FireEye SSL Appliance Intercept

Scopri gli attacchi che si celano nel traffico SSL

SCHEDA PRODOTTO

IN PRIMO PIANO

- Rendi visibile il traffico di rete protetto SSL
- Installa le appliance della Serie NX in modalità TAP oppure in linea
- Escludi i siti dalla decrittografia SSL suddividendo gli URL per categoria
- Bilancia il carico di traffico fra i dispositivi della Serie NX

FireEye SSL Intercept 10150

Protezione delle aziende contro gli attacchi e le intrusioni cifrate

La sempre maggiore adozione di protocolli per la protezione del traffico Internet, fra cui il Secure Socket Layer (SSL), sta paradossalmente dando ai criminali informatici un modo per eludere le difese di rete. La crittografia SSL mantiene riservate le comunicazioni rendendo illeggibile il traffico di rete. Tuttavia, questa stessa proprietà ostacola l'ispezione del traffico SSL da parte dei dispositivi di sicurezza di rete, che cercano i segni delle attività ostili. Un crescente numero di criminali informatici usa l'SSL come copertura per infiltrarsi nelle organizzazioni e restare immuni al rilevamento.

L'appliance FireEye SSL Intercept con FireEye Network Security (Serie NX) protegge le aziende da attacchi e intrusioni cifrate. La soluzione FireEye SSL Intercept è un proxy al livello delle applicazioni che dà alla Serie FireEye NX la visibilità sul traffico SSL inattendibile. È studiato per intercettare tutto il traffico di rete desiderato e inoltrarlo alla Serie FireEye NX per l'ispezione. FireEye SSL Intercept decifra temporaneamente, ispeziona e poi cifra nuovamente le sessioni SSL inattendibili, per impedire ai criminali informatici l'uso dell'SSL come copertura al fine di eludere il rilevamento. Con FireEye SSL Intercept le organizzazioni irrobustiscono la protezione della rete, grazie alla maggiore visibilità sul traffico che la attraversa ed ottengono un maggior valore dal proprio investimento nella Serie FireEye NX.

FireEye SSL Intercept è un'appliance di rete ad alte prestazioni che, nella modalità di installazione in linea, è in grado di servire simultaneamente fino a tre dispositivi della Serie FireEye NX. L'abbonamento incluso alla classificazione degli URL consente alle organizzazioni di restare conformi alle rispettive policy sulla privacy, oltre che alle norme di legge. I siti sensibili, come quelli per il banking, e le applicazioni medicali possono essere comodamente esclusi dalla decrittografia SSL in base alla loro categoria oppure singolarmente.

Il vantaggio della combinazione di FireEye SSL Intercept e Serie NX

Studiata per l'utilizzo con tutti i dispositivi FireEye NX Series, l'appliance FireEye SSL Intercept offre un eccezionale valore nelle seguenti tre aree fondamentali.

Visibilità

L'appliance FireEye SSL Intercept consente alla Serie FireEye NX di ispezionare il traffico SSL, sia in entrata che in uscita. Gli aggressori che usano i siti web SSL come quelli della posta basata sul web, dell'archiviazione nel cloud e dei blog, vengono identificati e bloccati dalla Serie FireEye NX. Stesso trattamento ricevono le chiamate in uscita per il comando e il controllo dei server e i kit di exploit per l'accesso tramite secure shell inversa. L'appliance SSL Intercept supporta tutte le versioni SSL/TLS comunemente utilizzate, le chiavi di tutte le lunghezze, le crittografie e gli hash.

La visibilità sul traffico SSL consente alla Serie FireEye NX di connettere tutti gli indicatori di attività ostile con le informazioni strategiche fornite da FireEye Advanced Threat Intelligence (ATI). La significativa automazione delle informazioni strategiche di ATI nella piattaforma FireEye produce una risposta più veloce e più efficace alle minacce avanzate. Il database di classificazione degli URL consente alle organizzazioni di includere ed escludere selettivamente i siti dall'ispezione SSL.

Prestazioni

L'appliance FireEye SSL Intercept supporta un throughput di 20 Gb/s per tutto il traffico HTTP e di 5,5 Gb/s per tutto il traffico SSL con le chiavi a 2048 bit. Grazie a queste velocità può essere impiegata con qualsiasi dispositivo della Serie FireEye NX, senza alcun impatto sulle prestazioni complessive. Le risorse della Serie FireEye NX rimangono dedicate al rilevamento delle minacce informatiche, anziché all'elaborazione SSL di routine, molto intensa dal punto di vista dell'elaborazione. L'architettura di offload SSL aiuta le organizzazioni a realizzare completamente il valore del proprio investimento nella Serie FireEye NX.

Scalabilità

L'appliance FireEye SSL Intercept è in grado di bilanciare il carico di traffico fra due dispositivi della Serie FireEye NX in modalità passiva (TAP) o fra tre di essi in modalità di blocco (in linea). Un gruppo di dispositivi della Serie FireEye NX può elaborare fino a 8 Gb/s di traffico nella modalità passiva e fino a 10 Gb/s nella modalità in linea. L'elevata densità di porta aiuta le aziende a proteggere il proprio investimento e a prepararsi per la futura crescita.

Descrizione del prodotto

L'appliance FireEye SSL Intercept funge da proxy di inoltro trasparente o esplicito per decrittografare i payload SSL e instradare il traffico decifrato alla Serie FireEye NX per l'analisi. Quando il traffico ritorna dalla Serie FireEye NX, FireEye SSL Intercept cifra nuovamente il payload SSL e lo inoltra alla destinazione originale. A seconda della configurazione, quando rileva un attacco, la Serie FireEye NX può inviare una pagina di avviso all'utente, mandare un'email di notifica all'amministratore, bloccare la connessione oppure eseguire varie altre azioni configurabili.

Caratteristiche

FireEye SSL Intercept 10150	
Caratteristiche generali • Servizio Trusted Site Identity (TSID) per bypassare selettivamente i siti web in base alla categoria dell'URL • Riconoscimento Server Name Indication (SNI) per bypassare selettivamente gli host esterni affidabili • Rilevamento del certificato client e bypass opzionale • Gestione dei certificati non attendibili • Riutilizzo dell'ID della sessione SSL	**Gestione** • Interfaccia di gestione dedicata (console, SSH, Telnet, HTTPS) • Interfaccia utente basata sul web con localizzazione linguistica • Interfaccia a riga di comando (CLI) • SNMP, Syslog, avvisi via email, NetFlow v9 e v10 (IPFIX), sFlow • Mirroring delle porte • API XML di tipo REST (aXAPI) • Supporto LDAP, TACACS+, RADIUS
Modalità di distribuzione • Distribuzione in linea con fino a tre dispositivi Serie NX • Distribuzione passiva con fino a due dispositivi Serie NX	

Caratteristiche tecniche

FireEye SSL Intercept 10150	
Throughput totale (100% HTTP)	20 Gbit/s
Throughput ispezione SSL (100% SSL)	5,5 Gbit/s
Flussi TCP simultanei	4.000.000
Sessioni SSL simultanee	400.000
Velocità di configurazione della sessione SSL	15.000 al secondo
Latenza di cut-through	60 us
Versioni SSL	SSL 3.0, TLS 1.0, 1.1 e 1.2
Chiavi RSA	512, 1024, 2048, 4096
Algoritmi delle chiavi pubbliche	RSA, DHE-RSA, ECDHE-RSA, ECDHE-ECDSA con supporto di Perfect Forward Secrecy (PFS)
Algoritmi delle chiavi simmetriche	AES 128, AES 128-GCM, AES 256, AES 256-GCM, ARC4, 3DES, DES,
Algoritmi di hashing	MD5, SHA-1, SHA-2 (SHA-256, SHA-384)
Modalità proxy	Esplicita Trasparente
Numero di porte per il monitoraggio della rete	8 (2 ingresso/uscita, 6 monitoraggio)
Tipi di porte per il monitoraggio della rete	1G/10G Base SX/SR SFP+ 1G/10G Base LX/LR SFP+ 10G Base Cu SFP+ 1G Base T SFP
Modalità delle porte per il monitoraggio della rete	Monitoraggio in linea (massimo 3 coppie di porte) TAP (massimo 2 porte)
Failover per il monitoraggio della rete	Kit di failover attivo esterno (in vendita separatamente)
Numero di porte per la gestione della rete	2
Tipi di porte per la gestione della rete	1G Base T RJ45 – Console 1G Base T RJ45 – Management/IPMI
Involucro	Rack 1U da 19"
Tipo unità	SSD
Dimensioni chassis (LxPxA)	444 x 434 x 44 mm
Alimentatore CA	Ridondante (1+1) da 600 watt, efficienza 80 Plus Platinum, 100 – 240 VCA, 8 – 3 A, 50 – 60 Hz, FRU
Alimentatore di corrente DC	Non disponibile
Ventole di raffreddamento	5 ventole intelligenti e sostituibili a caldo
Consumo energetico tipico/max	240/288 watt
Dissipazione termica massima	819/983 BTU/h
MTBF	91.051 h
Peso sola appliance / con la confezione	10,4 kg / 14,5 kg
Temperatura operativa	Da 0 °C a 40 °C
Temperatura non operativa	Da -20 °C a 70 °C
Umidità operativa relativa	5% - 95% (senza condensa)
Umidità non operativa relativa	5% - 95% (senza condensa)
Altitudine operativa	0 m - 2000 m
Certificazioni di sicurezza	UL/cUL, TUV, CB
Certificazioni EMC/EMI	FCC, CE, VCCI, BSMI, KCC
Conformità normativa	RoHS

Maggiori informazioni

FireEye offre un portafoglio completo di servizi. Per i dettagli completi, scrivici all'indirizzo services@FireEye.com o chiamaci al numero +1 855.692.2052.

Perché FireEye?

Competenza. Tecnologia. Intelligence.

In tutto il mondo FireEye protegge le risorse più preziose dai malintenzionati. La nostra combinazione di tecnologia, intelligence e competenza – potenziata dal team di reazione agli incidenti più efficiente nel settore – elimina l'impatto delle violazioni della sicurezza. Grazie a FireEye, potrai rilevare gli attacchi nel momento stesso in cui si verificano. Diverrai consapevole del rischio costituito da questi attacchi alle tue risorse più preziose. Disporrai delle armi per reagire e neutralizzare gli attacchi velocemente. La FireEye Global Defense Community comprende oltre 3100 clienti di 67 paesi, fra cui 200 imprese della classifica Fortune 500.

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