FireEye
SECURITY REIMAGINED

FireEye SSL Intercept Appliance

Expose Attacks Hiding in SSL Traffic

SECURITY
REIMAGINED

DATA SHEET

HIGHLIGHTS

- Gain visibility into SSL protected network traffic
- Deploy with NX Series in TAP or inline mode
- Exclude sites from SSL decryption by URL category
- Load balance traffic across NX Series devices

FireEye SSL Intercept 10150

Protecting Organizations Against Encrypted Attacks and Intrusions

The growing adoption of protocols to secure Internet traffic, including Secure Socket Layer (SSL), is paradoxically giving cyber criminals a way to evade network defenses. SSL encryption protects communication privacy by making network traffic unreadable. But this very property also makes it impossible for network security devices to inspect SSL traffic for signs of malicious activity. A growing number of cyber criminals is using SSL as a cover to slip into organizations and persist undetected.

The FireEye SSL Intercept appliance with FireEye Network Security (NX Series) protects organizations against encrypted attacks and intrusions. FireEye SSL Intercept is an application layer proxy that gives FireEye NX Series visibility into untrusted SSL traffic. It is designed to intercept and forward all desired network traffic to the FireEye NX Series for inspection. Temporarily decrypting, inspecting, and then re-encrypting untrusted SSL sessions, FireEye SSL Intercept ensures cyber criminals cannot use the cover of SSL to evade detection. With FireEye SSL Intercept, organizations get stronger network security though greater visibility into their network traffic and more value out of their FireEye NX Series investment.

FireEye SSL Intercept is a high performance network appliance that in an inline deployment mode can concurrently service up to three FireEye NX Series devices. The included URL classification subscription allows organizations to remain compliant with their privacy policies and regulatory requirements. Sensitive sites, such as banking or healthcare applications can be conveniently excluded by category, or individually from SSL decryption.

The FireEye SSL Intercept and NX Series Advantage

Designed for use with all FireEye NX Series devices, FireEye SSL Intercept appliance provides outstanding value in three key areas:

Visibility

The FireEye SSL Intercept appliance enables the FireEye NX Series to inspect both inbound and outbound SSL traffic. Attackers using SSL websites such as web-based mail, cloud storage, and blog sites, are identified and blocked by the FireEye NX Series. Outbound callbacks to command and control servers and exploit kits for reverse secure shell access are identified and blocked. The SSL Intercept appliance supports all commonly deployed SSL/TLS versions, key lengths, ciphers, and hashes.

Visibility into SSL traffic enables FireEye NX Series to connect all indicators of malicious activity with strategic intelligence provided by FireEye Advanced Threat Intelligence (ATI). Meaningful automation of strategic intelligence from ATI into the FireEye platform, results in a faster and more effective responses to advanced threats. The URL classification database enables organizations to selectively include and exclude sites in SSL inspection.

Performance

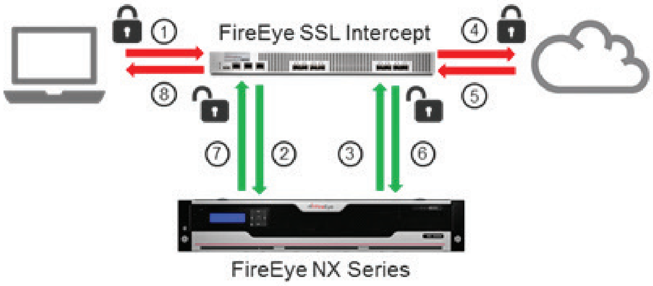
The FireEye SSL Intercept appliance supports 20 Gbps throughput for all HTTP traffic, and 5.5 Gbps all SSL traffic with 2048 bit keys. At this line rate it can be deployed with any of the FireEye NX Series devices with no impact on overall performance. FireEye NX Series resources remain dedicated to detecting cyber threats, not the computationally intensive, but routine SSL processing. The SSL offload architecture helps organizations realize full value of their FireEye NX Series investment.

Scalability

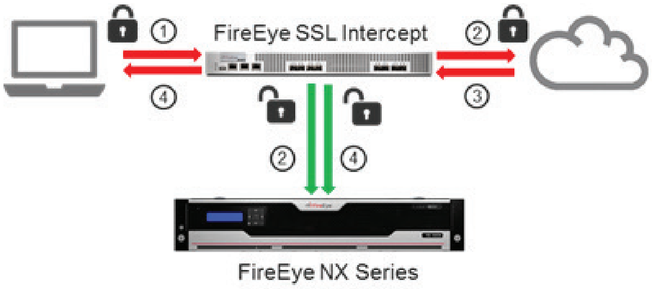
The FireEye SSL Intercept appliance can load balance traffic across two FireEye NX Series devices in passive (TAP) mode or three in blocking (inline) mode. Up to 8 Gbps of traffic can be processed in passive mode, and 10 Gbps of traffic in inline mode by a group of FireEye NX Series devices. Extended network port density helps organizations protect their investment and prepare for future growth.

Product Description

The FireEye SSL Intercept appliance acts as a transparent or explicit forward proxy to decrypt SSL payload and route the decrypted traffic to the FireEye NX Series for analysis. When the traffic returns from the FireEye NX Series, the FireEye SSL Intercept re-encrypts the SSL payload and forwards to the original destination. Depending on its configuration, the FireEye NX Series may deliver a warning page to the user, send an email notification to the administrator, block the connection, or perform a number of other configurable actions when it detects an attacks.



Active Intercept Deployment



Passive Intercept Deployment

Features

FireEye SSL Intercept 10150	
General Features • Trusted Site Identity (TSID) service to selectively bypass sensitive websites based on URL category • Server Name Indication (SNI) recognition to selectively bypass trusted external hosts • Client certificate detection and optional bypass • Untrusted certificate handling • SSL session ID reuse	**Management** • Dedicated management interface (Console, SSH, Telnet, HTTPS) • Web-based user interface with language localization • Command Line Interface (CLI) • SNMP, Syslog, email alerts, NetFlow v9 and v10 (IPFIX), sFlow • Port mirroring • REST-style XML API (aXAPI) • LDAP, TACACS+, RADIUS support
Deployment Modes • Inline deployment with up to three NX Series devices • Passive deployment with up to two NX Series devices	

Technical Specifications

	FireEye SSL Intercept 10150
Total Throughput (100% HTTP)	20 Gbps
SSL Inspection Throughput (100% SSL)	5.5 Gbps
Concurrent TCP Flows	4,000,000
Concurrent SSL Sessions	400,000
SSL Session Setup Rate	15,000 per second
Cut-through Latency	60 us
SSL Versions	SSL 3.0, TLS 1.0, 1.1 and 1.2
RSA Keys	512, 1024, 2048, 4096
Public Key Algorithms	RSA, DHE-RSA, ECDHE-RSA, ECDHE-ECDSA with Perfect Forward Secrecy (PFS) Support
Symmetric Key Algorithms	AES 128, AES 128-GCM, AES 256, AES 256-GCM, ARC4, 3DES, DES,
Hashing Algorithms	MD5, SHA-1, SHA-2 (SHA-256, SHA-384)
Proxy Mode	Explicit Transparent
Network Monitoring Port Count	8 (2 ingress/egress, 6 monitoring)
Network Monitoring Port Type	1G/10G Base SX/SR SFP+ 1G/10G Base LX/LR SFP+ 10G Base Cu SFP+ 1G Base T SFP
Network Monitoring Port Modes	Inline Monitor (Maximum 3 port pairs) TAP (Maximum 2 ports)
Network Monitoring Failover	External Active Failover Kit (sold separately)
Network Management Port Count	2
Network Management Port Types	1G Base T RJ45 – Console 1G Base T RJ45 – Management/IPMI
Enclosure	1U, Fits 19 inch Rack
Drive Type	SSD
Chassis Dimensions WxDxH	17.5” x 17.1” x 1.75” (444 x 434 x 44 mm)
AC Power Supply	Redundant (1+1) 600 watt, 80 Plus Platinum efficiency, 100 – 240 VAC, 8 – 3 A, 50 – 60 Hz, FRU
DC Power Supply	Not Available
Cooling Fans	5 Hot Swap Smart Fans
Power Consumption Typical/Maximum	240/288 watts
Thermal Dissipation Maximum	819/983 BTU/h
MTBF	91,051 h
Appliance Alone / As Shipped Weight	23 lbs / 32 lbs
Operating Temperature	0°C to 40°C
Non-Operating Temperature	-20°C to 70°C
Operating Relative Humidity	5% - 95% non-condensing
Non-Operating Relative Humidity	5% - 95% non-condensing
Operating Altitude	0 m - 2000 m
Safety Certifications	UL/cUL, TUV, CB
EMC/EMI Certifications	FCC, CE, VCCI, BSMI, KCC
Regulatory Compliance	RoHS

Learn More

FireEye offers a comprehensive portfolio of services. For full details, contact us at services@FireEye.com or +1 855.692.2052.

Why FireEye?

Expertise. Technology. Intelligence.

FireEye protects the most valuable assets in the world from those who have them in their sights. Our combination of technology, intelligence, and expertise—reinforced with the most aggressive incident response team—helps eliminate the impact of security breaches. With FireEye, you'll detect attacks as they happen. You'll understand the risk these attacks pose to your most valued assets. And you'll have the resources to quickly respond and resolve security incidents. The FireEye Global Defense Community includes more than 3,100 customers across 67 countries, including over 200 of the Fortune 500.