



## FICHA TÉCNICA

# FireEye Network Security

## Proteção eficaz contra violações cibernéticas para organizações de pequeno e médio porte

### Visão geral

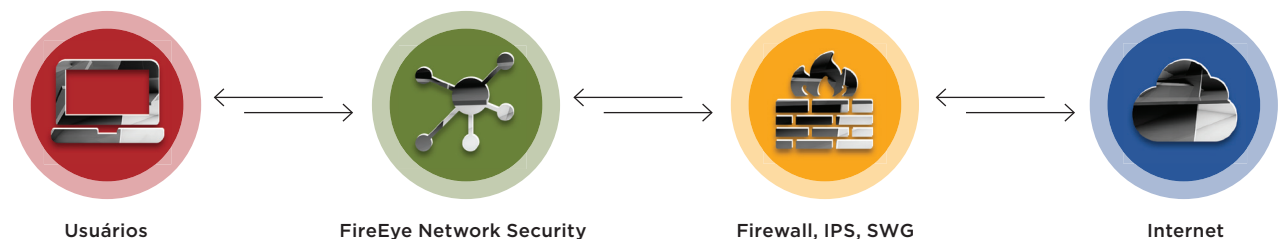
O FireEye Network Security é uma solução eficaz de proteção contra ameaças cibernéticas que ajuda as organizações a minimizar os riscos de violações onerosas, detectando com precisão e interrompendo imediatamente ataques avançados, direcionados e outros ataques evasivos escondidos no tráfego de internet. Ele possibilita resolver de maneira eficiente e em questão de minutos os incidentes de segurança detectados, com evidências concretas, inteligência decisiva e integração de fluxos de trabalho de resposta. Com o FireEye Network Security, as organizações são efetivamente protegidas contra as ameaças atuais, as quais exploram vulnerabilidades em aplicativos ou em sistemas operacionais Microsoft Windows ou Apple OS X, são direcionadas contra sedes corporativas ou filiais, ou se ocultam em um grande volume de tráfego de entrada de internet que precisa ser inspecionado em tempo real.

No núcleo do FireEye Network Security estão as tecnologias Multi-Vector Virtual Execution™ (MVX) e Intelligence-Driven Analysis (IDA). MVX é um mecanismo de análise dinâmica e sem assinaturas que inspeciona tráfego de rede suspeito para identificar

ataques que contornam defesas tradicionais com base em assinaturas e políticas. IDA é uma coletânea de mecanismos de regras dinâmicas contextuais, que detecta e bloqueia atividades nocivas, tanto em tempo real quanto retroativamente, com base na inteligência mais recente obtida de máquinas, atacantes e vítimas. O FireEye Network Security também inclui a tradicional tecnologia de sistema de prevenção de intrusões (*intrusion prevention system*, IPS) para detectar ataques comuns utilizando correspondência de assinatura convencional.

O FireEye Network Security está disponível em uma variedade de opções de formato físico, distribuição e desempenho. Ele costuma ser posicionado no caminho do tráfego de internet, atrás de appliances tradicionais de segurança de rede, como firewalls de última geração, IPS e gateways seguros da web (*secure web gateways*, SWG). O FireEye Network Security complementa essas soluções ao detectar rapidamente ataques conhecidos e desconhecidos com alta precisão e baixa taxa de falsos positivos, ao mesmo tempo que viabiliza uma resposta eficiente para cada alerta.

**Figura 1.** Configuração típica — Soluções de segurança de rede.



Capacidades	Vantagens
<b>Detecção</b>	
Detecção precisa de ataques avançados, direcionados e outros ataques cibernéticos evasivos	Minimiza o risco de violações cibernéticas onerosas
Arquitetura de segurança modular e expansível	Oferece proteção do investimento
Nível de proteção consistente para ambientes com múltiplos sistemas operacionais e todos os pontos de acesso à internet	Cria uma defesa forte por toda a organização, para todos os tipos de dispositivos
Opções de implantação integrada, múltipla, física, virtual, no local e na nuvem	Oferece flexibilidade, conforme as preferências e recursos da organização
Correlação multivetorial com a segurança de e-mail e de conteúdo	Proporciona visibilidade por uma superfície de ataque mais ampla
<b>Prevenção</b>	
Bloqueio imediato de ataques a velocidades de 10 Mbps a 8 Gbps	Oferece proteção em tempo real contra ataques evasivos
<b>Resposta</b>	
Baixa taxa de alertas falsos, categorização de riskware e validação automática de alertas de IPS	Reduz o custo operacional da triagem de alertas não confiáveis
Mudança para investigação e validação de alertas, contenção de endpoints e resposta a incidentes	Automatiza e simplifica os fluxos de trabalho de segurança
Evidência de execução e inteligência decisiva sobre ameaças com insights contextuais	Acelera a priorização e a resolução dos incidentes de segurança detectados
Expansibilidade de um local para milhares de locais	Acomoda o crescimento dos negócios

## Vantagens técnicas

### Detecção precisa de ameaças

O FireEye Network Security utiliza múltiplas técnicas de análise para detectar ataques com alta precisão e uma baixa taxa de alertas falsos:

- O mecanismo **Multi-Vector Virtual Execution™ (MVX)** detecta ataques de dia-zero, de fluxos múltiplos e outros ataques evasivos com análise dinâmica e sem assinaturas em um ambiente virtual seguro. Ele interrompe as fases de infecção e comprometimento da cadeia de destruição do ataque cibernético, identificando malware e exploits nunca antes vistos.
- Os mecanismos **Intelligence-Driven Analysis (IDA)** detectam e bloqueiam ataques escondidos, direcionados e outros ataques personalizados com análise contextual baseada em regras a partir de insights em tempo real obtidos nas linhas de frente de milhões de veredictos do MVX, milhares de horas de experiência em resposta a incidentes acumuladas pela Mandiant, uma empresa FireEye, e centenas de pesquisadores de ameaças do iSight. Ele bloqueia as fases de infecção, comprometimento e intrusão da cadeia de destruição do ataque cibernético identificando exploits maliciosos, malware e callbacks de comando e controle (CnC). Ele também extrai e envia o tráfego de rede suspeito ao mecanismo MVX para uma análise de veredicto definitiva.
- O **Structured Threat Intelligence eXpression (STIX)** permite a assimilação de inteligência de ameaças de terceiros utilizando um formato padrão da indústria para adicionar indicadores de ameaças personalizados aos mecanismos IDA.

### Proteção imediata e resistente

O FireEye Network Security oferece modos de configuração versáteis, incluindo:

- Monitoramento fora de banda por meio de um TAP/SPAN, monitoramento em linha ou bloqueio ativo em linha. O modo de bloqueio em linha interrompe automaticamente o malware e exploits de entrada e callbacks de múltiplos protocolos de saída. No modo de monitoramento em linha, são gerados alertas e as organizações decidem como

responder a eles. No modo de prevenção fora de banda, o FireEye Network Security envia pacotes "TCP reset" para o bloqueio fora de banda de conexões TCP, UDP ou HTTP.

- Modelos selecionados oferecem uma opção de alta disponibilidade (HA) ativa para proporcionar resistência em caso de falha de dispositivos ou da rede.

### Cobertura de uma ampla superfície de ataque

O FireEye Network Security oferece um nível de proteção consistente para os atuais ambientes de rede diversificados:

- Compatibilidade com os sistemas operacionais Microsoft Windows e Apple Mac OS X mais comuns
- Análise de mais de 140 tipos de arquivos diferentes, incluindo executáveis portáteis (*portable executables*, PEs), conteúdo da web, arquivos compactados, imagens, Java, aplicativos Microsoft e Adobe e arquivos multimídia
- Execução de tráfego de rede suspeito contra milhares de combinações de sistemas operacionais, Service Packs, tipos de aplicativos e versões de aplicativos
- Proteção contra ataques avançados e tipos de malware que são difíceis de detectar por meio de assinaturas: atualizações de web shell, execução de web shell, ransomware, cryptominers

### Alertas validados e priorizados

Além de detectar ataques genuínos, a tecnologia FireEye MVX também é utilizada para determinar a confiabilidade dos alertas detectados por métodos convencionais de correspondência de assinaturas e para identificar e priorizar ameaças críticas:

- O sistema de prevenção de intrusões (IPS), com validação pelo mecanismo MVX, reduz o tempo necessário para a triagem da detecção com base em assinaturas, tradicionalmente propensa a alertas falsos
- A categorização do riskware distingue entre tentativas autênticas de violação e atividades indesejadas, mas menos maliciosas (como adware e spyware) para priorizar a resposta aos alertas

### Insights decisivos sobre ameaças

Os alertas gerados pelo FireEye Network Security incluem evidências concretas e inteligência contextual para responder, priorizar e conter uma ameaça rapidamente:

- **Dynamic Threat Intelligence (DTI):** dados concretos, em tempo real e compartilhados globalmente para interromper, de maneira rápida e proativa, ataques direcionados e recém-descobertos
- **Advanced Threat Intelligence (ATI):** insights contextuais sobre o ataque para acelerar a resposta e a orientação prescritiva para conter a ameaça

### Integração de fluxos de trabalho de resposta

O FireEye Network Security pode ser complementado de diversas formas para automatizar os fluxos de trabalho de resposta a alertas:

- O FireEye Central Management correlaciona alertas do FireEye Network Security e do FireEye Email Security para uma visão mais ampla do ataque e para definir regras de bloqueio que impeçam o ataque de se espalhar ainda mais
- O FireEye Network Forensics integra-se com o FireEye Network Security para proporcionar capturas detalhadas de pacotes associados a um alerta, possibilitando investigações aprofundadas
- O FireEye Endpoint Security identifica, valida e contém comprometimentos detectados pelo FireEye Network Security para simplificar a contenção e a correção dos endpoints afetados

### Opções de distribuição versáteis

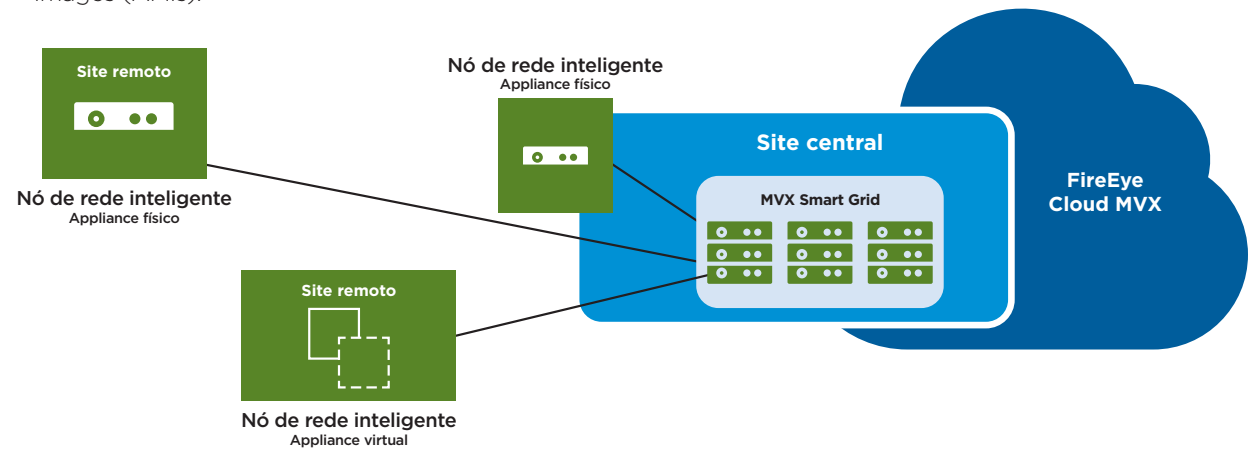
O FireEye Network Security oferece várias opções de distribuição, conforme as necessidades e o orçamento da organização:

- **Segurança de rede integrada:** appliance de hardware completo e autônomo, com um serviço MVX integrado para proteger um ponto de acesso à internet em um único local. O FireEye Network Security é uma plataforma fácil de gerenciar, sem clientes e que pode ser distribuída em menos de 60 minutos. Ele não requer regras, políticas ou ajustes.

- **Segurança de rede distribuída:** appliances expansíveis com um serviço MVX compartilhado centralmente, para proteger pontos de acesso à internet dentro das organizações
  - **Nó de rede inteligente:** appliances físicos ou virtuais, que analisam o tráfego de internet para detectar e bloquear tráfego nocivo e enviar atividades suspeitas através de uma conexão criptografada ao serviço MVX, para um veredito de análise definitivo
  - **MVX Smart Grid:** serviço MVX situado no local, centralizado e elástico, que oferece expansibilidade transparente, tolerância a falhas N+1 e balanceamento de carga automático
  - **FireEye Cloud MVX:** Assinatura do serviço MVX hospedado pela FireEye, que assegura privacidade ao analisar o tráfego no nó de rede inteligente. Somente objetos suspeitos são enviados por uma conexão criptografada para o serviço MVX, onde os objetos considerados benignos são descartados.
  - **Proteção no local ou na nuvem:** Além dos appliances autônomos e virtuais, a FireEye oferece Network Security na Nuvem Pública com a disponibilidade da Amazon Machine Images (AMIs).



**Figura 2.** Os exemplos de segurança de rede integrada incluem NX 2550, NX 3500, NX 5500 e NX 10550.



**Figura 3.** Modelos de distribuição múltipla da segurança de rede.

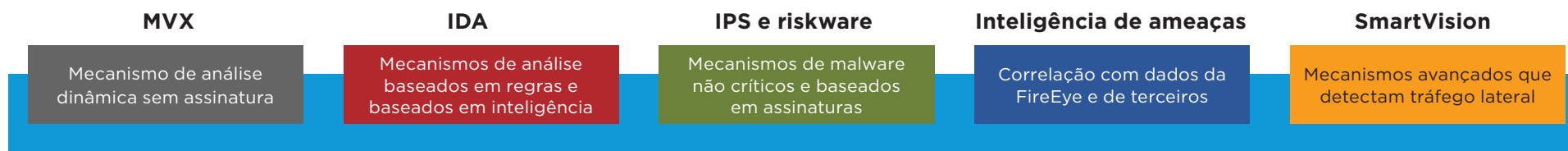


Figura 4. Componentes modulares do FireEye Network Security.

### Alto desempenho e expansibilidade

O FireEye Network Security protege os pontos de acesso à internet na velocidade da linha, com opções de desempenho para escritórios centrais e filiais de diversos portes:

A arquitetura expansível do MVX Smart Grid e do FireEye Cloud MVX permite que o serviço MVX acomode desde um até milhares de nós de rede inteligentes, expandindo-se perfeitamente conforme a necessidade.

Formato físico	Desempenho
Segurança de rede integrada	50 Mbps a 5 Gbps
Nó de rede inteligente físico	50 Mbps a 10 Gbps
Nó inteligente de rede de nuvem pública e virtual	50 Mbps a 1 Gbps

### Vantagens corporativas

Desenvolvido para satisfazer as necessidades de organizações situadas em um único local ou distribuídas por vários locais, o FireEye Network Security oferece várias vantagens:

### Minimiza o risco de violações cibernéticas

O FireEye Network Security é uma solução de defesa cibernética altamente eficaz que:

- Impede que intrusos invadam uma organização para roubar ativos valiosos ou perturbar seus negócios, ao interromper ataques avançados, direcionados e outros ataques evasivos

- Detém ataques e contém intrusões mais rapidamente com evidências concretas, inteligência decisiva, bloqueio em linha e automação dos fluxos de resposta
- Elimina os pontos fracos das defesas cibernéticas da organização com proteção consistente para vários sistemas operacionais, tipos de aplicativos e localizações centrais ou em filiais

### Retorno rápido do investimento

Segundo um estudo recente da Forrester Consulting<sup>1</sup>, os clientes do FireEye Network Security podem esperar uma economia de 152% no retorno do investimento ao longo de três anos e o retorno do investimento inicial em apenas 9,7 meses. O FireEye Network Security:

- Concentra os recursos da equipe de segurança em ataques reais para reduzir as despesas operacionais
- Otimiza o capital gasto com um serviço MVX compartilhado e uma grande variedade de pontos de desempenho para enxugar a distribuição e satisfazer os requisitos
- Prepara o investimento em segurança para o futuro ao se expandir harmoniosamente quando o número de filiais ou o volume de tráfego de internet aumenta
- Protege os investimentos existentes ao permitir uma migração sem custos de uma distribuição integrada para uma distribuição múltipla
- Reduz gastos futuros de capital, com sua arquitetura modular e expansível

### Prêmios e certificações

O portfólio de produtos FireEye Network Security ganhou vários prêmios e certificações setoriais e governamentais:

- Em 2018, a Frost & Sullivan reconheceu a FireEye como líder indiscutível de mercado, com 46% de participação, mais que os dez concorrentes seguintes juntos<sup>2</sup>
- O FireEye Network Security tem sido agraciado com vários prêmios do SANS Institute, SC Magazine, CRN e outros
- O FireEye Network Security foi a primeira solução de segurança do mercado a receber a certificação SAFETY Act do Departamento de Segurança Interna dos EUA



<sup>1</sup> Forrester (maio de 2016). The Total Economic Impact of FireEye.

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

**Tabela 1.** Especificações do FireEye Network Security, appliance integrado.

	<b>NX 2500</b>	<b>NX 2550</b>	<b>NX 3500</b>	<b>NX 4500</b>	<b>NX 5500</b>	<b>NX 6500</b>
<b>Sistemas operacionais compatíveis</b>	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
<b>Desempenho *</b>	Até 50 Mbps ou 100 Mbps	Até 250 Mbps	Até 500 Mbps	Até 1 Gbps	Até 2.5 Gbps	Até 5 Gbps
<b>Portas de monitoramento de rede</b>	4 portas 1GigE Bypass	4 portas 10GigE SFP+ 4 portas 1GigE Bypass	4 portas 10GigE SFP+ 4 portas 1GigE Bypass	8 portas 10GigE SFP+ 4 portas 1GigE Bypass	8 portas 10GigE SFP+ 4 portas 1GigE Bypass	8 portas 10GigE SFP+ 2 portas 40GigE QSFP+
<b>Modo de funcionamento das portas de rede</b>	Monitor em linha, Fail-Open, Fail-Close (HW Bypass) ou TAP/SPAN	Monitor em linha, Fail-Open, Fail-Close (HW Bypass) ou TAP/SPAN	Monitor em linha, Fail-Open, Fail-Close (HW Bypass) ou TAP/SPAN	Monitor em linha, Fail-Open, Fail-Close (HW Bypass) ou TAP/SPAN	Monitor em linha, Fail-Open, Fail-Close (HW Bypass) ou TAP/SPAN	Monitor em linha, TAP/SPAN
<b>Alta disponibilidade (HA)</b>	Não disponível	Não disponível	Não disponível	Disponível	Disponível	Disponível
<b>Portas de gerenciamento (painel traseiro)</b>	2 portas 10/100/1000 BASE-T	2 portas 1GigE	2 portas 1GigE	2 portas 1GigE	2 portas 1GigE	2 portas 1GigE
<b>Porta IPMI</b>	Painel frontal	Painel traseiro	Painel traseiro	Painel traseiro	Painel traseiro	Painel traseiro
<b>Teclado numérico e LCD frontal</b>	Não disponível	Não disponível	Não disponível	Não disponível	Não disponível	Não disponível
<b>Porta VGA</b>	Não	Sim	Sim	Sim	Sim	Sim
<b>Portas USB</b>	2 portas USB tipo A (painel frontal)	4 portas USB tipo A (tudo traseiro)	4 portas USB tipo A 2 frontais, 2 traseiras	4 portas USB tipo A 2 frontais, 2 traseiras	4 portas USB tipo A 2 frontais, 2 traseiras	2 portas USB tipo A
<b>Porta serial (painel traseiro)</b>	115.200 bps, sem paridade, 8 bits, 1 stop bit (conector RJ45; cabo adaptador de RJ45 para Dsub incluído)	115.200 bps, sem paridade, 8 bits, 1 stop bit	115.200 bps, sem paridade, 8 bits, 1 stop bit	115.200 bps, sem paridade, 8 bits, 1 stop bit	115.200 bps, sem paridade, 8 bits, 1 stop bit	115.200 bps, sem paridade, 8 bits, 1 stop bit
<b>Capacidade das unidades</b>	1 unidade de disco rígido de 1TB, SATA, 3,5 polegadas, interna e fixa	2 unidades de disco rígido de 4 TB, 3,5", SAS3, 7,2 krpm, FRU RAID1	2 unidades de disco rígido de 4 TB, 3,5", SAS3, 7,2 krpm, FRU RAID1	2 unidades de disco rígido de 4 TB, 3,5", SAS3, 7,2 krpm, FRU RAID1	2 unidades de disco rígido de 4 TB, 3,5", SAS3, 7,2 krpm, FRU RAID1	2 unidades de disco rígido de 10TB 3,5", SAS3, 7,2 krpm FRU RAID1
<b>Gabinete</b>	1 RU, para rack de 19"	1 RU, para rack de 19"	2 RU, para rack de 19"	2 RU, para rack de 19"	2 RU, para rack de 19"	2 RU, para rack de 19"
<b>Dimensões do chassi (LxPxX)</b>	437 mm x 500 mm x 43,2 mm	437 mm x 650 mm x 43,2 mm	438 mm x 620 mm x 88,4 mm	438 mm x 620 mm x 88,4 mm	438 mm x 620 mm x 88,4 mm	437 mm x 787 mm x 89 mm
<b>Fonte de alimentação CA</b>	Única de 250 W, 90-264 VCA, 3,5-1,5 A, 50-60 Hz, entrada IEC60320-C14, interna, fixa	Redundante (1+1) de 750 W, 100-240 VCA, 8,0-4,5 A, 50-60 Hz, entrada IEC60320-C14, FRU	Redundante (1+1) de 800 W, 100-240 VCA, 10,5-4,0 A, 50-60 Hz, entrada IEC60320-C14, FRU	Redundante (1+1) de 800 W, 100-240 VCA, 10,5-4,0 A, 50-60 Hz, entrada IEC60320-C14, FRU	Redundante (1+1) de 800 W, 100-240 VCA, 10,5-4,0 A, 50-60 Hz, entrada IEC60320-C14, FRU	Redundante (1+1) de 1000 watts, 100-240 VCA 10,5-4,0A, 50-60 Hz, entrada IEC60320-C14, FRU





**Tabela 2.** Desempenho do FireEye Network Security IPS, appliance integrado.

	<b>NX 2500</b>	<b>NX 2550</b>	<b>NX 3500</b>	<b>NX 4500</b>	<b>NX 5500</b>	<b>NX 6500</b>
<b>Desempenho máximo do IPS</b>	Até 50 Mbps ou 100 Mbps	Até 250 Mbps	Até 500 Mbps	Até 1 Gbps	Até 2.5 Gbps	Até 5 Gbps
<b>Máximo de conexões simultâneas</b>	15.000 ou 80.000	80.000	160.000	500.000	1.000.000	2.000.000
<b>Novas conexões por segundo</b>	750/s ou 4.000/s	4.000/s	8.000/s	10.000/s	20.000/s	40.000/s

**Tabela 3.** Especificações físicas do nó inteligente do FireEye Network Security.

	<b>NX 1500</b>	<b>NX 2500</b>	<b>NX 2550</b>	<b>NX 3500</b>	<b>NX 4500</b>	<b>NX 5500</b>	<b>NX 6500</b>
<b>Sistemas operacionais compatíveis</b>	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
<b>Desempenho</b>	Até 50 Mbps	Até 100 Mbps ou 250 Mbps	Até 500 Mbps	Até 1 Gbps	Até 2 Gbps	Até 5 Gbps	Até 10 Gbps
<b>Portas de monitoramento de rede</b>	4 portas 10/100/1000 BASE-T	4 portas 1GigE Bypass	4 portas 10GigE SFP+ 4 portas 1GigE Bypass	4 portas 10GigE SFP+ 4 portas 1GigE Bypass	8 portas 10GigE SFP+ 4 portas 1GigE Bypass	8 portas 10GigE SFP+ 4 portas 1GigE Bypass	8 portas 10GigE SFP+ 2 portas 40GigE QSFP+
<b>Modo de funcionamento das portas de rede</b>	Monitor em linha, Fail Close ou Tap	Monitor em linha, Fail-Open, Fail-Close (HW Bypass) ou TAP/SPAN	Monitor em linha, Fail-Open, Fail-Close (HW Bypass) ou TAP/SPAN	Monitor em linha, Fail-Open, Fail-Close (HW Bypass) ou TAP/SPAN	Monitor em linha, Fail-Open, Fail-Close (HW Bypass) ou TAP/SPAN	Monitor em linha, Fail-Open, Fail-Close (HW Bypass) ou TAP/SPAN	Monitor em linha, TAP/SPAN
<b>Alta disponibilidade (HA)</b>	Não disponível	Não disponível	Não disponível	Não disponível	Não disponível	Não disponível	Não disponível
<b>Portas de gerenciamento (painel traseiro)</b>	2 portas 10/100/1000 BASE-T	2 portas 1GigE	2 portas 1GigE	2 portas 1GigE	2 portas 1GigE	2 portas 1GigE	2 portas 1GigE
<b>Porta IPMI</b>	Não disponível	Painel frontal	Painel traseiro	Painel traseiro	Painel traseiro	Painel traseiro	Painel traseiro
<b>Teclado numérico e LCD frontal</b>	Não disponível	Não disponível	Não disponível	Não disponível	Não disponível	Não disponível	Não disponível
<b>Porta VGA</b>	Não disponível	Não disponível	Sim	Sim	Sim	Sim	Sim
<b>Portas USB</b>	2 portas USB tipo A	2 portas USB tipo A (painel frontal)	4 portas USB tipo A (tudo traseiro)	4 portas USB tipo A 2 frontais, 2 traseiras	4 portas USB tipo A 2 frontais, 2 traseiras	4 portas USB tipo A 2 frontais, 2 traseiras	2 portas USB tipo A





**Tabela 3.** Especificações físicas do nó inteligente do FireEye Network Security. (continuação)

	<b>NX 1500</b>	<b>NX 2500</b>	<b>NX 2550</b>	<b>NX 3500</b>	<b>NX 4500</b>	<b>NX 5500</b>	<b>NX 6500</b>	
<b>Conformidade regulatória de EMC</b>	FCC Parte 15 ICES-003 Classe 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 e V-3/2015	FCC Parte 15 ICES-003 Classe 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 e V-3/2015	FCC Parte 15 ICES-003 Classe 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 e V-3/2015	FCC Parte 15 ICES-003 Classe 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 e V-3/2015	FCC Parte 15 ICES-003 Classe 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 e V-3/2015	FCC Parte 15 ICES-003 Classe 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 e V-3/2015	FCC Parte 15 ICES-003 Classe 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 e V-3/2015	Segurança: EN 60950; C22.2; UL 60950; IEC 60950; CAN/CSA-C22.2; K 60950; AS/NZS 60950; GB 4943.1; J60950, SI60950 EMC: FCC Parte 15 SubParte B Classe A; ICES-003; EN55032; VCCI V-3; EN 55024; EN 61000; CNS 13438; CISPR32; KN 32; KN 35
<b>Conformidade ambiental</b>	Diretiva RoHS 2011/65/EU REACH Diretiva WEEE 2012/19/EU	Diretiva RoHS 2011/65/EU REACH Diretiva WEEE 2012/19/EU	Diretiva RoHS 2011/65/EU REACH Diretiva WEEE 2012/19/EU	Diretiva RoHS 2011/65/EU REACH Diretiva WEEE 2012/19/EU	Diretiva RoHS 2011/65/EU REACH Diretiva WEEE 2012/19/EU	Diretiva RoHS 2011/65/EU REACH Diretiva WEEE 2012/19/EU	RoHS; REACH; WEEE Minerais de conflito	
<b>Temperatura de funcionamento</b>	0-40 °C	0-40 °C	0-40 °C	0-40 °C	0-40 °C	0-40 °C	0-40 °C	
<b>Temperatura fora de funcionamento</b>	-20-80 °C	-20-80 °C	-30-70 °C	-40-70 °C	-40-70 °C	-40-70 °C	-30-70 °C	
<b>Umidade relativa de funcionamento</b>	10-95% a 40 °C, sem condensação	5-85% a 40 °C, sem condensação	10-95% a 40 °C, sem condensação	10-95% a 40 °C, sem condensação	10-95% a 40 °C, sem condensação	10-95% a 40 °C, sem condensação	10%-90% a 40 °C sem condensação	
<b>Umidade relativa fora de funcionamento</b>	10-95% a 60 °C sem condensação	5-95% a 40 °C sem condensação	10-95% a 60 °C, sem condensação	10-95% a 60 °C, sem condensação	10-95% a 60 °C, sem condensação	10-95% a 60 °C, sem condensação	10%-95% a 55 °C sem condensação	
<b>Altitude de funcionamento</b>	3.000 m 9.842 pés	3.000 m 9.842 pés	3.000 m 9.842 pés	3.000 m 9.842 pés	3.000 m 9.842 pés	3.000 m 9.842 pés	3.000 m 9.842 pés	

**Tabela 4.** Especificações físicas do IPS do nó inteligente do FireEye Network Security.

	<b>NX 1500</b>	<b>NX 2500</b>	<b>NX 2550</b>	<b>NX 3500</b>	<b>NX 4500</b>	<b>NX 5500</b>	<b>NX 6500</b>
<b>Desempenho máximo do IPS</b>	Até 50 Mbps	Até 100/250 Mbps	Até 500 Mbps	Até 1 Gbps	Até 2 Gbps	Até 5 Gbps	Até 10 Gbps
<b>Máximo de conexões simultâneas</b>	15.000	80.000	160.000	500.000	1.000.000	2.000.000	4.000.000
<b>Novas conexões por segundo</b>	750/s	4.000/s	8.000/s	10.000/s	20.000/s	40.000/s	80.000/s

**Tabela 5.** Especificações virtuais do nó inteligente do FireEye Network Security.

	VA-NXS 1500	VA-NXS 2500	VA-NXS 2550	VA-NXS 4500	VA-NXS 6500
<b>Sistemas operacionais compatíveis</b>	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
<b>Desempenho *</b>	Até 50 Mbps	Até 100 Mbps	Até 250 Mbps	Até 500 Mbps	Até 1 Gbps
<b>Portas de monitoramento de rede</b>	1-8	1-8	1-8	1-8	1-8
<b>Portas de gerenciamento de rede</b>	1 ou 2	1 ou 2	1 ou 2	1 ou 2	1 ou 2
<b>Modo de funcionamento das portas de rede</b>	Em linha, SPAN	Em linha, SPAN	Em linha, SPAN	Em linha, SPAN	Em linha, SPAN
<b>Núcleos de CPU</b>	3	6	8	8	16
<b>Memória</b>	10 GB	16 GB	16 GB	32 GB	32 GB
<b>Capacidade das unidades</b>	384 GB	384 GB	384 GB	512 GB	512 GB
<b>Adaptadores de rede</b>	VMXNet 3, vNIC	VMXNet 3, vNIC	VMXNet 3, vNIC	VMXNet 3, vNIC	VMXNet 3, vNIC
<b>Suporte para hipervisor</b>	VMWare ESXi6.0 ou posterior e KVM 1.5.3 ou posterior	VMWare ESXi6.0 ou posterior e KVM 1.5.3 ou posterior	VMWare ESXi6.0 ou posterior e KVM 1.5.3 ou posterior	VMWare ESXi6.0 ou posterior e KVM 1.5.3 ou posterior	VMWare ESXi6.0 ou posterior e KVM 1.5.3 ou posterior
<b>Certificações de segurança</b>	FIPS 140-2 Nível 1 CC NDPP v1.1 (em processo)	FIPS 140-2 Nível 1 CC NDPP v1.1 (em processo)	FIPS 140-2 Nível 1 CC NDPP v1.1 (em processo)	FIPS 140-2 Nível 1 CC NDPP v1.1 (em processo)	FIPS 140-2 Nível 1 CC NDPP v1.1 (em processo)

**Tabela 6.** Especificações virtuais do IPS do nó inteligente do FireEye Network Security.

	VA-NXS 1500	VA-NXS 2500	VA-NXS 2550	VA-NXS 4500	VA-NXS 6500
<b>Desempenho máximo do IPS</b>	Até 50 Mbps	Até 100 Mbps	Até 250 Mbps	Até 500 Mbps	Até 1 Gbps
<b>Máximo de conexões simultâneas</b>	15.000	80.000	80.000	160.000	500.000
<b>Novas conexões por segundo</b>	750/s	4.000/s	4.000/s	8.000/s	10.000/s

**Tabela 7.** Tamanhos de AMI suportados pelo FireEye Network Security em AWS.

Modelo	Transferência	vCPU	Memória	Disco	Interfaces de rede	Tipo de instância AWS
NX4500v	500 Mbps	8	32 GB	512 GB (EBS)	Um gerenciamento, uma submissão e duas portas de monitoramento (total 4 portas)	M5.2xlarge
NX6500v	1 Gbps	16	64 GB	512 GB (EBS)	Um gerenciamento, uma submissão e seis portas de monitoramento (total 8 portas)	M5.4xlarge

**Tabela 8.** Especificações do FireEye MVX Smart Grid.

	<b>VX 5500</b>	<b>VX 12550</b>
<b>Sistemas operacionais compatíveis</b>	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows
<b>Desempenho *</b>	Até 2 Gbps	Até 14 Gbps
<b>Alta disponibilidade (HA) **</b>	N+1	N+1
<b>Portas de gerenciamento (painel traseiro)</b>	1 porta BASE-T de 10/100/1000 Mbps	1 porta BASE-T de 10/100/1000 Mbps
<b>Portas de cluster (painel traseiro)</b>	3 portas BASE-T 10/100/1000 Mbps	1 porta BASE-T 10/100/1000 Mbps, 2 portas BASE-T 10 Gbps, 4 portas 10GigE SFP+
<b>Porta IPMI (painel traseiro)</b>	Incluídas	Incluídas
<b>Teclado numérico e LCD frontal</b>	Não disponível	Sem LCD
<b>Portas VGA</b>	Incluídas	Incluídas
<b>Portas USB (painel traseiro)</b>	4 portas USB tipo A	2 portas USB tipo A
<b>Porta serial (painel traseiro)</b>	115.200 bps, sem paridade, 8 bits, 1 stop bit	115.200 bps, sem paridade, 8 bits, 1 stop bit
<b>Capacidade das unidades</b>	2 unidades de disco rígido SAS3 de 2TB, 3,5", RAID 1, troca a quente, FRU	2 unidades de disco rígido SAS3 de 4TB, 3,5", RAID 1, troca a quente, FRU
<b>Gabinete</b>	1 RU, para rack de 19"	2 RU, para rack de 19"
<b>Dimensões do chassi (LxPxA)</b>	437 x 650 x 43,2 mm	437 x 787 x 89 mm
<b>Fonte de alimentação CC</b>	Não disponível	Não disponível
<b>Fonte de alimentação CA</b>	Redundante (1+1), 750 W, 100-240 VCA, 8-3,8 A, 50-60 Hz, entrada IEC60320-C14, troca a quente, FRU	Redundante (1+1) de 1000 watts, 100-240 VCA, 10,5-4,0 A, 50-60 Hz, entrada IEC60320-C14, FRU
<b>Consumo de energia máximo (W)</b>	285 W	660 W
<b>Dissipação térmica máxima (BTU/h)</b>	972 BTU/h	2.594 BTU/h
<b>MTBF (h)</b>	54.200 h	54.041 h
<b>Peso líquido/total (kg)</b>	12,2 kg/17,2 kg	20 kg/32,2 kg
<b>Certificação de segurança</b>	FIPS 140-2 Nível 1, CC NDPP v1.1 (pendente)	FIPS 140-2 Nível 1, CC NDPP v1.1 (pendente)
<b>Conformidade regulatória de segurança</b>	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2

**Tabela 9.** Especificações do FireEye MVX Smart Grid.

	<b>VX 5500</b>	<b>VX 12500</b>
<b>Conformidade regulatória de EMC</b>	FCC Parte 15 ICES-003 Classe 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 e V-3/2015	FCC Parte 15 ICES-003 Classe 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 e V-3/2015
<b>Conformidade ambiental</b>	Diretiva RoHS 2011/65/EU REACH Diretiva WEEE 2012/19/EU	Diretiva RoHS 2011/65/EU REACH Diretiva WEEE 2012/19/EU
<b>Temperatura de funcionamento</b>	0-40 °C	0-40 °C
<b>Temperatura fora de funcionamento</b>	-30-70 °C	-30-70 °C
<b>Umidade relativa de funcionamento</b>	10-95% a 40 °C sem condensação	10%-90% a 40 °C sem condensação
<b>Umidade relativa fora de funcionamento</b>	10-95% a 60 °C sem condensação	10%-95% a 55 °C sem condensação
<b>Altitude de funcionamento</b>	3000 m 9842 pés	3000 m 9842 pés

**Serviços de suporte**

A FireEye oferece programas de suporte simples e versáteis para maximizar o valor dos produtos e serviços FireEye. Quatro níveis diferentes de serviços de suporte estão disponíveis: Platinum, Platinum Priority Plus, Government e Government Priority Plus. Para obter mais informações sobre o suporte da FireEye, consulte os serviços de Suporte da FireEye.

Para saber mais sobre a FireEye, visite: [www.FireEye.com](http://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 os direitos reservados. FireEye é uma marca registrada da FireEye, Inc. Todos os outros nomes de marcas, produtos e serviços são ou podem ser marcas comerciais ou marcas de serviços de seus respectivos proprietários.  
NS-EXT-DS-US-EN-000048-10

**Sobre a FireEye, Inc**

A FireEye é a empresa líder em segurança orientada por inteligência. Atuando harmoniosamente como extensão expansível das operações de segurança dos clientes, a FireEye oferece uma plataforma única que mescla tecnologias de segurança inovadoras, inteligência de ameaças em nível governamental e a consultoria mundialmente reconhecida da Mandiant®. Com essa abordagem, a FireEye elimina a complexidade e o fardo da segurança cibernética para organizações empenhadas em se preparar, prevenir e responder a ataques cibernéticos.

