Universidad de Buenos Aires

Facultades de Ciencias Económicas, Ciencias Exactas y

Naturales e Ingeniería

Carrera de Maestría en Seguridad Informática

Trabajo Final de Maestría

Tema

Dispositivos UTM

Título

“Migración e implementación de un gestor unificado de amenazas (UTM)”

Autor: Ing. Javier Tiebas

Director: Ing. Hugo Pagola

Co-Director: Ing. Facundo Caram

Año de presentación 2019
Cohorte 2014-2015

1 Introducción

En una red de computadoras existen diversos dispositivos los cuales tienen funciones diferentes de acuerdo al papel que cumplan dentro de dicha red, uno de los dispositivos más importantes en cuanto a lo que se refiere a seguridad es el firewall, este es un dispositivo diseñado para bloquear el tráfico no autorizado o permitir el establecimiento de conexiones autorizadas, esta tarea la realiza a través de un conjunto de reglas preestablecidas donde se especifica qué tipo de tráfico se permitirá ingresar. Este tipo de dispositivo es la primera barrera de protección que tiene un equipo o una red frente a redes no confiables como Internet, aunque también pueden ser utilizados a nivel de una intranet para proteger segmentos sensibles dentro de una misma red. Estos dispositivos pueden existir tanto como hardware o como un software multiplataforma, en ambos casos los dispositivos deben estar actualizados para evitar la explotación de vulnerabilidades en los mismos. Con el avance de la tecnología los dispositivos van evolucionando y sumando características a su funcionalidad como es el caso de los dispositivos UTM (por sus siglas en inglés *Unified Threat Management*), estos dispositivos cumplen la función de un firewall y también agregan un conjunto de características de seguridad las cuales son administradas de forma centralizada desde una misma consola. Estas características suelen ofrecerse como un producto totalmente separado, pero en un dispositivo UTM vienen totalmente integradas lo que simplifica la administración y control de las mismas.

2 Objetivos

El objetivo de este trabajo es reemplazar el actual firewall por un sistema tipo UTM en busca de:

- aumentar y centralizar las herramientas de protección contra ataques maliciosos,
- mejorar la visibilidad de los eventos de seguridad que se producen en el perímetro de la red,
- incrementar la velocidad de respuesta ante un incidente de seguridad,
- aumentar el detalle de la información provista por reportes existentes y la generación de nuevos reportes,
- cumplir con las buenas prácticas en cuanto a soporte y mantenimiento de versiones del software instalado.

En el proceso de la migración se detallan el procedimiento a seguir, así como también los servicios adicionales que prestará el proveedor seleccionado.

3 Conceptos

Comenzaremos por definir un conjunto de conceptos.

3.1 UTM

Según Wikipedia [1] UTM (en inglés: Unified Threat Management) o Gestión Unificada de Amenazas, es un término que se refiere a un dispositivo de red único con múltiples funciones, las funcionalidades básicas que debe tener son:

Antivirus

Firewall (cortafuegos)

Sistema de detección/prevención de intrusos

Los más recientes dispositivos tienen las siguientes funcionalidades extras, haciéndolos más integrales:

- NAT
- VPN
- Antispam
- Antiphishing
- Antispyware
- Filtro de contenidos
- Detección/Prevención de Intrusos (IDS/IPS)

El término fue utilizado por primera vez por Charles J. Kolodgy, de International Data Corporation (IDC), en 2004. En un reporte llamado "Worldwide Threat Management Security Appliances 2004-2008 Forecast and 2003 Vendor Shares: The Rise of the Unified Threat Management Security Appliance", en el cual describe las funcionalidades básicas de un dispositivo UTM. Las siguientes características son ventajas y desventajas de un UTM:

Ventajas

- Flexibilidad

- Bajo costo
- Reduce la complejidad
- Integración Completa

  Desventajas
- Único punto de falla
- Puede tener problemas de rendimiento al tener todas las herramientas activas.
- Para algunos servicios requiere suscripción.

  Debido a que es el único punto de fallo, algunas empresas optan por un segundo UTM u otro firewall que le proporcione una seguridad adicional.

3.2 Diferencia entre UTM y NGFW

De acuerdo con el sitio oficial de Sophos [2]:

“Muchas veces, las compañías de seguridad usan términos técnicos de manera inconsistente, lo que lleva a cierta confusión. Nos gustaría aclarar lo que entendemos por administración de amenazas unificada (UTM) y firewalls de próxima generación (NGFW).

En esta simple infografía (fig 1), definimos lo que para Sophos significa un UTM, y explicamos cómo un UTM es similar pero diferente de un NGFW. Aunque algunas personas usan los términos indistintamente, existen diferencias clave.

Como explicamos a continuación, los firewalls de próxima generación (NGFW) se definen normalmente como firewalls mejorados con prevención de intrusos e inteligencia de aplicaciones. Por otro lado, los sistemas UTM incluyen esas características, además de tecnologías adicionales como seguridad de correo electrónico, filtrado de URL, seguridad inalámbrica, firewalls de aplicaciones web y redes privadas virtuales (VPN). En esta vista (fig 1), los sistemas UTM incluyen NGFW como componentes.”

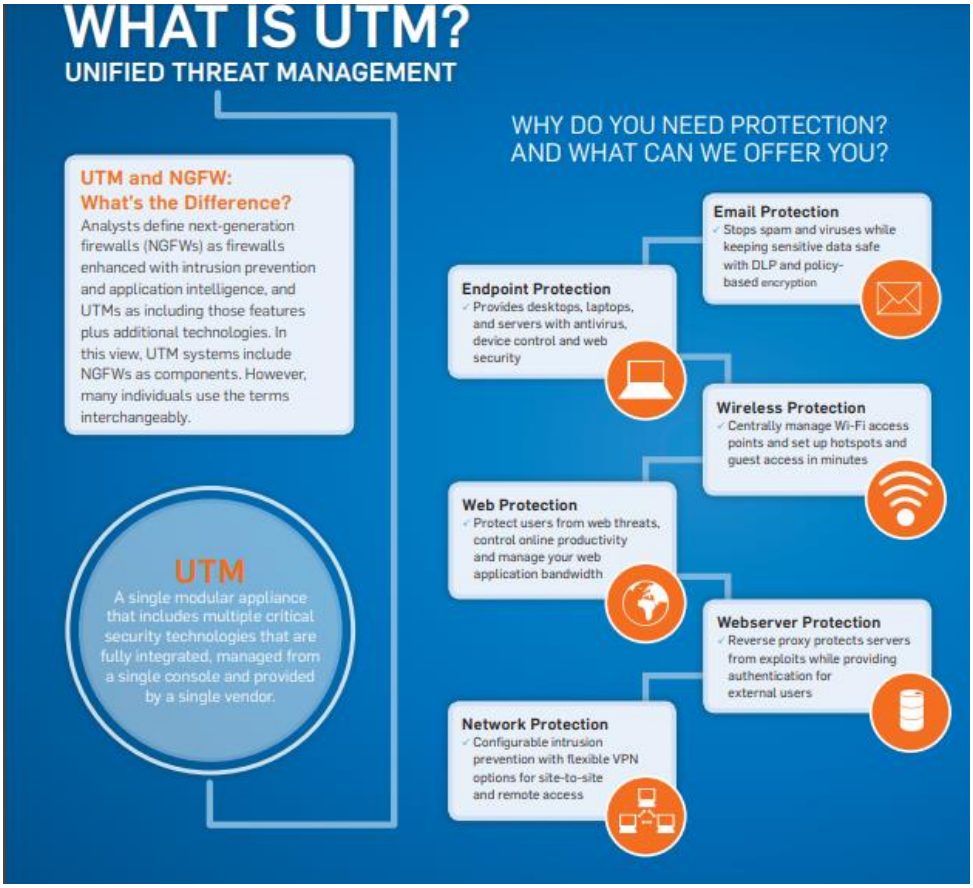


Fig 1

En libro de Kenneth Tam y Martin Hoz Salvador “UTM Security with Fortinet” [3] se desarrollan los siguientes conceptos, básicos para el entendimiento de un UTM.

3.3 Firewall

Probablemente el firewall sea la tecnología de seguridad de red más básica, necesaria e implementada. La responsabilidad del firewall es permitir o denegar las comunicaciones que entren o salgan de un host, una red o un grupo de redes. Las comunicaciones se permiten o deniegan según un conjunto de políticas o reglas. Estas reglas pueden ser algo simple (similar a las listas de control de acceso en un conmutador o enrutador) o algo realmente complejo, como la hora, los usuarios, los segmentos de red y mucha más información completa sobre el contexto

de la conexión. El firewall también es responsable de verificar la integridad de algunas comunicaciones, asegurar que las conexiones recibidas se adhieran a los estándares de la red y que no estén realizando actividades sospechosas u obviamente peligrosas. La tecnología de Firewall más utilizada en todo el mundo es la Inspección de estado, que permite rastrear las conexiones por estado, registradas en una tabla de sesión. Los firewalls también tienen tareas de autenticación, ya que es una forma de rastrear el origen de una conexión. Dado que el firewall es regularmente la base para otras inspecciones, es obligatorio que el firewall sea lo más rápido posible, preferiblemente una velocidad de cable a través de una amplia gama de tamaños de paquetes, ya que de lo contrario el firewall se convertiría en un cuello de botella en la red, aumentando la tentación de eliminarlo.

3.4 VPN (red privada virtual)

Permite que las comunicaciones entre dos o más puntos dados sean privadas. Dichos puntos pueden ser un host, una red o un grupo de redes. Las comunicaciones se aseguran utilizando uno de los diversos algoritmos de cifrado disponibles que ocultan la información que se transfiere y también aseguran que no se modifique mientras se encuentra en tránsito, lo que brinda privacidad. Las tecnologías VPN más comunes son IPSec VPN y SSL VPN. Dado que la VPN podría transportar la mayor parte del tráfico, si el intercambio de información se produce solo entre partes específicas, es de suma importancia tener el mejor rendimiento posible, y se prefiere la velocidad del cable. Una VPN es un complemento perfecto para un dispositivo de firewall, ya que de esa manera el firewall puede inspeccionar el tráfico que ingresa a la VPN, y la VPN puede proteger el tráfico permitido por el firewall.

Traffic Shaping: es un módulo que permite la regulación de la forma en que los recursos de red se asignan a las entidades que los solicitan. Una vez que las aplicaciones con uso intensivo de ancho de banda, como el

uso compartido de archivos o aplicaciones Peer-to-Peer (p2p) tienen que competir con aplicaciones sensibles al ancho de banda o latencia, como Voz sobre IP (VOIP) en una red que tiene límites, se hizo necesario tener una manera de regular cómo es asignado el ancho de banda. Los mecanismos de conformación de tráfico hacen esto retrasando los paquetes correspondientes a las aplicaciones, usuarios o direcciones IP etiquetadas con baja prioridad en un entorno de seguridad, el tráfico que se encuentra "limpio" por los mecanismos de seguridad se puede priorizar de acuerdo con las reglas comerciales, lo que podría ayudar a mantener la disponibilidad del servicio para Servicios críticos. Por este motivo, tiene sentido implementar Traffic Shaper en el mismo dispositivo físico que ejecuta un firewall.

3.5 IPS (Sistema de protección contra intrusiones)

También conocido como Sistema de prevención de intrusiones (IPS) o Sistema de detección y protección de intrusiones (IDP). Un IPS no debe confundirse con un IDS (Sistema de detección de intrusos), ya que un IDS solo puede detectar, pero no reaccionar, mientras que un IPS puede detectar y reaccionar ante un evento. Un IPS basado en la red realiza un análisis profundo del tráfico para que los ataques basados en la red puedan detectarse. Estos ataques a menudo se realizan tratando de aprovechar una vulnerabilidad conocida en el sistema operativo o el software de la aplicación. Una técnica típica de IPS es reconocer patrones de mal comportamiento conocido, de modo que cuando se realiza un ataque, se puede detectar simplemente identificando su "firma" (el patrón conocido). Esto se conoce como detección de mal uso. Otra técnica común consiste en aprender o pre configurar cuál es el comportamiento común y luego detectar las desviaciones, como las desviaciones de un estándar de protocolo o las estadísticas del entorno conocido. Esto se conoce como detección de anomalías. Los robustos sistemas de protección contra intrusiones utilizan ambas tecnologías para aumentar la eficacia. Un IPS

es un gran compañero de un servidor de seguridad porque entonces el tráfico permitido puede ser inspeccionado aún más y los ataques (intencionales o accidentales) generados por fuentes confiables pueden ser detectados y detenidos. A veces se usa un IPS para medir la efectividad del firewall, midiendo los ataques antes y después de que el firewall bloquee el tráfico.

3.6 Application Control (Control de aplicación)

Es un módulo que da lugar o permite el tráfico de una aplicación determinada, independientemente del método (puerto, protocolo, aplicación) utilizado para transferir el tráfico. Dado que las aplicaciones ejecutan cada vez más su tráfico en los mismos puertos de red para garantizar un comportamiento exitoso de la aplicación, es importante contar con un mecanismo que pueda identificar y controlar estas aplicaciones de manera efectiva. El control de aplicaciones es un mecanismo que se creó para resolver esta necesidad, y lo hace de manera muy similar a como IPS reconoce los ataques: creando "firmas" del tráfico generado por las aplicaciones y luego reconociendo estas firmas en el flujo de tráfico. Application Control es un gran compañero de un firewall porque permite una ejecución más profunda, al extender al nivel de la aplicación los criterios para permitir o denegar el tráfico.

3.7 AntiSpam

Es un módulo que detecta y elimina mensajes de correo electrónico no deseado (spam). Regularmente aplica mecanismos de verificación para determinar si el correo electrónico es spam. Algunos de estos mecanismos son bastante simples, como rechazar mensajes de una lista de delincuentes conocidos. Otros mecanismos implican comparar el mensaje recibido con una base de datos de mensajes mal conocidos y una lista centralizada de servidores de correo conocidos que se utilizan para enviar SPAM. Dado que normalmente los mensajes de SPAM provienen de fuera

de la organización, tiene sentido analizar el tráfico de correo en el borde de la red justo después de que haya sido autorizado por el firewall. Debe tenerse en cuenta que prevenir el envío de spam se vuelve importante cuando se considera en el contexto más amplio de su reputación en Internet.

3.8 Antivirus

Los virus son probablemente uno de los primeros problemas que tuvieron los usuarios de computadoras una vez que las computadoras se volvieron personales. Debido a esto, los virus son probablemente la forma más diversa de problemas informáticos relacionados con la seguridad, y se deduce que Antivirus es probablemente el mecanismo de protección más conocido. Básicamente, un antivirus es responsable de detectar, eliminar e informar sobre códigos maliciosos. El código malicioso (malware) puede ser un código de auto replicación que se adjunta a programas válidos (virus), programas que parecen ser una aplicación válida para que los usuarios los ejecuten (troyanos) u otro tipo de malware, como spyware o adware. Si bien el Antivirus se implementa normalmente en el nivel del host, un Antivirus de red, un mecanismo que detecta y detiene el código malicioso en el punto donde el contenido está saliendo o ingresando a una red, se vuelve importante cuando es necesario garantizar que todas las computadoras en dicha red tengan la Mismo nivel de protección, probablemente adicional a la protección ya implementada directamente en los hosts. Antivirus es un gran compañero de un sistema de firewall porque puede buscar códigos maliciosos de maneras muy específicas sobre el tráfico permitido, pero para hacerlo de manera efectiva necesita tener un alto rendimiento para que no se convierta en un cuello de botella: esta es la razón por la cual debe acelerarse y es por eso que es más efectiva si solo se ve en el tráfico que ha sido aprobado por un mecanismo de seguridad más rápido, como un firewall.

3.9 DLP (Prevención de fugas de datos)

Es un módulo que ayuda a rastrear el contenido específico que ingresa o sale de la red. Puede buscar contenidos muy específicos, como palabras dentro de un mensaje de correo electrónico o frases dentro de un archivo PDF. A medida que aumentan las regulaciones, el DLP se hizo más importante ya que puede distinguir entre ataques y comportamiento legítimo. Un ejemplo típico es cuando un empleado envía desde su correo electrónico corporativo información clasificada como listas de clientes, cuentas de cheques o números de tarjetas de crédito: no es un virus y ciertamente no es un ataque a la red. Sin embargo, si esto lo realiza alguien del departamento técnico y no el departamento de contabilidad, es posible que tenga motivos para preocuparse. Este es el problema genérico que DLP intenta resolver: detectar el mal comportamiento humano que no necesariamente infringe una regla desde el punto de vista técnico. Debido a esto, DLP es una gran adición a los dispositivos de firewall, IPS y Antivirus, ya que puede complementarlos detectando cosas que esos mecanismos simplemente no pueden debido a su naturaleza.

3.10 Filtro de contenido web (filtro de URL)

Es un mecanismo que permite o bloquea el tráfico web, según el tipo de contenido. El método más común es clasificar las páginas web en categorías. Estas categorías genéricas suelen ser amplias, como sitios web de Juegos, Finanzas y Banca, Uso compartido de archivos, almacenamiento o phishing. Tiene sentido implementar un filtro de contenido web en el mismo dispositivo donde se ejecuta un firewall, porque el filtro de contenido web puede mejorar enormemente la granularidad de la política de navegación web. Además, tiene mucho sentido implementar un Antivirus de red y un IPS en conjunto con el filtro de contenido web, ya que de esta manera se garantiza que los usuarios obtengan un tráfico limpio.

3.11 Caché

Un sistema de caché almacena localmente una copia de algún contenido que puede ser solicitado por más de un usuario, por lo que la próxima vez que un usuario lo solicite, no es necesario descargar el contenido del sitio remoto, lo que ahorra tiempo y ancho de banda. El tipo más común de caché es el caché web, pero no es el único. Tiene sentido implementar un sistema de caché junto con otras tecnologías de seguridad como un firewall, un Antivirus y un filtro de contenido web, porque es más eficiente almacenar contenido local que fue autorizado e inspeccionado previamente.

3.12 Optimización de WAN

Es una serie de mecanismos que ayudan a reducir la cantidad de tráfico que pasa a través de los enlaces WAN, evitando el uso de ancho de banda costoso. El caché es uno de los mecanismos utilizados para la optimización de WAN, pero no el único, ya que también se utilizan otras técnicas, como la optimización de TCP, la deduplicación y el almacenamiento en caché de bytes. Si bien esta no es necesariamente una tecnología de seguridad en sí misma, las técnicas de optimización de WAN pueden ayudar a reducir la posibilidad de ciertos ataques, como la denegación de servicio. Sin embargo, el beneficio real de esta tecnología es la posibilidad de reducir los costos del enlace WAN y, para ciertas aplicaciones como las aplicaciones web, le da al usuario la "ilusión" de que la aplicación es más rápida de lo que realmente es. Dado que las tecnologías de optimización de WAN suponen que el tráfico que procesarán es válido, es una buena idea asegurarse de que dicho tráfico esté limpio. Después de todo, no tiene sentido "optimizar" y asegurarse de que un ataque o la propagación de un virus obtenga mejores tiempos de respuesta de la red. Debido a esto, y al hecho de que la optimización de WAN se implementa normalmente en la frontera de la red, tiene sentido

integrar la optimización de WAN en un dispositivo de seguridad de red, especialmente uno que puede tener Firewall, Network Antivirus e IPS.

3.13 Inspección SSL

Proporciona la capacidad de inspeccionar contenido cifrado por aplicaciones que utilizan la técnica criptográfica Secure Socket Layer. La técnica utilizada para realizar esta función requiere que la comunicación fluya a través de la solución en la que realizaría una toma de control de la sesión SSL. Con esta capacidad, se pueden aplicar varias características de inspección de seguridad al contenido, como DLP, filtrado de contenido de páginas web y Antivirus. Ejemplo de aplicaciones cifradas basadas en SSL es la sesión de navegación web utilizando HTTPS, transferencias de archivos con FTPS y correo electrónico cifrado con SMTPS, POP3S e IMAPS.

4 Problemática actual

Actualmente nuestra empresa posee un producto de Microsoft denominado Threat Management Gateway o más conocido por su abreviatura TMG. Es un producto que posee varias características que lo convierten en una herramienta robusta, tiene configuradas y en uso gran parte del total de sus características.

El Forefront TMG ha dejado de tener soporte estándar en el año 2015 y cuyo soporte extendido finaliza en el año 2020. Si bien existe un soporte extendido el mismo no incluye solicitudes de cambios de características y diseño del producto, lo que significa que no ha recibido mejoras desde el año 2015, lo cual pone al TMG en desventaja con los nuevos productos de seguridad que existen en el mercado actualmente. Esta falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto y como resultado, es probable que se descubran vulnerabilidades de seguridad las cuales podrían no llegar a ser corregidas por parte de Microsoft.

Además del problema del soporte del producto, lo que también se buscaba era incorporar una herramienta que simplificara las tareas del área de Seguridad Informática en la protección contra diferentes tipos de amenazas de seguridad, es por eso que se focalizó la búsqueda en un producto tipo UTM que reuniera un conjunto de aplicaciones integradas en una misma consola de administración.

En base a esta problemática detallada se decide buscar un reemplazo para el viejo TMG y junto con esto incorporar nuevas características que permitan tener mayor protección y visibilidad de todos los eventos relacionados con la seguridad de la información que se van sucediendo en la infraestructura de la empresa.

4.1 UTMs

Como base para el análisis de los diferentes productos disponibles en el mercado se utilizó el reporte emitido por Gartner ya que es una empresa líder mundial de investigación y asesoramiento tecnológico y sus reportes son referentes mundiales para la toma de decisiones en la compra de TI. El conjunto de servicios que Gartner brinda incluye el asesoramiento estratégico y mejores prácticas comprobadas para ayudar a los clientes a tener éxito en su misión. Estos informes proporcionan información sobre las principales tendencias comerciales y tecnológicas que ayudan a las áreas responsables en la toma de decisiones.

¿Qué son los sistemas de gestión unificada de amenazas (UTM)? Según Gartner en [4] “Gartner define el mercado de la gestión unificada de amenazas (UTM) como los firewalls multifuncionales utilizados por pequeñas y medianas empresas (PYME). Típicamente, las empresas medianas tienen de 100 a 1,000 empleados. Los proveedores de UTM agregan continuamente nuevas funciones en las plataformas de UTM y, por lo tanto, abarcan el conjunto de características de muchas otras soluciones de seguridad de red, que incluyen:

- Firewall
- Sistemas de prevención de intrusos (IPS)
- VPN
- Pasarela web segura (SWG)
- Consola de administración centralizada
- Detección avanzada de malware.”

En su informe anual [5] Gartner define las necesidades de las pymes:

“Administración basada en navegador, facilidad de configuración, informes integrados, VPN, software localizado, el excelente soporte y la documentación por parte de los partners, no son requerimientos exclusivos de las grandes empresas, sino que son muy valorados por las pymes en este mercado. Gartner ve demandas muy diferentes de los mercados de firewall de grandes empresas y de las sucursales. Estas grandes

empresas generalmente requieren características de seguridad de red más complejas y son optimizadas para criterios de selección muy diferentes. Pequeñas empresas con menos de 100 empleados tienen aún más presiones presupuestarias y aún menos presiones de seguridad que las organizaciones más grandes. Por estas razones, este Magic Quadrant se centra en los productos UTM utilizados por las medianas empresas. A menudo las sucursales de las grandes empresas tienen diferentes demandas de seguridad que las medianas y pequeñas empresas, aunque sean de tamaño similar. Las grandes empresas a menudo utilizan productos empresariales de gama baja en sus sucursales para garantizar la interoperabilidad y para aprovechar las economías de escala al obtener mayores descuentos de sus proveedores de firewall. Por esta razón, Gartner asigna al firewall de sucursal al mercado de firewall de grandes empresas y no al mercado de UTM”

Gartner en su reporte ubica los diferentes proveedores en un diagrama denominado “cuadrante mágico de Gartner” (Fig 2), este diagrama es una herramienta gráfica en la cual compañías más relevantes de cada industria tecnológica se ven posicionadas de acuerdo a su desempeño anual dentro de su propio mercado y de esta manera permite la comparación con los diferentes proveedores.

Fig 2.

4.2 Cuadrante de Gartner

El cuadrante está dividido en cuatro sectores:

- Líderes,
- Retadores,
- Visionarios y
- Jugadores de Nicho.

Cada uno de estos cuadrantes están definidos por Gartner en [5].

4.2.1 Líderes

El cuadrante de líderes contiene proveedores a la vanguardia en la fabricación y venta de productos UTM que se construyen para los requisitos de la mediana empresa. Los requisitos necesarios para el liderazgo incluyen una amplia gama de modelos para cubrir casos de uso de medianas empresas, soporte para múltiples funciones y capacidad de gestión y generación de informes diseñada para facilitar su uso. Vendedores en este cuadrante lideran el mercado ofreciendo nuevas funciones de protección y permitiendo a los clientes implementarlas a un bajo costo sin afectar significativamente la experiencia del usuario final ni aumentando la carga de trabajo del personal. Estos proveedores también tienen un buen historial evitando vulnerabilidades en la seguridad de sus productos. Las características comunes incluyen confiabilidad, rendimiento consistente y productos que son intuitivos de gestionar y administrar.

4.2.2 Retadores

El cuadrante de Retadores (Challengers) contiene proveedores que han logrado una sólida base de clientes, pero no están liderando en características. Muchos Challengers tienen otros productos de seguridad exitosos en el mundo y se basan en la relación con el cliente o la fortaleza del canal, en lugar del producto para ganar nuevas ventas. Los productos de Challengers a menudo tienen un buen precio, y estos proveedores pueden ofrecer paquetes de productos económicos que otros no pueden. Muchos de los Challengers se abstienen de convertirse en líderes porque están obligados a mantener los productos de seguridad o firewall con una prioridad más baja en el conjunto de productos generales que ofrecen.

4.2.3 Visionarios

Los visionarios tienen los diseños y las características correctas para las medianas empresas, pero carecen de la base de ventas, estrategia o medios financieros para competir globalmente con Líderes y Retadores.

La mayoría de los productos de los Visionarios tienen buenas capacidades de seguridad, pero carecen de la capacidad de rendimiento y el soporte de red. Las organizaciones dispuestas a actualizar sus productos con frecuencia se ven beneficiadas y pueden ahorrar al realizar un cambio de proveedor. Si la seguridad de la tecnología es un elemento competitivo para la organización, entonces los Visionarios son candidatos.

4.2.4 Jugadores de nicho

La mayoría de los proveedores en el cuadrante de “Jugadores de nicho” están centrados en la empresa o en la pequeña oficina en su acercamiento a dispositivos UTM para pymes. Algunos jugadores especializados se centran en industrias verticales específicas o geografías. Si las PYMES ya son clientes de estos proveedores para otros productos, entonces los Jugadores de Nicho pueden ser preseleccionados.

5 Selección del producto

Para la selección del producto es muy importante realizar un análisis previo sobre las distintas alternativas y también de ser posible sería muy recomendable realizar pruebas con equipos reales en ambientes productivos (con pruebas en ambientes productivos nos referimos a únicamente medir el tráfico en la red), con esto se puede tener una visión más real sobre el producto y también se puede estimar el tipo y tamaño de equipo a adquirir, también es muy útil tener una consola donde se pudiera "jugar" un poco con el producto para poder conocerlo. Estas pruebas deben realizarse con varios productos, no únicamente con el elegido, ya que luego de utilizar las diferentes opciones se puede tener una visión mucho más objetiva sobre el producto a adquirir.

La selección del producto se basó en el reporte emitido por Gartner [5], de este informe se seleccionaron tres proveedores, dos correspondientes al cuadrante de líderes y uno del cuadrante de visionarios.

Dada una cuestión de prioridades en cuanto a los tiempos asignados para realizar el análisis de los productos, únicamente se seleccionaron los tres productos más relevantes a nuestro criterio y se puso el foco solamente en esos productos, estos fueron los correspondientes a Fortinet, Sophos y WatchGuard.

A continuación, se adjuntan los informes emitidos por Gartner para cada uno de los productos que hemos seleccionado:

5.1 Fortinet

Fortinet sigue siendo un líder, y lidera la participación de mercado en UTM con un margen enorme sobre otros vendedores de UTM en el mercado. También lidera en el mercado y en la ejecución de ventas. La ampliación de la cartera de sus productos está soportada con el crecimiento de los ingresos y con grandes acuerdos con empresas medianas que desean consolidar hacia un único proveedor de seguridad de red.

Fortinet es un jugador tanto de redes como de seguridad, con sede en Sunnyvale, California. Está regularmente expandiendo su cartera de productos, con las recientes incorporaciones de FortiWeb (su firewall de aplicaciones web),FortiMail, FortiSandbox, FortiSIEM y FortiCASB. Sus otros productos en la cartera cubren seguridad de red, seguridad de endpoint, access point inalámbricos y switches. Los firewalls de FortiGate siguen siendo su producto más popular y de mayor venta.

Las actualizaciones recientes incluyen que Fortinet amplíe su soporte a múltiples plataformas públicas de IaaS, incluidas Google, IBM y Oracle. También introdujo sus dispositivos de firewall E-Series. Las actualizaciones más importantes incluyen el lanzamiento de FortiOS 5.6 en 2017 y FortiOS 6.0 en agosto de 2018.

Fortinet sigue siendo visible en las listas de candidatos de UTM de SMB que buscan funciones sólidas de seguridad inalámbrica. También es una buena opción en la lista de candidatos para pymes que están buscando consolidar hacia un solo proveedor sus otras necesidades de seguridad de red, como los firewalls para aplicaciones web y los sistemas de información de seguridad y gestión de eventos (SIEM). El vendedor también está ganando negocios donde la adopción de SD-WAN es el principal caso de uso.

5.1.1 Fortalezas

5.1.1.1 Ejecución de ventas

Fortinet es preseleccionado frecuentemente por las PYMES, lo que lo convierte en uno de los principales proveedores con la mayor cuota de mercado en el mercado UTM. Fortinet es el proveedor de UTM más visible en la lista de candidatos de Gartner.

5.1.1.2 Ejecución del mercado

Fortinet muestra una sólida ejecución del mercado al centrarse en los lazos de asociación con los clientes. Eso tiene fuertes vínculos de asociación con múltiples MSSP (Managed Security Service Provider) clave a nivel mundial para admitir modelos híbridos y tradicionales en el

despliegue de productos. Su estrategia de producto tiene un fuerte enfoque en las características más favorables de MSSP, como la gestión centralizada que ofrece para dominios administrados, API XML / JSON para aprovisionamiento de back-end y portales personalizados.

5.1.1.3 Producto

La función de controlador inalámbrico integrado en la solución UTM de Fortinet es una herramienta sólida y una característica deseable para las pymes. Fortinet ha integrado un controlador inalámbrico completo en el firewall, permitiendo así la gestión de la red inalámbrica como parte de la solución de seguridad. Esto es totalmente gestionado por FortiCloud y FortiManager.

5.1.1.4 Capacidad

Fortinet ofrece control y administración unificados en sus múltiples líneas de productos a través de Fortinet Security Fabric y continúa centrándose en las mejoras en las características de Security Fabric. Esto permite a los clientes existentes de Fortinet que utilizan múltiples productos Fortinet tener monitoreo central y control a través de diferentes dispositivos Fortinet en sus redes o a través de múltiples redes.

5.1.1.5 Estrategia del producto

Fortinet ha ampliado el soporte para múltiples plataformas en la nube: AWS, Azure, Google Cloud Platform, IBM Cloud y Oracle Cloud Infrastructure (OCI; tanto VM como Bare Metal) - que muestra su compromiso y enfoque en la expansión de las plataformas públicas de IaaS.

5.1.1.6 Oferta

Fortinet ofrece el Servicio de Seguridad Industrial FortiGuard, que proporciona la firma de actualizaciones para los protocolos comunes de control de supervisión y adquisición de datos (SCADA). Esta viene como una suscripción independiente, que puede ser utilizada por las PYMES que operan estos sistemas.

5.1.2 Precauciones

5.1.2.1 Estrategia de producto

Fortinet se está enfocando más en las grandes empresas y en acuerdos más grandes que involucran múltiples productos Fortinet más allá de un simple firewall. Esto ha impactado su calidad de soporte de preventa para las pymes. Algunos clientes de Gartner han informado que han recibido poco apoyo de preventa por parte del equipo de Fortinet en comparación con otros competidores líderes en el mercado.

5.1.2.2 Característica

Fortinet UTM carece de soporte incorporado para la cuarentena y el cifrado del correo electrónico del usuario final. Los clientes tienen que usar FortiMail, que es un producto separado, para obtener estas características.

5.1.2.3 Producto

FortiCloud, que es el portal de administración centralizado y basado en la nube, ofrece una cantidad limitada de capacidades en comparación con las capacidades de gestión en las versiones on-premise y también carece funcionalidades granulares.

5.1.2.4 Experiencia del cliente

Los clientes encuestados han indicado que las principales actualizaciones de firmware vienen con importantes cambios en la interfaz de usuario de administración que dificultan la administración del firewall e involucran una curva de aprendizaje. También han destacado que las actualizaciones de firmware tienen errores y necesitan más pruebas antes de su lanzamiento.

5.1.2.5 Capacidades

FortiClient para la seguridad de endpoints ofrece parcialmente la funcionalidad de endpoint detection response (EDR). FortiCASB proporciona capacidades básicas para el monitoreo y control de SaaS, pero carece de integración con FortiManager. Gartner no ha visto la inclusión de FortiClient y FortiCASB con las ofertas de firewall.

5.2 Sophos

Sophos sigue siendo un líder este año debido a su fuerte enfoque continuo en la mejora en las capacidades de prevención de malware a través de sus firewalls e integración de plataforma de endpoint. Sigue siendo el líder del mercado, ofreciendo una gestión integrada, supervisión y monitoreo de los endpoints a través de una única consola en su oferta UTM, que proporciona facilidad de gestión y mejor prevención contra malware avanzado.

Sophos es un proveedor de seguridad de endpoints y redes con sede en Abingdon, U.K. La cartera de productos de Sophos incluye firewalls (series XG, las series más antiguas SG y CR). Sophos tiene 19 modelos XG y tres modelos de dispositivos Ethernet remotos (RED), que son dispositivos plug-and-play para pequeñas oficinas. Todavía vende sus antiguas líneas de productos, la serie de firewall SG y CR. También ofrece otras soluciones de seguridad para endpoints, punto de acceso inalámbrico (Sophos AP Series) y gestión unificada de endpoints (Sophos Mobile). Sophos Firewall Manager (SFM) es el nombre del software de administración centralizada, y Sophos Central es el portal de gestión centralizada basado en la nube para todos los productos de seguridad de Sophos.

Las actualizaciones recientes incluyen una nueva versión 17 para el Firewall XG con control mejorado de aplicaciones aprovechando la integración de endpoints, así como una actualización de su solución Sandstorm cloud Sandbox con la integración de su producto de endpoint de próxima generación (Intercept X).

Sophos es un buen candidato para pymes que buscan múltiples funciones integradas, como correo electrónico y DLP web, cifrado de correo electrónico y un web application firewall (WAF) dentro del firewall.

Sophos también es un buen candidato para PYMES que buscan una integración de endpoints fuerte y con capacidades maduras integradas

dentro de sus soluciones UTM para facilitar la gestión y la correlación de eventos.

5.2.1 Fortalezas

5.2.1.1 Ejecución de ventas

Sophos Cloud Firewall Manager es la solución gratuita de Sophos basada en la nube para que los socios gestionen múltiples firewalls en sus clientes. Las capacidades de Sophos Cloud Firewall Manager incluyen la mayoría de las funciones disponibles en la versión on-premise lo que facilita la administración de los firewalls.

5.2.1.2 Estrategia de ventas

Sophos tiene una sólida estrategia de canal, con una base de canales leales a nivel mundial. Lleva a cabo programas regulares de formación de los partners e intercambio de información en todo el mundo. Gartner ha visto que este canal tiene una gran confianza en el equipo de Sophos y su estrategia de ventas, especialmente después de la adquisición de Cyberoam. El equipo de preventa de Sophos recibe críticas positivas por trabajar directamente con los clientes en regiones como India y Medio Oriente, y con frecuencia recibe una calificación alta de los clientes.

5.2.1.3 Capacidad de respuesta del mercado

Sophos continúa aumentando la visibilidad, detección y capacidad de respuesta contra amenazas avanzadas para cumplir con el creciente requerimiento del mercado. También ha hecho mejoras en las funciones de control de aplicaciones existentes en los firewalls para una mejor visibilidad y control. Sophos también adquirió Barricade para mejorar las capacidades de análisis de seguridad, y ha integrado las capacidades de aprendizaje profundo de Invincea en su producto de sandbox Sandstorm.

5.2.1.4 Producto

Sophos XG Firewalls ofrece múltiples funciones de seguridad dentro de su solución UTM que solicitan las pymes. Esto incluye firewalls de aplicación

web incorporados, cifrado basado en DLP para Correos electrónicos y fuerte integración de endpoints.

5.2.1.5 Experiencia del cliente

Los clientes de Sophos encuestados han mencionado una integración fuerte entre el firewall y los endpoints como la mayor fortaleza del producto, y también han indicado una alta satisfacción por la tasa de detección de malware. Esto se debe a que, además de que tradicionalmente se gestionan los endpoints de forma centralizada desde la interfaz de usuario del firewall, ha creado capacidades de monitoreo y respuesta, para amenazas avanzadas utilizando su función de seguridad Heartbeat, que es parte de su Sistema de Seguridad Sincronizado.

5.2.1.6 Capacidad

Sophos tiene una gran capacidad de detección de ransomware y trabaja constantemente para mejorarla. Recientemente, Sophos ha anunciado Synchronized Application Control, otra característica de seguridad sincronizada que utiliza el endpoint para proporcionar visibilidad adicional al tráfico de aplicaciones en la red.

5.2.2 Precauciones

5.2.2.1 Estrategia de producto

A pesar de vender tres líneas de productos de firewall, XG, SG y CR, Sophos continúa enfocándose en mejorar las características de la serie XG. Las series SG y CR siguen siendo soportadas por el proveedor, y Sophos recientemente actualizó su serie de firewall SG y XG. Gartner recomienda a los clientes que evalúen cuidadosamente la hoja de ruta y las actualizaciones de firmware en caso de que aún quieran hacer nuevas compras de la serie CR y la serie SG, debido a la familiaridad con el producto.

5.2.2.2 Comentarios de clientes

Gartner ha notado una disminución en la satisfacción del cliente, particularmente sobre facilidad de despliegue y gestión de la serie XG.

5.2.2.3 Capacidades

Sophos no ofrece una función dedicada de SD-WAN. Sin embargo, ofrece funciones limitadas relacionadas con SD-WAN, tales como QoS, balanceo de enlaces (basado en volumen [peso]), sesiones y protocolos.

5.2.2.4 Capacidades

Sophos actualmente carece de un portal centralizado de administración de la nube para usuarios finales. Sophos ofrece Cloud Firewall Manager, que proporciona administración centralizada basada en la nube sólo a sus partners.

5.2.2.5 Experiencia del cliente

Los clientes encuestados calificaron la solución UTM de Sophos limitada. Basado en los comentarios de los clientes, la interfaz integrada del dispositivo es muy limitada. Para obtener mejores informes de toda la plataforma de Sophos, los clientes deben utilizar iView.

5.3 WatchGuard

WatchGuard se encuentra en el cuadrante de visionarios, ya que continúa centrándose en los requisitos de seguridad del mercado de las pymes. Constantemente introduce mejoras para mejorar las capacidades de prevención contra amenazas avanzadas y capacidades de correlación entre los endpoints y los UTM. Su hoja de ruta también muestra un fuerte enfoque en mejorar las capacidades de detección y respuesta de un usuario final en la red.

WatchGuard tiene su sede en Seattle, Washington. Su cartera de productos incluye ofertas de UTM, seguridad con múltiple factor de autenticación(MFA) para endpoints y puntos de acceso inalámbricos. Su línea de productos UTM se llama Firebox. WatchGuard Dimension es su producto de gestión centralizada. WatchGuard también ofrece dispositivos virtuales, como XTMv, FireboxV y Firebox Cloud para el despliegue en la nube pública. Su producto de endpoint se llama WatchGuard Host Sensor.

Las noticias recientes de WatchGuard incluyen la introducción de seis nuevos modelos UTM de la Serie T (sobre mesa) y cuatro nuevos modelos UTM de la Serie M (montaje en rack) de alto rendimiento. Las principales noticias incluyen la adquisición de Percipient Networks y el lanzamiento de DNSWatch, y también la adquisición de Datablink y posterior lanzamiento de AuthPoint, un servicio MFA (autenticación multifactor) basado en la nube. El vendedor también introdujo mejoras en su oferta de VPN.

WatchGuard es un buen candidato para PYMES y empresas distribuidas que necesitan un conjunto completo de características, con fácil licenciamiento incluido.

5.3.1 Fortalezas

5.3.1.1 Estrategia de producto

WatchGuard tiene un fuerte enfoque en la estrategia de PYMES, que se refleja en su producto, estrategia de ventas y en elementos del roadmap. Ofrece múltiples características que son deseables para las PYMES. Cuenta con licencias simples y una sólida estrategia de canal que también incluye pequeños partners que venden solo a pequeñas y medianas organizaciones.

5.3.1.2 Producto

WatchGuard ofrece WatchGuard Host Sensor, como parte de la licencia Total Security Suite. Está trabajando continuamente para construir mejores capacidades de correlación entre el Host Sensor y su producto UTM para ayudar a las organizaciones a detectar y responder a amenazas avanzadas. Esta oferta es atractiva para los compradores de pequeñas y medianas empresas con equipos de seguridad más pequeños que buscan consolidación hacia un solo vendedor.

5.3.1.3 Experiencia del cliente

Los clientes encuestados han calificado el nuevo producto Thread Detection and Response (TDR) de WatchGuard como uno de los mayores puntos fuertes de la Suite Total Security. Los partners encuestados han

calificado favorablemente la función WatchGuard RapidDeploy, que es una característica de despliegue y aprovisionamiento remoto.

5.3.1.4 Capacidad de respuesta del mercado

WatchGuard presentó ThreatSync, su nueva correlación basada en la nube y el motor de puntuación de amenazas, que utiliza fuentes de datos de eventos recopilados de WatchGuard Firebox, de los endpoints e inteligencia de la nube. Esto se alinea con la creciente demanda del mercado para una mejor correlación entre la red y los dispositivos endpoint, lo que proporciona una mejor detección y capacidades de remediación para malware avanzado.

5.3.1.5 Capacidades

WatchGuard UTM ofrece sólidas funciones de protección web, en asociación con para el filtrado de URL. Se ha introducido una nueva función DNSWatch, que proporciona educación contra el phishing a través de una página de bloqueo que incluye un video educacional.

5.3.2 Precauciones

5.3.2.1 Capacidad de respuesta del mercado

El portal Dimension, que es el sistema de administración centralizado basado en la nube de WatchGuard, tanto para socios como para usuarios finales, ofrece una configuración muy limitada de las características. Carece de capacidades maduras de gestión de cambios, como la capacidad de cambiar las reglas del firewall y aplicar actualizaciones de firmware en un grupo de soluciones UTM de manera centralizada. WatchGuard también ofrece un portal en la nube por separado para TDR y DNSWatch.

5.3.2.2 Comentarios de clientes

Los clientes encuestados informaron que WatchGuard carece de una fuerte integración entre sus sistemas de administración, especialmente Dimension, TDR y las líneas de productos inalámbricos.

5.3.2.3 Mercadotecnia

WatchGuard carece de mercadotecnia y promoción centradas en el usuario final en comparación con sus competidores directos de UTM en el mercado. Esto está especialmente relacionado con la falta de conocimiento de las nuevas funciones y mejoras del producto dentro de la base de clientes de PYMES.

5.3.2.4 Capacidad

El UTM de WatchGuard carece de la funcionalidad CASB (cloud accesss security broker) y ofrece informes y controles básicos de SaaS, utilizando la función de control de la aplicación como parte de su suscripción básica. También carece de funciones de control y gestión de SaaS granulares, solo proporcionadas por un CASB.

5.4 Proceso de selección

El proceso de selección se realizó en cinco etapas, las cuales pasamos a describir a continuación:

1. Búsqueda de partners. Se procedió a buscar partners de las marcas en Argentina, sobre cada partner seleccionado se hizo un análisis de reputación, clientes actuales, experiencia de la empresa con ese producto, etc.

2. Presentación del producto. Se coordinaron reuniones con cada uno de los partners locales seleccionados para que presenten a su empresa y producto y para presentar nuestra problemática actual y ver como cada producto podría solucionarla. Durante estas presentaciones se dieron a conocer las características extras de cada producto que podrían mejorar lo que actualmente tenemos y también características nuevas que serían muy beneficiosas de incorporarlas, por ejemplo, una mayor granularidad de reportes, mejorar la visibilidad de tráfico de red, protección contra APTs, etc. En estas reuniones participaron las áreas de TI y de Seguridad Informática, sin incluir personal técnico.

3. Presentación técnica del producto. Con cada uno de los partners de las marcas se realizó una demostración técnica de las capacidades del producto, se presentaron las interfaces y se hicieron demostraciones de cómo sería una migración de algunas funcionalidades actuales, por ejemplo, la creación de una nueva regla, la publicación de un sitio web o el establecimiento de una VPN. En estas demostraciones técnicas no participaron las gerencias, pero si el personal de infraestructura y networking junto con Seguridad Informática.

4. Presupuestos. Luego de haber conocido al partner y al producto se procedió a solicitar presupuestos por las diferentes ofertas de los partners, es importante aclarar que cada uno de los partner además del producto también ofrecían otro tipo de servicios como, por ejemplo, equipos en comodato, servicio de soporte, servicio de monitoreo, etc. Como base se solicitó presupuesto por los equipos físicos y también se solicitaron presupuestos adicionales por otros servicios que cada uno de ellos podría brindar.

5. Selección. La selección del producto se basó el análisis de los productos y entrevistas con los proveedores, y con esta información se realizó la confección de una planilla de ponderación (tabla 1) de las características del producto y de cada partner y este documento fue el que se incorporó en la presentación de las ofertas para dar sustento a la decisión tomada. A continuación, se muestra una planilla de ejemplo y su explicación:

Se tomaron 3 parámetros principales para ponderar y luego esos 3 parámetros se dividieron en diferentes categorías. A cada uno de los parámetros y categorías se le asignó un porcentaje de la ponderación.

Los parámetros fueron:

a- Experiencia del proveedor, se le asigna el 15 %

1-Experiencia en el mercado financiero 40%

2-Posicionamiento en el mercado financiero 40%

3-Experiencia con la empresa 20%

b- Características del producto, se le asigna el 50%

1-Firewall tipo appliance 20%

2-Bloqueador de APT 5%

3-Control de aplicaciones 5%

4-Prevención de intrusiones 5%

5-Filtrado de URLs 5%

6-Prevención de fuga de datos (DLP) 10%

7-DNS Watch 5%

8-Reportes 20%

9-Network discovery (mapa de red) 5%

10-Defensa basada en reputación 5%

11-Performance Throughput 10%

12-Gateway antivirus 5%

c- Hardware y servicios, se le asigna el restante 35%

1-Hardware por 3 años con licencias

2-Implementación

3-Capacitación online

(las 3 subcategorías se ponderaron en un único valor)

Análisis comparativo - tabla de ponderación	peso	%	WatchGuard	Sophos	Fortinet
Experiencia Proveedor	15%				
Experiencia el Mercado Financiero		40%	80	50	100
Pocisionamiento Mercado Financiero		40%	50	50	70
Experiencia con la empresa		20%	10	10	10
Total % experiencia proveedor			8,1	6,3	10,5
Características del producto ofrecidas	50%				
Firewall tipo appliance		20%	100	100	100
Bloqueador de APT		5%	100	100	100
Control de aplicaciones		5%	100	100	100
Prevención de intrusions		5%	100	100	100
Filtrado de URLs		5%	100	100	100
Prevención de fuga de datos (DLP)		10%	100	50	50
DNS Watch		5%	100	10	10
Reportes		20%	100	50	50
Network discovery (mapa de red)		5%	100	10	10
Defensa basada en la reputación		5%	100	10	10
Performance Throughput		10%	100	70	60
Gateway antivirus		5%	100	100	100

Total % productos ofrecidos		100	50	34,25	33,75
Hardware y servicios	35%				
Hardware x 3 años con licencias (análisis de logs)			39840	17734	59146
Implementación			4520	----	1200
capacitación online				----	
Monitoreo 7 x 24			2500		1400
Total			46860		61746
Peso en % de la propuesta		100%	60	100	40
Total % costos		100%	21	35	14
Total % ponderación			**79,1**	**75,55**	**58,25**

Tabla 1

La selección del proveedor debe ser muy cuidadosa y no debe menospreciarse ya que el nuevo proveedor jugará un papel crítico antes, durante y posteriormente al proceso de migración. Es importante que el proveedor tenga una experiencia sólida con la herramienta y también con la rama de negocios de la empresa cliente (este último punto fue evaluado a la hora seleccionar el proveedor). Este nuevo proveedor tiene una alta probabilidad de convertirse en un aliado para futuros proyectos y es por eso que no está demás a la hora de elegirlo tener en cuenta que otros servicios puede ofrecer a nuestra empresa. Otro punto importante es obtener referencias sobre el proveedor, las mismas pueden ser solicitadas a los actuales clientes del proveedor y con similares servicios provistos por este último. Debe considerarse también los recursos con los cuales cuenta el proveedor, principalmente los recursos técnicos que son aquellos con los cuales vamos a interactuar de manera intensa durante la implementación y en la etapa inmediata posterior, una empresa con un único recurso técnico especializado en la herramienta no sería una buena elección ya que ante la baja de este recurso no tendríamos soporte (o sería de menor calidad) hasta que se incorpore uno nuevo.

5.5 Presentación de las propuestas

Para poder obtener la aprobación de la compra de los equipos se realizó una presentación ante el consejo de administración, el cual es el ente encargado de autorizar o rechazar las nuevas adquisiciones.

Durante la presentación al consejo de administración se planteó la situación actual, explicando claramente y con lenguaje acorde al público lo que era un firewall, como nos protegía y los beneficios de migrar a un equipo tipo UTM.

Luego se presentó la matriz de ponderación explicada anteriormente, la cual consideraba el alcance propuesto, características y honorarios de los proveedores. Basados en esta matriz se propuso a cuál de los proveedores se debería elegir. Se explicaron las ventajas que incorporaría la selección de ese proveedor y los beneficios que traería a la empresa realizar el cambio. El consejo estuvo de acuerdo con la propuesta realizada por el área de Protección de Activos de Información y se procedió a autorizar la compra del producto con el proveedor propuesto.

6 Implementación

Luego de aprobada la compra por parte del consejo de administración se notifica a los diferentes proveedores de la decisión tomada y se procede a avanzar con la propuesta ganadora para planificar la etapa de implementación.

Como requisito previo a comenzar la implementación se realizó un análisis completo de todas las políticas del firewall depurando las mismas. Se actualizaron reglas y se eliminaron las que ya no eran utilizadas. Este proceso de revisión es muy útil para tener más claro el objetivo de cada política y de esta manera evitar migrar políticas obsoletas o duplicadas. También se realizó una revisión de reglas de nateo y de los diagramas de red ya que los nuevos equipos no solo reemplazarán al anterior firewall TMG sino que también cumplirán las funciones de otros equipos de comunicación, como el establecimiento de VPNs entre sitios de la empresa, el cual actualmente es realizado por otros equipos.

Una vez depuradas las políticas las mismas son enviadas al proveedor para que las vaya migrando a los nuevos equipos, además de las políticas se les enviaron las configuraciones de redes necesarias para interconectar los equipos firewall tanto en el datacenter primario como en el sitio de contingencia.

Luego de analizar diferentes estrategias de migración se optó por hacer una separación de los servicios que pasaban a través de firewall, (navegación por Internet, correo, vpn de terceros, etc.) y se planificó migrar servicio por servicio fuera del horario productivo.

6.1 Capacitación

Dado que los equipos adquiridos serían administrados por personal de la empresa, dentro de la contratación se incluyó un curso de capacitación para el área de networking y para el área de seguridad informática.

Esta capacitación tiene como objetivo que los administradores puedan conocer mejor los firewalls de WatchGuard, conocer los diferentes tipos de licencias, las herramientas de administración y monitoreo.

6.2 Migración de servicios

Se comenzó migrando por el servicio más simple de configurar y con el menor impacto, una vez comprobado su funcionamiento y realizado varias pruebas con los usuarios finales se daba por finalizada la migración de ese servicio y se procedía a planificar la migración del siguiente servicio. Cada migración se utilizaba como retroalimentación para la siguiente etapa.

Al finalizar la migración de todos los servicios se verificó durante unos días que los viejos firewalls no estuvieran recibiendo ningún tipo de tráfico, una vez constatado esto se procedió a deshabilitar las interfaces, luego de unos días se realizó el apagado de los mismos.

Con esto finalizó la implementación, más allá de que durante unos días se fueron ajustando algunas reglas, los firewalls quedaron en ambiente productivo con la finalización de la migración de todos los servicios.

Luego de unas semanas de utilización del firewall se utilizaron las estadísticas de uso de cada política para desactivar las reglas que no tuvieron ningún acceso durante ese período, con esto se finalizó la depuración de las reglas migradas a los nuevos firewalls.

7 Activación de características del UTM

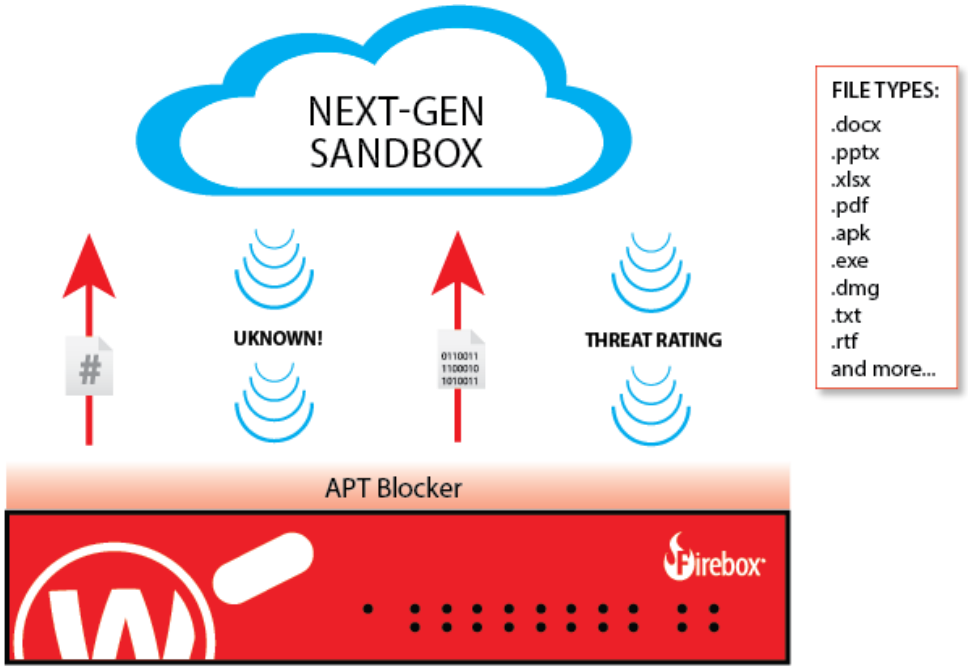
Con los equipos UTM ya funcionando se continuó con la activación de las características disponibles en el UTM, esto se fue realizando por etapas para poder ir verificando el correcto funcionamiento de cada característica implementada.

A continuación, se describen las características activadas.

De acuerdo con la documentación de WatchGuard publicada en su sitio oficial:

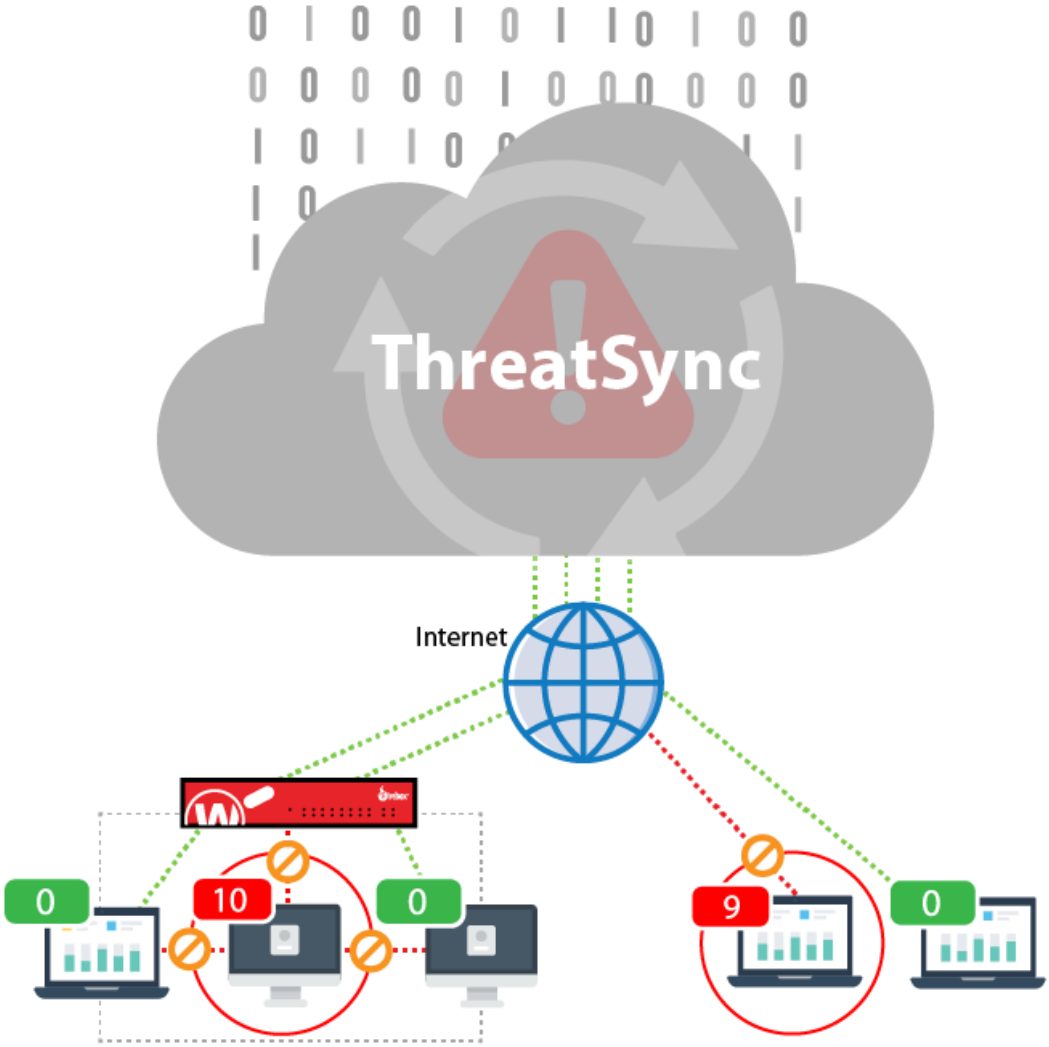
7.1 APT Blocker [6]

WatchGuard APT Blocker trabaja en conjunto con WatchGuard Gateway AntiVirus para obtener la mejor solución para detectar y prevenir malware avanzado. Si el archivo pasa el análisis de Gateway AntiVirus, se envía un hash al APT Blocker en la sandbox de la nube para determinar si se trata de una amenaza conocida. Si no se reconoce el hash del archivo, APT Blocker solicita a Firebox que envíe el archivo completo, que se ejecuta en un entorno que simula el hardware físico para un análisis completo de amenazas. Los administradores son alertados si el archivo es sospechoso con una clasificación de amenaza.



7.2 Thread Detection and Response (TDR) [7]

Las amenazas detectadas en Firebox o mediante el Host Sensor se envían a ThreatSync, donde se correlacionan y analizan continuamente, luego se califican y se clasifican según la gravedad. Luego, las amenazas se pueden remediar rápidamente con las opciones de respuesta con un solo clic, o aprovechando las políticas para habilitar una respuesta automatizada que incluya la cuarentena del archivo, el proceso y eliminar la persistencia de la clave de registro.

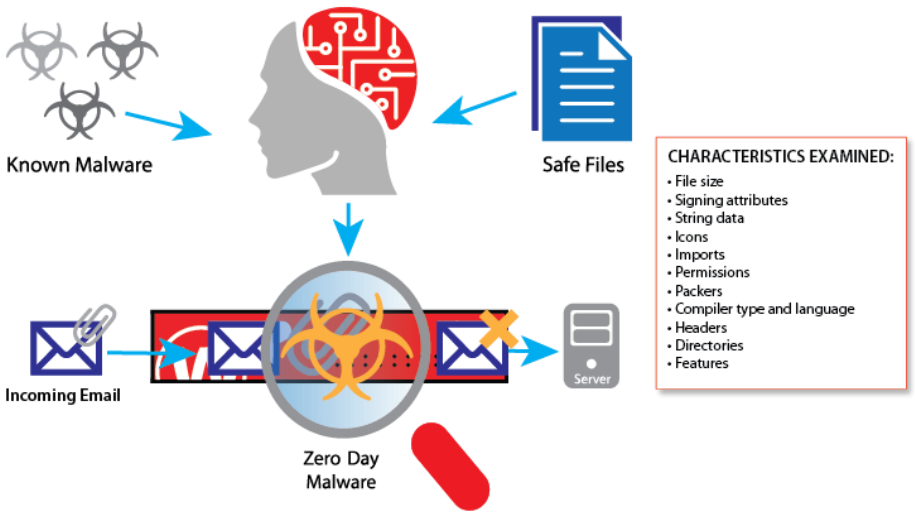


7.3 Inteligent AV [8]

IntelligentAV aprovecha un motor de aprendizaje automático para defenderse mejor contra el malware de día cero de evolución continua. Si bien las soluciones de AV basadas en firmas solo son capaces de detectar amenazas conocidas, IntelligentAV hace posible predecir las amenazas meses antes de su lanzamiento, proporcionando una poderosa protección predictiva que antes no estaba disponible para las pequeñas y medianas empresas.

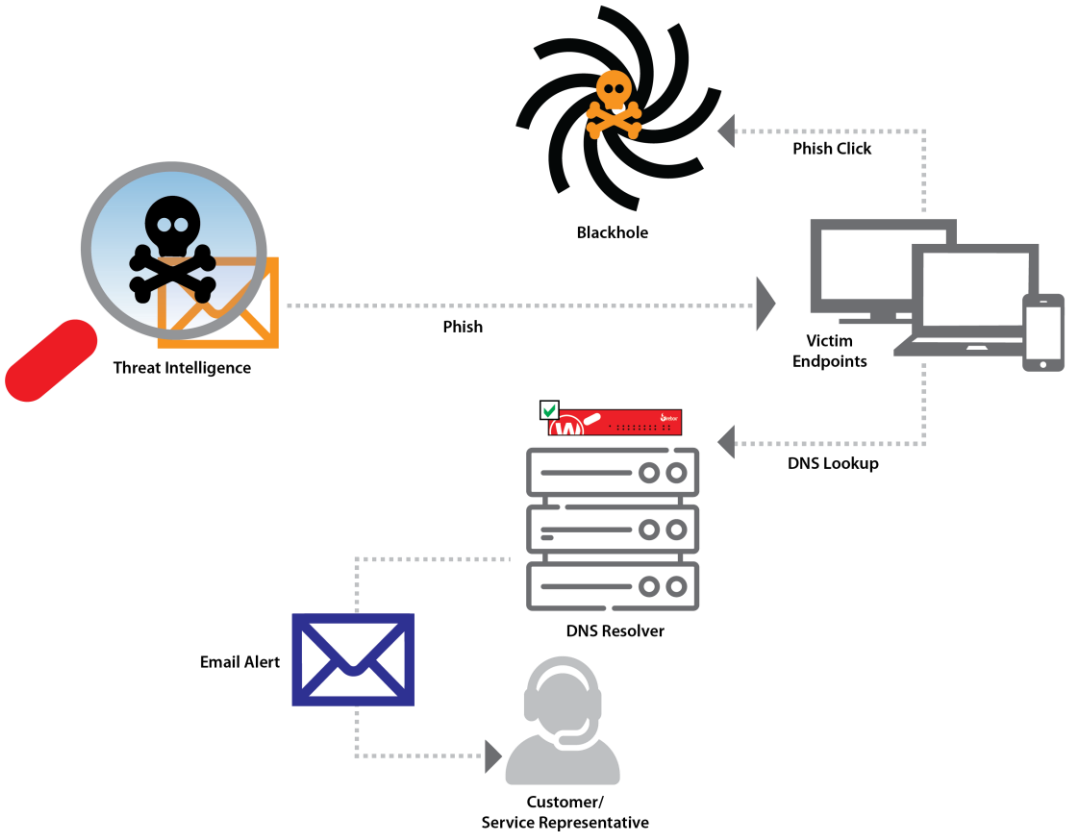
IntelligentAV está capacitado para identificar amenazas dividiendo millones de archivos en sus componentes fundamentales y luego

examinando millones de características de cada archivo en combinación para identificar indicadores de intenciones maliciosas. Si se identifica malware, el archivo se bloquea antes de que pueda ejecutarse.



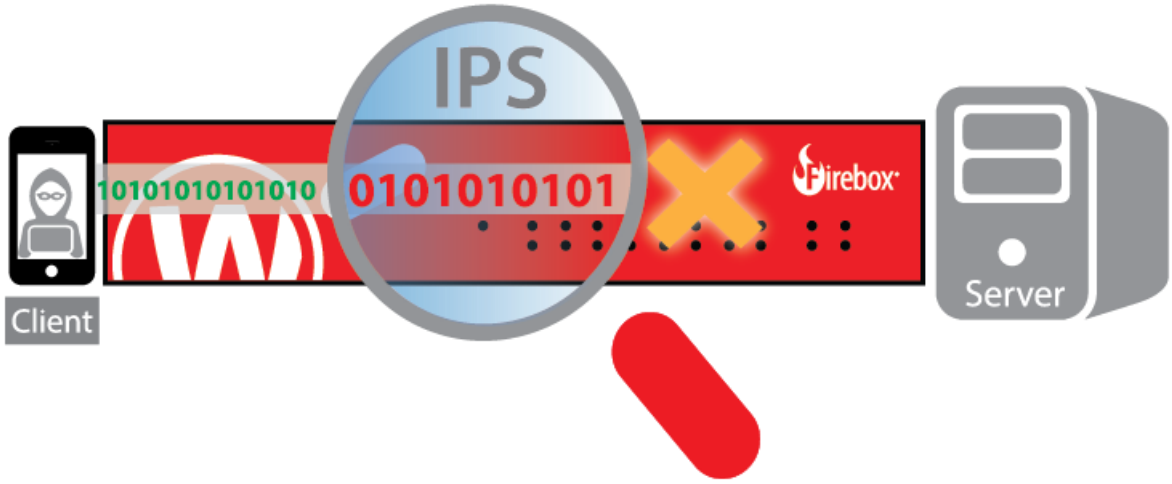
7.4 DNSWatch [9]

WatchGuard DNSWatch es un servicio basado en la nube que agrega filtrado a nivel de DNS para detectar y bloquear conexiones potencialmente peligrosas y proteger a las redes y los empleados de ataques dañinos. Los analistas de WatchGuard clasifican las alertas críticas y hacen un seguimiento de una contabilidad fácil de comprender que incluye información detallada sobre la posible infección. Cuando el ataque utiliza phishing y un empleado hace clic en el enlace, DNSWatch los redirige automáticamente fuera del sitio malicioso y ofrece recursos que refuerzan la educación sobre phishing.



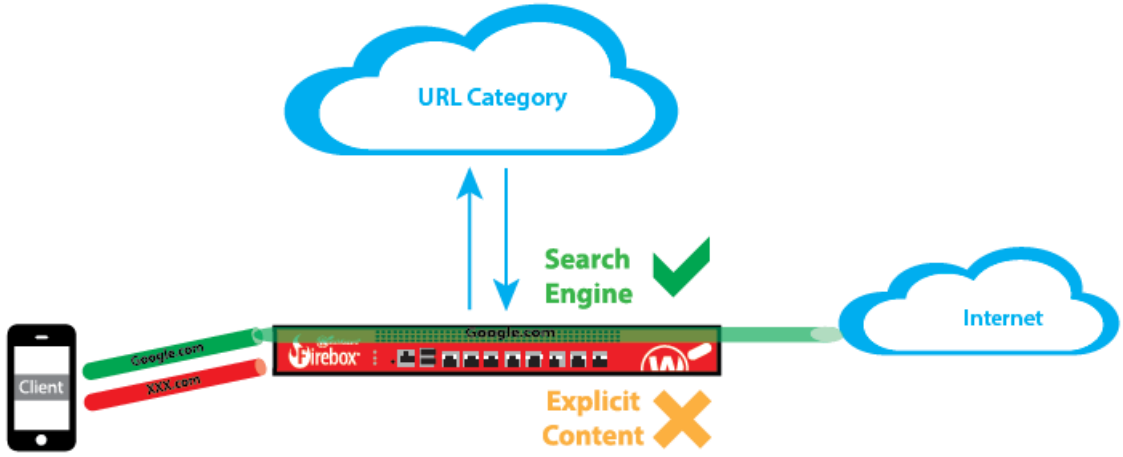
7.5 IPS [10]

Intrusion Prevension Service (IPS) examina el tráfico en el nivel más bajo para identificar amenazas conocidas al hacer coincidir los patrones de tráfico con una base de datos de firmas completa y continuamente actualizada. Si se identifica una amenaza, Firebox realiza acciones basadas en políticas establecidas para bloquear o notificar al administrador.



7.6 WebBlocker [11]

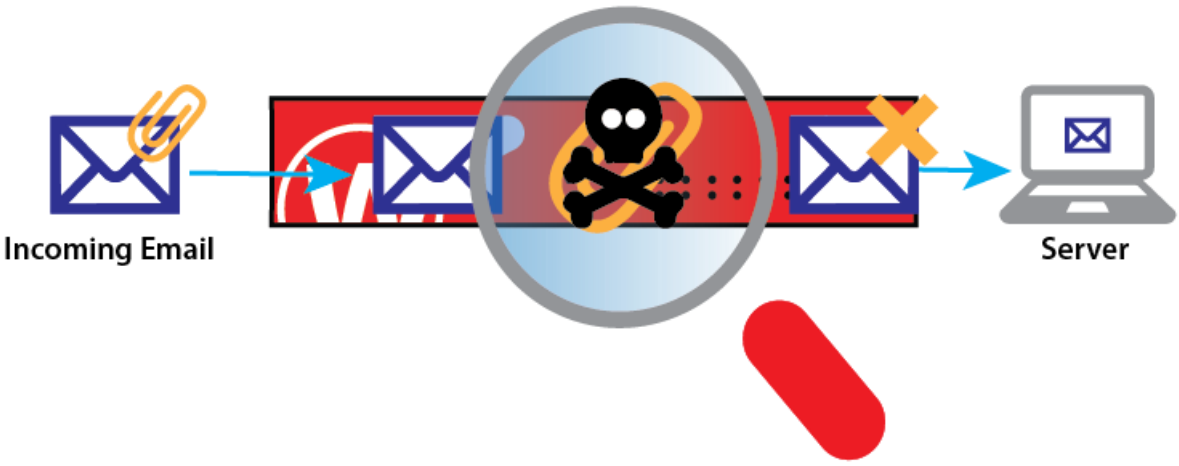
WebBlocker identifica la URL solicitada y luego envía una consulta a la nube para clasificar la categoría y subcategoría de URL. Firebox permite o deniega el acceso a la URL en función de la configuración de políticas, incluidos el usuario, el grupo y la programación de horarios.



7.7 Gateway AV [12]

Gateway AntiVirus escanea los archivos y el tráfico que fluye a través de Firebox para identificar malware conocido y software de riesgo.

Si se identifica una amenaza en función de la coincidencia de firmas, se bloquea la conexión o se elimina el archivo.

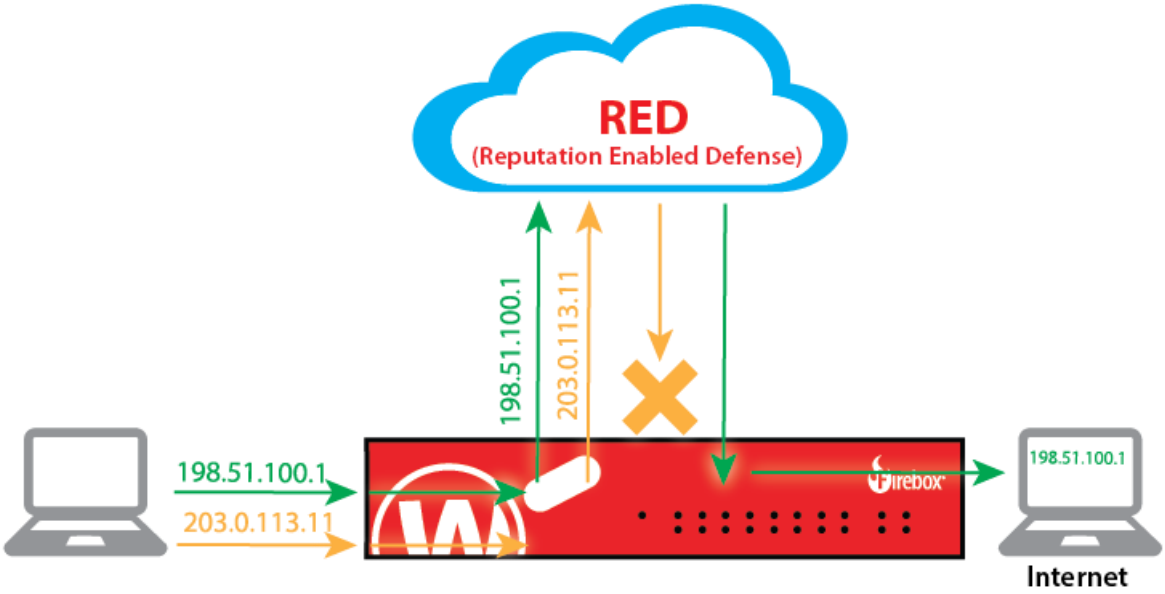


7.8 Network Discovery [13]

Network Discovery explora e identifica todos los hosts conectados a una red detrás de Firebox, hace una recopilación de detalles del dispositivo, como versiones del sistema operativo, puertos abiertos y protocolos.

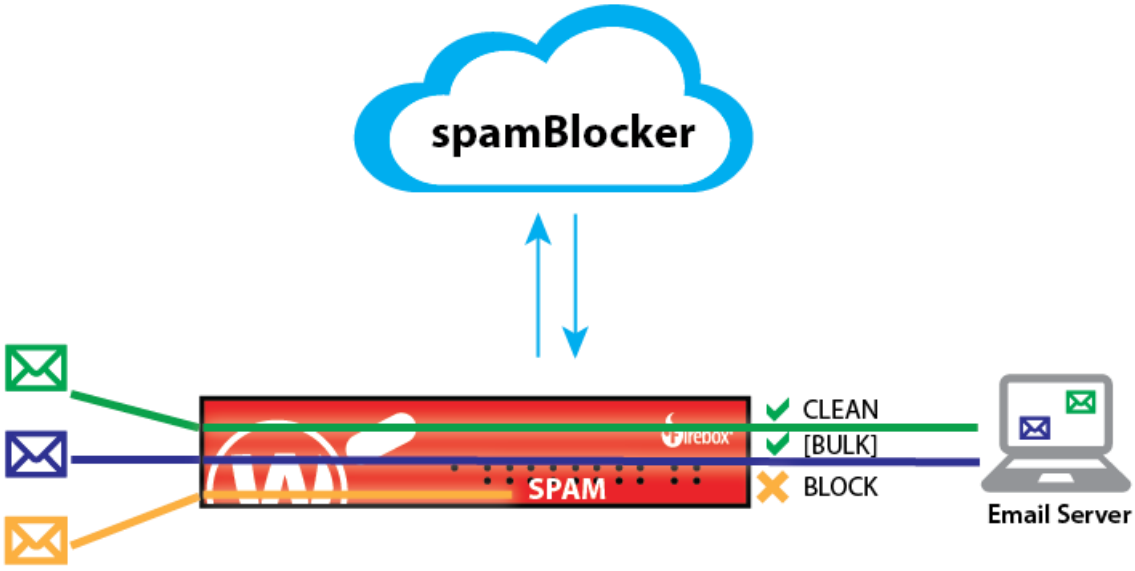
7.9 Reputation-Based Threat Prevention [14]

Reputation Enabled Defense revisa el destino de las conexiones salientes e identifica su nivel de amenaza según las fuentes de inteligencia. Al usar el puntaje de amenaza devuelto, las amenazas conocidas se bloquean y se permiten destinos seguros con una omisión de Gateway Antivirus para aumentar el rendimiento de la red.



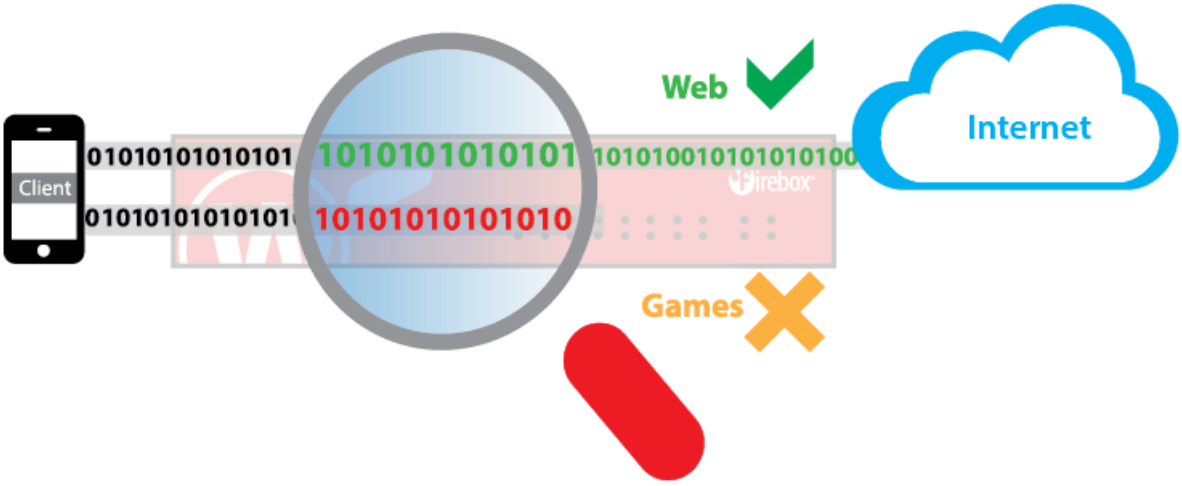
7.10 Spam Prevention [15]

Cuando Firebox recibe el correo electrónico entrante, consulta el servicio en la nube de spamBlocker para que coincida con los datos para determinar si se conoce como correo no deseado, y luego permite, bloquea o pone en cuarentena el correo electrónico según la puntuación del correo no deseado.



7.11 Application Control [16]

Application Control revisa el tráfico que fluye a través de Firebox e identifica los patrones de tráfico que coinciden con una lista de aplicaciones configurables. El control de la aplicación luego permite, niega o limita la conexión según las configuraciones de políticas.



8 Reportes generados

El producto de Watchguard tiene un portal denominado Dimension, el cual produce una gran cantidad de reportes con mucha información, en el anexo 1 se listan los reportes que pueden ser generados, a su vez estos reportes pueden ser programados para ejecutarse automáticamente, mensualmente, semanalmente, etc.

Se configuraron un total de 6 reportes los cuales se ejecutan periódicamente y son enviados por email. Está dentro de nuestros planes seguir implementado nuevos reportes en la medida que sea necesario.

Los reportes actualmente programados son los siguientes:

- Resumen ejecutivo: Informe que incluye un resumen de las principales características, sin un alto nivel de detalle pero que da una visión completa de la activad controlada por el dispositivo.
- Principales clientes: Lista los principales clientes, incluidos los clientes dentro y fuera de su red, que generan la mayor cantidad de tráfico. Incluye el nombre del cliente o la dirección IP, el número de bytes y el número de visitas para el tráfico a través del filtro de paquetes y las políticas de proxy.
- Uso de aplicaciones: Informe resumido de los datos de uso de las aplicaciones para conexiones permitidas. Incluye datos de transacciones de conexión TCP-UDP-Proxy entrante y saliente, cuando estén disponibles.
- Principales ataques bloqueados: Los principales ataques de intrusión que fueron bloqueados por el Servicio de prevención de intrusiones (IPS). Incluye el nombre del ataque y la cantidad de hits.
- VPN: Conexiones de VPN realizadas, incluye el usuario, IP de origen, hora de conexión, IP interna asignada.
- Email: Resumen de la actividad del servidor SMTP (para cuentas de correo electrónico internas y externas).
- Utilización de políticas: Resumen de todas las políticas incluidas en la configuración del firewall. Para cada política, aparecen el nombre de la

política, el número de aciertos, la cantidad de bytes y la fecha y hora en que se utilizó por última vez. Las políticas que se han eliminado aparecen en rojo con Eliminado en la columna Estado.

- Monitoreo: Informe sobre el estado de los equipos, consumo de CPU, memoria. También se genera otro informe con la disponibilidad de los enlaces.

9 Conclusión

La migración se concretó de manera exitosa, se reemplazó el firewall por un nuevo equipo de tipo UTM. Entre las mejoras que produjo la migración encontramos que se aumentó la cantidad de herramientas de protección contra ataques maliciosos, se sumaron un total de 9 características para reforzar la seguridad y además se centralizó el uso de otras 2 características dentro de la consola de administración del UTM.

Se mejoró la visibilidad de los eventos que se producen en el perímetro de la red a través representaciones gráficas y dinámicas en contraste con el listado de logs en modo texto que producía la herramienta anterior.

Se incrementó la velocidad de respuesta ante un incidente de seguridad utilizando el monitoreo de 7 x 24 que se contrató al proveedor, con el producto anterior esto no era posible y la detección de los incidentes de producía de manera tardía.

Se mejoró el detalle de 2 reportes que se emiten mensualmente y se incorporaron otros 6 nuevos reportes.

Con la instalación de un producto vigente en el mercado se cumplió con la buena práctica de poseer un software con soporte por parte del proveedor y que a su vez reciba las últimas actualizaciones de seguridad.

Como lecciones aprendidas podemos destacar la importancia de realizar una adecuada planificación que tenga en cuenta la mayor cantidad de detalles posibles y junto con esto llevar a cabo una correcta verificación luego de implementar cada fase del proceso. Los testeos de reglas y servicios fueron vitales no solo para la continuidad de la operatoria de la empresa sino también para no dejar huecos en la seguridad.

Por lo expuesto anteriormente podemos concluir que el reemplazo de la herramienta cumplió con los objetivos planificados.

Anexo 1 Reportes

Reportes disponibles en la herramienta.

Executive Summary Report

Report Type	Description
Top Zero-Day Malware (APT)	The top malware that was not **identified** by APT Blocker until after it passed through the firewall. Includes the threat index, threat ID, content name, threat level, and number of hits.
Top Blocked Advanced Malware (APT)	The advanced malware threats that APT Blocker detected and that were blocked. Includes the threat index, threat ID, content name, and number of hits.
Top Blocked Malware	The malware that has been blocked on the network by Gateway AntiVirus. Includes the name of the malware and the number of hits.
Top Blocked Attacks	The top intrusion attacks that were blocked by the Intrusion Prevention Service (IPS). Includes the name of the attack and the number of hits.
Top Clients	The top clients, including clients both inside and outside your network, that generate the most traffic. Includes the client name or IP address, number of bytes, and number of hits for traffic through packet filter and proxy policies.
Top Domains	The top web domains in use on your network. Includes the domain name, number of bytes, and number of hits.
Top Blocked Botnet Sites	The top botnet sites that clients on your network tried to contact.
Top Blocked Botnet Clients	The top clients on your network that tried to contact a botnet site.
Top URL Categories	The top ten categories of Internet activity on your network that WebBlocker identified. Includes the category name and number of hits.
Top Applications	The top applications that are in use on your network. Includes the application name, number of bytes, and number of hits.
Top Application Categories	The top categories for application traffic. Includes the application category name, number of bytes, and number of hits.
Top Blocked Applications	The top applications that were blocked. Includes the application name and number of hits.
Top Blocked Application Categories	The top categories of applications that were blocked. Includes the application category name and number of hits.
Top Mobile Devices	The mobile devices on your network that generate the most traffic. Includes the mobile device name, number of bytes, and number of hits.

Per Client Reports

Report Type	Report Category	Description
Web Activity Trend	Summary	Hourly trend data for websites visited by clients.
Most Popular Domains	Summary	Top websites visited by clients.

Report Type	Report Category	Description
Application Usage	Summary	Summary report of application usage data for allowed connections. Includes TCP-UDP-Proxy incoming and outgoing connection transaction data, when available.
Data Loss Violations (DLP)	Summary	All Data Loss Prevention activity and actions on the Firebox.
Data Loss Violations (DLP) by Detail	Detail	Data Loss Prevention activity and actions on the Firebox, organized by the detail type.
URL Audit Detail	Detail	Detailed report of traffic through the Firebox, organized by URL. Includes the Event Time, Policy, Disposition, Destination, and Path for the traffic.
Application Usage by Category	Detail	Application usage data for allowed connections, by category.
Web Audit by Category	Summary	Summary report of web traffic by category.
Web Audit by Category Detail	Detail	Detailed report of web traffic by category, organized by the category details.

Traffic

Report Type	Pivot Name	Pivot Option	Description	Report Schedule Destination
Packet Filter Traffic	Activity Trend		Summary of packet-filter traffic data, organized by the activity. To include this report in a schedule, select the *Packet-Filter Summaries* > *Activity Trend* report.	Email, Directory
	Source	Hits, Bandwidth	Summary of packet-filter traffic data, organized by the host name. To include this report in a schedule, select the *Packet-Filter Summaries* > *Host Summary* report.	Email, Directory
	Destination	Hits, Bandwidth	Summary of packet-filter traffic data, organized by the destination address.	
	Service	Hits, Bandwidth	Summary of packet-filter traffic data, organized by the service name. To include this report in a schedule, select the *Packet-Filter Summaries* > *Service Summary* report.	Email, Directory
	Session	Hits, Bandwidth	Summary of packet-filter traffic data, organized by the session. To include this report in a schedule, select the *Packet-Filter Summaries* > *Session Summary* report.	Email, Directory
Proxy Traffic	Activity Trend		Summary of proxied traffic data, organized by the activity. To include this report in a schedule, select the *Proxy Summaries* > *Activity Trend* report.	Email, Directory

Report Type	Pivot Name	Pivot Option	Description	Report Schedule Destination
	Source	Hits, Bandwidth	Summary of proxied traffic data, organized by the host name. To include this report in a schedule, select the *Proxy Summaries* > *Host Summary* report.	Email, Directory
	Destination	Hits, Bandwidth	Summary of proxied traffic data, organized by the destination address.	
	Protocol	Hits, Bandwidth	Summary of proxied traffic data, organized by the protocol. To include this report in a schedule, select the *Proxy Summaries* > *Proxy Summary* report.	Email, Directory
	Session	Hits, Bandwidth	Summary of proxied traffic data, organized by the session. To include this report in a schedule, select the *Proxy Summaries* > *Session Summary* report.	Email, Directory
External Bandwidth			Information about the bandwidth/transfer rate for external interfaces. The data sampling interval is based on the report time range. The minimum interval is 1 minute. The published report samples data every 10 minutes. To include this report in a schedule, select the *Firebox Reports* > *Bandwidth (for External Interfaces and VPN Tunnels* report.	Email, Directory
	Data Transfer Amount		Summary of the bandwidth information on the amount of data through the external interfaces.	
	Data Transfer Rate		Summary of the bandwidth information on the rate that the data transferred through the external interfaces.	
VPN Bandwidth			Includes information on upload and download bandwidth by rate for BOVPN and Mobile VPN tunnels. The data sampling interval is based on the report time range. The minimum interval is 1 minute. The published report samples data every 10 minutes. To include this report in a schedule, select the *Firebox Reports* > *Bandwidth (for External Interfaces and VPN Tunnels* report.	Email, Directory
	Amount of Data Transferred		Summary of the bandwidth information on the amount of data through the VPN tunnel.	
	Rate of Data Transfer		Summary of the bandwidth information on the rate that the data transferred through the VPN tunnel.	

Report Type	Pivot Name	Pivot Option	Description	Report Schedule Destination
Top Clients		Hits, Bandwidth	Summary of the clients that use the most bandwidth on your network, or have the most hits. You can refine the data in this report to see Per Client Reports data.	
	Hosts (Sent & Received)		Summary of the bandwidth data or hits for the clients based on the host names used to send and receive the traffic. To include this report in a schedule, select one of these reports: *Client Reports > Top Clients by Users, Host, and Mobile devices (by Bandwidth)* *Client Reports > Top Clients by Hits*	Email, Directory
	Users (Sent & Received)		Summary of the bandwidth data or hits for the clients based on the user names used to send and receive the traffic. To include this report in a schedule, select one of these reports: *Client Reports > Top Clients by Users, Host, and Mobile devices (by Bandwidth)* *Client Reports > Top Clients by Hits*	Email, Directory
	Mobile Devices (Sent & Received)		Summary of the bandwidth data or hits for the clients based on the mobile devices used to send and receive the traffic. To include this report in a schedule, select one of these reports: *Client Reports > Top Clients by Users, Host, and Mobile devices (by Bandwidth)* *Client Reports > Top Clients by Hits*	Email, Directory
	Hosts (Sent)		Summary of the bandwidth data or hits for the clients based on the host names used to send the traffic. To include this report in a schedule, select one of these reports: *Client Reports > Top Clients by Users, Host, and Mobile devices (by Bandwidth)* *Client Reports > Top Clients by Hits*	Email, Directory
	Users (Sent)		Summary of the bandwidth data or hits for the clients based on the user names used to send the traffic. To include this report in a schedule, select one of these reports: *Client Reports > Top Clients by Users, Host, and Mobile devices (by*	Email, Directory

Report Type	Pivot Name	Pivot Option	Description	Report Schedule Destination
			Bandwidth)Top Clients by Bandwidth (Sent) *Client Reports > Top Clients by Hits*	
	Mobile Devices (Sent)		Summary of the bandwidth data or hits for the clients based on the mobile devices used to send the traffic. To include this report in a schedule, select one of these reports: *Client Reports > Top Clients by Users, Host, and Mobile devices (by Bandwidth)* *Client Reports > Top Clients by Hits*	Email, Directory
	Users (Received)		Summary of the bandwidth data or hits for the clients based on the user names that received the traffic. To include this report in a schedule, select one of these reports: *Client Reports > Top Clients by Users, Host, and Mobile devices (by Bandwidth)* *Client Reports > Top Clients by Hits*	Email, Directory
	Hosts (Received)		Summary of the bandwidth data or hits for the clients based on the host names that received the traffic. To include this report in a schedule, select one of these reports: *Client Reports > Top Clients by Users, Host, and Mobile devices (by Bandwidth)* *Client Reports > Top Clients by Hits*	Email, Directory
	Mobile Devices (Received)		Summary of the bandwidth data or hits for the clients based on the mobile devices that received the traffic. To include this report in a schedule, select one of these reports: *Client Reports > Top Clients by Users, Host, and Mobile devices (by Bandwidth)* *Client Reports > Top Clients by Hits*	Email, Directory

Web

Report Type	Pivot Name	Description	Report Schedule Destination
Most Active Clients	Hits	Summary of the top web traffic for clients and mobile devices, by hits. You can refine the data in this report to see Per Client Reports data. To include this report in a schedule, select the *Web Traffic Reports > Most Active Clients* report.	Email, Directory
	Bytes	Summary of the top web traffic for clients and mobile devices, by bytes transferred. You can	Email, Directory

Report Type	Pivot Name	Description	Report Schedule Destination
		refine the data in this report to see Per Client Reports data. To include this report in a schedule, select the *Web Traffic Reports > Most Active Clients* report.	
Most Popular Domains	Hits	Summary of the top websites visited by clients, by hits. To include this report in a schedule, select the *Web Traffic Reports > Most Popular Domains* report.	Email, Directory, ConnectWise
	Bytes	Summary of the top websites visited by clients, by bytes transferred. To include this report in a schedule, select the *Web Traffic Reports > Most Popular Domains* report.	Email, Directory, ConnectWise
Web Audit	Category	Summary of the trends, active clients, most popular domains, WebBlocker details, and websites traffic for connections allowed by proxy rules, by category. To include this report in a schedule, select the *Web Audit Reports > Web Audit (Summary, by Category and Client)* report.	Email, Directory
	Client	Summary of the trends, active clients, most popular domains, WebBlocker details, and websites traffic for connections allowed by proxy rules, by client. To include this report in a schedule, select the *Web Audit Reports > Web Audit (Summary, by Category and Client)* report.	Email, Directory
	Mobile Device	Summary of the trends, active clients, most popular domains, WebBlocker details, and websites traffic for connections allowed by proxy rules, by mobile device. To include this report in a schedule, select the *Web Audit Reports > Web Audit (Summary, by Mobile Device)* report.	Email, Directory
Web Activity Trend		Summary of the hourly trend data for web traffic activity. To include this report in a schedule, select the *Web Traffic Reports > Activity Trend* report.	Email, Directory
Web Traffic Summary		Summary of the top websites and top web categories visited by clients. To include this report in a schedule, select the *Web Traffic Reports > Web Traffic Summary* report.	Email, Directory

Mail

Report Type	Pivot Name	Description	Report Schedule Destination
SMTP	Sender	Summary of the SMTP proxy action records by sender.	
	Recipient	Summary of the SMTP proxy action records by recipient.	
	Server Summary	Summary of the SMTP server activity (for internal and external email accounts). To include this report in a schedule, select the *SMTP Proxy > SMTP Summary (Email and Server)* report.	Email, Directory
POP3	User	Summary of the POP3 user activity. To include this report in a schedule, select the *POP3 Proxy > POP3 Summary (Email and Server)* report.	Email, Directory
	Server Summary	Summary of the POP3 server activity. To include this report in a schedule, select the *POP3 Proxy > POP3 Summary (Email and Server)* report.	Email, Directory

Services

Report Type	Pivot Name	Description	Report Schedule Destination
Application Usage	Summary	Summary of application usage data for allowed connections. Includes TCP-UDP-Proxy incoming and outgoing connection transaction data, when available. You can refine the data in this report type to see Per Client Reports data in a Top Clients report. To include this report in a schedule, select the *Application Control > Application Usage Summary* report. To include the Top Clients report in a schedule, select the *Client Reports > Top Clients by Application Usage* report.	Email, Directory
	Top Applications by User	Summary of the applications with the most users, by user name.	
	Top Applications by Host	Summary of the applications with the most users, organized by host name.	
	Top Applications by Mobile Device	Summary of the applications with the most users, organized by mobile device.	
	Top Users by Application	Summary of the users most often blocked by Application Control, organized by application.	
	Top Hosts by Application	Summary of the hosts most often blocked by Application Control, organized by application.	

Report Type	Pivot Name	Description	Report Schedule Destination
	Top Mobile Devices by Application	Summary of the mobile devices most often blocked by Application Control, organized by application.	
Advanced Malware (APT)	Advanced Malware (APT) Summary	Summary of the malware detected by APT Blocker. This report is only available when you create a report schedule. To include this report in a schedule, select the *Advanced Malware (APT) Reports > Advanced Malware (APT) Summary* report.	Email, Directory
	Content Name	Summary of the malware detected by APT Blocker, organized by content name. Includes allowed and denied hits. To include this report in a schedule, select the *Advanced Malware (APT) Reports > Detail by Content Name* report.	Email, Directory
	Activity Trend	Summary report of a trend of the malware that was detected by APT Blocker. To include this report in a schedule, select the *Advanced Malware (APT) Reports > Malware Activity Trend* report.	Email, Directory
	Threat ID	Summary of the malware detected by APT Blocker, organized by the Threat ID. To include this report in a schedule, select the *Advanced Malware (APT) Reports > Detail by Threat ID* report.	Email, Directory
	Malicious Activity	Summary of the malicious activity on your network that was detected by APT Blocker. To include this report in a schedule, select the *Advanced Malware (APT) Reports > Detail by Malicious Activity* report.	Email, Directory
	MIME Type	Summary of the MIME types used on your network. To include this report in a schedule, select the *Advanced Malware (APT) Reports > Detail by MIME Type* report.	Email, Directory
	Protocol	Summary of the protocols used for malicious activity on your network that was detected by APT Blocker. To include this report in a schedule, select the *Advanced Malware (APT) Reports > Detail by Protocol* report.	Email, Directory
	Recipient/Destination	Summary of the recipient names and destination addresses for malicious activity on your network. To include this report in a schedule, select the *Advanced Malware (APT) Reports > Detail by Destination* report.	Email, Directory

Report Type	Pivot Name	Description	Report Schedule Destination
	Sender/Source	Summary of the sender names and source addresses for malicious activity on your network. To include this report in a schedule, select the *Advanced Malware (APT) Reports > Detail by Source* report.	Email, Directory
	Threat Level	Summary of the threat levels assigned to malicious activity on your network. To include this report in a schedule, select the *Advanced Malware (APT) Reports > Detail by Threat Level* report.	Email, Directory
Botnet Detection	By Client	Summary report of all the activity on you network related to botnet sites, by client. Summary data shows the top 50 clients that were blocked before they connected to botnet sites. You can click the IP address in the **Client** column to see the detail report filtered by the selected IP address. To include this report in a schedule, select *Botnet Detection > Botnet Detection by Client*.	Email, Directory
	By Activity Trend	Summary report of a trend of the sites that were scanned in relation to the number of blocked botnet sites. To include this report in a schedule, select *Botnet Detection > Activity Trend*.	Email, Directory
	By Destination	Summary report of all the activity on you network related to botnet sites, by destination. Summary data shows the top 50 destinations that botnet sites tried to connect to and were blocked. You can click the IP address in the **Destination** column to see the detail report filtered by the selected IP address. To include this report in a schedule, select *Botnet Detection > Botnet Detection by Destination*	Email, Directory
	Blocked Botnet Sites	Summary report of the top 50 blocked botnet sites. You can click the IP address in the **Name** column to see the detail report filtered by the selected IP address. To include this report in a schedule, select *Botnet Detection > Blocked Botnet Site Summary*	Email, Directory
Blocked Applications		Summary of the applications used on your network that were blocked by Application Control. Includes TCP-UDP-Proxy incoming and outgoing connection transaction data, when available.	Email, Directory

Report Type	Pivot Name	Description	Report Schedule Destination
		You can refine the data in this report type to see Per Client Reports data. To include this report in a schedule, select the *Application Control > Blocked Application Summary* report.	
	Top Blocked by User	Summary of the applications that were most blocked, organized by user name.	
	Top Blocked by Host	Summary of the applications that were most blocked, organized by host name.	
	Top Blocked by Mobile Device	Summary of the applications that were most blocked, organized by mobile device.	
	Top Users Blocked	Summary of the user names that were most blocked.	
	Top Hosts Blocked	Summary of the host names that were most blocked.	
	Top Mobile Devices Blocked	Summary of the mobile devices that were most blocked.	
Blocked Websites	Category	Summary of the websites blocked by WebBlocker, organized by category. To include this report in a schedule, select the *Blocked Websites Reports > Blocked Websites (Summary, by Category and Client)* report.	Email, Directory, ConnectWise
	Activity Trend	Summary report of a trend of the sites that were scanned in relation to the number of blocked websites. To include this report in a schedule, select the *Blocked Websites Reports > Blocked Websites Activity Trend* report.	
	Client	Summary of the websites blocked by WebBlocker, organized by client. To include this report in a schedule, select the *Blocked Websites Reports > Blocked Websites (Summary, by Category and Client)* report.	Email, Directory, ConnectWise
	Mobile Device	Summary of the websites blocked by WebBlocker, organized by mobile device. To include this report in a schedule, select the *Blocked Websites Reports > Blocked Websites (Summary, by Mobile Devices)* report.	Email, Directory, ConnectWise
Data Loss Violations (DLP)		Summary reports of the top 50 hits for Data Loss Prevention activity and actions. Includes allowed and denied violations.	
	Rules	Summary of the denied violations by rule name. To include this report in a schedule, select the *Data Loss Violations (DLP) > DLP Rules Summary* report.	Email, Directory

Report Type	Pivot Name	Description	Report Schedule Destination
	Activity Trend	Summary of the traffic scanned by Data Loss Prevention. Data includes the total number of scans, the allowed violations, denied violations, and quarantined violations. To include this report in a schedule, select the *Data Loss Violations (DLP) > DLP Activity Trend* report.	Email, Directory
	Sender/Source	Summary of the denied violations by the sender or source address. To include this report in a schedule, select the *Data Loss Violations (DLP) > DLP Source Summary* report.	Email, Directory
	Recipient/Destination	Summary of the denied violations by the recipient or destination address. To include this report in a schedule, select the *Data Loss Violations (DLP) > DLP Destination Summary* report.	Email, Directory
Intrusions (IPS)		Includes the signature name in each of the reports. Includes allowed and denied hits. To include this report in a schedule, select the *Intrusion (IPS) Reports > Intrusions (IPS) Summary* report.	Email, Directory
	Activity Trend	Summary report of a trend of the intrusions on your network. To include this report in a schedule, select the *Intrusion (IPS) Reports > Intrusions (IPS) Activity Trend* report.	Email, Directory
	Signatures	Summary of the IPS actions, organized by signature. To include this report in a schedule, select the *Intrusion (IPS) Reports > Intrusions (IPS) Detail by Signature* report.	Email, Directory
	Source IP	Summary of the IPS actions, organized by the IP address where the traffic originated. To include this report in a schedule, select the *Intrusion (IPS) Reports > Intrusions (IPS) Detail by Source* report.	
	Threat Level	Summary of the IPS actions, organized by the threat level. To include this report in a schedule, select the *Intrusion (IPS) Reports > Intrusions (IPS) Detail by Threat Level* report.	
	Protocol	Summary of the IPS actions, organized by the protocol used for the traffic. To include this report in a schedule, select the *Intrusion (IPS) Reports > Intrusions (IPS) Detail by Protocol* report.	

Report Type	Pivot Name	Description	Report Schedule Destination
Reputation Enabled Defense	Action	Summary of all the Reputation Enabled Defense actions for traffic through the device. To include this report in a schedule, select the *Reputation Enabled Defense > Reputation Enabled Defense Summary* report.	Email, Directory
	Activity Trend	Summary report of a trend of the URLs that were scanned and the URL responses. To include this report in a schedule, select the *Reputation Enabled Defense > RED Activity Trend* report.	Email, Directory
spam	spam Level	Summary of all the spamBlocker categories for mail traffic through the Firebox. Statistics include the message type, the count of email messages in each category, and the percent of email messages that the count represents. To include this report in a schedule, select the *spam Summary > spam Summary* report.	Email, Directory
	Action	Summary of all the spamBlocker actions for traffic through the Firebox. Statistics include the action type, the count of email messages, and the percent of email messages that the count represents.	
	Activity Trend	Summary report of a trend of the traffic that was scanned by spamBlocker in relation to the amount of spam that was detected. To include this report in a schedule, select the *spam Summary > spam Activity Trend* report.	Email, Directory
Virus (GAV)	Virus	Summary of the Gateway AntiVirus actions, organized by virus name. Includes allowed and denied hits. To include this report in a schedule, select the *Virus (GAV) Reports > Virus (GAV) Summary* report.	Email, Directory
	Activity Trend	Summary report of a trend of the traffic that was scanned by GAV in relation to the number of viruses detected. To include this report in a schedule, select the *Virus (GAV) Reports > Virus (GAV) Activity Trend* report.	Email, Directory
	Host (HTTP)	Summary of the Gateway AntiVirus actions, organized by host name.	
	Protocol	Summary of the Gateway AntiVirus actions, organized by the protocol used for the traffic.	

Report Type	Pivot Name	Description	Report Schedule Destination
	Email Sender	Summary of the Gateway AntiVirus actions, organized by the email address that sent the message. Available for the SMTP and POP3 proxies.	
Zero-Day Malware (APT)	Zero-Day Malware (APT) Summary	Summary of the zero-day malware detected by APT Blocker. This report is only available for a report schedule.	Email
	Content Name	Summary of the malware identified as Zero-Day Malware by APT Blocker, organized by content name.	
	Threat ID	Summary of the malware identified as Zero-Day Malware by APT Blocker, organized by the Threat ID.	
	Malicious Activity	Summary of the malicious activity on your network that was identified as Zero-Day Malware by APT Blocker.	
	Recipient/Destination	Summary of the recipient names and destination addresses for activity on your network identified as Zero-Day Malware by APT Blocker.	
	Threat Level	Summary of the threat levels assigned to activity on your network identified as Zero-Day Malware by APT Blocker.	

Device

Report Type	Pivot Name	Description	Report Schedule Destination
Denied Packets		Summary of all the incoming and outgoing packets that were denied access through the device. This report also includes traffic denied for users who exceed the bandwidth and time quota settings on your device. To include this report in a schedule for reports sent to an email destination, select the *Exceptions > Denied Packets Summary* report. To include this report in a schedule for reports sent to a directory destination, select the *Exceptions > Denied Packets (Summary and Detail)* or the *Exceptions > Denied Packets by Client (Summary)* reports.	Email, Directory
Denied Quota		Summary of the denied traffic by hits for users who exceed the bandwidth and time quotas configured on your device. Includes the name of the user, the count of user attempts to connect, and the percentage of denied connections for each user. To include this report in a schedule, select the *Exceptions > Denied Quota Summary* report.	Email

Report Type	Pivot Name	Description	Report Schedule Destination
Alarms		Summary of all the alarm records generated for the device. To include this report in a schedule, select the *Exceptions > Alarms Summary Report* report.	Email, Directory
Authentication	Allowed	Summary of all users who successfully authenticated to the device. Includes the login time, logout time, duration, and connection method. If bandwidth and time quotas are enabled on your Firebox, the quota usage details also appear for each user. To include this report in a schedule, select the *Firebox Reports > User Authentication* report.	Directory
	Denied	Summary of all users who were not allowed to authenticate to the device. Includes the date, time, and reason authentication failed. To include this report in a schedule, select the *Firebox Reports > User Authentication Denied* report.	Directory
Audit Trail		Summary of all audited configuration changes for a device. Includes the user account that made the change, the change that was made, the date and time of the change, and any comments that were added about the changes. To include this report in a schedule, select the *Firebox Reports > Audit Trail* report.	Directory
Blocked Default Threats		*Default Threat Protection* feature. To include this report in a schedule, select the *Firebox Reports > Blocked Default Threats* report.	Directory
DHCP Lease Activity		Summary of all activity on the device related to the DHCP lease. To include this report in a schedule, select the *Firebox Reports > DHCP Lease Activity* report.	Directory
Device Statistics		Summary of the bandwidth statistics for all interfaces on the Firebox. Includes TCP-UDP-Proxy incoming and outgoing connection transaction data, when available. To include this report in a schedule for reports sent to the ConnectWise destination, select the *ConnectWise > Firebox Statistics* report. To include this report in a schedule for reports sent to an email or directory destination, select the *Firebox Reports > Device Statistics* report.	Email, Directory, ConnectWise
Policy Usage		Summary of all policies included in the Firebox configuration. For each policy, the policy name, number of hits, number of bytes, and the date and time the policy was last used appear. Policies that have been deleted appear in red with *Deleted* in the **Status** column.	Directory

Report Type	Pivot Name	Description	Report Schedule Destination
		Before you can see this report, *Dimension Command* must be enabled in your Firebox feature key. The Firebox must be configured as a managed device in Dimension to generate policy usage reports about the Firebox. You can export the Policy Usage report as a .CSV file. To include this report in a schedule, select the *Firebox Reports > Policy Usage* report.	
Wireless Intrusion Detection	Summary	Summary of all Wireless Intrusion Detection actions. Rogue access point detection must be enabled on a device to see this information for the device. To include this report in a schedule, select the *Wireless Intrusion Detection > Wireless Intrusion Detection Summary* report.	Email, Directory

Detail

Report Type	Pivot Name	Description	Report Schedule Destination
Zero-Day Malware (APT)	Zero-Day Malware (APT) Detail	Detailed report of all the threats identified by APT Blocker as Zero-Day Malware (not identified until after the traffic passed through the firewall). Each threat includes the time, threat level, threat ID, content name, source and destination IP addresses, the policy and protocol, the host, the sender and recipient addresses, and the number of attempts. To see more detailed information (includes MD5 and Threat Level information), click **Threat Details** for each threat in the report. This report is only available when you create a report schedule. To include this report in a schedule, select the *Zero-Day Malware (APT) Reports > Zero-Day Malware (APT) Detail* report.	Directory
	Content Name	Detailed report of the malware identified as Zero-Day Malware by APT Blocker, organized by content name. This report is only available when you create a report schedule. To include this report in a schedule, select the *Zero-Day Malware (APT) Reports > Detail by Content Type* report.	Directory

Report Type	Pivot Name	Description	Report Schedule Destination
	Threat ID	Detailed report of the malware identified as Zero-Day Malware by APT Blocker, organized by the Threat ID. This report is only available when you create a report schedule. To include this report in a schedule, select the *Zero-Day Malware (APT) Reports > Detail by Threat ID* report.	Directory
	Malicious Activity	Detailed report of the malicious activity on your network that was identified as Zero-Day Malware by APT Blocker. This report is only available when you create a report schedule. To include this report in a schedule, select the *Zero-Day Malware (APT) Reports > Detail by Malicious Activity* report.	Directory
	Recipient/Destination	Detailed report of the recipient names and destination addresses for activity on your network identified as Zero-Day Malware by APT Blocker. This report is only available when you create a report schedule. To include this report in a schedule, select the *Zero-Day Malware (APT) Reports > Detail by Destination* report.	Directory
	Threat Level	Detailed report of the threat levels assigned to activity on your network identified as Zero-Day Malware by APT Blocker. This report is only available when you create a report schedule. To include this report in a schedule, select the *Zero-Day Malware (APT) Reports > Detail by Threat Level* report.	Directory
Advanced Malware (APT)	Advanced Malware (APT) Detail	Detailed report of all the threats identified by APT Blocker. Each threat includes the time, threat level, threat ID, content name, source and destination IP addresses, the policy and protocol, the host, the sender and recipient addresses, and the number of attempts. To see more detailed information (includes MD5 and Threat Level information), click **Threat Details** for each threat in the report. This report is only available when you create a report schedule. To include this report in a schedule, select the *Advanced Malware (APT) Reports > Advanced Malware (APT) Detail* report.	Directory
	Content Name	Detailed report of the malware detected by APT Blocker, organized by content name. Includes allowed and denied hits.	Directory

Report Type	Pivot Name	Description	Report Schedule Destination
		This report is only available when you create a report schedule. To include this report in a schedule, select the *Advanced Malware (APT) Reports* > *Detail by Content Name* report.	
	Threat ID	Detailed report of the malware detected by APT Blocker, organized by the Threat ID. This report is only available when you create a report schedule. To include this report in a schedule, select the *Advanced Malware (APT) Reports* > *Detail by Threat ID* report.	Directory
	Malicious Activity	Detailed report of the malicious activity on your network that was detected by APT Blocker. This report is only available when you create a report schedule. To include this report in a schedule, select the *Advanced Malware (APT) Reports* > *Detail by Malicious Activity* report.	Directory
	MIME Type	Detailed report of the MIME types used on your network. This report is only available when you create a report schedule. To include this report in a schedule, select the *Advanced Malware (APT) Reports* > *Detail by MIME Type* report.	Directory
	Protocol	Detailed report of the protocols used for malicious activity on your network that was detected by APT Blocker. This report is only available when you create a report schedule. To include this report in a schedule, select the *Advanced Malware (APT) Reports* > *Detail by Protocol* report.	Directory
	Recipient/Destination	Detailed report of the recipient names and destination addresses for malicious activity on your network. This report is only available when you create a report schedule. To include this report in a schedule, select the *Advanced Malware (APT) Reports* > *Detail by Destination* report.	Directory
	Sender/Source	Detailed report of the sender names and source addresses for malicious activity on your network. This report is only available when you create a report schedule. To include this report in a schedule, select the *Advanced Malware (APT) Reports* > *Detail by Source* report.	Directory

Report Type	Pivot Name	Description	Report Schedule Destination
Alarms	Threat Level	Detailed report of the threat levels assigned to malicious activity on your network. Includes the time of the event, the name of the alarm, and an informational message for each alarm event. To include this report in a schedule, select the *Exceptions > Alarms* report.	Directory
Application Usage	Client	Detailed report about the applications used by clients on your network, by bandwidth or hits. To include this report in a schedule, select the *Application Control > Application Usage Summary* report.	Directory
	Source	Detailed report about the source IP address of applications used on your network, by bandwidth or hits. To include this report in a schedule, select the *Application Control > Application Usage Summary* report.	Directory
	Mobile Device	Detailed report about the source IP address of applications used on your network, by bandwidth or hits. To include this report in a schedule, select the *Application Control > Application Usage Summary* report.	Directory
	Category	Detailed report about the categories of applications used on your network, by bandwidth or hits. To include this report in a schedule, select the *Application Control > Application Usage Summary* report.	Directory
	Application	Detailed report about the applications used on your network, by bandwidth or hits. To include this report in a schedule, select the *Application Control > Application Usage Summary* report.	Directory
Blocked Applications	Client	Detailed report about the applications used on your network that were blocked by Application Control, by client. To include this report in a schedule, select the *Application Control > Blocked Application Summary* report.	Directory
	Source	Detailed report about the applications used on your network that were blocked by Application Control, by source IP address. To include this report in a schedule, select the *Application Control > Blocked Application Summary* report.	Directory
	Mobile Device	Detailed report about the applications used on your network that were blocked by Application Control, by mobile device.	Directory

Report Type	Pivot Name	Description	Report Schedule Destination
		To include this report in a schedule, select the *Application Control > Blocked Application Summary* report.	
	Category	Detailed report about the applications used on your network that were blocked by Application Control, by category. To include this report in a schedule, select the *Application Control > Blocked Application Summary* report.	Directory
	Application	Detailed report about the applications used on your network that were blocked by Application Control, by application. To include this report in a schedule, select the *Application Control > Blocked Application Summary* report.	Directory
Blocked Websites	By Category	Detailed report about all websites that were blocked, organized by category. To include this report in a schedule, select the *Blocked Websites Reports > Blocked Websites (Summary, by Category and Client)* report.	Directory
	By Client	Detailed report about all websites that were blocked, organized by client. To include this report in a schedule, select the *Blocked Websites Reports > Blocked Websites (Summary, by Category and Client)* report.	Directory
	By Mobile Device	Detailed report about all websites that were blocked, organized by mobile device. To include this report in a schedule, select the *Blocked Websites Reports > Blocked Websites (Summary, by Mobile Devices)* report.	Directory
Botnet Detection		Detailed report about the traffic sent to and from a botnet address. Includes the date and time of the traffic, the source and destination addresses, the number of attempts made to send traffic to the botnet site, the protocol used, and whether the address was the source or destination. You can click the client or destination to filter the report data on that data. To include this report in a schedule, select the *Botnet Detection > Blocked Botnet Site Detail*.	Directory
Data Loss Violations (DLP)		Detailed report about all the violations of the Data Loss Prevention rules configured on your device. To include this report in a schedule, select the *Data Loss Violations (DLP) > DLP Detail* report.	Directory

Report Type	Pivot Name	Description	Report Schedule Destination
Denied Packets	By Detail	Detailed report of all the packets denied by your device, organized by detail. Includes the time of the first action, the source and destination IP addresses, the number of attempts for each packet, the protocol and port, and the action.	Directory
	By Client Detail	Detailed report of all the packets denied by your device, organized by client. Includes the IP address of the client, the first and last date/time the packet was denied, the intended packet destination, the protocol and port , and the number of attempts for each packet.	Directory
Denied Quota		Detailed report of traffic denied because of bandwidth and time quota settings on your Firebox. Includes the time of the first action, the source and destination of the traffic, the number of connection attempts, the protocol applied to the traffic, and the quota action applied.	
Mobile Devices		Detailed report of all the mobile device connections through your Firebox. Details include the date/time, mobile device name, connection status, user name, UUID of FireClient, compliance check results, IP address of the mobile device, MAC address of the mobile device, device type, OS version of the mobile device, and VPN type. This report can be exported to a .CSV file. To include this report in a schedule, select the *Mobile Device Reports > Mobile Device Summary* report.	Directory
Virus (GAV)	By Detail	Detailed report of all Gateway AntiVirus actions, organized by detail. This report is only available when you create a report schedule. To include this report in a schedule, select the *Virus (GAV) Reports > Virus (GAV) Detail* report.	Directory
	By Email Sender	Detailed report of Gateway AntiVirus actions, organized by the email address that sent the message. Available for the SMTP and POP3 proxies. This report is only available when you create a report schedule. To include this report in a schedule, select the *Virus (GAV) Reports > Detail by Email Sender* report.	Directory
	By Host (HTTP)	Detailed report of Gateway AntiVirus actions, organized by host name.	Directory

Report Type	Pivot Name	Description	Report Schedule Destination
		This report is only available when you create a report schedule. To include this report in a schedule, select the *Virus (GAV) Reports > Detail by Host (HTTP)* report.	
	By Protocol	Detailed report of Gateway AntiVirus actions, organized by the protocol used for the traffic. This report is only available when you create a report schedule. To include this report in a schedule, select the *Virus (GAV) Reports > Detail by Protocol* report.	Directory
	By Virus	Detailed report of Gateway AntiVirus actions, organized by virus name. Includes allowed and denied hits. This report is only available when you create a report schedule. To include this report in a schedule, select the *Virus (GAV) Reports > Detail by Virus* report.	Directory
Intrusions (IPS)		Detailed report of all Intrusion Prevention Service actions. To include this report in a schedule, select the *Intrusions (IPS) Reports > Intrusions (IPS) Detail* report.	Directory
	By IP-Spoofed Packets	Detailed report of Intrusion Prevention service actions, by IP-spoofed packets. This report is only available when you create a report schedule. To include this report in a schedule, select the *Intrusions (IPS) Reports > Detail by IP-Spoofed Packets* report.	Directory
	By Protocol	Detailed report of Intrusion Prevention service actions, by protocol. This report is only available when you create a report schedule. To include this report in a schedule, select the *Intrusions (IPS) Reports > Detail by Protocol* report.	Directory
	By Signature	Detailed report of Intrusion Prevention service actions, by the signature ID. This report is only available when you create a report schedule. To include this report in a schedule, select the *Intrusions (IPS) Reports > Detail by Signature* report.	Directory
	By Source	Detailed report of Intrusion Prevention service actions, by the source address. This report is only available when you create a report schedule.	Directory

Report Type	Pivot Name	Description	Report Schedule Destination
		To include this report in a schedule, select the *Intrusions (IPS) Reports > Detail by Source* report.	
	By Threat Level	Detailed report of Intrusion Prevention service actions, by threat level. This report is only available when you create a report schedule. To include this report in a schedule, select the *Intrusions (IPS) Reports > Detail by Threat Level* report.	Directory
POP3 Proxy		Detailed report about all traffic through the POP3-proxy. To include this report in a schedule, select the *POP3 Proxy > POP3 Proxy Detail* report.	Directory
SMTP Proxy		Detailed report about all traffic through the SMTP-proxy. To include this report in a schedule, select the *SMTP Proxy > SMTP Proxy Detail* report.	Directory
Web Audit	By Category	Detailed report about all allowed web traffic connections through your device, organized by category. To include this report in a schedule, select the *Web Audit Reports > Web Audit (Summary, By Category and Client* report.	Directory
	By Client	Detailed report about all allowed web traffic connections through your device, organized by client. To include this report in a schedule, select the *Web Audit Reports > Web Audit (Summary, By Category and Client* report.	Directory
	By Mobile Device	Detailed report about all allowed web traffic connections through your device, organized by mobile device. To include this report in a schedule, select the *Web Audit Reports > Web Audit (Summary, By Mobile Device* report.	Directory
AP Device Events		Detailed report of all events that occur on the AP devices connected to your Firebox. Includes the event time, the AP device name. and the event message.	
Rogue Access Points		Detailed report of all rogue access point detection events. Includes the SSID, BSSID, and time of each rogue access point detection event.	

Health

Report Type	Pivot Name	Description	Report Schedule Destination
Health Summary		Detailed statistics about memory usage, CPU usage, and the physical interfaces on the Firebox. Includes minimum, average, and maximum values.	Email, Directory
Usage Summary		Detailed report with a list and a chart of the memory and CPU usage statistics.	Email, Directory
Interface Summary	Physical Interfaces	Detailed report with a list and a chart of the sent and received statistics for each interface. Can pivot by byte, rate, and packets	Email, Directory

Compliance

Report Type	Pivot Name	Description	Report Schedule Destination
PCI		Summary of the compliance report data related to PCI. This report is only available for a report schedule. To include this report in a schedule, select the *Compliance Reports* > *PCI* report.	Email, Directory
	Zero-Day Malware (APT)	Detailed report of all the threats identified by APT Blocker as Zero-Day Malware (not identified until after the traffic passed through the firewall), that are relevant to PCI. Each threat includes the time, threat level, threat ID, content name, source and destination IP addresses, the policy and protocol, the host, the sender and recipient addresses, and the number of attempts.	
	Advanced Malware (APT)	Detailed report of all the threats identified by APT Blocker, that are relevant to PCI. Each threat includes the time, threat level, threat ID, content name, source and destination IP addresses, the policy and protocol, the host, the sender and recipient addresses, and the number of attempts.	
	Virus (GAV)	Detailed report of the Gateway AntiVirus actions, that are relevant to PCI.	
	Intrusions (IPS)	Detailed report of all Intrusion Prevention Service actions, that are relevant to PCI.	
	Audit Trail	Detailed report of all audited configuration changes for a device, that are relevant to PCI. Includes the user account that made the change, the change that was made, the date and time of the change, and any comments that were added about the changes.	
	Alarms	Summary report of alarm records on the device, that are relevant to PCI.	
	User Authentication	Detailed list of users authentication to the device, that are relevant to PCI.	

Report Type	Pivot Name	Description	Report Schedule Destination
		Includes the date, time, status (allowed or denied) and reason for authentication failure (if authentication was denied).	
HIPAA		Summary of the compliance report data related to HIPAA. This report is only available for a report schedule. To include this report in a schedule, select the *Compliance Reports* > *HIPAA* report.	Email, Directory
	Intrusions (IPS)	Detailed report of all Intrusion Prevention Service actions, that are relevant to HIPAA.	
	Audit Trail	Detailed report of all audited configuration changes for a device, that are relevant to HIPAA. Includes the user account that made the change, the change that was made, the date and time of the change, and any comments that were added about the changes.	
	Alarms	Summary report of alarm records on the device, that are relevant to HIPAA.	
	User Authentication	Detailed list of users authentication to the device, that are relevant to HIPAA. Includes the date, time, status (allowed or denied) and reason for authentication failure (if authentication was denied).	

10 Bibliografía

[1] Wikipedia,"UTM", https://es.wikipedia.org/wiki/Unified_Threat_Management, 2019.

[2] Sophos, https://news.sophos.com/en-us/2014/01/28/utm-and-next-gen-firewalls-whats-the-difference-infographic, 2019.

[3] Kenneth Tam, Martin Hoz Salvador, "UTM Security with Fortinet", Syngress, Noviembre 2012

[4] Gartner, "Reviews for Unified Threat Management (UTM), Worldwide", https://www.gartner.com/reviews/market/unified-threat-management, 2019

[5] Gartner, "Magic Quadrant for Unified Threat Management (SMB Multifunction Firewalls)", Gartner, 2018

[6] Watchguard,"APT Blocker", https://www.watchguard.com/wgrd-products/security-services/apt-blocker, 2019

[7] Watchguard,"TDR", https://www.watchguard.com/wgrd-products/security-services/threat-detection-and-response, 2019

[8] Watchguard,"Intelligent AV", https://www.watchguard.com/wgrd-products/security-services/intelligentav, 2019

[9] Watchguard,"DNS Watch", https://www.watchguard.com/wgrd-products/security-services/dnswatch, 2019

[10] Watchguard,"Intrusion Prevention Service", https://www.watchguard.com/wgrd-products/security-services/Intrusion-prevention-service, 2019

[11] Watchguard,"Web Blocker", https://www.watchguard.com/wgrd-products/security-services/webblocker-url-filtering, 2019

[12] Watchguard,"Gateway AV", https://www.watchguard.com/wgrd-products/security-services/gateway-av, 2019

[13] Watchguard,"Network Discovery", https://www.watchguard.com/wgrd-products/security-services/network-discovery, 2019

[14] Watchguard,"Reputation Enabled Defense", https://www.watchguard.com/wgrd-products/reputation-based-threat-prevention/, 2019

[15] Watchguard,"Spam Prevention", https://www.watchguard.com/wgrd-products/spam-prevention/, 2019

[16] Watchguard,"Application Control", https://www.watchguard.com/wgrd-products/application-control/, 2019