FireEye
SECURITY REIMAGINED

Appliance FireEye SSL Intercept

Exponha os ataques que se escondem no tráfego SSL

SEGURANÇA REIMAGINADA

DATASHEET

DESTAQUES

- Obtenha visibilidade sobre o tráfego de rede protegido por SSL
- Distribua com a série NX em modo TAP ou em linha
- Exclua sites da descriptografia SSL por categoria de URL
- Faça balanceamento de carga do tráfego entre dispositivos série NX

FireEye SSL Intercept 10150

Proteção de organizações contra intrusões e ataques criptografados

Paradoxalmente, a adoção crescente de protocolos para tornar seguro o tráfego na Internet, incluindo o Secure Socket Layer (SSL), está proporcionando aos criminosos cibernéticos uma maneira de contornar defesas de rede. A criptografia do SSL protege a privacidade das comunicações ao tornar impossível ler o tráfego de rede. Porém, essa mesma propriedade também impossibilita a dispositivos de segurança de rede inspecionar o tráfego SSL quanto a indícios de atividade maliciosa. Cada vez mais criminosos cibernéticos estão usando o SSL como um disfarce para se infiltrarem em organizações sem serem detectados.

O appliance FireEye SSL Intercept, com segurança de rede FireEye (série NX), protege as organizações contra intrusões e ataques criptografados. O FireEye SSL Intercept é um proxy em camada de aplicativo que dá à série FireEye NX visibilidade sobre o tráfego SSL não confiável. Ele foi desenvolvido para interceptar e encaminhar todo o tráfego de rede desejado à série FireEye NX para inspeção. Ao descriptografar temporariamente, inspecionar e, então, recriptografar sessões SSL não confiáveis, o FireEye SSL Intercept garante que os criminosos cibernéticos não possam usar o SSL como forma de evitar a detecção. Com o FireEye SSL Intercept, as organizações obtêm uma segurança de rede mais forte, pela maior visibilidade sobre seu tráfego de rede, e mais retorno de seu investimento na série FireEye NX.

O FireEye SSL Intercept é um appliance de rede de alto desempenho que, em um modo de distribuição em linha, pode atender simultaneamente até três dispositivos da série FireEye NX. A assinatura de classificação de URLs que o acompanha permite que as organizações permaneçam em conformidade com suas políticas de privacidade e requisitos regulatórios. Sites com informações confidenciais, como aplicativos de acesso a banco ou assistência médica, podem ser convenientemente excluídos da descriptografia SSL, individualmente ou por categoria.

A vantagem do FireEye SSL Intercept e da série NX

Desenvolvido para uso com todos os dispositivos da série FireEye NX, o appliance FireEye SSL Intercept oferece grande valor em três áreas:

Visibilidade

O appliance FireEye SSL Intercept permite à série FireEye NX inspecionar o tráfego SSL, tanto de entrada quanto de saída. Atacantes que utilizam sites com SSL, como sites de blogs, armazenamento na nuvem e webmail, são identificados e bloqueados pela série FireEye NX. Callbacks de saída para servidores de comando e controle e kits de exploits para acesso reverso a shell seguro são identificados e bloqueados. O appliance SSL Intercept é compatível com todas as versões, comprimentos de chave, cifras e hashes de SSL/TLS normalmente distribuídas.

A visibilidade sobre o tráfego SSL permite que a série FireEye NX conecte todos os indícios de atividade maliciosa com a inteligência estratégica proporcionada pelo FireEye Advanced Threat Intelligence (ATI). Uma automação expressiva de inteligência estratégica do ATI na plataforma FireEye resulta em respostas mais rápidas e mais efetivas a ameaças avançadas. O banco de dados de classificação de URLs permite que as organizações incluam ou excluam, seletivamente, sites na inspeção de SSL.

Desempenho

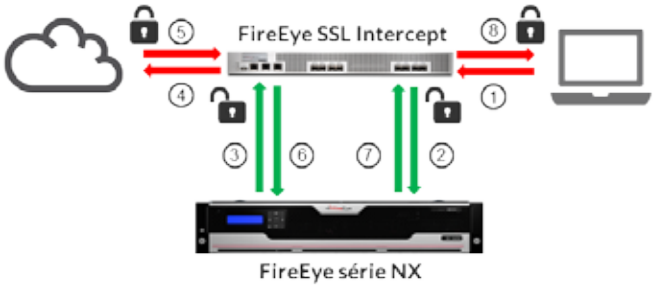
O appliance FireEye SSL Intercept comporta taxas de transferência de até 20 Gbps para todo o tráfego HTTP, e até 5,5 Gbps para todo o tráfego SSL com chaves de 2.048 bits. Nessas taxas, ele pode ser distribuído com quaisquer dispositivos da série FireEye NX, sem impacto sobre o desempenho geral. Os recursos da série FireEye NX permanecem dedicados à detecção de ameaças cibernéticas, e não ao processamento rotineiro de SSL, intensivo em termos de processamento. A arquitetura delegada do SSL ajuda as organizações a obter o máximo de seu investimento na série FireEye NX.

Expansibilidade

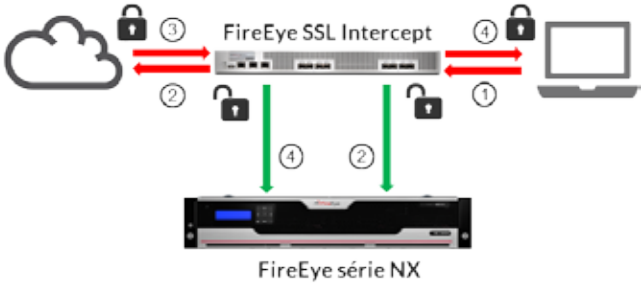
O appliance FireEye SSL Intercept pode fazer balanceamento de carga do tráfego entre dois dispositivos da série FireEye NX em modo passivo (TAP) ou três em modo de bloqueio (em linha). Até 8 Gbps de tráfego podem ser processados no modo passivo e até 10 Gbps no modo em linha por um grupo de dispositivos da série FireEye NX. A densidade de portas de rede estendida ajuda as organizações a protegerem seu investimento e a se prepararem para o crescimento futuro.

Descrição do produto

O appliance FireEye SSL Intercept atua como um proxy de encaminhamento explícito ou transparente para descriptografar a carga SSL e rotear o tráfego descriptografado para a série FireEye NX para análise. Quando o tráfego retorna da série FireEye NX, o FireEye SSL Intercept recriptografa a carga SSL e a encaminha para o destino original. Dependendo de sua configuração, a série FireEye NX pode fornecer uma página de aviso ao usuário, enviar uma notificação por e-mail ao administrador, bloquear a conexão ou realizar várias outras ações configuráveis ao detectar um ataque.



Distribuição ativa do Intercept



Distribuição passiva do Intercept

Características

FireEye SSL Intercept 10150	
Características gerais • Serviço Trusted Site Identity (TSID) para deixar passar, seletivamente, sites com informações confidenciais, com base na categoria do URL • Reconhecimento de Server Name Indication (SNI) para deixar passar, seletivamente, hosts externos confiáveis • Detecção de certificado do cliente e passagem direta opcional • Tratamento de certificados não confiáveis • Reutilização de identificações de sessões SSL	**Gerenciamento** • Interface de gerenciamento dedicada (Console, SSH, Telnet e HTTPS) • Interface de usuário com base na Web disponível em vários idiomas • Command Line Interface (CLI) • SNMP, Syslog, alertas via e-mail, NetFlow v9 e v10 (IPFIX), sFlow • Espelhamento de portas • API XML estilo REST (aXAPI) • Suporte para LDAP, TACACS+ e RADIUS
Modos de distribuição • Distribuição em linha com até três dispositivos da série NX • Distribuição passiva com até dois dispositivos da série NX	

Especificações técnicas

FireEye SSL Intercept 10150	
Taxa de transferência total (100% HTTP)	20 Gbps
Taxa de transferência na inspeção de SSL (100% SSL)	5,5 Gbps
Fluxos TCP simultâneos	4.000.000
Sessões SSL simultâneas	400.000
Taxa de configuração de sessões SSL	15.000 por segundo
Latência de "cut-through"	60 us
Versões do SSL	SSL 3.0, TLS 1.0, 1.1 e 1.2
Chaves RSA	512, 1.024, 2.048, 4.096
Algoritmos de chave pública	RSA, DHE-RSA, ECDHE-RSA, ECDHE-ECDSA com suporte para Perfect Forward Secrecy (PFS)
Algoritmos de chave simétrica	AES 128, AES 128-GCM, AES 256, AES 256-GCM, ARC4, 3DES, DES,
Algoritmos de hashing	MD5, SHA-1, SHA-2 (SHA-256, SHA-384)
Modo de proxy	Explícito Transparente
Quantidade de portas de monitoramento de rede	8 (2 de entrada/saída, 6 de monitoramento)
Tipo de porta de monitoramento de rede	1G/10G Base SX/SR SFP+ 1G/10G Base LX/LR SFP+ 10G Base de cobre SFP+ 1G Base T SFP
Modos das portas de monitoramento de rede	Monitoramento em linha (máximo de 3 pares de portas) TAP (máximo de 2 portas)
Failover de monitoramento de rede	Kit de failover ativo externo (vendido separadamente)
Quantidade de portas de gerenciamento de rede	2
Tipos de porta de gerenciamento de rede	1G Base T RJ45 – Console 1G Base T RJ45 – Gerenciamento/IPMI
Gabinete	1U, para rack de 19"
Tipo de unidade	SSD
Dimensões do chassi (LxPxA)	444 x 434 x 44 mm
Fonte de alimentação CA	Redundante (1+1) de 600 watts, eficiência 80 Plus Platinum, 100 – 240 VCA, 8 – 3 A, 50 – 60 Hz, FRU
Fonte de alimentação CC	Não disponível
Ventoinhas de arrefecimento	5 ventoinhas inteligentes com troca a quente
Consumo de energia típico/máximo	240/288 watts
Dissipação térmica máxima	819/983 BTU/h
Tempo médio entre falhas (MTBF)	91.051 h
Peso líquido / enviado	10,5 Kg / 14,6 kg
Temperatura de funcionamento	0 a 40°C
Temperatura fora de funcionamento	-20 a 70°C
Umidade relativa de funcionamento	5 a 95% (sem condensação)
Umidade relativa fora de funcionamento	5 a 95% (sem condensação)
Altitude de funcionamento	0 a 2.000 m
Certificações de segurança	UL/cUL, TUV, CB
Certificações EMC/EMI	FCC, CE, VCCI, BSMI, KCC
Conformidade regulatória	RoHS

Saiba mais

A FireEye oferece um amplo portfólio de serviços. Para mais informações, entre em contato conosco pelo e-mail services@FireEye.com ou pelo telefone +1 855.692.2052.

Por que escolher a FireEye?

Conhecimento. Tecnologia. Inteligência.

A FireEye protege os ativos mais valiosos do mundo contra quem os cobiça. Nossa combinação de tecnologia, inteligência e conhecimentos — corroborada pela equipe de resposta a incidentes mais forte da indústria — ajuda a eliminar o impacto das violações de segurança. Com a FireEye, você vai detectar os ataques conforme eles acontecerem. Você compreenderá os riscos que esses ataques representam aos seus ativos mais valiosos. E você terá os recursos para responder e resolver rapidamente os incidentes. A comunidade global de defesa da FireEye conta com mais de 3.100 clientes espalhados por 67 países, entre os quais mais de 200 despontam na lista Fortune 500.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408.321.6300 | 877.FIREEYE (347.3393) | LATAM@fireeye.com | **www.fireeye.com**