FORCEPOINT
POWERED BY Raytheon

Karta produktu

Forcepoint Next Generation Firewall

FORCEPOINT NEXT GENERATION FIREWALL (NGFW) ŁĄCZY I ZABEZPIECZA CENTRA DANYCH, OBRZEŻA SIECI, ODDZIAŁY PRZEDSIĘBIORSTW O STRUKTURZE ROZPROSZONEJ I CHMURĘ, Z NAJWYŻSZYM POZIOMEM BEZPIECZEŃSTWA, ZARZĄDZANIA I DOSTĘPNOŚCI. KLIENCI, KTÓRZY WDRAŻAJĄ ROZWIĄZANIE NGFW FORCEPOINT, ODNOTOWUJĄ 86% SPADEK LICZBY CYBERATAKÓW, MNIEJSZE O 53% NAKŁADY PONIESIONE NA IT ORAZ 70% MNIEJ CZASU POŚWIĘCONEGO NA UTRZYMANIE.*

***"Quantifying the Operational and Security Results of Switching to Forcepoint NGFW", R. Ayoub & M. Marden, IDC Research, May 2017.**

Forcepoint Next Generation Firewall (NGFW) łączy warstwę sieci z najlepszymi w branży zabezpieczeniami w celu ochrony użytkowników i danych w szybko zmieniających się środowiskach sieciowych nowoczesnych przedsiębiorstw. Dzięki rozwiązaniom NGFW zaprojektowanym od podstaw, zapewniającym wysoką dostępność i skalowalność oraz scentralizowanemu zarządzaniu z pełną widocznością 360°, Forcepoint zapewnia spójne bezpieczeństwo, wydajność i łatwość zarządzania systemami fizycznymi, wirtualnymi oraz działającymi w chmurze.

Forcepoint w wyjątkowy sposób łączy kontrolę dostępu i inspekcji każdego połączenia, zapewniając jednocześnie wysoką wydajność i bezpieczeństwo na najwyższym poziomie. Dostarcza kontrolę aplikacji, mechanizm wykrywania i zapobiegania włamaniom (IPS), wbudowaną obsługę wirtualnych sieci prywatnych (IPSec i SSL VPN) oraz proxy aplikacyjne, wszystko za pomocą wydajnego, rozszerzalnego i wysoce skalowalnego systemu. Nasze zaawansowane technologie zapobiegające obejściom zabezpieczeń (AET), dekodują i normalizują ruch sieciowy na wszystkich warstwach protokołu IP jeszcze przed ich dogłębną inspekcją, w celu wykrycia i zablokowania najbardziej zaawansowanych metod ataku.

BLOKADA ZAAWANSOWANYCH ATAKÓW NARUSZENIA BEZPIECZEŃSTWA DANYCH

Firmy i organizacje z różnych branż nieustannie padają ofiarami spektakularnych naruszeń bezpieczeństwa danych. Teraz możesz im zapobiec dzięki ochronie przed eksfiltracją danych w warstwie aplikacji. Rozwiązania NGFW Forcepoint mogą selektywnie i automatycznie umieszczać na białej lub na czarnej liście ruch sieciowy z poszczególnych aplikacji zainstalowanych na komputerach PC, laptopach, serwerach plików i innych urządzeniach końcowych w oparciu o bardzo szczegółowe dane kontekstowe. Wykracza to poza typowe zapory ogniowe, dzięki czemu możliwe jest zapobieganie eksfiltracji wrażliwych danych z punktów końcowych za pośrednictwem nieautoryzowanych programów, aplikacji webowych, użytkowników i kanałów komunikacyjnych.

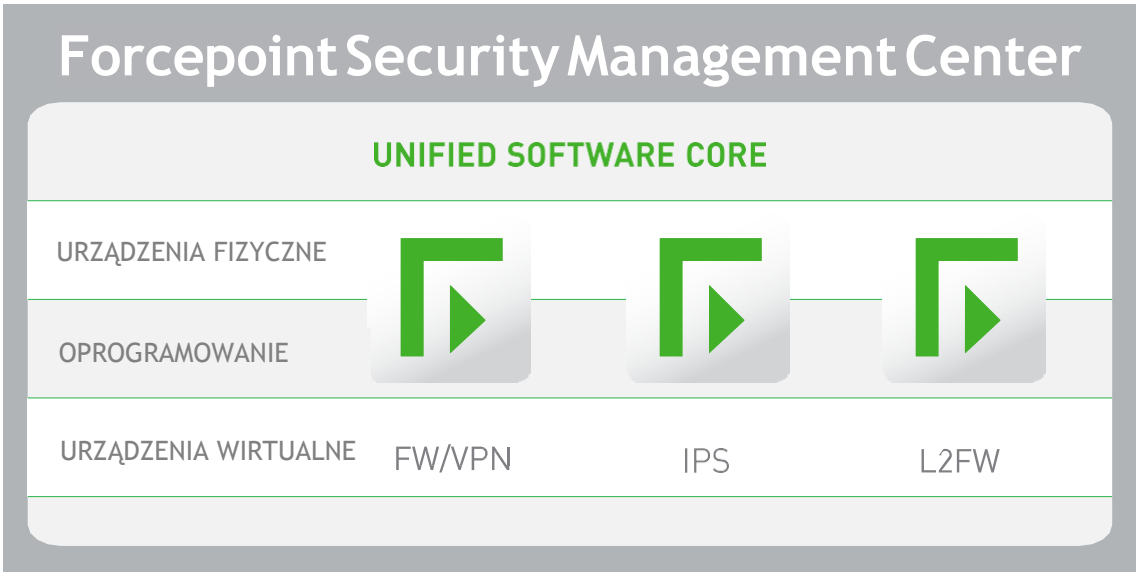
WYJDŹ NAPRZECIW ZMIENIAJĄCYM SIĘ POTRZEBOM ZABEZPIECZEŃ

Zunifikowane oprogramowanie umożliwia rozwiązaniom NGFW Forcepoint łatwą zmianę ról bezpieczeństwa w dynamicznych środowiskach biznesowych, od zapory ogniowej/VPN, IPS po zaporę warstwy 2. Rozwiązania NGFW Forcepoint można wdrażać na różne sposoby: w formie urządzeń fizycznych, wirtualnych i w chmurze. Wszystkie zarządzane są za pomocą jednej konsoli zarządzającej.

TWOJE NAJWAŻNIEJSZE APLIKACJE ZABEZPIECZONE DZIĘKI WYSOKIEJ SKALOWALNOŚĆ I DOSTĘPNOŚĆ

Firmy szukają skutecznych rozwiązań dla zapewnienia bezpieczeństwa sieci. System NGFW Forcepoint zapewnia wysoką skalowalność i dostępność na wszystkich poziomach:

- Klastrowanie typu active-active lub active-standby: klastrować można do 16 węzłów różnych modeli sprzętowych działających w oparciu o różne wersje oprogramowania, zapewniając doskonałą elastyczność, wydajność i wysoką dostępność dla krytycznych usług takich jak VPN.
- Bezproblemowe aktualizacje polityki bezpieczeństwa i uaktualnień oprogramowania: najlepsza w branży dostępność i zarządzanie systemem bezpieczeństwa Forcepoint umożliwia bezproblemowe aktualizacje polityki bezpieczeństwa, oraz aktualizacje oprogramowania bez przerywania ciągłości usług, i to nawet w przypadku klastra.
- Klastrowanie sieci SD-WAN: Rozszerza zakres wysokiej dostępności na połączenia sieciowe i VPN. Zapewnia skuteczność zabezpieczeń oraz ich wysoką dostępność, które mogą teraz korzystać z lokalnych połączeń szerokopasmowych w celu uzupełnienia lub zastąpienia kosztownych łączy dzierżawionych, takich jak np. MPLS.



BEZPIECZEŃSTWO TWOJEGO BIZNESU

Każdego dnia hakerzy stają się coraz skuteczniejsi w penetrowaniu sieci korporacyjnych, aplikacji, centrów danych i punktów końcowych. Gdy dostaną się do środka, mogą ukraść własność intelektualną, informacje o klientach i inne wrażliwe dane, powodując nieodwracalne szkody dla działania firmy i jej reputacji.

Coraz częściej używają oni zaawansowanych technik obejść zabezpieczeń (ang. advanced evasion techniques, AET), które są w stanie ominąć większość dzisiejszych urządzeń zabezpieczających sieć. Techniki AET wprowadzają do sieci exploity i złośliwe oprogramowanie dzieląc je i transmitując na różnych warstwach sieci lub protokołów za pomocą technik takich jak „masking" i „obfuscation". Gdy zawartość zostanie dostarczona i zrekonstruowana, ataki takie mogą pozostać w ukryciu przez dni, miesiące a nawet lata, powodując eksfiltrację danych.

Rozwiązanie NGFW Forcepoint stosuje warstwowe techniki wykrywania zagrożeń w ruchu sieciowym, szczegółowo identyfikując aplikacje iużytkowników, tak by polityki bezpieczeństwa mogły zostać wdrożone zgodnie z procesami biznesowymi. Następnie przeprowadza wyspecjalizowaną, dogłębną inspekcję, stosując zaawansowane techniki, takie jak pełna normalizacja stosu IP i kontrola w oparciu o tzw. „data stream-based inspection". Dzięki tym technikom NGFW Forcepoint może odpowiednio kontrolować wszystkie protokoły i warstwy w celu ujawnienia AET i anomalii w ruchu sieciowym, które często omijają konkurencyjne zapory nowej generacji.

Ponadto rozwiązanie NGFW Forcepoint zapewnia wysokowydajne deszyfrowanie zaszyfrowanego ruchu, takiego jak połączenia HTTPS, wraz ze szczegółowymi mechanizmami kontroli prywatności, które chronią firmę i użytkowników w szybko zmieniającym się świecie. NGFW może nawet ograniczyć dostęp do wybranych aplikacji końcowych w celu blokowania urządzenia lub uniemożliwienia korzystania z nieaktualnego oprogramowania.

GŁÓWNE KORZYŚCI

- Najlepsza ochrona twojej firmy i zasobów cyfrowych
- Blokuje próby eksfiltracji danych z punktów końcowych
- Łatwo dostosowuje się do wymogów bezpieczeństwa
- Bezproblemowo skaluje się w miarę rozwoju firmy
- Optymalizuje produktywność pracowników i klientów
- Obniża TCO dotyczące bezpieczeństwa i infrastruktury sieci

GŁÓWNE CECHY

- Wydajne deszyfrowanie dzięki szczegółowej kontroli prywatności
- Biała lista/czarna lista dla aplikacji klienckich i możliwość blokady urządzenia
- Ochrona przed eksfiltracją warstwy aplikacji
- Zaawansowana ochrona przed technikami obchodzenia zabezpieczeń (AET)
- Zunifikowana warstwa oprogramowania
- Wiele opcji dla zabezpieczenia infrastruktury sieci
- Wydajne scentralizowane zarządzanie
- Wbudowany IPsec i SSL VPN
- Proxy aplikacyjne „Sidewinder" dla krytycznych aplikacji

SPECYFIKACJA FORCEPOINT NEXT GENERATION FIREWALL (NGFW)

OBSŁUGIWANE PLATFORMY	
Urządzenia	Wiele wersji sprzętowych/modularnych przeznaczonych dla centrów danych, obrzeży sieci i oddziałów firmy
Infrastruktura chmury	Amazon Web Services, Microsoft Azure
Urządzenie wirtualne	Systemy x86 64-bit; VMware ESXi, VMware NSX, Microsoft Hyper-V i środowisko wirtualizowane KVM
Punkty końcowe (endpoints)	Endpoint Context Agent (ECA)
Obsługiwane role	Firewall/VPN (layer 3), tryb IPS (layer 2), Layer 2 Firewall oraz tryb mieszany (Layer2/Layer3)
Konteksty wirtualne	Oddzielne, wirtualne konteksty logiczne (FW, IPS lub L2FW) - separacja interfejsów, adresowania, trasowania i polityk dla każdego wirtualnego kontekstu w obrębie pojedynczego urządzenia fizycznego typu Master
FUNKCJONALNA ROLA FIREWALL/VPN	
Ogólna	Filtrowanie typu stateful i stateless, deep inspection, zaawansowane proxy aplikacyjne dla HTTP, HTTPS i SSH, ogólne proxy aplikacyjne dla TCP i UDP oraz biała/czarna lista w według nazwy i wersji aplikacji
Uwierzytelnianie	Baza użytkowników wewnętrznych, LDAP, Microsoft Active Directory, RADIUS, TACACS+, Forcepoint User ID (FUID) Services
Wysoka dostępność	• Klastrowanie active-active/active-standby do 16 węzłów • Stateful failover (w tym połączenia VPN) • Równoważenie obciążenia dla serwerów za zaporą • Agregacja łączy (802.3ad) • Wykrywanie awarii łączy
ISP Multi-Homing	Multi-Link network clustering: wysoka dostępność i równoważenie obciążenia między wieloma ISP, w tym połączeniami VPN, agregacja łączy Multi-Link VPN, selekcja łączy na podstawie polityki QoS
Przypisywanie adresu IP	• Klastry FW: static, IPv4, IPv6 • Pojedyncze węzły FW: IPv4 static, DHCP, PPPoA, PPPoE; IPv6 static, SLAAC, DHCPv6 • Usługi: DHCP Server dla IPv4 i DHCP Relay dla IPv4
Translacja adresów	• IPv4, IPv6 • Static NAT, źródłowy NAT z translacją portów (PAT), docelowy NAT z PAT
Trasowanie	Static IPv4 i IPv6, policy-based routing, static multicast routing
Trasowanie dynamiczne	IGMP proxy, RIPv2, RIPng, OSPFv2, OSPFv3, BGP, PIM-SM, PIM-SSM
IPv6	Dual stack IPv4/IPv6, ICMPv6, DNSv6
SIP	Pozwala na dynamiczny stream RTP, NAT traversal, deep inspection, zgodność z urządzeniami SIP (RFC3261)
Przekierowanie CIS	Przekierowanie protokołów HTTP, FTP, SMTP do serwera content inspection server (CIS)
Geo-Protection	Kontrola dostępu wg kraju lub kontynentu
Lista adresów IP	Kontrola dostępu wg predefiniowanych kategorii IP lub wykorzystanie własnych list adresów IP
Lista adresów URL	Kontrola dostępu wg wlasnych list adresów URL
Lista aplikacji końcowych	Kontrola dostępu wg nazwy i wersji aplikacji
Sidewinder Security Proxies	TCP, UDP, HTTP, HTTPS, SSH
Forcepoint Web Security Redirect	Przekierowuje ruch HTTP/HTTPS do Forcepoint Cloud Web Security za pomocą tunelu IPSec dla ruchu wchodzącego/wychodzącego

SPECYFIKACJA FORCEPOINT NEXT GENERATION FIREWALL (NGFW) C.D.

IPsec VPN	
Protokoły	IKEv1, IKEv2 i IPsec z IPv4 i IPv6
Szyfrowanie	AES-128, AES-256, AES-GCM-128, AES-GCM-256, Blowfish, DES, 3DES
Algorytmy Message Digest	AES-XCBC-MAC, MD5, SHA-1, SHA-2-256, SHA-2-512
Diffie-Hellman	DH group 1, 2, 5, 14, 15, 16, 17, 18, 19, 20, 21
Uwierzytelnianie	Sygnatury RSA, DSS, ECDSA z certyfikatami X.509, pre-shared keys, hybrid, XAUTH, EAP
Inne	• IPCOMP deflate compression • NAT-T • Dead peer detection • MOBIKE
Site-to-Site VPN	• Policy-based VPN, Route-based VPN • Wsparcie dla topologii: Hub and Spoke, Full mesh, Partial mesh • Dynamiczny wybów łącza (fuzzy-logic) Multi-Link NGFW Forcepoint • Tryby Multi-Link NGFW Forcepoint: load-balancing, active/standby, link aggregation
Mobilny VPN	• Klient VPN dla Microsoft Windows • Automatyczna aktualizacja konfiguracji pobierana z VPN gateway • Automatyczny failover z Multi-Link • Kontrola stanu zabezpieczeń klienta • Bezpieczne logowanie do domeny
SSL VPN	
Client-Based Access	Obsługiwane platformy: Android 4.0, Mac OS X 10.7 i Windows Vista SP2 (i nowsze wersje)
Clientless Access *(niedostępny dla modeli 110 i 115)*	Dostęp Web Portal do usług opartych na HTTP za pomocą predefiniowanych serwisów i URL

SPECYFIKACJA FORCEPOINT NEXT GENERATION FIREWALL (NGFW) C.D.

KONTROLA	
Anti-Botnet	• Wykrywanie oparte na deszyfrowaniu transmisji • Analiza sekwencji długości komunikatów
Dynamic Context Detection	Protokół, aplikacja, typ pliku
Protocol-Specific Normalization/ Inspection/Traffic Handling	Ethernet, H.323, GRE, IPv4, IPv6, ICMP, IP-in-IP, enkapsulacja IPv6, UDP, TCP, DNS, FTP, HTTP, HTTPS, IMAP, IMAPS, MGCP, 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, zintegrowana kontrola za pomocą proxy Sidewinder
Protocol-Independent Fingerprinting	Każdy protokół TCP/UDP
Wykrywanie prób obejścia zabezpieczeń (AET) i anomalii ruchu sieciowego	• Wielowartswowa normalizacja ruchu sieciowego • Fingerprint w oparciu o podatności • W pełni rozbudowany, oparty na oprogramowaniu silnik inspekcji • Logowanie prób obejścia i anomalii
Custom Fingerprinting	• Dopasowanie fingerprint'u niezależnie od protokołu • Tworzenie własnych fingerprint z użyciem regular expression • Fingerprint dla własnych, niestandardowych aplikacji
Kontrola TLS/SSL	• Deszyfrowanie i inspekcja HTTPS (dla serwerów i klientów) • Sprawdzanie ważności certyfikatu TLS • Lista wyjątków na podstawie nazwy domeny certyfikatu
Korelacja	Korelacja lokalna, korelacja na serwerze logów
Ochrona DoS/DDoS	• Wykrywanie SYN/UDP flood • Ograniczanie ilości jednoczesnych połączeń, kompresja logów per interfejs • Ochrona przed slow HTTP request, limit półotwartych połączeń • Rozdzielenie Control Plane i Data Plane
Rozpoznanie skanowania	Skan TCP/UDP/ICMP, wykrywanie metod stealh i slow scan w IPv4 i IPv6
Metody blokowania	Bezpośrednie blokowanie, resetowanie połączenia, blacklisting (lokalny i rozproszony), HTML response, HTTP redirect
Rejestracja ruchu	Automatyczna rejestracja ruchu/pcap z zapisem ataku
Aktualizacje	• Dynamiczne aktualizacje za pomocą Forcepoint Security Management Center (SMC)

SPECYFIKACJA FORCEPOINT NEXT GENERATION FIREWALL (NGFW) C.D.

FILTROWANIE ADRESÓW URL	
Kategoryzacja URL	Za pomocą Forcepoint ThreatSeeker Intelligence, taki sam jak w przypadku Forcepoint Web Security i Forcepoint Email Security
Własne listy URL	Dopasowanie dla własnych zestawów list URL
Protokoły	HTTP, HTTPS
Baza danych	• Ponad 280 milionów domen najwyższego poziomu i podstron (miliardy adresów URL) • Obsługa ponad 43 języków, 82 kategorii
Safe Search	Wymuszenie użycia Safe Search w wyszukiwarkach internetowych Google, Bing, Yahoo, DuckDuckGo
ZAAWANSOWANE WYKRYWANIE ZŁOŚLIWEGO OPROGRAMOWANIA I KONTROLA PLIKU	
Protokoły	FTP, HTTP, HTTPS, POP3, IMAP, SMTP
Filtrowanie plików	Polityka filtrowania plików. Ponad 200 obsługiwanych typów plików w 19 kategoriach
Reputacja pliku	Kontrola i blokowanie złośliwego oprogramowania na podstawie reputacji pliku (usługa w chmurze). Opcjonalne, lokalna kontrola reputacji z pomocą McAfee TIE przez DxL.
Antywirus	Lokalny silnik antywirusowy*
Zero-Day Sandboxing	SANDBOX - Forcepoint Advanced Malware Detection dostępny w opcji w chmurze jak i w postaci appliance
ZARZĄDZANIE I MONITORING	
Interfejsy zarządzania	• Scentralizowany system zarządzania na poziomie przedsiębiorstwa z funkcjami analizy, monitorowania i raportowania logów • Szczegółowe informacje w karcie produktu Forcepoint Security Management Center.
Monitoring SNMP	SNMPv1, SNMPv2c i SNMPv3
Rejestracja ruchu	Narzędzie tcpdump, rejestracja zdalna przez Forcepoint Security Management Center
High Security Management Communication	Szyfrowanie komunikacji pomiędzy komponentami systemu z użyciem klucza 256-bit
Certyfikaty bezpieczeństwa	Common Criteria Network Devices Protection Profile with Extended Package Stateful Traffic Filter Firewall, FIPS 140-2 crypto certificate, CSPN by ANSSI, (First Level Security Certification USGv6)

* Niedostępne dla urządzeń 110/115.

KONTAKT
www.forcepoint.com/contact

ABOUT FORCEPOINT

[DATASHEET_FORCEPOINT_NGFW_EN] 100033.092917