuentre un dispositivo que haga traducciones de IP.

- Keepalive Frequency. Si se selecciona esta opción, se debe especificar una frecuencia de revisión de conectividad con el par.

- Dead Peer Detection. Permite reestablecer túneles VPN sobre conexiones ociosas. Normalmente se reestablece cuando alguno de los pares cambia su dirección IP.

6.5.2 Fase 2.

Parámetros para el levantamiento del túnel de fase 2 IPsec.

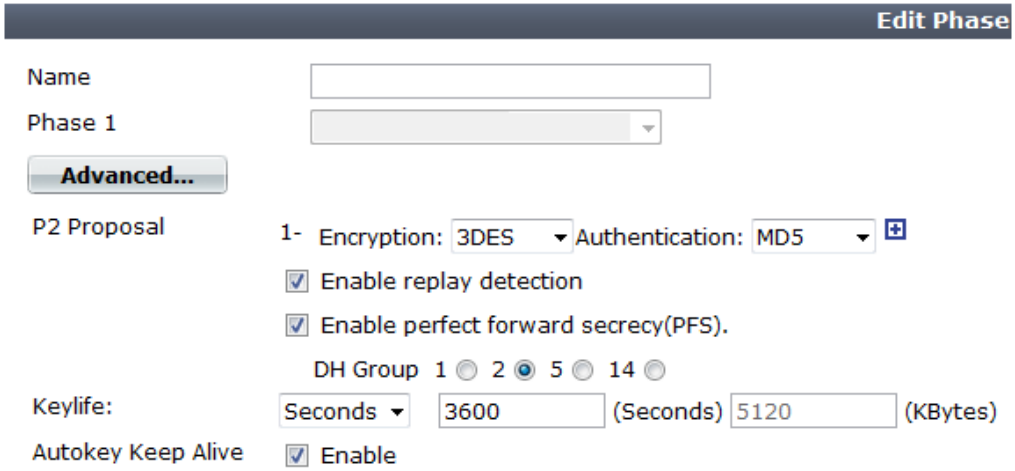

Figura 41. Continuación de la especificación de parámetros de fase 1 para la configuración de una VPN en un equipo Fortigate 3950B.

- Name: Se nombra la fase 2.
- Phase 1. Se especifica el Gateway local, creado en la fase anterior.
- Se configura una propuesta de fase 2. Por ejemplo, cifrado 3DES y autenticación MD5.
  Enable replay detection. Para evitar “Replay Attacks” en los que una tercera parte intercepta paquetes IPsec y los devuelve al túnel.
  Enable perfect forward secrecy (PFS). Obliga un intercambio Diffie-Hellman, siempre que expire la llave.
  Opcionalmente se puede elegir un grupo Diffie-Hellman para el intercambio de llaves.
- Keylife. Puede especificarse un tiempo de vida para la llave. Cuando caduca, debe renegociarse.
- Autokey Keep Alive. Para mantener al túnel activo, aún si no hay tráfico circulando a través de éste.

6.5.3 Creación de una ruta estática.

Teniendo las fases configuradas y haciendo coincidir al menos una propuesta por fase en cada equipo terminal, se procede a crear una ruta estática.

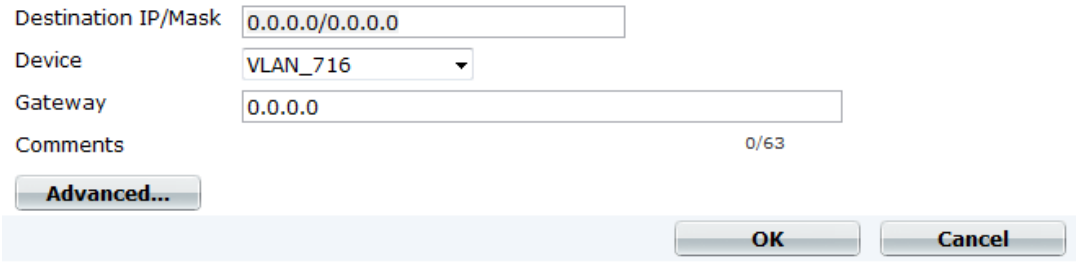

Figura 42. Creación de una ruta estática en un equipo Fortigate 3950B (parte 1).

- Destination IP/Mask. Se especifica la dirección IP del destino.
- Device. Se selecciona la interface o zona origen.
- Gateway. Se indica la dirección IP del Gateway o puerta de enlace.
- Advanced. Como opciones avanzadas se puede establecer una prioridad y una distancia.

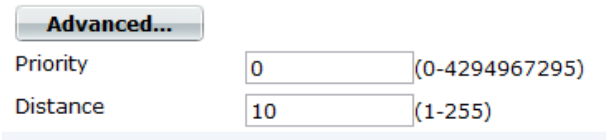

Figura 43. Creación de una ruta estática en un equipo Fortigate 3950B (parte 2).

Finalmente se configura una política desde las interfaces virtuales o zonas origen, hacia la interface virtual terminal de la VPN, o de manera inversa (procedimiento explicado en párrafos anteriores).

6.6 Monitoreo de la red.

6.6.1 Procedimiento para el monitoreo de la red de datos, cuya solución de seguridad perimetral utiliza un equipo CISCO ASA.

Gráficamente y de forma constante realicé el monitoreo de la red, con el apoyo del software ASDM.

Por cada cliente operando en un contexto virtual de firewall ASA, revisé lo siguiente:

- Procesador y memoria interna.

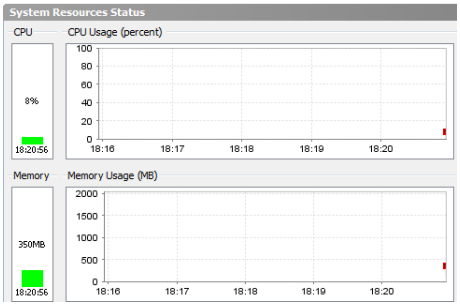

Figura 44. Procesador y memoria interna.

Nivel de procesamiento en la CPU, de acuerdo con normas internas, no debe excederse el 90%.

Uso de la memoria interna. Similarmente se consideran niveles adecuados por debajo del 90% de su utilización.

- Analicé el estatus de las interfaces.

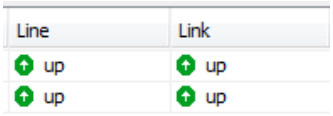

Figura 45. Analicé el estatus de las interfaces.

Para su correcta operación, ambas interfaces deben mostrarse como “Up” en los parámetros de línea y de enlace.

Monitoreé la cantidad de conexiones por segundo, de acuerdo al protocolo de comunicación.

- Finalmente realicé el monitoreo de tráfico recibido por la interface conectada a la red pública.

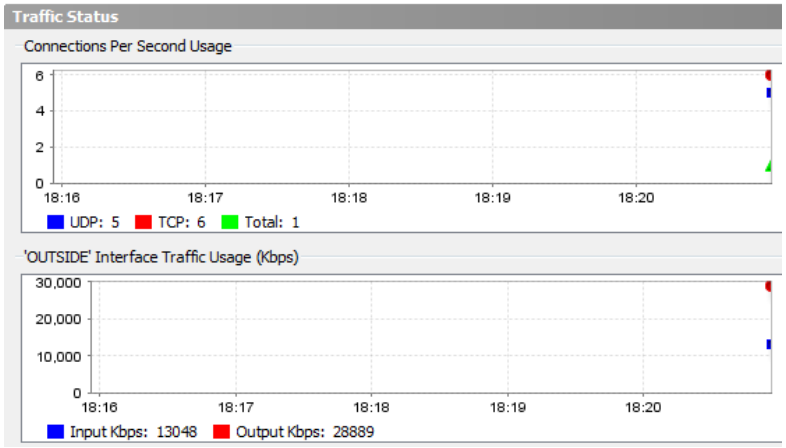

Figura 46. Monitoreo de tráfico.

Al presentarse valores anómalos (dependiendo del comportamiento registrado y documentado del cliente) en los parámetros mencionados, procedí a detectar las direcciones IP desde las cuales se generaban las peticiones, una vez localizadas, se bloquearon a nivel de firewall.

6.6.2 Procedimiento para el monitoreo de la red de datos, cuya solución de seguridad perimetral utiliza un equipo FORTINET FORTIGATE.

Monitoreé por cada cliente el comportamiento de su dominio virtual.

La revisión se hacía sobre lo siguiente:

- Recursos del sistema.

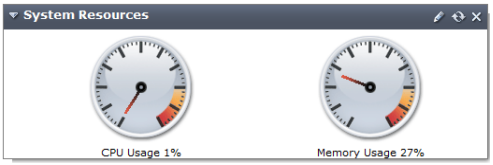

Figura 47. Recursos del sistema.

Porcentajes de CPU y memoria utilizados, valores internamente acordados para no exceder el 90%.

- La “Historia del tráfico”.

Analicé el tráfico en la interface conectada a la red pública de cada uno de los clientes.

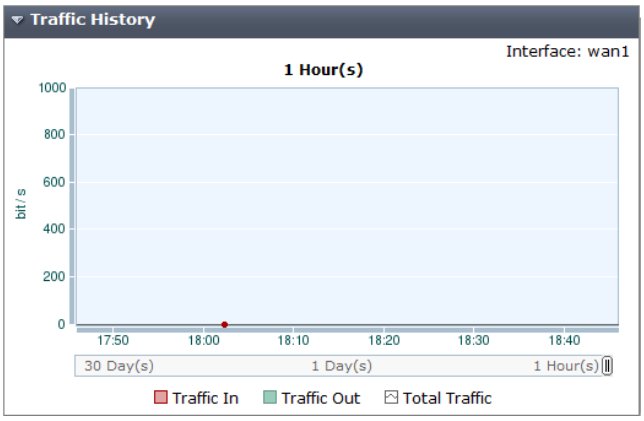

Figura 48. Historia del tráfico.

- Mensajes de alerta en la consola.

Monitoreé los logs generados por el sistema, validando su impacto en la página de soporte del fabricante, con el objetivo de tomar las acciones recomendadas.

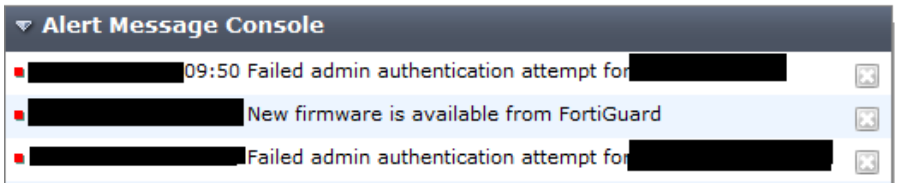

Figura 49. Mensajes de alerta en la consola.

- Monitoreo de interfaces físicas.

Llevé a cabo el monitoreo de interfaces, no solamente con la interface gráfica, sino también con apoyo del área de monitoreo, la cual puso en funcionamiento herramientas especializadas para estas tareas.

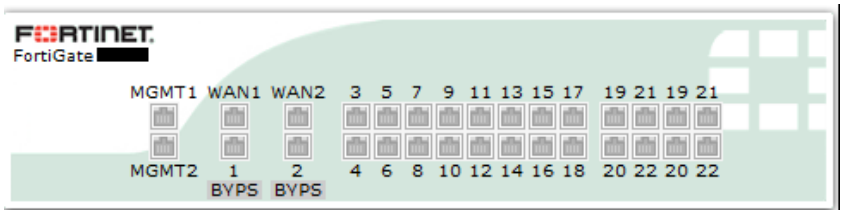

Figura 50. Monitoreo de interfaces físicas.

6.6.3 Procedimiento para el monitoreo de la red de datos, cuya solución de seguridad perimetral utiliza un equipo IPS HP TippingPoint.

Ejecuté el monitoreo principalmente de las siguientes características e información proporcionada:

- El estado físico del equipo.

Figura 51. El estado físico del equipo.

Esperando los siguientes valores: la memoria y la CPU por debajo del 90% de utilización; la temperatura menor a 73° C (por indicación del fabricante).

- La gráfica de los ataques con mayor frecuencia.

Figura 52. Gráfica de los ataques con mayor frecuencia.

Supervisé que el tráfico no fuera excesivo (de acuerdo al comportamiento documentado) analizando el número de peticiones y observando que ataques estaban siendo bloqueados. Los ataques en general fueron de impacto bajo, de acuerdo a la clasificación del propio fabricante.

- La gráfica con los servidores (identificados por dirección IP) más solicitados en los ataques.

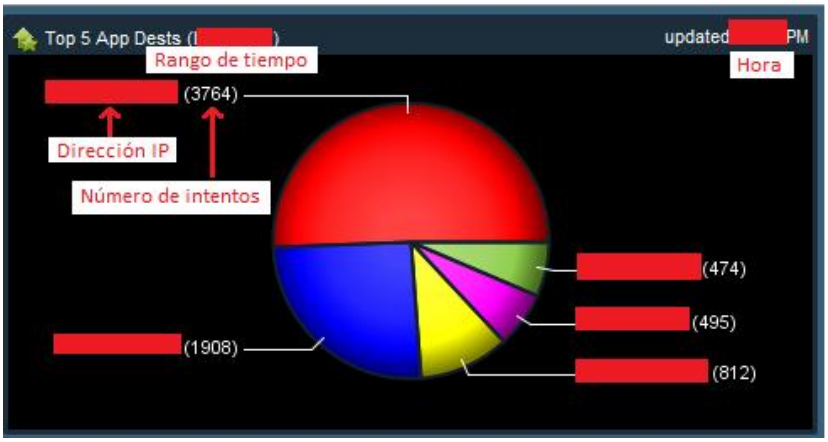

Figura 53. Gráfica con los servidores (identificados por dirección IP) más solicitados en los ataques.

- La tabla con el número de peticiones por IP y ubicación geográfica.

Figura 54. Tabla con el número de peticiones por IP y ubicación geográfica.

- La gráfica de los destinos más frecuentes en los ataques.

Figura 55. Gráfica de los destinos más frecuentes en los ataques.

- La ubicación geográfica origen de los vectores de ataque.

Figura 56. Ubicación geográfica origen de los vectores de ataque.

- La gráfica de eventos registrados.

De los eventos, se pueden distinguir las siguientes acciones:

- Permit. Todas las conexiones son permitidas.
- Block. Todas las conexiones son bloqueadas.
- Rate limit. Conexiones que se bloquearon a partir de exceder el número permitido.
- Quarantine. Conexiones detectadas como peligrosas, que se aíslan para confirmar sus intenciones.
- Trust. Aquellas conexiones cuyo tráfico se le permite continuar, sin ser comparadas con otras reglas de filtrado.

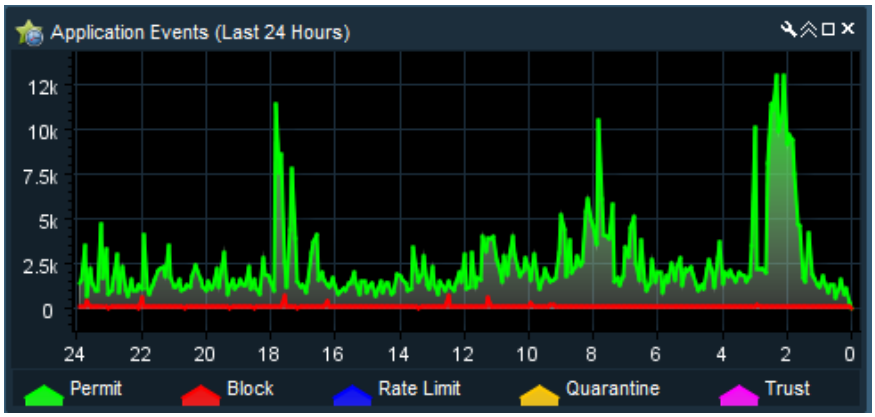

Figura 57. Gráfica de eventos registrados.

6.7 Atención a incidentes.

Atendí incidentes en las diversas infraestructuras de los clientes, a continuación se enlistan los más comunes:

6.7.1 Falla de conectividad hacia uno o varios equipos, los cuales están configurados en una o varias políticas de acceso.

Ante este tipo de fallas procedí de la siguiente manera:

1. Prueba de capa física, de enlace de datos y de red.
   Empleando el protocolo ICMP, ejecuté pings desde el equipo firewall (operando como Gateway), hacia la dirección IP del equipo interno.

   En caso de que no se obtuviera el correspondiente ICMP reply, los canalizaba al área correspondiente que hacía una prueba en la capa de enlace de datos.

2. Si el equipo superaba la anterior, realizaba una prueba en la capa de transporte.

   Realizaba la búsqueda de la política de acceso, cuyos permisos eran aplicables al caso.

   Ejecutando la instrucción telnet, especificaba un puerto en el cual se esperaba el establecimiento de la conexión con el equipo, si la conexión no resultaba exitosa, procedía a su correspondiente canalización al área de administración de equipos, para su posterior análisis en las capas de sesión, presentación y aplicación.

3. Cuando el punto anterior era superado, realizaba la inspección de las políticas encontradas. Analizaba el orden de procesamiento de las políticas o listas de acceso, con la finalidad de descartar posibles incongruencias.

   Si existía un problema con el orden, las reordenaban. Si el problema era alguna incongruencia, eliminaba la o las políticas de acceso inútiles.

4. Confirmado la inexistencia de incongruencias en el equipo firewall, procedía a revisar el equipo de detección de intrusos, ya que por una detección de intento de explotación de vulnerabilidad, el origen pudo ser bloqueado.

   Aplicando un filtro de búsqueda en el dispositivo IPS, comprobaba lo anterior.

   Si el problema residía en un bloqueo, analizaba si se trataba de un falso positivo, o bien, realmente era un verdadero positivo. Determinando con el cliente si el equipo origen no estaba siendo explotado por malware, si contaba con las últimas actualizaciones para su sistema operativo, si tenía una versión actualizada de software antivirus, si su programa de protección de punto final estaba al día (en caso de aplicar), si los programas instalados eran completamente de confianza y en éste no se habían instalado programas de terceros no autorizados, si no se empleaba para realizar descargas de datos potencialmente peligrosos y si éste no accede a sitios de internet en lista negra.

   Superado lo anterior y si el cliente se responsabilizaba del riesgo, se procedía a permitir el paso del tráfico que estaba siendo bloqueado.

5. En caso de que el dispositivo IPS no fuera responsable, procedía a hacer un análisis de la ruta en colaboración con el área de enrutamiento.

   Desde el equipo firewall, realizaba una traza de la ruta hacia la infraestructura origen, así mismo pedía realizarla en la dirección opuesta, en caso de fallar una o ambas, hacía la canalización completa al área de enrutamiento.

6.7.2 Detección de falla operativa en alguno de los equipos de seguridad perimetral.

Si se presentaba una falla en alguna de las interfaces, procedía a realizar la revisión con las áreas de enrutamiento o la encargada de los equipos operativos en capa 2.

1. Primeramente revisaban si las interfaces estaban conectadas y activadas, por lo general siempre fue así, en el caso contrario eran conectadas y activadas.

2. Validado lo anterior, si se trataba de una interface de salida hacia la red pública, verificaba las rutas, si estas estaban correctas se ejecutaban comandos ping para corroborar que los equipos fueran visibles en la capa de red ante los enrutadores y viceversa.

3. Si los equipos superaban lo anterior, revisaba que la configuración de las interfaces empatara en cuanto a tasas y tipo de transmisión.

   Hecho lo anterior, el problema era mitigado.

4. Si se trataba de una interface hacia la red interna, realizaba una prueba enviando un ICMP echo hacia la interface virtual de administración del equipo en capa dos, si recibía respuesta, verificaba la dirección MAC aprendida en cada uno de los equipos, el de capa dos (conmutador) y el firewall.

   En caso de que la tabla de ARP del equipo en capa de enlace de datos, mostrara dos direcciones MAC diferentes para la misma dirección IP (la del firewall), el área correspondiente realizaba pruebas para encontrar por qué existía un bucle (loop) en la infraestructura (cabe mencionar que los equipo son protegidos de bucles, gracias al Spanning Tree Protocol).

5. Si no se trataba de un bucle, procedía a revisar que coincidieran las tasas y tipo de transmisión.

Hecho lo anterior, el problema era mitigado.

6.7.3 Detección de tráfico anormal en alguna de las infraestructuras.

1. Al detectar tráfico anormal en alguno de los monitores de los equipos de seguridad perimetral, procedía a bloquear al o los orígenes

responsables, de acuerdo con la implementación de defensa a profundidad.

2. Establecía listas de acceso en los enrutadores, activaba una respuesta en el sistema de prevención de intrusos y aplicaban políticas de seguridad en los firewalls (en hardware y software).

3. Daba seguimiento a la estrategia de defensa a profundidad, con analizadores de red conectados en las interfaces involucradas. Con los resultados obtenidos, mejoraba en tiempo real las configuraciones destinadas a la protección de la infraestructura.

6.7.4 Detección de anomalías originadas en infraestructuras internas.

1. Cuando alguno de los equipos firewall o IPS, al realizar una inspección de contenido del tráfico saliente de la infraestructura, detectaba tráfico anómalo generado de manera interna, éstos procedían a bloquear al equipo de cómputo responsable del envío de dicho tráfico.

   Al ocurrir, lo canalizaba al área administradora de los equipos operantes en la capa dos, con la finalidad de deshabilitar la interface en donde el equipo infectado se conectaba a la subred interna y así evitar la propagación del malware responsable hacia todos los demás. Por otra parte lo canalizaba a una unidad especializada encargada de llevar a cabo los análisis forenses.

6.8 Atención a requerimientos.

Se atendieron diversos requerimientos de la red interna del centro público y de la red perteneciente a los clientes.

Los requerimientos implicaban realizar las siguientes actividades:

6.8.1 Solicitud de políticas.

Al requerir un usuario acceso a algún equipo, se me enviaba el formato correspondiente, especificando el o los orígenes por dirección IP, el o los destinos por dirección IP y el o los puertos.

Si el acceso era justificado, procedía a configurar la solicitud, en caso contrario, lo denegaba.

6.8.2 Solicitud de asignación de una o varias direcciones internas.

Al ser solicitada una dirección interna para algún servidor, validaba cuál sería su función, quién lo administraría y lo más importante, el software que se le instalaría. Hecho lo anterior, le asignaba la dirección en la correspondiente zona desmilitarizada.

6.8.3 Solicitud de traducción de una dirección IP privada a una pública.

Cuando algún servidor se destinaría a publicar algún servicio, realizaba una asignación estática de una dirección homologada. Validado al administrador y los puertos que requeriría para su funcionamiento, aplicaba la traducción (NAT).

6.9 Realización de entregables.

Elaboré documentos mensuales reportando los acontecimientos más relevantes de las infraestructuras administradas de los clientes, de acuerdo con el formato previamente acordado por contrato.

6.10 Administración de servidor ACS.

Administré los servidores de autenticación, creando borrando y modificando privilegios de los diversos administradores de la red.

Por medio del servidor, realicé asignaciones de direcciones IP estáticas para los usuarios que requerían una comunicación segura hacia los recursos internos de la red. Para lo anterior se empleó la tecnología de redes privadas virtuales con el protocolo IPsec (Internet Protocol Security).

Configuré redes privadas virtuales LAN hacia LAN, entre los clientes y la organización. La negociación de los túneles para la comunicación segura, era realizada por los firewalls. Comúnmente una red privada virtual era para los segmentos de administración y otra para fines de monitoreo.

6.11 Realización periódica de respaldos.

Realicé continuamente respaldos de los distintos equipos de seguridad perimetral, con la finalidad de tener la capacidad de regresar a puntos de funcionamiento anteriores, (en los casos necesarios), o bien, para poder realizar comparaciones de cambios en los equipos dentro de períodos determinados. Lo anterior para garantizar un mejor control sobre el comportamiento de la red.

6.12 Participación en migraciones y mantenimiento (preventivo y correctivo) de la infraestructura.

Con la finalidad de seguir proporcionando los niveles de servicio comprometidos con los clientes, periódicamente se realizaron ventanas de mantenimiento a la

infraestructura de seguridad, durante las cuales se interrumpirán los servicios de conectividad.

En las ventanas, realicé actividades tales como:

- Actualizaciones de software.
- Cambios profundos en las configuraciones de los equipos.
- Cambios en los enlaces físicos.
- Sustitución de equipos.
- Integración de un nuevo dispositivo en la infraestructura.
- Integración o sustitución de componentes de un sistema.
- Migración de sistemas.

7. Resultados y aportaciones.

Proporcioné seguridad de la información a nivel perimetral a la organización y a los distintos clientes de la misma.

Con base en un enfoque de defensa a profundidad, por parte del área de implementación, se consideró un despliegue multicapas que conformó las distintas líneas de protección de la infraestructura. Se emplearon sistemas de prevención de intrusos, firewalls, enrutadores, conmutadores, software de protección para los usuarios finales y servidores, analizadores de redes y la consciencia acerca de vulnerabilidades capaces de explotarse con técnicas de ingeniería social.

Como miembro del área de seguridad perimetral, me encargué de administrar, operar y mantener en correcto funcionamiento los equipos firewall, IPS y sistemas especializados en análisis del tráfico de red. Además brindé apoyo a las diferentes áreas responsables de la operación de los demás dispositivos. Todo lo anterior, para cada una de las implementaciones de los clientes y la organización.

Posteriormente, apoyé en la integración de la más reciente solución de seguridad UTM, la cual permitió una administración más rápida de la solución perimetral (en cuanto a cambios en la configuración de los sistemas y garantía de la consistencia de dichas configuraciones entre éstos) ya que en un único dispositivo se integran las más útiles funcionalidades: firewall, establecimiento de VPN, IPS, Antivirus, Antispam, Filtrado de contenido, control de aplicación y prevención de pérdida de datos.

La solución UTM se implementó con otras líneas de protección, ya que el esquema de defensa a profundidad establece que una red se asegurará de forma efectiva, cuando se tienen múltiples mecanismos entre el adversario y el objetivo.

“An effective countermeasure is to deploy multiple defense mechanisms between the adversary and his target/…”[6].

Proveí atención a incidentes y requerimientos, con la finalidad de mantener en adecuada operación todas las infraestructuras, siempre con estricto apego a la documentación sobre la política de seguridad de la información de cada cliente, derivada del contrato con cada uno de éstos.

Monitoreé cada una de las infraestructuras, con la finalidad de que no se sobrepasaran los umbrales detectados de operación normal, ya que implicaría un riesgo potencial para los recursos el desviarse de la línea base. En las ocasiones

[6] Defense in depth. A practical strategy for achieving Information Assurance in today´s highly networked environments. National Security Agency. September, 2000

en que detecté anomalías, proporcioné una respuesta conforme al procedimiento previamente descrito.

8. Conclusiones.

Las situaciones siempre se mantuvieron bajo control y por lo general no se presentaron cantidades considerables de incidentes. Por otra parte, los incidentes generados no eran de gravedad. El apoyo que dediqué para la administración y operación de los equipos de seguridad perimetral, lo realicé de la manera correcta, apegada a las recomendaciones internacionales de organizaciones especialistas en ingeniería de ciberseguridad como NIST y CERT, foros globales de respuesta a incidentes de seguridad como FIRST y estándares de organizaciones como ISO.

En cuanto a mi experiencia profesional, la integración al área de seguridad perimetral me pareció rápida, ya que conté con el apoyo de mis compañeros y poseía fundamentos sólidos en cuanto al funcionamiento de redes de datos y configuraciones de dispositivos.

En general, empleé diversos conocimientos adquiridos a lo largo de la carrera, sobre todo en las materias impartidas de redes de datos y normalización. Contando con esa base de conocimiento, continué mi preparación tomando un curso de certificación del fabricante CISCO, paralelamente ingresando al Fondo de Información y Documentación para la Industria.

A lo largo de mi estancia, se me brindó capacitación para operar, mantener y administrar equipos de diversos fabricantes, lo cual no resulta complicado de aprender cuando se cuenta con un marco teórico adecuado.

La formación que obtuve de la Facultad de Ingeniería, me preparó para poder desempeñarme en diversas actividades, pues adquirí conocimiento de una amplia gama de tecnologías de la información, por lo que al optar por la parte de redes de datos, concretamente en la seguridad informática, contaba con lo requerido para desarrollarme no solamente gracias a la base teórica y práctica que adquirí a lo largo de mis estudios, sino también a hábitos como el autoestudio y de investigación en diversas fuentes bibliográficas y mesográficas, los cuales también fueron el resultado de dicha formación.

Es importante ser conscientes de las amenazas existentes (como las expuestas a lo largo de este informe), para entender los grandes beneficios en particular de la seguridad perimetral y su apoyo en la ardua tarea de protección de datos, evitando entre otros, fraudes y robo de información.

En el futuro cercano, pienso continuar capacitándome técnicamente y adquirir una mayor experiencia en cuanto a operación y administración de redes de datos, complementando mis conocimientos con temáticas orientadas al diseño e implementación, empleando las nuevas tecnologías que ofrecen los diversos fabricantes.

9. Bibliografía.

Watkins, Michael; Wallace Kevin.
CCNA Security.
CISCO Press.
USA, 2008

Tittel, Ed.
Unified Threat Management for Dummies.
Wiley.
USA, 2012

Tam, Kenneth; Hoz, Martín; McAlpine, Ken; Basile, Rick; Matsugu, Bruce; More, Josh.
UTM Security with Fortinet.
Syngress.
USA, 2013

Cole, Eric; Krutz, Ronald; Conley, James.
Network Secrity.
Wiley Publishing.
Secund Edition.
Canada, 2009

Fortigate Multi-Threat Security Systems I
Fortinet Training Services.
USA, 2011

Manual. Secure Network Deployment and IPsec VPN.
Fortinet Training Services.
USA, 2011