



## STORMSHIELD

OCHRONA SIECI

# STORMSHIELD ELASTIC VIRTUAL APPLIANCE



Idealne rozwiązanie do zmieniającego się wirtualnego środowiska IT

63 Gbps

WYDAJNOŚĆ  
FIREWALLA

33 Gbps

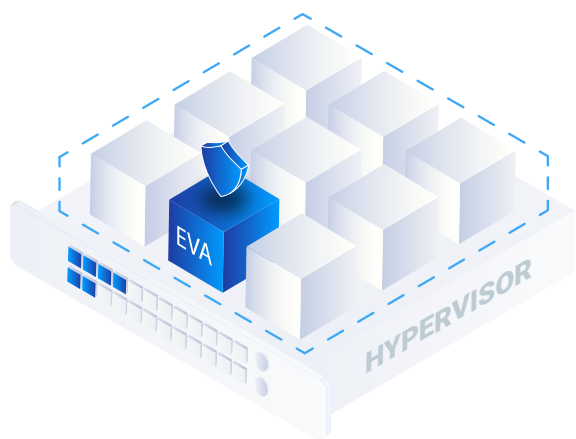
WYDAJNOŚĆ  
IPS

10.6 Gbps

WYDAJNOŚĆ  
IPSEC VPN

Skalowalność

DOPASUJ  
DO SWOICH POTRZEB



### 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 hypervisor
- 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

CITRIX

VMWARE

MICROSOFT  
HYPER-V

KVM

WINDOWS AZURE

AMAZON

OUTSCALE

NEXT GENERATION UTM  
& FIREWALL

CHMURA PUBLICZNA,  
PRYWATNA I HYBRYDOWA

[WWW.STORMSHIELD.PL](http://WWW.STORMSHIELD.PL)

## ROZMIARY

SYSTEM	EVA1	EVA2	EVA3	EVA4	EVAU
Pamięć (max. - GB)	<b>1-2</b>	<b>2-3</b>	<b>3-6</b>	<b>6-8</b>	<b>8-64</b>
Maks. liczba wirt. procesorów (vCPU)	<b>1</b>	<b>2</b>	<b>4</b>	<b>4</b>	<b>16</b>
Maks. liczba reguł bezpieczeństwa	<b>1 024</b>	<b>2 048</b>	<b>4 096</b>	<b>8 192</b>	<b>8 192</b>
Maks. liczba obiektów	<b>5 000</b>	<b>5 000</b>	<b>5 000</b>	<b>5 000</b>	<b>20 000</b>
Maks. rozmiar bazy danych użytkowników	<b>2 048</b>	<b>2 048</b>	<b>5 120</b>	<b>5 120</b>	<b>10 240</b>
POŁĄCZENIA SIECIOWE	EVA1	EVA2	EVA3	EVA4	EVAU
Maks. liczba jednoczesnych połączeń	<b>200 000</b>	<b>400 000</b>	<b>1 000 000</b>	<b>1 500 000</b>	<b>5 000 000</b>
Maks. liczba tras statycznych	<b>512</b>	<b>2 048</b>	<b>5 120</b>	<b>5 120</b>	<b>10 240</b>
Maks. liczba tras dynamicznych	<b>10 000</b>	<b>350 000</b>	<b>350 000</b>	<b>350 000</b>	<b>700 000</b>
802.1Q VLAN	<b>128</b>	<b>256</b>	<b>512</b>	<b>512</b>	<b>1 024</b>
VPN	EVA1	EVA2	EVA3	EVA4	EVAU
Maks. liczba tuneli IPSec VPN	<b>200</b>	<b>500</b>	<b>750</b>	<b>5 000</b>	<b>10 000</b>
Maks. liczba SSL VPN (tryb Portal)	<b>50</b>	<b>512</b>	<b>512</b>	<b>1 024</b>	<b>4 096</b>
Maks. liczba jednoczesnych klientów SSL VPN	<b>100</b>	<b>150</b>	<b>200</b>	<b>250</b>	<b>500</b>

Przedstawione wartości są maksymalnymi ograniczeniami każdego modelu w zależności od rozmiaru pamięci przydzielonej do produktu Elastic Virtual Appliance. Zmniejszenie przydzielonej pamięci może wpłynąć na skonfigurowane zasoby.

## SPECYFIKACJA TECHNICZNA

WYDAJNOŚĆ*	EVA1	EVA2	EVA3	EVA4	EVAU
Przepust. firewall (1518 bajtów UDP)	<b>16.4 Gbps</b>	<b>27 Gbps</b>	<b>45 Gbps</b>	<b>45 Gbps</b>	<b>63 Gbps</b>
Przepustowość IPS (1518 bajtów UDP)	<b>8.6 Gbps</b>	<b>12.7 Gbps</b>	<b>20 Gbps</b>	<b>20 Gbps</b>	<b>33 Gbps</b>
Przepustowość IPS (1 MB HTTP)	<b>5 Gbps</b>	<b>8.5 Gbps</b>	<b>12.7 Gbps</b>	<b>12.7 Gbps</b>	<b>14.5 Gbps</b>
Przepustowość antywirusa	<b>0.9 Gbps</b>	<b>1.7 Gbps</b>	<b>3.1 Gbps</b>	<b>3.1 Gbps</b>	<b>7.1 Gbps</b>
Przepustowość IPSec	<b>2.5 Gbps</b>	<b>3.7 Gbps</b>	<b>6.7 Gbps</b>	<b>6.7 Gbps</b>	<b>10.6 Gbps</b>
Nowe sesje na sekundę	<b>44 000</b>	<b>74 000</b>	<b>93 000</b>	<b>93 000</b>	<b>112 000</b>
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 6.5, 6.7 i 7.0  
**Citrix Xen Server**  
Wersja 7.6

**Linux KVM**  
Red Hat Enterprise 7.9  
**Microsoft Hyper-V**  
Windows Server 2012 R2 i 2019

## 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; opcja).

### 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-cache, HTTP proxy, zarządzanie wieloma łączami (balancing, failover), jawne proxy, SD-WAN, uwierzytelnianie wieloskładnikowe (MFA).

### ZARZĄDZANIE

Interfejs webowy zarządzany z trybem prywatności (zgodność z RODO), 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 agent v1, v2c, v3, IPFIX, automatyczne tworzenie kopii zapasowych konfiguracji, Open API, nagrywanie skryptów.

Dokument nie jest umową. Wymienione funkcje dotyczą wersji 4.x.