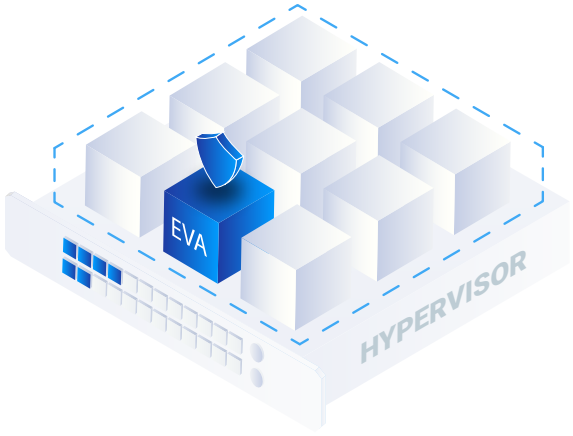
STORMSHIELD

OCHRONA SIECI

STORMSHIELD **ELASTIC VIRTUAL APPLIANCE**

Idealne rozwiązanie do zmieniającego się wirtualnego środowiska IT

63 Gbps	33 Gbps	10.6 Gbps	Skalowalność
WYDAJNOŚĆ FIREWALLA	WYDAJNOŚĆ IPS	WYDAJNOŚĆ IPSEC VPN	DOPASUJ DO SWOICH POTRZEB



CITRIX vmware Microsoft Hyper-V KVM Windows Azure aws

Dostosowany do Twojej sieci

Elastic Virtual Appliance STORMSHIELD (EVA) dostosowuje swoje możliwości do zasobów przydzielanych przez hypervisor. Uruchom wirtualny obraz, który będzie pokazywać zmiany w Twojej infrastrukturze.

Ochrona środowisk wirtualnych

- Segmentacja sieci wirtualnych
- Bezpieczna komunikacja typu site-to-site
- Ochrona dostępu mobilnego

Optymalizacja kosztów

- Dostosowanie do zasobów hypervisora
- Optymalne wykorzystanie pamięci RAM i liczby rdzeni procesora

Przenośność

- Migracja z jednej platformy chmurowej do drugiej
- Szeroki zakres obsługiwanych środowisk (Microsoft Hyper-V, VMWare, KVM, Citrix, Microsoft Azure, Amazon Web Services)
- Możliwość tworzenia kopii zapasowych, wdrażania i ich odtwarzania

ROZMIARY

SYSTEM	EVA1	EVA2	EVA3	EVA4	EVAU
Pamięć (max. - GB)	2	3	6	8	64
Maks. liczba wirt. procesorów (vCPU)	1	2	4	4	16
Maks. liczba reguł bezpieczeństwa	1 024	2 048	4 096	8 192	8 192
Maks. liczba obiektów	5 000	5 000	5 000	5 000	20 000
Maks. rozmiar bazy danych użytkowników	2 048	2 048	5 120	5 120	10 240

POŁĄCZENIA SIECIOWE	EVA1	EVA2	EVA3	EVA4	EVAU
Maks. liczba jednoczesnych połączeń	200 000	400 000	1 000 000	1 500 000	5 000 000
Maks. liczba tras statycznych	512	2 048	5 120	5 120	10 240
Maks. liczba tras dynamicznych	10 000	350 000	350 000	350 000	700 000
802.1Q VLAN	128	256	512	512	1 024

VPN	EVA1	EVA2	EVA3	EVA4	EVAU
Maks. liczba tuneli IPSec VPN	200	500	750	5 000	10 000
Maks. liczba SSL VPN (tryb Portal)	50	512	512	1 024	4 096
Maks. liczba jednoczesnych klientów SSL VPN	100	150	200	250	500

SPECYFIKACJA TECHNICZNA

WYDAJNOŚĆ*	EVA1	EVA2	EVA3	EVA4	EVAU
Przepust. firewall (1518 bajtów UDP)	16.4 Gbps	27 Gbps	45 Gbps	45 Gbps	63 Gbps
Przepustowość IPS (1518 bajtów UDP)	8.6 Gbps	12.7 Gbps	20 Gbps	20 Gbps	33 Gbps
Przepustowość IPS (1 MB HTTP)	5 Gbps	8.5 Gbps	12.7 Gbps	12.7 Gbps	14.5 Gbps
Przepustowość antywirusa	0.9 Gbps	1.7 Gbps	3.1 Gbps	3.1 Gbps	7.1 Gpbs
Przepustowość IPSec	2.5 Gbps	3.7 Gbps	6.7 Gbps	6.7 Gbps	10.6 Gbps
Nowe sesje na sekundę	44 000	74 000	93 000	93 000	112 000

REDUNDANCJA	EVA1	EVA2	EVA3	EVA4	EVAU
High Availability (Active/Passive)	✔	✔	✔	✔	✔

**: Dane techniczne stacji, na której dokonano pomiarów: Intel Platinum 8168 24C@2.7GHz CPU, karta sieciowa Intel XL710 - VMware vSphere 6.7 - SR-IOV włączone.*

WSPIERANE PLATFORMY

VMware ESX/ESXi
Wersja 6.0 i wyższa
Citrix Xen Server
Wersja 7.1 i wyższa

Linux KVM
Wersja 7.4 i wyższa
Microsoft Hyper-V
Windows Server 2012 i nowsze wersje

FUNKCJONALNOŚCI

KONTROLA WYKORZYSTANIA SIECI
Firewall/IPS/IDS, firewall aplikacyjny, filtrowanie Microsoft Services, przemysłowy Firewall/IPS/IDS wykrywanie i kontrola wykorzystywanych urządzeń mobilnych, przegląd używanych w sieci aplikacji (opcja), wykrywanie podatności (opcja), filtrowanie oparte o geolokację (kraje, kontynenty), dynamiczna reputacja hosta, filtrowanie adresów URL (filtr chmurowy lub wbudowany), transparentne uwierzytelnianie (Active Directory SSO agent, certyfikaty SSL, SPNEGO), uwierzytelnianie wielu użytkowników w trybie cookies (Citrix-TSE) - wiele metod uwierzytelniania gości, globalna / lokalna polityka bezpieczeństwa.

OCHRONA PRZED ZAGROŻENIAMI
Zapobieganie włamaniom, automatyczne wykrywanie i skanowanie protokołów, kontrola aplikacji, ochrona przed atakami Denial of Service (DoS), ochrona przed SQL injection, ochrona przed CrossSite Scripting (XSS), ochrona przed złośliwym kodem Web2.0 i skryptami, wykrywanie trojanów, wykrywanie interaktywnych połączeń (botnety, Command & Control), zaawansowane zarządzanie fragmentacją, automatyczna kwarantanna w przypadku ataku, antyspam i antyphishing, reputacja na bazie analizy heurystycznej, wbudowane oprogramowanie antywirusowe (HTTP, SMTP, POP3, FTP), deszyfracja i kontrola ruchu SSL, ochrona VoIP (SIP), dostosowanie polityki filtrowania do zdarzeń bezpieczeństwa lub wykrywanie luk w zabezpieczeniach, wykrywanie niezidentyfikowanych dotychczas zagrożeń różnego typu poprzez Sandboxing w chmurze (datacenter w Europie).

POUFNOŚĆ WYMIANY DANYCH
Site-to-site lub Client-to-site IPSec VPN, zdalny tunel SSL VPN w trybie Multi-OS (Windows, Android, iOS, itp.), automatycznie konfigurowany klient SSL VPN (Windows), wsparcie dla Android / iPhone IPSec VPN.

SIEĆ - INTEGRACJA
IPv6, NAT, PAT, tryb transparentny (bridge) / router / hybrydowy, dynamiczny routing (RIP, OSPF, BGP), wielopoziomowe wewnętrzne lub zewnętrzne zarządzanie PKI, integracja z wieloma bazami użytkowników (w tym wewnętrzna baza LDAP), routing oparty na regułach (PBR), zarządzanie QoS, DHCP klient / relay / serwer, klient NTP, DNS proxy, HTTP proxy.

ZARZĄDZANIE
Interfejs webowy, anonimizacja logów, obiektowe zarządzanie politykami, licznik użycia reguł, analizator poprawności reguł, ponad 15 kreatorów konfiguracji, globalna / lokalna polityka bezpieczeństwa, wbudowane raportowanie i narzędzia do analizy, interaktywne i konfigurowalne raporty, wysyłanie logów do serwera syslog UDP / TCP / TLS, SNMP v1, v2, v3, IPFIX, NetFlow, automatyczne tworzenie kopii zapasowych konfiguracji - pamięć zewnętrzna (opcjonalnie), Open API, Skrypty.

Dokument nie jest umową. Wymienione funkcje dotyczą wersji 3.x.