



FICHA TÉCNICA

FireEye Network Security

Protección efectiva contra infracciones de datos para organizaciones medianas a grandes

Descripción general

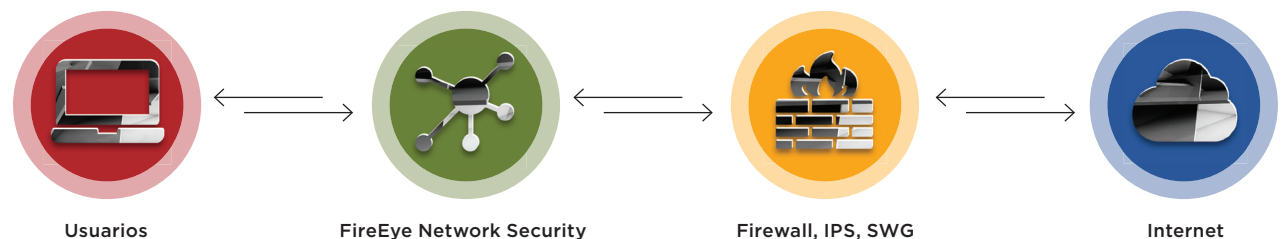
FireEye Network Security es una solución efectiva de protección contra las amenazas cibernéticas que ayuda a las organizaciones a minimizar el riesgo de costosas brechas de seguridad al detectar con precisión y detener de inmediato ataques avanzados, individualizados y otros ataques evasivos ocultos en el tráfico de Internet. Facilita la resolución eficiente de incidentes de seguridad detectados en minutos con evidencia concreta, inteligencia accionable e integración del flujo de trabajo de respuesta. Con FireEye Network Security, las organizaciones están protegidas efectivamente contra las amenazas de hoy en día, ya sea que estas aprovechen las vulnerabilidades de sistemas operativos de Microsoft Windows, Apple OS X o de aplicaciones, que estén destinadas a sedes centrales o sucursales o que estén escondidas en un gran volumen de tráfico de Internet entrante que tiene que inspeccionarse en tiempo real.

La parte central de FireEye Network Security son las tecnologías Multi-Vector Virtual Execution™ (MVX) e Intelligence-Driven Analysis (IDA). MVX es un motor de análisis dinámico y sin firma que inspecciona el tráfico de

red sospechoso para identificar ataques que evaden las defensas tradicionales basadas en políticas y en firmas. IDA es una recopilación de motores de reglas dinámicos y contextuales que detecta y bloquea la actividad maliciosa en tiempo real y retroactivamente, según la inteligencia más reciente de la máquina, del atacante y de la víctima. FireEye Network Security también incluye la tecnología del sistema de detección de intrusiones (*Intrusion Prevention System, IPS*) para detectar ataques comunes que usan la correspondencia convencional de firmas.

FireEye Network Security está disponible en una variedad de opciones de factor de forma, implementación y rendimiento. Se coloca típicamente en el camino del tráfico de Internet detrás de dispositivos de seguridad de red tradicionales como firewalls, IPS y puertas de enlace web seguras (*secure web gateways, SWG*) de última generación. FireEye Network Security complementa estas soluciones detectando rápidamente ataques conocidos y desconocidos con una alta precisión y un bajo índice de falsos positivos a la vez que ofrecer una respuesta eficiente a cada alerta.

Figura 1. Configuración típica de las soluciones de seguridad de la red.



Capacidades	Ventajas
Detección	
Detección precisa de ataques cibernéticos avanzados, individualizados y otros ataques evasivos	Minimiza el riesgo de costosas cibervulneraciones
Arquitectura de seguridad modular y extensible	Ofrece protección de las inversiones
Nivel de protección constante para entornos de varios sistemas operativos y todos los puntos de acceso de Internet	Crea una fuerte defensa en toda la organización para todos los tipos de dispositivos
Opciones de implementación en la nube, en el sitio, virtual, física, distribuida e integrada.	Ofrece la flexibilidad de ajustarse a las preferencias y los recursos de las organizaciones
Correlación multivectorial con la seguridad del correo electrónico y del contenido	Ofrece visibilidad en una superficie de ataque más amplia
Prevención	
Bloqueo inmediato de ataques a velocidades lineales de 10 Mbit/s a 8 Gbit/s	Ofrece protección en tiempo real contra ataques evasivos
Respuesta	
Bajo índice de alertas falsas, categorización de software de riesgo y validación de alertas de IPS automatizadas	Reduce el costo operativo de priorizar alertas no confiables
Pase a la investigación y validación de alertas, contención del endpoint y respuesta ante incidentes	Automatiza y simplifica los flujos de trabajo de seguridad
Evidencia de ejecución e inteligencia de amenazas accionable con perspectiva contextual	Acelera la priorización y resolución de incidentes de seguridad detectados
Escalabilidad de un sitio a miles de sitios	Es compatible con el crecimiento de la empresa

Ventajas técnicas

Detección precisa de amenazas

FireEye Network Security usa varias técnicas de análisis para detectar ataques con alta precisión y un bajo índice de alertas falsas:

- El motor **Multi-Vector Virtual Execution™ (MVX)** detecta ataques desconocidos, de flujo múltiple y otros ataques evasivos al usar un análisis dinámico y sin firma en un entorno seguro y virtual. Detiene las fases de infección y compromiso de la cadena letal de ataque cibernético al identificar exploits y malware no vistos anteriormente.
- Los **motores Intelligence-Driven Analysis (IDA)** detectan y bloquean ataques confusos, individualizados y otros ataques personalizados con un análisis basado en reglas y contextual a partir de información en tiempo real recopilada en la primera línea de millones de veredictos MVX, miles de horas de experiencia de respuesta a incidentes recopiladas por Mandiant, una empresa de FireEye, y miles de investigadores de amenazas iSight. Detiene las fases de infección, compromiso e intrusión de la cadena letal de ataque cibernético identificando exploits maliciosos, malware y devoluciones de llamada de Comando y Control (CnC). También extrae y envía el tráfico de red sospechoso al motor MVX para realizar un análisis de veredicto definitivo.
- **Structured Threat Intelligence eXpression (STIX)** permite la ingestión de inteligencia de amenazas de terceros usando un formato estándar de la industria para agregar indicadores de amenaza personalizados a los motores IDA.

Protección inmediata y resiliente

FireEye Network Security ofrece modos de configuración flexibles que incluyen:

- Supervisión fuera de banda a través de TAP/SPAN, supervisión en línea o bloqueo activo en línea. El modo de bloqueo en línea neutraliza automáticamente exploits y malware entrantes, y devoluciones de llamadas multiprotocolo salientes. En el modo de supervisión en línea se generan alertas, y las organizaciones deciden cómo responder a ellas. En modo de prevención

fuera de banda, FireEye Network Security genera restablecimientos TCP para el bloqueo fuera de banda de conexiones TCP, UDP o HTTP.

- Algunos modelos ofrecen una opción de alta disponibilidad (*High Availability*, HA) activa para proporcionar resiliencia en caso de fallas en la red o el dispositivo.

Amplia cobertura de la superficie de ataque

FireEye Network Security ofrece un nivel constante de protección para los diversos entornos de red actuales:

- Compatibilidad con los sistemas operativos más comunes de Microsoft Windows y Apple Mac OS X.
- Análisis de más de 140 tipos de archivo diferentes, incluidos los archivos portables ejecutables (*portable executables*, PE), contenido web, archivos, imágenes, aplicaciones de Java, Microsoft y Adobe, y multimedia.
- Ejecución de tráfico de red sospechoso en comparación con miles de combinaciones de versión de aplicación y tipo de aplicación, paquete de servicios y sistema operativo.
- Protección mediante firmas contra ataques avanzados y tipos de malware que son difíciles de detectar: cargas de web shell, ejecución de web shell, ransomware, criptominerías.

Alertas validadas y priorizadas

Además de detectar ataques verdaderos, la tecnología FireEye MVX también se usa para determinar la veracidad de las alertas detectadas por los métodos de correspondencia convencional de firmas, y para identificar y priorizar las amenazas críticas:

- La validación del Sistema de detección de intrusiones (IPS) con el motor MVX reduce el tiempo necesario para priorizar la detección basada en firmas que tradicionalmente es propensa a crear alertas falsas.
- La categorización de software de riesgo separa los intentos de ataque genuinos de la actividad indeseable pero menos maliciosa (como adware y spyware) para priorizar la respuesta a las alertas.

Información de amenazas accionable

Las alertas que genera FireEye Network Security incluyen evidencia concreta e inteligencia contextual para responder rápidamente a fin de priorizar y contener una amenaza:

- **Dynamic Threat Intelligence (DTI):** datos concretos, compartidos globalmente y en tiempo real para detener rápida y proactivamente los ataques individualizados y recién descubiertos.
- **Advanced Threat Intelligence (ATI):** información contextual sobre el ataque para acelerar la respuesta y orientación normativa para contener la amenaza.

Integración del flujo de trabajo de respuesta

FireEye Network Security puede incrementarse de varias maneras para automatizar los flujos de trabajo de respuesta a alertas:

- FireEye Central Management correlaciona las alertas de FireEye Network Security y FireEye Email Security para obtener una visión más amplia de un ataque y establecer reglas de bloqueo a fin de evitar que se propague el ataque.
- FireEye Network Forensics se integra con FireEye Network Security para proporcionar capturas de paquetes detalladas asociadas con una alerta y permitir investigaciones en profundidad.
- FireEye Endpoint Security identifica, valida y contiene los compromisos detectados por FireEye Network Security para simplificar la contención y corrección de los endpoints afectados.

Opciones de implementación flexibles

FireEye Network Security ofrece distintas opciones de implementación para que se ajusten a las necesidades y el presupuesto de una organización:

- **Seguridad de red integrada:** dispositivo de hardware independiente todo en uno con servicio MVX integrado para proteger un punto de acceso a Internet en un solo sitio. FireEye Network Security es una plataforma fácil de gestionar y sin cliente que se implementa en menos de 60 minutos. No requiere reglas, políticas o configuración.

- **Seguridad de red distribuida:** dispositivos extensibles con servicio MVX compartido centralmente a fin de proteger los puntos de acceso a Internet dentro de las organizaciones.
 - **Nodo inteligente de red:** dispositivos físicos o virtuales que analizan el tráfico de Internet para detectar y bloquear el tráfico malicioso y enviar la actividad sospechosa por medio de una conexión cifrada al servicio MVX para realizarle un análisis de veredicto definitivo.
 - **Cuadro inteligente de MVX:** servicio MVX elástico, ubicado centralmente y en el sitio que ofrece escalabilidad transparente, tolerancia a errores N+1 incorporada y equilibrio de carga automatizado.
 - **FireEye Cloud MVX:** Suscripción al servicio MVX alojado por FireEye que garantiza la privacidad analizando el tráfico en el Nodo inteligente de red. Solamente los objetos sospechosos se envían por medio de una conexión cifrada al servicio MVX, donde los objetos benignos se descartan.
 - **Protección en el sitio o en la nube:** Además de dispositivos independientes y virtuales, FireEye ofrece Seguridad de red en la nube pública con disponibilidad de imágenes de máquina de Amazon (*Amazon Machine Images, AMI*).



Figura 2. Algunos ejemplos de seguridad de red integrada incluyen NX 2550, NX 3500, NX 5500, NX 10550.

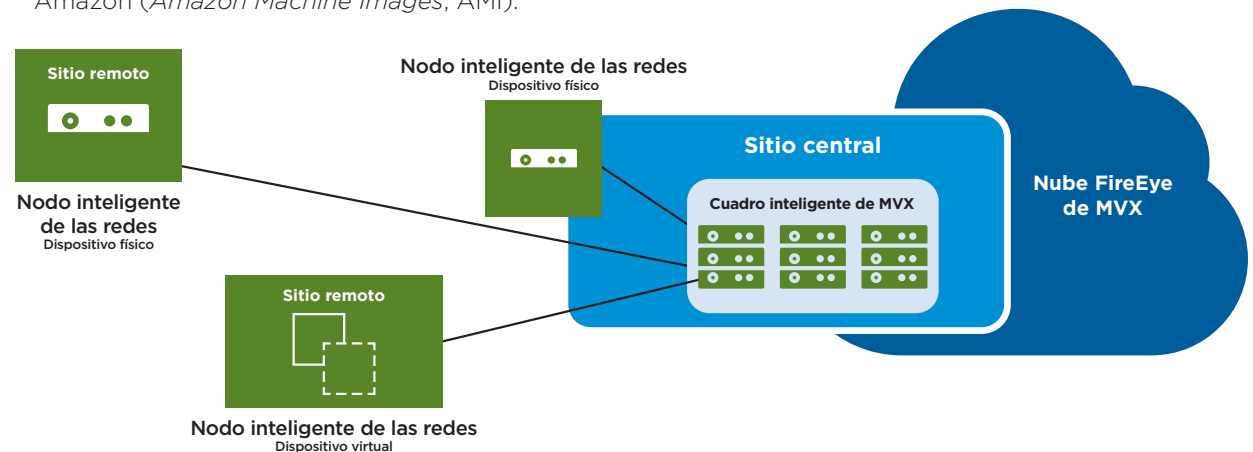


Figura 3. Modelos de implementación distribuida para seguridad de red.

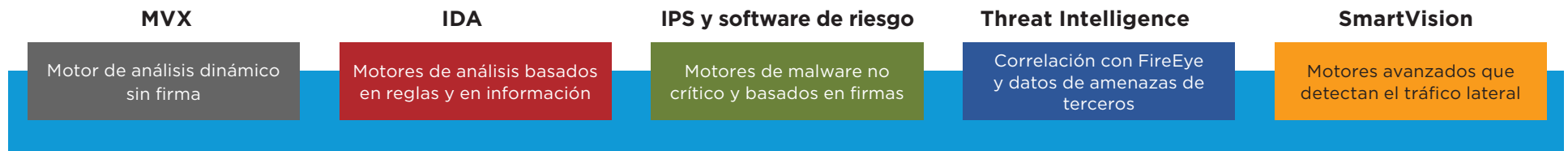


Figura 4. Componentes modulares de FireEye Network Security.

Alto rendimiento y escalabilidad

FireEye Network Security protege los puntos de acceso a Internet a velocidad lineal con opciones de rendimiento para una amplia variedad de tamaños de sede central y sucursal:

La arquitectura escalable de Cuadro inteligente de MVX y FireEye Cloud MVX le permite al servicio MVX admitir un nodo inteligente de red para miles y escalar sin interrupciones según sea necesario.

Factor de forma	Rendimiento
Seguridad de red integrada	50 Mbit/s a 5 Gbit/s
Nodo inteligente de red física	50 Mbit/s a 10 Gbit/s
Nodo inteligente de red para nube virtual y pública	50 Mbit/s a 1 Gbit/s

Ventajas comerciales

FireEye Network Security, diseñado para satisfacer las necesidades de organizaciones distribuidas en múltiples sitios y de sitio único, ofrece varias ventajas:

Minimiza el riesgo de cibervulneraciones

FireEye Network Security es una solución de defensa cibernética muy efectiva que:

- Evita que los intrusos ingresen en una organización para robar valiosos recursos o interrumpir las operaciones comerciales al detener ataques avanzados, individualizados y otros ataques evasivos.

- Detiene los ataques y contiene intrusiones más rápidamente con evidencia concreta, inteligencia accionable, bloqueo en línea y automatización del flujo de trabajo de respuesta.
- Elimina los puntos débiles de las defensas cibernéticas de una organización con protección constante de distintos sistemas operativos, tipos de aplicación, sucursales y sitios centrales.

Breve período de recuperación del capital invertido

Según un estudio reciente de Forrester Consulting¹, los clientes de FireEye Network Security pueden esperar un 152 % en ahorros de retorno de la inversión durante un plazo de tres años y la recuperación de su inversión inicial en tan solo 9,7 meses. FireEye Network Security:

- Centra los recursos del equipo de seguridad en ataques reales para reducir los gastos operativos.
- Optimiza el gasto de capital con un servicio MVX compartido y una gran variedad de puntos de rendimiento para reestructurar la implementación a fin de cumplir requisitos.
- Garantiza el futuro de la inversión en seguridad al escalar sin interrupciones cuando la cantidad de sucursales o el volumen de tráfico de Internet aumentan.
- Protege las inversiones existentes permitiendo la migración sin costos de una implementación integrada a una distribuida.
- Reduce el desembolso de capital futuro con una arquitectura modular y extensible.

Premios y certificaciones

La cartera de productos de FireEye Network Security ha recibido varios premios y certificaciones de la industria y del gobierno:

- En 2018, Frost & Sullivan reconoció a FireEye como el líder indiscutido del mercado con un 46 % de participación en el mercado, más que los posteriores diez competidores combinados².
- FireEye Network Security ha recibido muchos premios de SANS Institute, SC Magazine, CRN y otros.
- FireEye Network Security fue la primera solución de seguridad del mercado en recibir la Certificación de la Ley de SEGURIDAD (SAFETY Act Certification) del Departamento de Seguridad Nacional de los Estados Unidos.



¹ Forrester (mayo de 2016). El impacto económico total de FireEye.

² Frost & Sullivan (2018) Advanced Malware Sandbox (AMS) Solutions Market, Global, Forecast to 2022.

Tabla 1. Especificaciones de FireEye Network Security, dispositivo integrado.

	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Asistencia OS	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows
Rendimiento*	Hasta 50 Mbit/s o 100 Mbit/s	Hasta 250 Mbit/s	Hasta 500 Mbit/s	Hasta 1 Gbit/s	Hasta 2,5 Gbit/s	Hasta 5 Gbit/s
Puertos de supervisión de red	4 derivaciones de 1 GigE	4 SFP+ de 10 GigE 4 derivaciones de 1 GigE	4 SFP+ de 10 GigE 4 derivaciones de 1 GigE	8 SFP+ de 10 GigE 4 derivaciones de 1 GigE	8 SFP+ de 10 GigE 4 derivaciones de 1 GigE	8 SFP+ de 10 GigE 2 QSFP+ de 40 GigE
Modo de funcionamiento de los puertos de red	Supervisión en línea, Fail Open, Fail Close (derivación de HW) o TAP/SPAN	Supervisión en línea, Fail Open, Fail Close (derivación de HW) o TAP/SPAN	Supervisión en línea, Fail Open, Fail Close (derivación de HW) o TAP/SPAN	Supervisión en línea, Fail Open, Fail Close (derivación de HW) o TAP/SPAN	Supervisión en línea, Fail Open, Fail Close (derivación de HW) o TAP/SPAN	Supervisión en línea, TAP/SPAN
Alta disponibilidad (HA)	No disponible	No disponible	No disponible	Disponible	Disponible	Disponible
Puertos de administración (panel posterior)	2 puertos BASE-T 10/100/1000	2 puertos de 1 GigE	2 puertos de 1 GigE	2 puertos de 1 GigE	2 puertos de 1 GigE	2 puertos de 1 GigE
Puerto IPMI	Panel frontal	Panel posterior	Panel posterior	Panel posterior	Panel posterior	Panel posterior
Monitor LCD delantero y teclado	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible
Puerto VGA	No	Sí	Sí	Sí	Sí	Sí
Puertos USB	2 puertos USB tipo A (panel frontal)	4 puertos USB tipo A (todos los paneles posteriores)	4 puertos USB tipo A 2 frontales, 2 posteriores	4 puertos USB tipo A 2 frontales, 2 posteriores	4 puertos USB tipo A 2 frontales, 2 posteriores	2 puertos USB tipo A
Puerto serie (panel trasero)	115 200 bits/s, sin paridad, 8 bits, 1 bit de parada (conector RJ45, incluye cable adaptador de RJ45 a Dsub)	115 200 bits/s, sin paridad, 8 bits, 1 bit de parada	115 200 bits/s, sin paridad, 8 bits, 1 bit de parada	115 200 bits/s, sin paridad, 8 bits, 1 bit de parada	115 200 bits/s, sin paridad, 8 bits, 1 bit de parada	115 200 bits/s, sin paridad, 8 bits, 1 bit de parada
Capacidad del disco	Unidad SATA HDD de 1 TB, 3,5 pulgadas, interna, fija y única	2 unidades HDD de 4 TB, 3,5 pulgadas, SAS3, 7,2k rpm, FRU RAID1	2 unidades HDD de 4 TB, 3,5 pulgadas, SAS3, 7,2k rpm, FRU RAID1	2 unidades HDD de 4 TB, 3,5 pulgadas, SAS3, 7,2k rpm, FRU RAID1	2 unidades HDD de 4 TB, 3,5 pulgadas, SAS3, 7,2k rpm, FRU RAID1	2 unidades HDD de 10 TB 3,5 pulgadas, SAS3, 7,2k rpm, FRU RAID1
Empaque	Montaje en bastidor 1RU, para un rack de 19 pulgadas	Montaje en bastidor 1RU, para un rack de 19 pulgadas	Montaje en bastidor 2RU, para un rack de 19 pulgadas	Montaje en bastidor 2RU, para un rack de 19 pulgadas	Montaje en bastidor 2RU, para un rack de 19 pulgadas	Montaje en bastidor 2RU, para un rack de 19 pulgadas
Dimensiones del bastidor ancho x fondo x alto	437 mm (17,2 in) x 500 mm (19,7 in) x 43,2 mm (1,7 in)	437 mm (17,2 in) x 650 mm (25,6 in) x 43,2 mm (1,7 in)	438 mm (17,24 in) x 620 mm (24,41 in) x 88,4 mm (3,48 in)	438 mm (17,24 in) x 620 mm (24,41 in) x 88,4 mm (3,48 in)	438 mm (17,24 in) x 620 mm (24,41 in) x 88,4 mm (3,48 in)	437 mm (17,2 in) x 787 mm (31,0 in) x 89 mm (3,5 in)
Alimentación eléctrica (CA)	Única de 250 W, 90 a 264 VCA, 3,5 a 1,5 A, conector IEC60320-C14 de 50 a 60 Hz, interno, fijo	Redundante (1+1) 750 W, 100 a 240 VCA, 8,0 a 4,5 A, conector IEC60320-C14 de 50 a 60 Hz, FRU	Redundante (1+1) 800 W, 100 a 240 VCA 10,5 a 4,0 A, conector IEC60320-C14 de 50 a 60 Hz, FRU	Redundante (1+1) 800 W, 100 a 240 VCA 10,5 a 4,0 A, conector IEC60320-C14 de 50 a 60 Hz, FRU	Redundante (1+1) 800 W, 100 a 240 VCA 10,5 a 4,0 A, conector IEC60320-C14 de 50 a 60 Hz, FRU	Redundante (1+1) de 1000 vatios, 100 a 240 VCA 10,5 a 4,0 A, conector IEC60320-C14 de 50 a 60 Hz, FRU

Tabla 2. Rendimiento de IPS de seguridad de red FireEye, dispositivo integrado.

	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Rendimiento máx. de IPS	Hasta 50 Mbit/s o 100 Mbit/s	Hasta 250 Mbit/s	Hasta 500 Mbit/s	Hasta 1 Gbit/s	Hasta 2,5 Gbit/s	Hasta 5 Gbit/s
Conexiones simultáneas máx.	15 000 u 80 000	80 000	160 000	500 000	1 millón	2 millones
Nuevas conexiones por segundo	750/segundo o 4000/segundo	4000/segundo	8000/segundo	10 000/segundo	20 000/segundo	40 000/segundo

Tabla 3. Nodo inteligente de FireEye Network Security, especificaciones físicas.

	NX 1500	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Asistencia OS	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows
Rendimiento	Hasta 50 Mbit/s	Hasta 100 Mbit/s o 250 Mbit/s	Hasta 500 Mbit/s	Hasta 1 Gbit/s	Hasta 2 Gbit/s	Hasta 5 Gbit/s	Hasta 10 Gbit/s
Puertos de supervisión de red	4 puertos BASE-T 10/100/1000	4 derivaciones de 1 GigE	4 SFP+ de 10 GigE 4 derivaciones de 1 GigE	4 SFP+ de 10 GigE 4 derivaciones de 1 GigE	8 SFP+ de 10 GigE 4 derivaciones de 1 GigE	8 SFP+ de 10 GigE 4 derivaciones de 1 GigE	8 SFP+ de 10 GigE 2 QSFP+ de 40 GigE
Modo de funcionamiento de los puertos de red	Supervisión en línea, Fail Close o Tap	Supervisión en línea, Fail Open, Fail Close (derivación de HW) o TAP/SPAN	Supervisión en línea, Fail Open, Fail Close (derivación de HW) o TAP/SPAN	Supervisión en línea, Fail Open, Fail Close (derivación de HW) o TAP/SPAN	Supervisión en línea, Fail Open, Fail Close (derivación de HW) o TAP/SPAN	Supervisión en línea, Fail Open, Fail Close (derivación de HW) o TAP/SPAN	Supervisión en línea, TAP/SPAN
Alta disponibilidad (HA)	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible
Puertos de administración (panel posterior)	2 puertos BASE-T 10/100/1000	2 puertos de 1 GigE	2 puertos de 1 GigE	2 puertos de 1 GigE	2 puertos de 1 GigE	2 puertos de 1 GigE	2 puertos de 1 GigE
Puerto IPMI	No disponible	Panel frontal	Panel posterior	Panel posterior	Panel posterior	Panel posterior	Panel posterior
Monitor LCD delantero y teclado	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible
Puerto VGA	No disponible	No disponible	Sí	Sí	Sí	Sí	Sí
Puertos USB	2 puertos USB tipo A	2 puertos USB tipo A (panel frontal)	4 puertos USB tipo A (todos los paneles posteriores)	4 puertos USB tipo A 2 frontales, 2 posteriores	4 puertos USB tipo A 2 frontales, 2 posteriores	4 puertos USB tipo A 2 frontales, 2 posteriores	2 puertos USB tipo A

Tabla 3. Nodo inteligente de FireEye Network Security, especificaciones físicas. (continuación)

	NX 1500	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500	
Cumplimiento de normativas de la compatibilidad electromagnética	FCC Parte 15 ICES-003 Clase A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 y V-3/2015	FCC Parte 15 ICES-003 Clase A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 y V-3/2015	FCC Parte 15 ICES-003 Clase A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 y V-3/2015	FCC Parte 15 ICES-003 Clase A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 y V-3/2015	FCC Parte 15 ICES-003 Clase A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 y V-3/2015	FCC Parte 15 ICES-003 Clase A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 y V-3/2015	FCC Parte 15 ICES-003 Clase A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 y V-3/2015	Seguridad: EN 60950; C22.2; UL 60950; IEC 60950; CAN/CSA-C22.2; K 60950; AS/NZS 60950; GB 4943.1; J60950, SI60950 CEM: FCC Parte 15 Subparte B Clase A; ICES-003; EN55032; VCCI V-3; EN 55024; EN 61000; CNS 13438; CISPR32; KN 32; KN 35
Cumplimiento ambiental	Directiva RoHS 2011/65/UE REACH Directiva WEEE 2012/19/UE	Directiva RoHS 2011/65/UE REACH Directiva WEEE 2012/19/UE	Directiva RoHS 2011/65/UE REACH Directiva WEEE 2012/19/UE	Directiva RoHS 2011/65/UE REACH Directiva WEEE 2012/19/UE	Directiva RoHS 2011/65/UE REACH Directiva WEEE 2012/19/UE	Directiva RoHS 2011/65/UE REACH Directiva WEEE 2012/19/UE	Directiva RoHS 2011/65/UE REACH Directiva WEEE 2012/19/UE	RoHS; REACH; WEEE Minerales en conflicto
Temperatura de funcionamiento	0 a 40 °C 32 a 104 °F	0 a 40 °C 32 a 104 °F	0 a 40 °C 32 a 104 °F	0 a 40 °C 32 a 104 °F	0 a 40 °C 32 a 104 °F	0 a 40 °C 32 a 104 °F	0 a 40 °C 32 a 104 °F	
Temperatura sin funcionar	-20 a 80 °C -4 a 176 °F	-20 a 80 °C -4 a 176 °F	-30 a 70 °C (-22 a 158 °F)	-40 a 70 °C -40 a 158 °F	-40 a 70 °C -40 a 158 °F	-40 a 70 °C -40 a 158 °F	-30 a 70 °C -22 a 158 °F	
Humedad relativa de funcionamiento	10 a 95 % a 40 °C sin condensación	5 a 85 % a 40 °C sin condensación	10 a 95 % a 40 °C, sin condensación	10 a 95 % a 40 °C, sin condensación	10 a 95 % a 40 °C, sin condensación	10 a 95 % a 40 °C, sin condensación	10 % a 90 % a 40 °C sin condensación	
Humedad relativa sin funcionar	10 a 95 % a 60 °C sin condensación	5 a 95 % a 40 °C sin condensación	10 a 95 % a 60 °C, sin condensación	10 a 95 % a 60 °C, sin condensación	10 a 95 % a 60 °C sin condensación	10 a 95 % a 60 °C sin condensación	10 % a 95 % a 55 °C sin condensación	
Altitud de funcionamiento	3000 m 9842 pies	3000 m 9842 pies	3000 m 9842 pies	3000 m 9842 pies	3000 m 9842 pies	3000 m 9842 pies	3000 m 9842 pies	

Tabla 4. IPS del nodo inteligente de FireEye Network Security, especificaciones físicas.

	NX 1500	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Rendimiento máx. de IPS	Hasta 50 Mbit/s	Hasta 100/250 Mbit/s	Hasta 500 Mbit/s	Hasta 1 Gbit/s	Hasta 2 Gbit/s	Hasta 5 Gbit/s	Hasta 10 Gbit/s
Conexiones simultáneas máx.	15 000	80 000	160 000	500 000	1 millón	2 millones	4 millones
Nuevas conexiones por segundo	750/segundo	4000/segundo	8000/segundo	10 000/segundo	20 000/segundo	40 000/segundo	80 000/segundo

Tabla 5. Nodo inteligente de FireEye Network Security, especificaciones virtuales.

	VA-NXS 1500	VA-NXS 2500	VA-NXS 2550	VA-NXS 4500	VA-NXS 6500
Asistencia OS	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows
Rendimiento*	Hasta 50 Mbit/s	Hasta 100 Mbit/s	Hasta 250 Mbit/s	Hasta 500 Mbit/s	Hasta 1 Gbit/s
Puertos de supervisión de red	De 1 a 8	De 1 a 8	De 1 a 8	De 1 a 8	De 1 a 8
Puertos de administración de red	1 o 2	1 o 2	1 o 2	1 o 2	1 o 2
Modo de funcionamiento de los puertos de red	En línea, SPAN	En línea, SPAN	En línea, SPAN	En línea, SPAN	En línea, SPAN
Núcleos del CPU	3	6	8	8	16
Memoria	10 GB	16 GB	16 GB	32 GB	32 GB
Capacidad del disco	384 GB	384 GB	384 GB	512 GB	512 GB
Adaptadores de red	VMXNet 3, vNIC	VMXNet 3, vNIC	VMXNet 3, vNIC	VMXNet 3, vNIC	VMXNet 3, vNIC
Compatibilidad con hipervisores	VMWare ESXi 6.0 o posterior y KVM 1.5.3 o posterior	VMWare ESXi 6.0 o posterior y KVM 1.5.3 o posterior	VMWare ESXi 6.0 o posterior y KVM 1.5.3 o posterior	VMWare ESXi 6.0 o posterior y KVM 1.5.3 o posterior	VMWare ESXi 6.0 o posterior y KVM 1.5.3 o posterior
Certificaciones de seguridad	FIPS 140-2 Nivel 1 CC NDPP v1.1 (En proceso)	FIPS 140-2 Nivel 1 CC NDPP v1.1 (En proceso)	FIPS 140-2 Nivel 1 CC NDPP v1.1 (En proceso)	FIPS 140-2 Nivel 1 CC NDPP v1.1 (En proceso)	FIPS 140-2 Nivel 1 CC NDPP v1.1 (En proceso)

Tabla 6. IPS del nodo inteligente de FireEye Network Security, especificaciones virtuales.

	VA-NXS 1500	VA-NXS 2500	VA-NXS 2550	VA-NXS 4500	VA-NXS 6500
Rendimiento máx. de IPS	Hasta 50 Mbit/s	Hasta 100 Mbit/s	Hasta 250 Mbit/s	Hasta 500 Mbit/s	Hasta 1 Gbit/s
Conexiones simultáneas máx.	15 000	80 000	80 000	160 000	500 000
Nuevas conexiones por segundo	750/segundo	4000/segundo	4000/segundo	8000/segundo	10 000/segundo

Tabla 7. Tamaños de AMI compatibles con FireEye Network Security en AWS.

Modelo	Rendimiento	vCPU	Memoria	Disco	Interfaces de red	Tipo de instancia de AWS
NX4500v	500 Mbit/s	8	32 GB	512 GB (EBS)	Un puerto de administración, un puerto de envío y dos puertos de supervisión (4 puertos en total)	M5.2xlarge
NX6500v	1 Gbit/s	16	64 GB	512 GB (EBS)	Un puerto de administración, un puerto de envío y seis puertos de supervisión (8 puertos en total)	M5.4xlarge

Tabla 8. Especificaciones del cuadro inteligente de FireEye MVX.

	VX 5500	VX 12550
Asistencia OS	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows
Rendimiento*	Hasta 2 Gbit/s	Hasta 14 Gbit/s
Alta disponibilidad**	N+1	N+1
Puertos de administración (panel posterior)	1 puerto BASE-T de 10/100/1000 Mbit/s	1 puerto BASE-T de 10/100/1000 Mbit/s
Puertos de clúster (panel posterior)	3 puertos BASE-T de 10/100/1000 Mbit/s	1 puerto BASE-T 10/100/1000 Mbit/s, 2 puertos BASE-T de 10 Gbit/s, 4 puertos 10 GigE SFP+
Puerto IPMI (panel trasero)	Incluidos	Incluidos
Monitor LCD delantero y teclado	No disponible	Sin monitor LCD
Puertos VGA	Incluidos	Incluidos
Puertos USB (panel trasero)	4 puertos USB tipo A	2 puertos USB tipo A
Puerto serie (panel trasero)	115 200 bits/s, sin paridad, 8 bits, 1 bit de parada	115 200 bits/s, sin paridad, 8 bits, 1 bit de parada
Capacidad del disco	2 unidades SAS3 HDD de 2 TB, 3,5 in, RAID 1, intercambiable sobre la marcha, FRU	2 unidades SAS3 HDD de 4 TB, 3,5 in, RAID 1, intercambiable sobre la marcha, FRU
Empaque	Montaje en bastidor 1RU, para un rack de 19 pulgadas	Montaje en bastidor 2RU, para un rack de 19 pulgadas
Dimensiones del bastidor ancho x fondo x alto	437 mm x 650 mm x 43,2 mm (17,2 x 25,6 x 1,7 in)	437 mm x 787 mm x 89 mm (17,2 x 31 x 3,5 in)
Alimentación eléctrica (CC)	No disponible	No disponible
Alimentación eléctrica (CA)	Redundante (1+1) 750 W, 100 a 240 VCA, 8 a 3,8 A, conector IEC60320-C14 de 50 a 60 Hz, intercambiable sobre la marcha, FRU	Redundante (1+1) 100 W, 100 a 240 VCA, 10,5 a 4,0 A, conector IEC60320-C14 de 50 a 60 Hz, FRU
Potencia máxima (vatios)	285 W	660 W
Disipación térmica máxima (BTU/h)	972 BTU/h	2594 BTU/h
Tiempo medio entre fallos (h)	54 200 h	54 041 h
Peso neto/embalado kg (lb)	12,2 kg (27,0 lb)/17,2 kg (38,0 lb)	20 kg (44 lb)/32,2 kg (71 lb)
Certificación de seguridad	FIPS 140-2 Nivel 1, CC NDPP v1.1 (Pendiente)	FIPS 140-2 Nivel 1, CC NDPP v1.1 (Pendiente)
Cumplimiento de normativas de seguridad	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2

Tabla 9. Especificaciones del cuadro inteligente de FireEye MVX.

	VX 5500	VX 12500
Cumplimiento de normativas de la compatibilidad electromagnética	FCC Parte 15 ICES-003 Clase A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 y V-3/2015	FCC Parte 15 ICES-003 Clase A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 y V-3/2015
Cumplimiento ambiental	Directiva RoHS 2011/65/UE REACH Directiva WEEE 2012/19/UE	Directiva RoHS 2011/65/UE REACH Directiva WEEE 2012/19/UE
Temperatura de funcionamiento	0 a 40 °C (32 a 104 °F)	0 a 40 °C (32 a 104 °F)
Temperatura sin funcionar	-30 a 70 °C (-22 a 158 °F)	-30 a 70 °C (-22 a 158 °F)
Humedad relativa de funcionamiento	10 a 95 % a 40 °C sin condensación	10 % a 90 % a 40 °C sin condensación
Humedad relativa sin funcionar	10 a 95 % a 60 °C sin condensación	10 % a 95 % a 55 °C sin condensación
Altitud de funcionamiento	3000 m 9842 pies	3000 m 9842 pies

Servicios de soporte

FireEye ofrece programas de soporte simples y flexibles para maximizar el valor de sus productos y servicios de FireEye. Hay disponibles cuatro niveles diferentes de servicios de soporte: Platino, Platino Prioridad Plus, Gobierno y Gobierno Prioridad Plus. Para obtener más información sobre el soporte de FireEye, consulte los servicios de Soporte de FireEye.

Para obtener más información sobre FireEye, visite: www.FireEye.com

FireEye, Inc.

601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

© 2019 FireEye, Inc. Todos los derechos reservados. FireEye es una marca comercial registrada de FireEye, Inc. Todas las demás marcas, productos o nombres de servicios son o pueden ser marcas comerciales o marcas de servicios de sus respectivos propietarios.
NS-EXT-DS-US-EN-000048-10

Acerca de FireEye, Inc.

FireEye es una empresa de seguridad basada en información. FireEye, que funciona como una extensión escalable y transparente de las operaciones de seguridad del cliente, ofrece una sola plataforma que combina tecnologías innovadoras de seguridad, inteligencia sobre amenazas similar a la de una nación y los servicios de consultoría de fama mundial de Mandiant®. Gracias a este enfoque, FireEye elimina la complejidad y la carga de la seguridad cibernética para las organizaciones que desean estar preparadas y responder ante los ataques cibernéticos, además de prevenirlos.

