FORCEPOINT
POWERED BY Raytheon

Datenblatt

Forcepoint™ Stonesoft® Next Generation Firewall

NEXT GENERATION FIREWALLS (NGFW) VON STONESOFT SCHÜTZEN UNTERNEHMENSNETZWERKE VERLÄSSLICH GEGEN ATTACKEN VON AUSSEN UND SIND DANK ECHTZEIT-UPDATES STETHS AUF AKTUELLEM STAND. SO BESTEHT DIE STONESOFT-NGFW AUCH GEGEN RAFFINIERTE VERSCHLEIERUNG DER ANGRIFFE. DABEI IST ES EGAL, OB DIE STONESOFT-NGFW AN WEITEREN FIRMENSITZEN, NIEDERLASSUNGEN ODER RECHENZENTREN ZUM EINSATZ KOMMT ODER ZUM SCHUTZ DES INTERNEN NETZWERKS (PERIMETER-SCHUTZ).

Die Forcepoint Stonesoft Next Generation Firewall (NGFW) verfügt bereits in der Grundausstattung über ein solides Fundament von Sicherheitsfunktionen das granulare Anwendungskontrolle, Intrusion Prevention (IPS), integriertes Virtual Private Network (VPN) und umfassende Untersuchung einzelner Datenpakete („Deep Packet Inspection") in einem effizientem, erweiterbarem und äußerst skalierbarem integriertem Design bietet. Darüber hinaus stehen leistungsstarke Technologien zur Bekämpfung von Ausweichmanövern zur Verfügung, die den Datenverkehr im Netzwerk — noch vor der Analyse und über sämtliche Protokollebenen hinweg — decodieren und normalisieren, um auch die ausgereiftesten Angriffsmethoden zu enttarnen und zu blockieren.

BLOCKIEREN SIE FORTSCHRITTLICHE KOMPROMITTIERUNGS-ANGRIFFE AUF IHRE DATEN

Unternehmen und Organisationen in allen vertikalen Branchen haben nach wie vor mit weitläufigen Datenkompromittierungen zu kämpfen. Jetzt können Sie sich aktiv zur Wehr setzen, indem Sie Datenabfluss auf Anwendungsebene verhindern. Mit dieser Technologie ist Stonesoft NGFW in der Lage, Netzwerkdatenverkehr der von PCs, Laptops, Servern, Netzlaufwerken und anderen Endpunktgeräten ausgeht auf der Basis äußerst detaillierter Endpunkt-Kontextdaten selektiv und automatisch zu sperren. Schutz vor Datenabfluss auf Anwendungsebene ist die einzige Lösung, die über typische Next Generation Firewall-Funktionalität hinausgeht, wenn vertrauliche Daten über unbefugte Programme, Web-Anwendungen, Benutzer oder Kommunikationskanäle von Endpunkten herausgeschleust werden sollen.

ÜBERLEGENE FLEXIBILITÄT HÄLT MIT IHREN SICH VERÄNDERNDEN SICHERHEITSANFORDERUNGEN SCHRITT

Die einheitliche Softwarebasis versetzt die Stonesoft NGFW in die Lage, in dynamischen Unternehmensumgebungen Änderungen von Sicherheitsregeln, von Firewall/VPN über IPS bis hin zu Layer 2 Firewall schnell umzusetzen. Außerdem optimiert die Software auf diese Weise Datenebenen, was unabhängig von der Sicherheitsrolle oder der Anzahl aktiver Sicherheitsfunktionen erhebliche Leistungsvorteile bietet. Um die Flexibilität zusätzlich zu steigern, kann die Stonesoft NGFW in unterschiedlichsten Formaten implementiert werden — als physische Appliance, als Softwarelösung, als virtuelle Appliance oder als virtueller Kontext auf einer physischen Appliance.

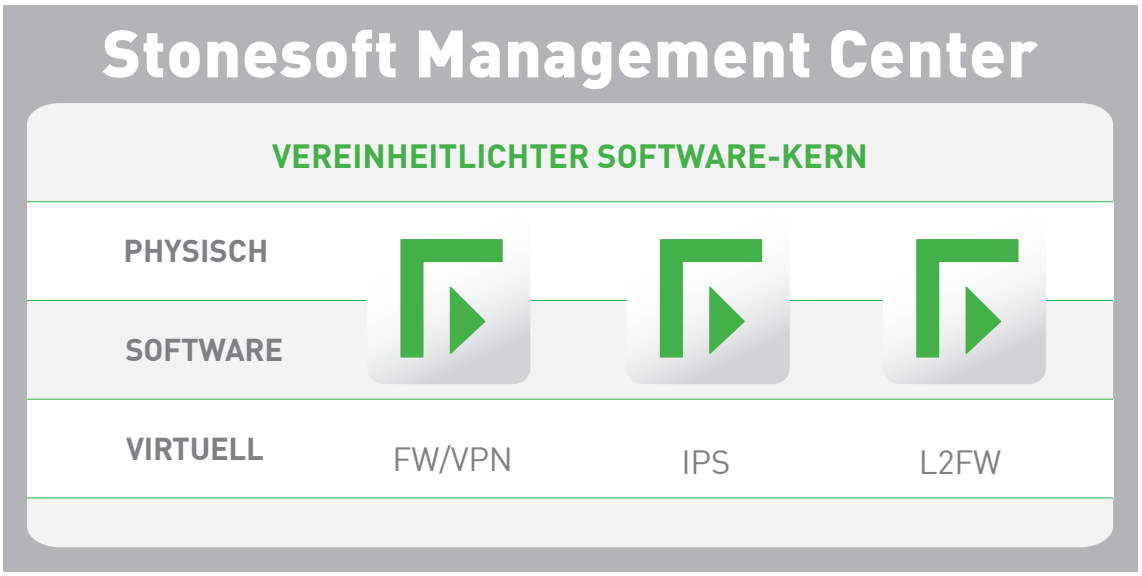
HOHE SKALIERBARKEIT UND VERFÜGBARKEIT SCHÜTZEN IHRE GESCHÄFTSKRITISCHEN ANWENDUNGEN

Unternehmen benötigen heutzutage äußerst widerstandsfähige Netzwerksicherheitslösungen. Die Forcepoint Stonesoft NGFW setzt auf drei leistungsstarke Funktionen, um eine hohe Skalierbarkeit und Verfügbarkeit zu gewährleisten:

- Natives Active-Active-Clustering: Bis zu 16 Knotenpunkte können als Cluster zusammengeführt werden, was bei der Ausführung anspruchsvoller Sicherheitsanwendungen wie Deep Packet Inspektion und VPNs erhebliche Leistungsvorteile und erhöhte Widerstandsfähigkeit bietet.

- Transparentes Session-Failover: Bietet höchste Verfügbarkeit und Bedienbarkeit für Sicherheitssysteme. Die Stonesoft NGFW unterstützt transparentes Failover sogar für mehrere Software- und Hardware-Versionen innerhalb desselben Clusters.

- Multi-Link: Erweitert die hochverfügbare Verfügbarkeit auf Netzwerk- und VPN-Verbindungen. Gewährleistet ununterbrochene Sicherheit sowie höchste Leistung für sämtliche Implementierungen.



UNÜBERTROFFENER SCHUTZ SICHERT DIE EXISTENZ IHRES UNTERNEHMENS

Angreifer werden von Tag zu Tag besser darin, sich Zugang zu Unternehmensnetzwerken, Anwendungen, Rechenzentren und Endpunkten zu verschaffen. Wenn sie einmal eingedrungen sind, können sie geistiges Eigentum, Kundendaten und andere vertrauliche Daten stehlen und damit Ihrem Unternehmen und Ihrem Ruf irreparablen Schaden zufügen.

Einige Angreifer nutzen hochentwickelte Verschleierungstechniken (advanced evasion techniques – AETs), die in der Lage sind, den Großteil der heutzutage eingesetzten Netzwerk-Sicherheitsmaßnahmen zu umgehen. Diese AETs nutzen Verfahren wie Maskierung und Verschleierung, um Malware Stück für Stück über Netzwerkebenen bzw. Protokolle hinweg zu übermitteln. Nachdem sie einmal ins Netzwerk gelangt sind, werden die einzelnen Komponenten der Bedrohung wieder zusammengesetzt und sind in der Lage, sich zu verstecken und über Tage, Monate oder gar Jahre hinweg vertrauliche Daten auszuschleusen.

Die Forcepoint Stonesoft NGFW wendet mehrstufige Verfahren an, um Bedrohungen für den Datenverkehr in Ihrem Netzwerk zu erkennen und um Anwendungen und Benutzer auf einer granularen Ebene zu identifizieren. So können Sicherheitsrichtlinien angewendet werden, die den Vorschriften des Unternehmens entsprechen. Anschließend werden die einzelnen Datenpakete einer speziellen Untersuchung unterzogen, bei der fortschrittliche Verfahren wie Full Stack-Normalisierung und horizontale Datenstream-basierte Inspektionen zur Anwendung kommen. Diese Verfahren sorgen für eine vollständige Normalisierung des Datenverkehrs, sodass jede Stonesoft NGFW in der Lage ist, fortschrittliche Umgehungsmethoden und auffällige Muster im Datenverkehr aufzuspüren, die von anderen Next Generation Firewalls unerkannt bleiben. Erst nachdem der Datenverkehr vollständig normalisiert wurde, kann er korrekt über sämtliche Protokolle und Ebenen hinweg auf Bedrohungen und Malware untersucht werden. Und nur die Stonesoft NGFW hat Tests mit mehr als 800 Millionen fortschrittlichen Umgehungsmethoden erfolgreich bestanden.

DIE WICHTIGSTEN VORTEILE

- Bestmöglicher Schutz für Ihr Unternehmen und ihre digitalen Ressourcen
- Blockiert Versuche, Daten von Endpunkten auszuschleusen
- Lässt sich leicht an Ihre Sicherheitsanforderungen anpassen
- Lässt sich problemlos skalieren, wenn Ihr Unternehmen wächst
- Optimiert die Produktivität von Mitarbeitern und Kunden
- Senkt die Gesamtbetriebskosten für die Sicherheits- und Netzwerkinfrastruktur

DIE WICHTIGSTEN MERKMALE

- Datenorientierte Sicherheitskontrollen
- Schutz vor Datenausschleusung auf Anwendungsebene
- Verhinderung hochentwickelter Umgehungsmethoden
- Vereinheitlichtes Software-Kern-Design
- Zahlreiche Optionen für Sicherheits- und Netzwerkinfrastrukturen
- Leistungsstarke zentralisierte Verwaltung
- Integriertes IPsec und SSL VPN

SPEZIFIKATIONEN DER FORCEPOINT STONESOFT NEXT GENERATION FIREWALL

UNTERSTÜTZTE PLATTFORMEN	
Appliances	Mehrere Hardware-Appliance-Optionen, von Zweigniederlassungs- bis hin zu Rechenzentrumsinstallationen
Software-Appliance	X86-basierte Systeme
Virtuelle Appliance	Unterstützung für VMware ESX, Oracle VM und KVM
Unterstützte Funktionen	• Mit NGF-Lizenz: Firewall/VPN (Layer 3), IPS-Modus (Layer 2), Layer 2 Firewall • Mit FWL-Lizenz: Firewall/VPN (Layer 3)
Virtuelle Kontexte (nur NGF-Lizenz)	Virtualisierung zur Trennung logischer Kontexte (FW, IPS oder L2FW) mit unterschiedlichen Schnittstellen, Adressen, Routing und Richtlinien
FUNKTIONALE ROLLE VON FIREWALL/VPN	
Allgemein	Stateful und Stateless Packet Filtering, Circuit-level Firewall mit TCP Proxy-Protokoll-Agent
Benutzerauthentifizierung	Interne Benutzerdatenbank, LDAP, Microsoft Active Directory, RADIUS, TACACS+
Hochverfügbarkeit	• Active-Active-/Active-Standby-Firewall-Clustering für bis zu 16 Knoten • Zustandsbehaftetes Failover (einschließlich VPN-Verbindungen) • VRRP • Server-Loadbalancing • Link Aggregation (802.3ad) • Link-Ausfallerkennung
ISP Multi-Homing	Multi-Link: Hochverfügbarkeit und Loadbalancing zwischen mehreren ISPs, einschließlich VPN-Verbindungen, Multi-Link VPN Link Aggregation, QoS-basierte Linkauswahl
IP-Adresszuordnung	• FW-Cluster: statisch, IPv4, IPv6 • FW-Einzelknoten: statisch, DHCP, PPoA, PPoE) IPv6 (statisch, SLAAC) • Dienste: DHCP Server und DHCP Relay für IPv4
Adressübersetzung	• IPv4, IPv6 • Statisches NAT, Source NAT mit Portadressenübersetzung (PAT), Ziel-NAT mit PAT
Routing	Statisches IPv4- und IPv6-Routen, richtlinienbasiertes Routing, statisches Multicast-Routing
Dynamisches Routing	IGMP Proxy, RIPv2, RIPng, OSPFv2, OSPFv3, BGP, PIM-SM
IPv6	Dual Stack IPv4/IPv6, ICMPv6, DNSv6
SIP	Erlaubt dynamische RTP-Medienstreams, NAT-Traversal, Deep Inspection, Interoperabilität mit RFC3261-konformen SIP-Geräten
CIS-Umleitung	Umleitung von HTTP-, FTP- und SMTP-Protokollen an Server für Inhaltsuntersuchung (CIS)

SPEZIFIKATIONEN DER STONESOFT NEXT GENERATION FIREWALL (FORTSETZUNG)

IPsec VPN	
Protokolle	IKEv1, IKEv2 und IPsec mit IPv4 und IPv6
Verschlüsselung	AES-128, AES-256, AES-GCM-128, AES-GCM-256, Blowfish, DES, 3DES[1]
Message Digest-Algorithmen	AES-XCBC-MAC, MD5, SHA-1, SHA-2-256, SHA-2-512
Diffie-Hellman	DH Gruppe 1, 2, 5, 14, 19, 20, 21
Authentifizierung	RSA-, DSS- und ECDSA-Signaturen mit X.509-Zertifikaten, Pre-Shared Keys, hybrid, XAUTH, EAP
Sonstiges	• IPCOMP Deflate Compression • NAT-T • Dead Peer Detection • MOBIKE
Site-to-Site VPN	• Richtlinienbasiertes VPN, routenbasiertes VPN (GRE, IP-IP, SIT) • Hub-and-Spoke-, Full-Mesh- und Partial-Mesh-Topologien • Stonesoft Multi-Link dynamische Linkauswahl auf Basis von Fuzzy-Logik • Stonesoft Multi-Link-Modi: Lastverteilung, Active/Standby, Link Aggregation
Mobiles VPN	• VPN-Client für Microsoft Windows • Automatische Konfigurations-Updates vom Gateway • Automatisches Failover mit Multi-Link • Client-Sicherheitsprüfungen • Sichere Domänenanmeldung
SSL VPN (NUR NGF-LIZENZ)	
Client-basierter Zugang	• Unterstützte Plattformen: Android 4.0, Mac OS X 10.7 und Windows Vista SP2 (und neuere Versionen)
Portal-basierter Zugang	• OWA- und Intranet-Zugang über SSL-VPN-Portal über einen Browser

SPEZIFIKATIONEN DER STONESOFT NEXT GENERATION FIREWALL (FORTSETZUNG)

INSPEKTION	
Anti-Botnet	• Entschlüsselungsbasierte Erkennung • Sequenzielle Analyse der Nachrichtenlänge
Dynamische Kontexterkennung	Protokoll-, Anwendungs- und Dateityp
Erweiterte Malware-Bekämpfung	Richtlinienbasiertes Dateifiltern
Sandboxing	Unterstützung für McAfee Advanced Threat Defense
Datei-Reputation	Klassifizierung von McAfee GTI Cloud-Service oder optional von lokalem McAfee Threat Information Exchange
Anti-Malware Engine	McAfee Anti-Malware Engine. Durchsuchte Protokolle: FTP, HTTP, HTTPS, POP3, IMAP, SMTP
Protokollspezifische Normalisierung/ Inspektion/Datenstromhandhabun[3]	Ethernet, H.323, GRE, IPv4, IPv6, ICMP, IP-in-IP, IPv6 Kapselung, UDP, TCP, DNS, FTP, HTTP, HTTPS, IMAP, IMAPS, MGCP, Modbus/TCP, MSRPC, NetBios Datagram, OPC Classic, OPC UA, Oracle SQL Net, POP3, POP3S, RSH, RSTP, SIP, SMTP, SSH, SunRPC, NBT, SCCP, SMB, SMB2, SIP, TCP Proxy, TFTP
Protokollunabhängiges Fingerprinting	Jegliches TCP-/UDP-Protokoll
Erkennen von Umgehungsversuchen und Anomalien	• Mehrstufige Normalisierung des Datenverkehrs • Schwachstellenbasierte Fingerprints • Vollständig aktualisierbare softwarebasierte Inspektions-Engine • Protokollierung von Umgehungsversuchen und Anomalien
Benutzerdefiniertes Fingerprinting	• Protokollunabhängiger Abgleich von Fingerprints • Fingerprintsprache auf Basis regulärer Ausdrücke • Benutzerdefiniertes Fingerprinting für Anwendungen
TLS-Inspektion	• Entschlüsselung und Inspektion von HTTPS-Client und Server-Stream • Validitätsprüfungen für TLS-Zertifikat • Ausnahmeliste auf Basis zertifizierter Domänennamen
Korrelation	Lokale Korrelation, Protokollserverkorrelation
Schutz vor DoS/DDoS	• Erkennung von SYN/UDP Floods • Begrenzung gleichzeitiger Verbindungen, schnittstellenbasierte Protokollkomprimierung • Schutz vor langsamen HTTP-Request-Methoden
Erkundung	TCP/UDP/ICMP-Durchsuchung, Erkennung von Tarnverhalten und langsamen Scans in IPv4 und IPv6
Blockierungsmethoden	Direktes Blockieren, Zurücksetzen von Verbindungen, Negativlisten (lokale und dezentral), HTML-Reaktion, HTTP-Umleitung
Aufzeichnung von Datenverkehr	Automatische Aufzeichnung von Datenverkehr/Auszüge von Missbrauchssituationen
Updates	• Automatische dynamische Updates über Stonesoft Management Center • Aktuelle Abdeckung von ca. 4.700 geschützten Schwachstellen

SPEZIFIKATIONEN DER FORCEPOINT NEXT GENERATION FIREWALL (FORTSETZUNG)

URL-FILTERUNG	
Protokolle	HTTP, HTTPS
Engine	URL-Filterung auf Basis der Webroot-Kategorie, Negativliste/Positivliste
Datenbank	• Mehr als 280 Millionen Top-Level-Domänen und Unterseiten (Milliarden URLs) • Unterstützung für mehr als 43 Sprachen, 82 Kategorien
Sichere Suche	Erzwingen vin Nutzung sicherer Websuchen über Google, Bing, Yahoo und DuckDuckGo
VERWALTUNG & ÜBERWACHUNG	
Verwaltungsoberflächen	• Zentralisiertes Verwaltungs-, Protokollierungs- und Berichtssystem auf Enterprise-Ebene. • Für nähere Einzelheiten, siehe Datenblatt zum Stonesoft Management Center.
SNMP-Überwachung	SNMPv1, SNMPv2c und SNMPv3
Erfassen von Datenverkehr	Konsolen-Tcpdump, Remote-Erfassung über SMC
Hochsichere Managementkommunikation	256-Bit-Sicherheitsstärke für Kommunikation zwischen Engine und Verwaltungsoberfläche
Sicherheitszertifizierungen	Common Criteria EAL4+, FIPS 140-2 Crypto-Zertifikat, CSPN von ANSSI (First Level Security Certification USGv6)

[1] Welche Verschlüsselungsalgorithmen unterstützt werden, hängt von der genutzten Lizenz ab.

[2] Nur Firewall/VPN-Rolle.

[3] Siehe lizenzbezogene Beschränkungen für Firewall.

KONTAKT

www.forcepoint.com/contact

ÜBER FORCEPOINT

[DATASHEET_NEXT_GEN_FIREWALL_DE] 100033.020216