RESUMEN DE LA SOLUCIÓN

Permita una visibilidad profunda de aplicaciones, usuarios y dispositivos con los Next-Generation Firewalls de FortiGate

Resumen ejecutivo

Los firewalls tradicionales solo suelen permitir conexiones, o bloquearlas, en función del puerto y del protocolo. Sin embargo, el acceso a la red es ahora dinámico y contextual, y funciona según los principios de confianza cero. Además, la empresa moderna es híbrida, y abarca centros de datos locales, nubes públicas, sucursales y campus corporativos, así como sitios remotos. Los equipos de TI actuales necesitan una visibilidad profunda de las aplicaciones, los usuarios y los dispositivos para defender las redes empresariales contra las ciberamenazas en todo el entorno, pero esto a menudo supone un desafío.

El problema de la visibilidad se ve agravado por el hecho de que casi todo el tráfico de Internet actualmente está cifrado . Las empresas se están encontrando con grandes zonas de puntos ciegos en la red al pasar de costosas arquitecturas de red radial a modelos distribuidos con acceso directo a Internet en el lugar. Los agentes malintencionados pueden aprovechar estas lagunas de la red para ocultar amenazas en el tráfico cifrado.

Más del 95 % del tráfico de Internet ahora está cifrado.[1]

Los Next-Generation Firewalls (NGFW) de FortiGate ofrecen la visibilidad del tráfico cifrado y de la actividad de usuarios, aplicaciones y dispositivos necesaria para crear políticas de red y seguridad contextuales y evolutivas que garanticen la transformación digital. Los NGFW de FortiGate pueden identificar y controlar a todos los usuarios, aplicaciones y dispositivos de la red con técnicas avanzadas de recopilación y análisis de datos. Como componente clave de una solución de firewall de malla híbrida (HMF), los NGFW de FortiGate integran esta visibilidad y protección en todos los dominios de TI, cubriendo toda la infraestructura de red.

Control de Aplicaciones

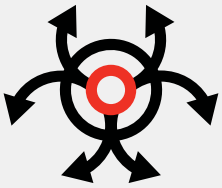
El servicio de control de aplicaciones FortiGuard se conecta a los NGFW de FortiGate e identifica rápidamente las aplicaciones conocidas y desconocidas que atraviesan la red. Permite crear con facilidad políticas para permitir, denegar y restringir el acceso a las aplicaciones, a determinadas funciones dentro de las aplicaciones y a categorías de aplicaciones.

#	Riesgo	Aplicación	Categoría	Tecnología	Usuarios	Ancho de banda	Sesión
1	5	Asprox.Botnet	Botnet	Client-Server	1	1.74 MB	587
2	5	Proxy.HTTP	Proxy	Network-Protocol	11	7.10 MB	457
3	5	Onavo.Protect	Proxy	Client-Server	1	1.78 KB	9
4	5	Hotspot.Shield	Proxy	Client-Server	2	203.99 KB	8
5	5	Skyfire	Proxy	Client-Server	3	27.20 KB	3
6	4	Rsh	Remote.Access	Client-Server	67	9.82 GB	302,237
7	4	BitTorrent	P2P	Peer-to-Peer	8	1.79 MB	5,096
8	4	Telnet	Remote.Access	Client-Server	9	37.81 MB	681
9	4	RDP	Remote.Access	Client-Server	14	9.89 MB	48
10	4	TeamViewer	Remote.Access	Client-Server	22	1.13 MB	38

Los NGFW de FortiGate pueden identificar aplicaciones no solo por la coincidencia de su puerto y protocolo, sino también por la firma de la aplicación, los comportamientos heurísticos y otros indicadores de identificación. Con una vista combinada a las firmas de las aplicaciones y a las aplicaciones de la base de datos de servicios de Internet (ISDB), FortiGate puede establecer más de 4.200 reglas de control de aplicaciones. A continuación se muestran algunas de las formas en las que FortiGate identifica aplicaciones más allá de las Capas 3 y 4.

Firmas de aplicaciones: al tráfico de red permitido se le asigna una firma en función de las características de la transacción y de si el puerto de la aplicación es predeterminado o no. Se examina el tráfico en busca de amenazas y se analiza en profundidad.

Cifrado: si FortiGate detecta cifrado, como capa de sockets seguros (SSL)/seguridad de la capa de transporte (TLS), protocolo de transferencia de hipertexto seguro (HTTPS) o shell seguro (SSH), y se ha implementado una regla de política de descifrado, se descifra la sesión y se vuelven a aplicar las firmas de aplicación en el flujo descifrado.



"... las empresas que inspeccionaron el tráfico entrante afirmaron que el 70% del malware llegó a través de una conexión cifrada".[2]

Descodificadores: si se conoce el protocolo de la aplicación, se utiliza para aplicar firmas adicionales basadas en el contexto con el fin de detectar otras aplicaciones que puedan estar realizando túneles dentro del protocolo. Los descodificadores validan que el tráfico se ajuste a la especificación del protocolo y ofrecen soporte para el recorrido de la traducción de direcciones de red (NAT) y la apertura de agujeros de dinámicos para aplicaciones como el protocolo de inicio de sesión (SIP) y el protocolo de transferencia de archivos (FTP).

Heurística: el análisis heurístico de FortiGate utiliza análisis de comportamiento para determinar la identidad de las aplicaciones evasivas. Esto incluye aplicaciones que utilizan el puerto 80, el puerto 443 o que saltan de puerto en puerto; por ejemplo, aplicaciones de voz sobre protocolo de Internet (VoIP), colaboración de punto a punto (P2P) que no se pueden identificar mediante análisis avanzados de firmas y protocolos.

Si FortiGate no puede identificar una aplicación basándose en su firma, lo hará en características de comportamiento a través de la heurística, clasificando la aplicación previamente desconocida en un grupo de aplicaciones existente y aplicando filtros dinámicos o reenvío basado en políticas para conseguir el resultado deseado.

La identificación de aplicaciones puede proporcionar un contexto significativo sobre la red. FortiGate puede revelar información sobre la función inherente, los puertos de aplicación, el protocolo, la tecnología y las características de comportamiento de la aplicación, lo que permite a los equipos de TI realizar políticas de acceso seguras y fundamentadas. Una vez que el equipo comprende cómo se utiliza una aplicación en la red, se pueden aplicar una variedad de políticas y respuestas más allá de permitir y bloquear.

FortiGuard Application Control también permite a las organizaciones crear políticas y funciones de control dentro de cada aplicación. Algunos ejemplos son:

- Permitir el acceso a Facebook, pero bloquear la transferencia de archivos de Facebook Messenger
- Permitir a los usuarios acceder a Gmail, pero deshabilitar Google Chat
- Bloquear cargas de archivos a Dropbox, Box o Google Drive
- Filtrar categorías de vídeos no deseados para que no se vean en YouTube

FortiOS, el sistema operativo de FortiGate, proporciona una amplia visibilidad del uso de las aplicaciones en tiempo real, así como de las tendencias a lo largo del tiempo a través de vistas, visualizaciones e informes. El control de aplicaciones mantiene las aplicaciones maliciosas, de riesgo y no deseadas fuera de la red a través de puntos de control en el perímetro, en el centro de datos e, internamente, entre los segmentos de la red.

Identificación del usuario

La identificación de los usuarios más allá de sus direcciones IP es otra parte crítica de la seguridad empresarial. FortiOS puede identificar a los usuarios basándose en una variedad de orígenes y métodos, como Microsoft Active Directory (AD), servidores LDAP, syslog, asignación de puertos y encabezados XFF.

La identificación de usuarios de FortiGate proporciona una mejor visibilidad de la actividad de la red y detección frente a comportamientos malintencionados o perjudiciales. La identificación de usuarios de FortiGate identifica a los usuarios en todos los sistemas operativos y en cualquier ubicación, lo que proporciona una mejor visibilidad del uso de las aplicaciones en función de los usuarios. Esto proporciona a los equipos de TI una imagen más relevante de la actividad de la red.

El poder de la identificación de usuarios se hace evidente cuando se encuentra una aplicación desconocida en la red. Ya sea utilizando FortiView o los registros de control de aplicaciones, los equipos de seguridad pueden distinguir:

- La aplicación
- El usuario
- El consumo de ancho de banda y sesión
- El origen y destino del tráfico de la aplicación
- Las amenazas asociadas

Asignación de usuarios

FortiGate puede crear perfiles de usuarios en la red y hacer coincidir los nombres de usuario con las direcciones IP de los paquetes recibidos. La información de los usuarios se puede asignar a políticas de seguridad para un uso más seguro de la red, reservando el acceso a las aplicaciones solo a quienes tengan una necesidad empresarial. La asignación de usuarios puede habilitar un conjunto de reglas o políticas para aplicaciones menos arriesgadas, como SalesForce o PowerPoint, y al mismo tiempo, establecer políticas más estrictas para aplicaciones sensibles, como herramientas de pruebas de penetración o controladores de escritorio remoto.

Asignación de grupos

La definición de reglas de políticas basadas en grupos de usuarios puede simplificar la gestión de TI, ya que las políticas y reglas ya están implementadas y no es necesario reconfigurarlas cuando se añaden nuevos usuarios a diferentes grupos. FortiGate puede aplicar estas reglas y actualizaciones de grupos, y es compatible con varios servidores de directorio, como Microsoft AD, Novell eDirectory y Sun ONE Directory Server. Tras habilitar la identificación de usuarios y aprovechar la asignación de grupos, se pueden configurar políticas de seguridad para usuarios y grupos específicos, que incluyen categorías y subcategorías de aplicaciones, tecnologías subyacentes y características de aplicaciones. Se pueden definir reglas de políticas para habilitar aplicaciones de forma segura en función de los usuarios y grupos de usuarios, tanto en direcciones salientes como entrantes.

Algunos ejemplos de políticas basadas en usuarios y grupos son:

- Herramientas como SSH, Telnet y FTP en puertos estándar están restringidas a TI corporativa
- Políticas como:
  - Permitir a ventas acceder a SalesForce y Microsoft 365
  - Permitir a todos los usuarios ver YouTube, pero bloquear categorías de vídeo específicas

La identificación de usuarios ayuda a dar forma a las políticas que apoyan y protegen a los empleados, invitados y otras partes interesadas. FortiGate puede proporcionar una visión profunda de los usuarios y automatizar los controles de políticas.

Identificación de dispositivos

Mientras que la identificación de usuarios ofrece políticas basadas en usuarios, y la de aplicaciones facilita políticas basadas en estas, la identificación de dispositivos proporciona reglas de políticas que se basan en un dispositivo, con independencia de los cambios en su dirección IP o ubicación. Al facilitar trazabilidad para dispositivos y asociar eventos de red con dispositivos específicos, la identificación proporciona contexto sobre cómo se relacionan los eventos con los dispositivos. Escribe políticas asociadas a dispositivos en lugar de con usuarios, ubicaciones o direcciones IP, que pueden cambiar con el tiempo. La identificación de dispositivos es importante para las políticas de seguridad, descifrado, calidad de servicio (QoS) y autenticación.

Con FortiGate, las políticas avanzadas de dispositivos y la priorización se pueden clasificar por:

- Clase, como dispositivos en red seguros
- Dispositivos críticos, como servidores y aparatos médicos
- Dispositivos relacionados con el entorno, como lectores de tarjetas, cámaras y alarmas contra incendios
- Dispositivos de Internet de las Cosas (IoT), como relojes y otros dispositivos “inteligentes” conectados

Descifrado SSL/TLS 1.3

Dado que el malware se oculta a menudo en tráfico cifrado, es fundamental examinarlo. Los NGFW de FortiGate ofrecen descifrado SSL/TLS 1.3 sin ralentizaciones de la red. Además, los FortiGate pueden descifrar tipos específicos de tráfico y realizar exclusiones basadas en sitios o categorías. Con las unidades de procesamiento de seguridad propias de alto rendimiento de Fortinet, no hay necesidad de elegir entre seguridad y rendimiento.

Gestión centralizada y unificada

La gestión centralizada y unificada es la capacidad más crítica de un HMF. Si dominios separados, como sitios corporativos, nubes públicas y privadas, y trabajadores remotos, requieren protección a través de paneles independientes, la complejidad de TI aumenta mientras que la visibilidad se reduce en gran medida.

La gestión centralizada coordina y unifica dominios de seguridad dispares en una única solución de seguridad de TI empresarial: una protección sencilla, unificada y automatizada que se extiende desde las sedes corporativas hasta la nube y los trabajadores remotos. Y dado que las distintas organizaciones tienen requisitos diferentes para gestionar sus firewalls de red dispersos, deben admitirse todos los factores de forma de la gestión centralizada, incluidos dispositivos, máquinas virtuales, SaaS y servicios de firewall gestionados.

La gestión centralizada también aporta un enorme valor al reunir a los equipos del centro de operaciones de red (NOC) y del centro de operaciones de seguridad (SOC) mediante un panel único para gestionar, supervisar y proteger toda la superficie de ataque.

Servicios de seguridad impulsada por la IA de FortiGuard

Con más de 8 millones de sensores implementados en todo el mundo, los NGFW FortiGate son capaces de aprovechar la última inteligencia global sobre amenazas a través de los servicios de seguridad impulsados de la IA de FortiGuard. Con actualizaciones de seguridad completas y en tiempo real, FortiGate puede proteger toda la red con defensas de seguridad multicapa, como filtrado de URL y DNS, antimalware y sandboxing en línea, así como IPS acelerado por hardware para parches virtuales de alto rendimiento. Estos servicios de ciberseguridad protegen a la empresa tanto de ataques conocidos como de los desconocidos hasta ahora. Las pruebas independientes de CyberRatings.org[3] muestran una eficacia del 99,88 % de los NGFW FortiGate frente a vulnerabilidades y maniobras evasivas malintencionadas.

Conclusión

La identificación de aplicaciones, usuarios y dispositivos en la red es una capacidad importante en la gestión y protección de redes empresariales. Los NGFW FortiGate son conocidos por su control y visibilidad avanzados sobre el tráfico de red, así como por su rendimiento sin precedentes. FortiGate define y automatiza las políticas que garantizan un uso adecuado, detienen las amenazas y reducen la superficie de ataque de la empresa. La gestión centralizada y unificada integra el dispositivo FortiGate con otros factores de forma de seguridad, como firewalls virtuales, firewalls nativos de la nube y firewall como servicio, para crear una solución HMF sin fisuras en todo el entorno de TI. Los últimos servicios de seguridad impulsados por la IA de FortiGuard garantizan defensas actualizadas incluso contra los ataques más recientes y avanzados.

[1] "HTTPS encryption on the web," Google Transparency Report, Google, acceso del 15 de mayo de 2023.

[2] Maria Korolov, "Network Encryption: A Double-edged Sword for Cybersecurity," Datacenter Knowledge, 8 de marzo de 2023.

[3] "Fortinet FortiGate 600F," Enterprise Firewall, CyberRatings.org, T2 de 2023.

junio 26, 2023 1:25 p. m.
1711466-A-0-ES