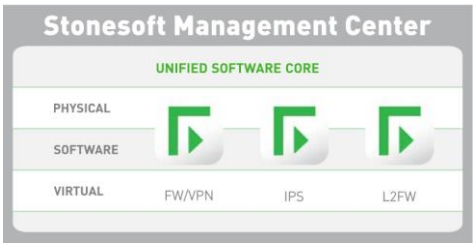
FORCEPOINT
POWERED BY Raytheon

Next Generation Firewall

Modulární bezpečnostní platforma

Forcepoint Stonesoft Next Generation Firewall je vysoce výkonné univerzální řešení, které se vyznačuje především modularitou. Přináší kontrolu a přehled nad síťovým provozem a poskytuje ochranu před pokročilými technikami útoků, které nejsou schopny tradiční zařízení zastavit. Tato platforma je vhodná jak pro vzdálené pobočky společností, tak i pro datová centra, která vyžadují udržení nepřetržitého provozu při zachování maxima bezpečnostních funkcí a výkonu.

Vysoká variabilita řešení



Celé řešení je nabízeno ve třech základních variantách, a to jako software, hardware appliance a virtual appliance. Dále lze volit mezi moduly, které zahrnují next generation firewall, klasický firewall s VPN funkcionalitou a Intrusion Prevention System (IPS) s FW na druhé vrstvě. Pouze dokoupením licencí je možné doplnit funkcionalitu typu filtrování webu, antivir a antispamové ochrany jsou součástí ceny firewallu. Zároveň lze zapojit až 16 zařízení do aktivního clusteru, přičemž jednotlivé firewally nabízejí propustnost až 120 Gbps a všechny jsou spravovány pomocí jednotného managementu (Forcepoint Security Management Center).

Nástroj proti Advance Evasion technikám

Ochranu proti pokročilým technikám útoků zajišťuje vestavěný štít chránící síť proti novým sofistikovaným útokům. Forcepoint Next Generation Firewall analyzuje skutečný obsah datového toku a zajišťuje tak ochranu před známými a neznámými technikami útoků vč. pokročilých perzistentních hrozeb (advanced persistent threats), i když jsou aplikovány na více protokolových vrstvách. Firewall dále zaznamenává a poskytuje podrobné zprávy o všech útocích, které se snaží obejít klasické bezpečnostní řešení. Rozpoznání takového útoku je založeno na normalizaci a inspekci datového toku přes všechny vrstvy OSI/ISO modelu (full stack). Výkonný systém DFA (data-flow analysis) s 64-bitovou pamětí zaručuje, že provedená analýza nemá významný dopad na celkovou propustnost řešení. Forcepoint NGFW byl úspěšně testován na více než 800 milionech pokročilých technik útoků a jejich kombinací.

Advanced Malware Detection (AMD) přesně identifikuje dnešní pokročilý malware – nulovými false positives – díky čemuž se mohou administrátoři přesně zaměřit na skutečné hrozby, kterým čelí síťová infrastruktura. Jelikož AMD interaguje s malwarem, může sledovat každou akci, kterou malware provádí i v tom případě, že jsou tyto škodlivé akce delegovány na operační systém nebo jiné programy. Dokáže objevit i potenciálně nečinný škodlivý kód, který není spuštěn. A to vše díky tomu, že AMD využívá jeden z nejlepších sandboxů na trhu s dynamickou behaviorální analýzou, která odhaluje Zero-Day útoky a další pokročilé hrozby, které mohou být skryty v souborech atd. Díky práci z cloudu doplňuje reputaci souborů a skenování škodlivého softwaru, které jsou integrovány do Next Generation Firewallu. Společně AMD a Forcepoint Next Generation Firewall poskytují velmi účinný a efektivní způsob, jak vyhledat škodlivý kód a rychle ho zablokovat, než útočníci stihnout porušit Vaši síť a začnou krást data. Bezkonkurenční přesnost technologie AMD byla oceněnana i NSS Labs, kdy tato technologie prošla všemi testovacími kategoriemi se 100% úspěšností detekce.

Vysoká dostupnost a škálovatelnost

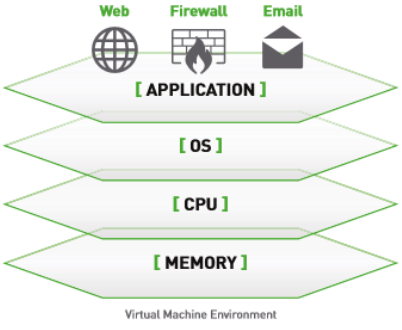
Forcepoint Next Generation Firewall je vybaven vestavěnou funkcí clusteru a umožňuje propojení až 16 aktivních appliancí s provozní rychlostí až 120 Gb a bez nutnosti využití produktů třetích stran. Vysoká dostupnost a vysoký výkon vyhoví i těm nejnáročnějším nasazením. Všechna zařízení v clusteru jsou spravována pomocí centrálního managementu a do clusteru mohou být zapojena zařízení ve formě hardwaru, virtuální appliance, softwaru nebo jejich kombinací. Další výhodu představuje možnost vytvoření virtuální kontextů na firewallu, kdy pomocí licence lze rozdělit firewall na více nezávislých logických celků, pro které lze separátně vytvářet a aplikovat různé politiky.

Centrální správa

Forcepoint Security Management Center powered by Stonesoft zahrnuje jeden server pro správu a jeden pro ukládání logů, který může být umístěn na stejném nebo separátním fyzickém serveru. Centrální management je navržen pro správu rozsáhlých geograficky oddělených sítí. Nabízí možnost distribuce konfigurací pro všechna zařízení pod jeho správou, monitorování, informace o stavu firewallů, provádění vzdálených updatů a upgradů a generování podrobných zpráv. Navíc umožňuje monitorovat zařízení od dalších výrobců (200 per log server) a přijímat logy ve formátech CEF, LEEF, CLF a WELF. Dále umožňuje sběr a zpracování dat z protokolů NetFlow v9 a IPFIX.

Přínosy

- Dostupnost ve formě softwaru, hardwarové nebo virtuální appliance,
- možnost zapojení až 16 zařízení do aktivního clusteru,
- **ochrana proti Advanced Evasion technikám, Advanced Malware Detection (AMD)**
- sběr logů a jejich vyhodnocení i od dalších výrobců (základní SIEM funcionalita),
- Load Balancing a ISP Link Balancing,
- virtuální kontexty,
- ochrana proti DoS a DDoS útokům,
- pokročilé funkce QoS,
- Client-based a portal-based SSL VPN,
- automatické updaty zranitelností přes SMC,
- certifikace Common Criteria EAL 4+, FIPS 140-2, ICSA Labs,
- **možnost volby síťových modulů.**



Deep Content Inspection Delivers Unmatched Visibility

COMGUARD
security & networking

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel.: + 420 513 035 400
info@comguard.cz | **www.comguard.cz**

FORCEPOINT
POWERED BY Raytheon

Next Generation Firewall

Přehled hlavních funkcí, vlastností modelů

Obecné vlastnosti

- Softwarové appliance podporují systémy založené na X86.
- Virtuální appliance podporují VMware ESX a KVM platformu.
- Podporované role: Firewall/VPN (2. vrstva), IPS/IDS (2. vrstva), Firewall na 2. vrstvě
- **Virtuální kontexty:** virtualizace FW/VPN, virtualizace pro oddělení logických enginů s rozdílným rozhraním, politikami, adresováním a routováním

Funkcionalita Firewall/VPN

- Firewall provádí filtrování paketů a obsahuje TCP proxy.
- Podporované protokoly: FTP, H.323, HTTP, HTTPS, IMAP4, MGCP, MS RPC, NetBios Datagram, Oracle SQL Net, POP3, RSH, SCCP, SIP, SMTP, SSH, SunRPC, TCP Proxy, TFTP
- Autentizace uživatelů: interní databáze uživatelů, LDAP, MS Active Directory, RADIUS, TACACS+
- **IPSec VPN**
  - Podporované protokoly: IKEv1, IKEv2, and IPsec with IPv4 and IPv6v6
  - Šifrování VPN: AES-128, AES-256, AES-GCM-128, AES-GCM-256, Blowfish, DES, 3DES
  - Kontrolní algoritmy zpráv: AES-XCBC-MAC, MD5, SHA-1, SHA-2-256, SHA-2-512
  - Autentizace: RSA, DSS, ECDSA signatury s X.509 certifikátem, před sdílené klíče, hybridní, XAUTH, EAP

  Site-to-site VPN:
  - Policy-based VPN, Route-Based VPN (GRE, IP-IP, SIT)
  - Hub and spoke, full mesh, partial mesh topologies
  - Dynamický výběr linek založen na Multilink fuzzy-logic
  - Multilink režimy: sdílení zátěže, active/standby, agregace linek

  Client-to-gateway VPN:
  - IPsec VPN klient pro Microsoft Windows
  - Automatické aktualizace konfigurací získané z firewallu
  - Automatický failover s multilinkem
  - Bezpečnostní kontrola klientů
  - Zabezpečený přístup do domény
- **SSL VPN**
  - Klientský přístup: podporované platformy: Android 4.0, Mac 10.7 a Windows Vista SP2 a vyšší verze
  - Přístup přes portál: OWA nebo webový prohlížeč přes SSL VPN
- **High Availability**
  - Active-active/active-standby firewall clustering up to 16 nodes
  - Stateful failover (včetně VPN connections)
  - VRRP
  - Server load balancing
  - Link aggregation (802.3ad)
  - Link failure detection
- **ISP Multihoming:** vysoká dostupnost a load balancing mezi linkami od více ISP, včetně VPN spojení, multilink VPN link aggregation, výběr linek založen na QoS
- **Přidělování IP adress:**
  - FW cluster: statické, IPv4, IPv6
  - FW single nodes: statické, DHCP, PPPoA, PPPoE, IPv4, statické IPv6
  - Služby: DHCP Server a DHCP relay pro IPv4
- **Překlad adres:** IPv4, IPv6, statický NAT, zdrojový NAT s port address translation (PAT), cílový NAT s PAT
- **Routování:** Static IPv4 and IPv6 routes, policy-based routing, static multicast routing
- **Dynamické routování:** IGMP proxy, RIPv2, OSPFv2,BGP, PIM-SM
- **SIP:** umožňuje dynamicky streamovat RTP media, NAT traversal, hloubková inspekce, spolupráce se zařízeními SIP dle standardu RFC3261
- **CIS:** Přesměrování protokolů HTTP, FTP a SMTP na content inspection server

IPS a Layer 2 Firewall

- **Obecné vlastnosti:**
  - Bezstavové filtrování paketů pro protokoly Ethernet (Dix/IEEE)
  - Stavové filtrování paketů pro IP protokoly
  - VLAN re-tagging
  - Filtrování MAC adress
  - Přiřazování logických a fyzických rozhraní pro VLAN
- **Vysoká dostupnost (HA):**
  - Layer 2 firewall clustering (active-passive)
  - IDS clustering (active-active/active-passive)
  - IPS serial clustering (active-active)
  - Podpora pro fail-open rozhraní (IPS role)
  - Dynamická inspekce pro overload handling (IPS role)

Funkcionalita podporovaná všechny moduly

- **Zapouzdření:** Ethernet, 802.1q VLAN; pouze pro FW/VPN: PPPoA, PPPoE
- **Řízení přístupu:** IPv4 a IPv6 tunelované IP, IP-in-IP, zapouzdření IPV6, GRE
- **Pokročilé řízení přístupu:** zóny rozhraní, čas, informace TLS, doménová jména, informace o uživatelích, aplikace
- **Správa provozu a QoS:** traffic shaping na základě politik, priority pro garantované / maximální /přenosové pásmo, Differentiated services code point (DSCP), matching/marking, Concurrent session limiting, Přepisování TCP MSS na základě politik
- **Anti-Botnet:** detekce založená na dešifrování, sekvenční analýza délky zpráv
- **McAfee Antivirus**:
  - Skenování protokolů: HTTP, HTTPS, POP3,IMAP, SMTP a FTP
  - Skenování založené na typech souborů, databáze lokálních signatur, automatické updaty v reálném čase
- **Filtrování dle reputace souborů:** na základě politik, kategorií (exe, archivy, soubory typu média, MS Office dokumenty), typů (Flash, GIF, JPEG, MPEG, OLE, PDF, PNG, Riff, RTF, ZIP), klasifikace na základě GTI
- **Možnost přesměrování souborů do Advanced Threat Defense**
- **Dynamická detekce obsahu:** protokoly, aplikace, Typy souborů (Flash, GIF, JPEG, MPEG, OLE, PDF, PNG, RIFF, RTF, textové soubory, binární soubory)
- **Normalizace protokolů:** úplná normalizace protokolů pro Ethernet, IPv4, IPv6, ICMP, UDP, TCP, DNS, FTP, HTTP, IMAP, IMAPS, SMTP, SSH, NBT, SMB, SMB2, MSRPC, POP3, POP3S, SIP, TFTP, HTTPS (SSL/TLS), GRE, IP-in-IP, zapouzdřené IPv6
- **Specifická inspekce protokolů:** DNS, FTP, HTTP, IMAP, IMAPS, SMTP, SSH, NBT, SMB, SMB2, MSRPC, POP3, POP3S, SIP, TFTP, HTTPS
- Fingerprinting pro protokoly UDP / TCP
- **Antispam**:
  - Skenování protokolu SMTP
  - Detekce spamu na základě skóre
  - Přizpůsobitelná kontrola na základě obálky/hlavičky/obsahu emailů
  - Lokální antispoofing a relay
  - Honeypot filtering
  - Přiřazování záznamů SPF/MX
  - Blacklist založený na DNS
- **Detekce anomálií a evasion technik:** normalizace provozu na více vrstvách OSI modelu, fingerprinty založené na zranitelnostech, možnost upgrade softwarově založeného inspekčního engine, logování evasion technik a anomálií
- **Fingerprinting:** přiřazování otisků protokolů, otisky založené na regulárních výrazech, konvertor Snort signatur, otisky zvolených aplikací
- **Inspekce TLS:** dešifrování HTTPS na straně klienta i serveru
- **DoS/DDoS protection:** SYN/UDP flood detection
- Skenování TCP/UDP/ICMP, detekce pomocí skenování stealth and slow
- **Korelace:** lokální korelace, korelace na log serveru
- Metody blokování: přímé blokování, reset připojení, blacklist (lokální, distribuovaný), přesměrování, HTML response
- Automatické zaznamenávání provozu
- Automatické updaty přes Forcepoint Security Management Center chrání před více jak 4000 zranitelností
- **Filtrování webu** (vyžaduje dokoupení licence):
  - Kontrola protokolů HTTP a HTTPS
  - Filtrování založena na 82 kategoriích stránek, blacklist / whitelist
  - Databáze obsahuje více jak 280 mil top-level domén, podporuje více jak 43 různých jazyků
- **Management a monitorování:**
  - Monitorování SNMP: SNMPv1, SNMPv2c, and SNMPv3
  - Zachycení provozu: tcpdump, vzdálené zachycení přes SMC
  - Zabezpečená komunikace s centrální správou pomocí 256-bit enginu
- **Síťové moduly:**
  - 8 port nebo 4 port RJ45
  - 4 port SFP modul
  - Gigabit Fail-Open moduly: 4 port RJ45, 2 port optický LC modul, 4 port optický LC modul (pouze IPS)
  - 2 port nebo 4 port 10 Gigabit Ethernet modul
  - 10 Gigabit Fail-Open moduly: 2 port 10Gbps RJ45, 2 port LR nebo SR modul (pouze IPS)
  - 2 port 10 Gigabit RJ45 modul

Model Next Generation FW	110 / 115	321 / 325	1035 /1065	1401/1402	3201 / 3207	3305
Celková propustnost	1,5 Gbps	4 Gbps	10 / 20 Gbps	30/40 Gbps	80 / 120 Gbps	160 Gbps
Propustnost při inspekci	0,5 Gbps	0,85 Gbps	1 / 3 Gbps	8/14 Gbps	30Gbps	30 Gbps
Met. Ethernet rozh./max.	10	5 / 13	4 / 12	4/20 // 4/20	2 -34/ 2 - 26	2 / 34
10G porty	0	0	Až 4	Až 8/8	Až 16 / až 12	Až 16
40G porty	0	0	0	Až 4 / až 4	Až 8 / až 6	1 / 9
Přídavný modul (rozh.)	- / 1	- / 2	1	2/2	4/3	4
IPSec VPN AES-128-GCM	500 Mbps	1000 Mbps	1200 / 3000 Mbps	6/11 Gbps	18 / 20 Gbps	22 Gbps
Maximum SSL VPN portal uživ.	-	500	1 000 / 2000	5 000 / 10 000	20 000 / 30 000	30 000
Počet IPSec VPN tunelů	500	6 000	20 000	20 000 / 20 000	200 000	200 000
Současná spojení	1 mil.	2 mil.	5 / 8 mil.	12 / 20 mil.	30 / 40 mil.	50 mil.
Nová spojení (TCP) za sek.	10 000	15 000	35 000 / 100 000	150 000/200 000	300 000/400 000	500 000
Současná spojení. inspekce	100 000	100 000	150 000 / 1 mil.	4 / 6 mil.	12 / 14 mil.	15 mil.
Inspekce HTTP	150 Mbps	200 Mbps	400 / 1200 Mbps	3 / 4,5 Gbps	9 / 11 Gbps	15 Gbps
Inspekce SSL/TLS	100 Mbps	150 Mbps	150 / 500 Mbps	2 / 1,5 Gbps	5 / 8 Gbps	14 Gbps
Virtuální kontexty (inc/max)	-	3/3	5/5	5/25 – 10/100	10/100 // 25/250	10/250
Redundantní zdroj	NE	NE	NE	Volitelně / ANO	ANO	ANO
Velikost HW appliance	Desktop	Desktop	1U	1U/1U	2U	2U
Certifikace	ICSA Labs IPSec VPN, **Common Criteria EAL4+**, **FIPS 140-2, Level 2**, **CSPN by ANSSI**					
Forcepoint fw Virtual appliance	Podpora pro 1, 2, 4, 8, 16, 32 jader (Software appliances) nebo 1, 2, 4, 8 CPU alokovaných jader (virtuální appliance)					

COMGUARD
security & networking

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel.: + 420 513 035 400
info@comguard.cz | **www.comguard.cz**