Introducción

La oferta de seguridad de Miray Operador se basa en un cluster de firewalls “Fortinet” de alta disponibilidad, alojado y centralizado en el núcleo de la red, con el fin de ofrecer un funcionamiento de tipo “**Firewall As A Service**”, disponible para todos los enlaces de acceso y máquinas virtuales de miray.consulting.sl.

Su función principal es controlar los flujos y bloquear los accesos no autorizados, una función que se está haciendo más compleja con el tiempo y con la aparición de nuevas amenazas y técnicas de evasión, así como el aumento del volumen de datos y la diversidad de los medios de acceso.

Las principales características de este servicio son las siguientes:

- Firewall Stateful
- Traducción de direcciones y puertos (NAT/PAT)
- Proxy
- VPN IPSec y SSL
- IPS (Intrusion Prevention System)
- Antivirus
- Control de aplicaciones
- Filtrado web

Estas funcionalidades se dividen en 2 niveles de servicios, estándar y avanzados:

La gestión del Firewall se basa en los ASIC NP (Network Processor) que permiten la aceleración del procesamiento datos basado en el hardware. Este posicionamiento, único en el mercado de la seguridad, ofrece la mejor garantía de rendimiento, sea cual sea el tamaño de los paquetes. El uso de los ASIC también proporcional a latencia más baja del mercado.

Además, FortiOS, el sistema operativo de Fortinet facilita la gestión de las políticas de seguridad que pueden estar compuestas por varios miles de reglas. El uso de "arrastrar y soltar", menús contextuales, búsquedas inteligentes y diversas posibilidades de realizar comentarios facilitan el trabajo diario de los administradores.

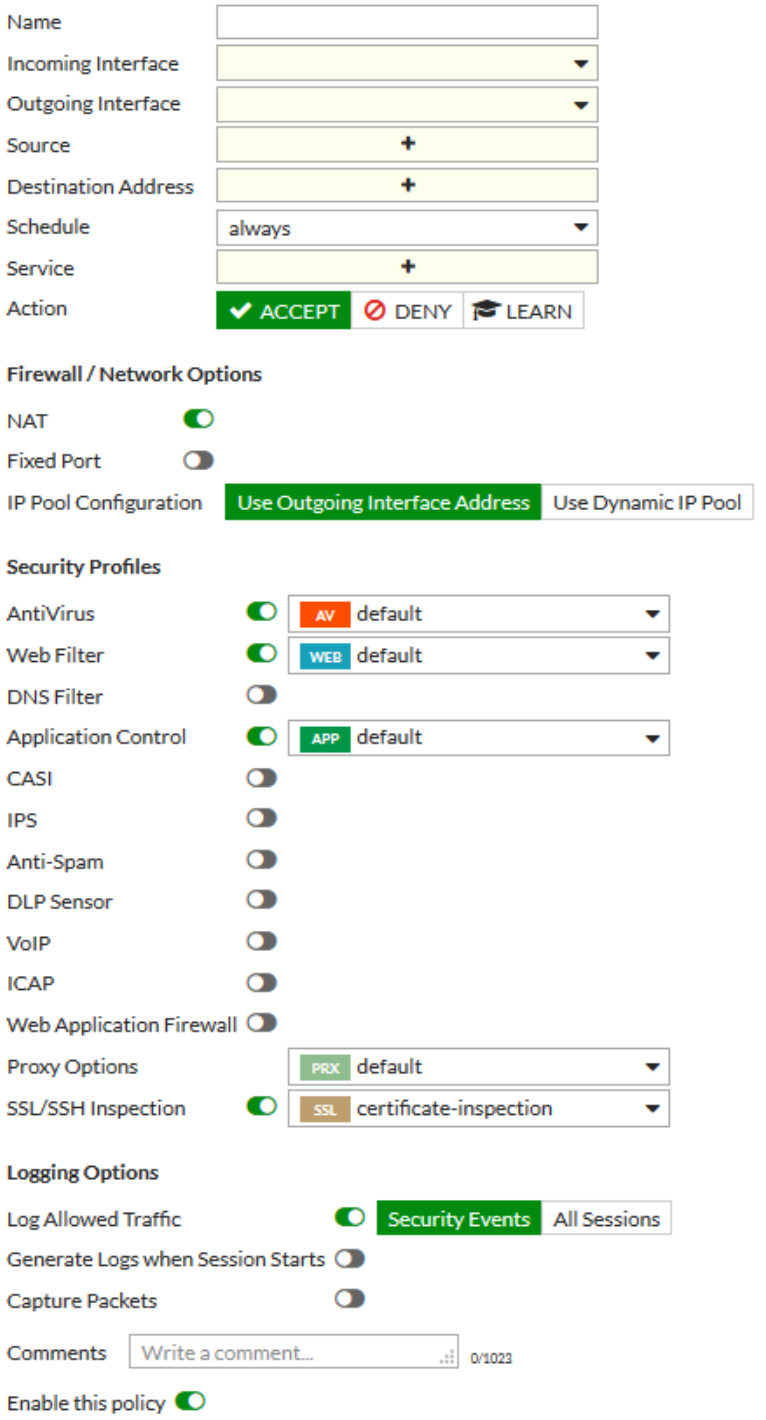
La oferta de Cloud Firewall le da acceso directo al a interfaz de gestión de Fortinet "FortiOS" y le permite configurar y administrar usted mismo su política de seguridad.

Configuración de una política de seguridad

Una política de seguridad consiste en un conjunto de reglas de Firewall.

Las reglas se analizan de arriba abajo, de acuerdo con una serie de criterios, tales como interfaces fuente/destino, IP/usuarios/máquinas fuente/destino, servicios o una noción temporal de validez de la regla.

A continuación, se muestra una captura de pantalla que muestra los principales elementos de configuración de una regla de cortafuegos.



Los criterios para “emparejar” una regla son las interfaces de origen y destino, las direcciones IP/máquinas/usuario de origen, las direcciones IP de destino, el servicio y la franja horaria.

Funcionalidades Estándar

Firewall “Stateful”

El Firewall de FortiOS es de tipo “Stateful inspection”. Le permite controlar y administrar reglas por sesión para mejorar la seguridad y el rendimiento del procesamiento en comparación con un Firewall “Stateless” que procesa los paquetes como una unidad.

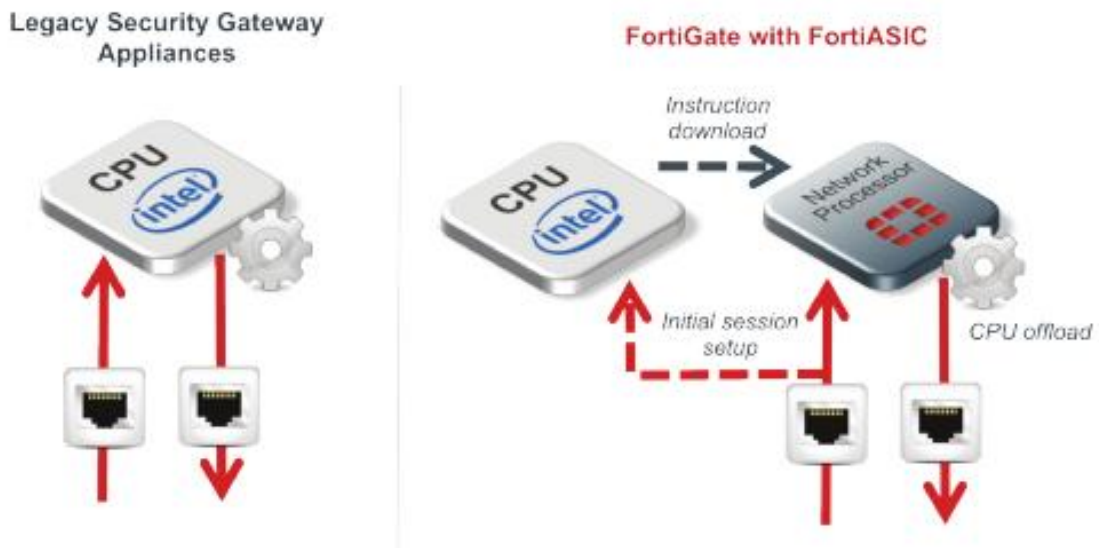
Por cada nueva sesión aceptada, el dispositivo FortiGate añade una entrada en una caché de conexión activa de alta velocidad. Posteriormente, los paquetes interceptados son aceptados inmediatamente si coinciden con sesiones válidas en la caché.

El motor de escaneo de Firewall puede reconocer la mayoría de los protocolos que se basan en la señalización y los canales de datos como el FTP. Su papel es entonces recoger la información que describa el canal de datos que se está negociando con el fin de pre-registrarlo en la caché de las conexiones válidas. En este caso, incluso el paquete que abre el canal de datos será aceptado inmediatamente gracias a la entrada en esta caché.

Rendimiento y aceleración del hardware

Cuando se recibe un paquete, el cortafuegos lo analiza para extraer la información necesaria para su procesamiento, como las direcciones IP de origen y destino o el protocolo El Firewall determinará entonces el tratamiento que se le aplicará, si pertenece a una sesión existente o no, lo bloqueará o lo permitirá potencialmente con un análisis adicional (Antivirus, IPS, control de aplicaciones…)

Una vez que la sesión se ha establecido a nivel de Firewall, todos los siguientes paquetes ya no serán procesados por la CPU sino por un procesador de red ASIC. Las ventajas son múltiples: descargar al procesador que se puede utilizar para otras tareas, acelerar el procesamiento de datos y garantizar el rendimiento sea cual sea la aplicación.



Traducciones de direcciones (NAT) y de puertos (PAT)

FortiOS soporta todos los mecanismos NAT:

- **Source NAT:** Para ocultar las direcciones IP de origen de los paquetes salientes. En el caso más simple, la dirección IP original de origen es reemplazada por la dirección IP de la interfaz de Firewall a través de la cual se enruta el paquete. Pero, por supuesto, es posible elegir una dirección IP de reemplazo específica o incluso elegir la dirección IP de reemplazo de un grupo de direcciones IP.
- **Destination NAT:** para sustituir las direcciones IP de destino de los paquetes entrantes. Este modo de traducción muy completo tiene extensiones como NAPT (Network Address and Port Translation) y NAPT condicional (dependiendo de las direcciones IP de origen).
- **El mismo paquete puede ser traducido tanto en origen como en destino.**

Estas características de NAT pueden ser gestionadas de forma muy granular a nivel de reglas del Firewall o de forma centralizada a nivel de la tabla central de NAT. Los mecanismos de NAT son aplicables en modo transparente y en modo enrutado. La función NAT está totalmente soportada en un contexto VPN: un flujo que entra o sale de un túnel puede ser traducido al origen y/o destino. El dispositivo FortiGate es compatible con las tecnologías IPv6 NAT.

Proxy transparente o explícito

FortiGate puede ser utilizado como un proxy transparente o explícito para el tráfico IPv4 e IPv6. En el caso de un proxy explícito, la IP de FortiGate debe ser declarada en los navegadores de los clientes.

En esta configuración, el FortiGate es capaz de almacenar en cache página web u objetos en su disco para mejorar el rendimiento de la navegación web. El almacenamiento en caché web no es compatible con el contenido de audio, vídeo y

streaming. Se pueden establecer excepciones para los sitios que no deben ser almacenados en caché.

Acceso remoto (VPN)

En esta sección se describen dos tipos de VPNs, aunque también hay otros modos disponibles como VPNs PPTP o L2TP o GRE. Actualmente, las VPN de tipo IPsec y SSL son las más utilizados por sus respectivas ventajas.

Funcionalidades VPN SSL

HTTPS en un protocolo basado en SSL (Secure Sockets Layer) que es soportado por la mayoría de los navegadores web para el intercambio seguro de información sensible entre un servidor y un cliente web. El SSL establece un enlace cifrado y garantiza que todos los datos transmitidos entre el servidor web y el navegador del cliente permanecen privados y seguros. La principal ventaja de esta solución VPN es que no es necesario instalar un cliente pesado en la estación de trabajo del cliente y que el protocolo HTTPS, de fácil uso, suele permitir el paso a través de los dispositivos de seguridad.

Existen tres modos en la configuración de un túnel VPN SSL:

- **Modo túnel:** La conexión VPN SSL se realiza entre un cliente completo (navegador + activeX, cliente pesado, etc.) y la puerta de enlace SSL que desencapsula los paquetes antes de enrutarlos hacia su destino. Todos los protocolos IP pueden ser tunelizados, garantizando así una perfecta compatibilidad con la red existente.
- **Modo portal web:** el enlace VPN SSL se realiza entre un cliente simple (navegador) y la puerta de enlace SSL que presenta un portal web al usuario. El usuario puede entonces iniciar flujos desde este portal, y la puerta de enlace se convierte en cliente para estas solicitudes. Dependiendo de las aplicaciones cliente disponibles en el portal, ciertos recursos se vuelven accesibles para el usuario, así como un entorno virtual. Se pueden añadir funciones adicionales al portal web como marcadores, personalización de enlaces, mensajes de bienvenida, etc.
- **Modo port-forwarding:** el modo túnel proporciona un acceso de nivel 3 a la red interna y a todas las aplicaciones, pero requiere la instalación de un cliente. El modo web limita las aplicaciones disponibles. El modo port-forwarding es una solución intermedia para la cual se configura un puerto de escucha en la estación de trabajo del usuario. El módulo VPN SSL redirige estos flujos capturados en el túnel SSL a la puerta de enlace, que los descifra y los transmite al servidor correspondiente. El módulo de redireccionamiento de puertos funciona con un applet Java, que se descarga y ejecuta en el ordenador del usuario. El applet también proporciona estadísticas sobre los flujos enviados y recibidos.

Funcionalidades VPN IPsec

FortiOS soporta túneles VPN IPsec cuya fase 1 se basa en el protocolo IKE (versión 1 o 2), así como funciones "NAT Traversal" para la negociación de parámetros del túnel, autenticación, generación de claves de cifrado de datos, establecimiento del túnel y protocolo ESP para la transmisión de datos (ip-protocol 50)

Todas estas funciones se realizan a través de los FortiASICs instalados en el equipo y , por lo tanto, pueden beneficiarse de la aceleración del hardware y de un mayor nivel de rendimiento. Gracias a las prestaciones del hardware, el nivel de seguridad puede ser aumentado sin degradar el rendimiento global del sistema. El FortiOS soporta altos algoritmos de encriptación y autenticación como AES256, SHA512 o grupos Diffie Hellmann de 1 a 21.

Por supuesto, se respetan los estándares IPsec, manteniendo al mismo tiempo un alto grado de flexibilidad de configuración al admitir diferentes modos de configuración:

- Modo configuración IKE
- Modo de servidor de políticas para túneles "Dialup" para usuarios nómadas.
- Entrega automatizada de direcciones a través del túnel (DHCP sobre IPsec)

La configuración del túnel se facilita mediante asistentes de configuración de 3 a 5 pasos basados en modelos de configuración con equipos de Fortinet o de terceros.

Cliente VPN para estaciones de trabajo cliente

Los usuarios remotos pueden utilizar el software FortiClient para iniciar un túnel VPN SSL y conectarse a la red interna. FortiClient utiliza el puerto TCP local 1024 para establecer una conexión cifrada SSL con el FortiGate en el puerto TCP 443. Durante esta conexión, FortiGate autentica la solicitud de FortiClient VPN SSL basándose en las opciones del grupo de usuarios. El FortiGate establece un túnel con el cliente y le asigna una dirección IP virtual. Una vez establecido el túnel, el usuario puede acceder a la red detrás del FortiGate. El software FortiClient está disponible para su descarga en www.forticlient.com para Windows, Mac OS X, apple iOS y Android.

Clientes VPN para dispositivos móviles.

El FortiClient también está disponible en una versión para Android, Windows e iOS.

Funcionalidades Avanzadas

Antivirus

El antivirus, desarrollado por Fortinet, proporciona una solución completa e integrada al Firewall para eliminar un amplio espectro de ataques y actividades maliciosas incluyendo virus, troyanos, gusanos, spyware, botnets, grayware y adware. El

antivirus Fortinet utiliza una doble detección basada tanto en una base de firmas como a través de un algoritmo de análisis heurístico.

El alto nivel de rendimiento del motor se debe en particular al lenguaje CPRL "Content Pattern Recognition Language", que acelera el escaneo antivirus y la detección de anomalías.

Protocolos analizados

FortiGate es capaz de escanear un gran número de protocolos:

- HTTP
- HTTPS (con descifrado SSL)
- SMTP
- POP3
- IMAP
- MAPI
- FTP
- NNT

Así como ciertos formatos de compresión utilizados con frecuencia, en particular en el marco de las siguientes técnicas:

- GZIP
- RAR
- IZH
- IHA
- CAB
- ARJ
- ZIP

Rendimiento

El procesador de contenido FortiASIC ayuda a la CPU a analizar los flujos para identificar y bloquear las amenazas. Este ASIC acelera el proceso de escaneo, ya sea basado en la firma o en la heurística. Los aparatos FortiGate con FortiASIC CP se benefician de un mejor rendimiento.

Inspección en modo "Flow"

Además del modo proxy de escaneo antivirus estándar, FortiGate incluye un motor de escaneo llamado "sobre la marcha" o "Flow". Este modo significa que el FortiGate será capaz de escanear flujos y archivos independientemente de su tamaño. Además, el modo "Flow" también es capaz de escanear archivos comprimidos.

Control de aplicaciones o Application Control

El reconocimiento del flujo de aplicaciones se basa en el análisis del tráfico en tiempo real y en la consulta sobre una base de datos de firmas incorporadas en el equipo y que hace referencia a más de 3500 aplicaciones. Esta base de datos se actualiza a través del servicio FortiGuard.

La gestión del filtrado de aplicaciones se basa en la definición de perfiles que contienen uno o más filtros de detección. Los perfiles pueden utilizarse de forma muy flexible y granular aplicándolos a nivel de una regla de Firewall, ofreciendo una inspección basada en reglas.

Cada filtro se define o bien en base a una selección de aplicaciones de la base de datos actualizada continuamente a través de FortiGuard (que actualmente contiene más de 3500 aplicaciones) o bien en base a una selección de un grupo de aplicaciones con los siguientes criterios de selección:

- Categorías (Botnet, Game, FileSharing, P2P, Business …)
- Editores (AOL, Adobe, Google, Apple, IBM, Cisco, Citrix, …)
- Tecnologías (Browser-Based, Client-Server, Network-Protocol, Peer-to-Peer)
- Protocolos (BO, DCERPC, DHCP, DNP3, DNS, FTP, H323, HTTP, SIP, SSH, SMTP …)
- Popularidad (de 1 a 5)

Para cada filtro son posibles varias acciones: permitir, monitorizar, bloquear, enviar un reset.

El perfil se asocia entonces a una política de seguridad, como también ocurre con otras características avanzadas, lo que permite un control muy fino de los comportamientos de la aplicación.

Filtrado de URLs y protocolos

El filtrado Web se utiliza para controlar las solicitudes de los usuarios a los sitios web.

El control de navegación se utiliza para evitar:

- Pérdida de productividad relacionada con el acceso de los empleados a Internet por razones personales o no relacionadas con el negocio.
- Congestión de la red: Cuando se consume una gran cantidad de ancho de banda por razones equivocadas, las aplicaciones legítimas sufren.
- La pérdida o exposición de información confidencial a través de sitios de chat, sistemas de mensajería no aprobados o el intercambio “peer to peer”.
- Mayor riesgo de exposición a las amenazas por el uso de sitios cuestionables.
- La responsabilidad legal de la empresa relacionada con el acceso o la descarga de contenidos protegidos o ilegales.

Los diferentes modos de filtrado

Los equipos FortiGate tienen varios tipos de filtrado:

- Filtrado por URL
- Filtrado por categorías (FortiGuard)
- Filtrado de contenidos
- Filtrado de scripts

Es posible utilizar los diferentes tipos de filtrado simultáneamente en los flujos asociados.

Filtrado por URL

Este método le permite autorizar, desautorizar, supervisar o eximir una URL o un dominio de cualquier otro control.

Las entradas pueden ser una única y simple URL utilizando meta caracteres (Wildcard o expresiones regulares) De hecho, se trata de listas blancas y listas negras con una funcionalidad más rica que en el modo simple de todo o nada.

Filtrado por categorías

Se trata de un modo de filtrado basado en las categorías de URL proporcionadas por FortiGuard. Los beneficios de este modo de filtrado son múltiples. Por un lado, los equipos de FortiGuard Labs trabajan las 24 horas del día para garantizar la actualización constante de las bases de datos para tener una clasificación lo más cercana posible a la realidad. Por otro lado, la gestión de los servidores que proporcionan la base de datos de páginas web clasificadas es realizada por Fortinet y ya no es responsabilidad de la empresa. La empresa ya no tiene que operar y mantener un servidor en la red local.

Funcionamiento del filtrado FortiGuard

El FortiGate intercepta las peticiones web de los usuarios y determina si tienen derecho a ver la página. Los servidores de FortiGuard mantienen una base de datos de varios cientos de millones de páginas.

Cuando el navegador web consulta una URL, la solicitud es procesada por la red de la siguiente manera:

1. El equipo FortiGate intercepta la petición en la red local.
2. Si el FortiGate ya tiene el nombre de la categoría correspondiente a la página web en caché, este nombre se compara inmediatamente con los nombres de las categorías permitidas.
3. Si esta categoría está permitida, la solicitud web se reenvía al sitio de destino y una solicitud de clasificación se reenvía simultáneamente a un servidor FortiGuard.

4. El FortiGate recibe el nombre de la categoría a la que pertenece la página desde el servidor FortiGuard. Esta categoría se compara con la lista de categorías permitidas. Al mismo tiempo, el FortiGate recibe los datos del sitio web consultado.
5. Si la política es permitir la visualización de la página, la respuesta del sitio web se remite al usuario. De lo contrario, se envía un mensaje de anulación personalizable al usuario y se registra el evento.

El sistema FortiGuard tiene 78 categorías en 6 grupos principales:

- Riesgos de seguridad
- Interés General – Negocios
- Interés General – Personal
- Contenido para adultos
- Consumo de ancho de banda
- Legal / Potencialmente Responsable

Esta lista se puede consultar en el siguiente enlace:
http://www.fortiguard.com/static/webfiltering.html

La configuración de los derechos de acceso asociados a cada categoría se realiza de forma sencilla a nivel de perfil de filtrado web, donde para cada categoría y/o grupo es suficiente con definir la acción correspondiente:

- Acceso autorizado
- Acceso prohibido (bloqueado)
- Acceso supervisado (log)
- Acceso autenticado (SSO o login)
- Acceso desaconsejado (mensaje de alerta)
- Acceso limitado (cupo)

Filtrado de contenidos

Es posible controlar el contenido de las páginas a las que acceden los usuarios bloqueando los sitios que contienen palabras o patrones de palabras específicos. De esta manera se evita el acceso a páginas de contenido dudoso.

Este análisis se configura a través de filtros de contenido, definidos por correspondencia con palabras, frases, meta caracteres y expresiones regulares de tipo “Perl”. Cada perfil de filtrado web puede tener su propio filtro de contenido. Esta función de filtrado analiza el contenido de cada página a la que se accede.

El administrador especifica una lista de palabras, frases o expresiones prohibidas y asigna un valor numérico, o puntuación, a cada elemento de la lista, dependiendo de la importancia de cada ocurrencia en la lista.

Cada vez que el sistema de filtrado de contenidos encuentra una coincidencia en una página, aumenta la puntuación de la página. Si el valor de la suma final de la puntuación de la página es mayor que el umbral establecido por el administrador, la página se bloqueará.

Filtrado de scripts y opciones de proxy

Las funciones de filtrado permiten que cada perfil de filtrado web establezca opciones a nivel de proxy (no disponible en el modo DNS o de flujo). Hay muchas opciones de seguridad como:

- Forzar búsquedas seguras en los motores de búsqueda
- Filtros de YouTube
- Registrar todas las palabras clave de búsqueda
- Bloquear URLs no válidas
- Realizar el filtrado de URL por simple patterns, regular expressions o Wildcards
- Bloquear las URLs maliciosas descubiertas por el FortiSandbox
- Búsqueda de las palabras clave en las URL
- Evaluar las URLs por dominio y dirección IP
- Bloquear redirecciones HTTP basadas en la reputación
- Evaluar las imágenes con respecto a las URL y sustituirlas si es necesario

Existen otras opciones de filtrado disponibles como:

- Restringir el uso de las cuentas de Google a determinados dominios
- Ver detalles de los errores HTTP de las series 400 y 500
- Bloquear HTTP POST
- Eliminar Java, Cookies y applets ActiveX

Implementación de una política de filtrado web

Al igual que todas las características de análisis en profundidad asociadas a los Firewalls de nueva generación, el filtrado Web se configura asociando un perfil Web a una regla de cortafuegos.

Es posible diferenciar las reglas por identidad de usuario, origen, destino, etc.

El administrador definirá a nivel de perfil las categorías y las acciones asociadas, las listas blancas y negras (filtrado de URL), las posibles opciones de filtrado de contenidos y las opciones avanzadas.

Anti-intrusión IPS (Intrusion Prevention System)

El módulo IPS integrado de FortiOS ayuda a proteger las redes de los ataques de los ciberdelincuentes, analizando el tráfico y bloqueando las amenazas antes de que lleguen a los recursos potencialmente vulnerables.

El sistema IPS de FortiGuard puede bloquear hasta190.000 intentos de intrusión cada minuto. La base de protección incluye más de 15.000 reglas utilizadas en más de 7.500 firmas, y cada semana se actualizan o crean unas 100 reglas.

El módulo IPS está compuesto por diferentes funcionalidades que pueden ser activadas bajo demanda y configuradas fácilmente de forma granular. Estas funcionalidades son la detección de anomalías en los protocolos y la gestión de las sondas de los IPS.

El módulo IPS puede ser desplegado y utilizado de manera muy flexible en diferentes ambientes, en modo enrutado o transparente, o en modo "one-arm" o "sniffer". Utiliza la tecnología FortiASIC para proporcionar un servicio de protección eficaz, basado en el centro de investigación FortiGuard, al tiempo que garantiza un rendimiento muy alto y una latencia extremadamente baja.

Configuración de una sonda IPS

La configuración de IPS se basa en la en el concepto de sondas IPS, y se logra de manera muy flexible y granular al asociar una sonda IPS a una regla del Firewall, la misma sonda puede asociarse, si es necesario, a varias reglas de Firewall.

Si se desea contar con un análisis más global de los IPS y no vinculado específicamente a una regla de Firewall, también es posible aplicar un perfil de IPS a las denominadas reglas de "interface policies", cuyo objetivo es permitir la aplicación global de perfiles de protección como los IPS, la DLP o el filtrado web.

Una sonda IPS consiste en un conjunto de filtros configurables y ordenados. Cada filtro también está asociado a una acción.

Los criterios son los siguientes:

- **Gravedad:** Crítica, alta, media, baja, información.
- **Objetivo:** Cliente, servidor.
- **Sistema Operativo:** BSD, Linux, MacOS, Solaris, Windows y otros.
- **Aplicación:** Adobe, Apache, Apple, CGI_app, Cisco, HP, IBM, IE, IIS, Mozilla, MS_Office, Novell, Oracle, PHP_app, Sun, ASP_app, CA, DB2, IM, Ipswitch, MailEnable, MediaPlayer, MS_Exchange, MSSQL, MySQL, Netscape, P2P, PostgreSQL, Real, Samba, SAP, SCADA, Sendmail, Veritas, Winamp, otros.
- **Protocolos:** DNS, FTP, HTTP, ICMP, IMAP, LDAP, POP3, SCCP, SIP, SMTP, SNMP, SSH, SSL, TCP, UDP, BO, DCERPC, DHCP, DNP3, H323, IM, MSSQL, NBSS, NNTP, P2P, RADIUS, RDT, RPC, RTCP, RTP, RTSP, TELNET, TFN, otros.

Por cada filtro, las acciones posibles son:

- Aplicar la configuración por defecto definida por Fortinet
- Supervisar
- Bloquear

- Bloqueo con envío de un reset
- Cuarentena durante un periodo de tiempo configurable.

Detección de anomalías de protocolo y decodificadores

El módulo IPS integrado de FortiOS también incluye la funcionalidad de detección de anomalías en el protocolo y en el decodificador.

Esto permite bloquear los datos malformados, protegiendo así los recursos detrás del equipo FortiGate de tales ataques. Por ejemplo, el decodificador del protocolo HTTP identificará los paquetes HTTP que no cumplen los estándares de protocolo HTTP.

Fail open

Si, por cualquier razón, el módulo IPS deja de funcionar, se configura por defecto en modo “fail open”, permitiendo el paso del tráfico sin el análisis de IPS, lo que permite que el Firewall siga funcionando sin bloquear el tráfico legítimo. En este caso, estamos en entornos donde se prefiere la productividad a la seguridad. De lo contrario, para mayor seguridad, el modulo IPS puede configurarse en modo “fail closed”, lo que permite bloquear el tráfico hasta que se haya sometido a un análisis IPS.

Protección IPS efectiva, probada y certificada

El modulo IPS, al igual que los demás módulos de protección incorporados en FortiOS, se basa en nuestro servicio FortiGuard que proporciona a nuestros clientes las últimas defensas en tiempo real contra las amenazas. FortiGuard proporciona actualizaciones continuas del motor y de la base de datos de firmas incorporadas en los equipos FortiGate. El trabajo del centro de investigación FortiGuard nos permite protegernos muy eficazmente de amenazas desconocidas actualizando la base de datos de IPS lo antes posible, idealmente antes de que aparezcan las primeras amenazas.