



Nová generace firewallu

Barracuda NG Firewall je navržen tak, aby chránil firemní síťovou infrastrukturu a zjednodušil správu síťového provozu. Barracuda NG Firewall v sobě integruje technologie VPN, správu aplikací na úrovni sedmé vrstvy, Intrusion prevention, filtrování webu, anti-virus, anti-spam a řízení přístupu k síti. Dále umožňuje jednotnou centrální správu, která může pokrývat celou rozsáhlou síť včetně poboček a datových center.

Ochrana síťového provozu | NG Firewall chrání síť proti narušení, malwaru, spamu, DDoS/DoS útokům a dalším „moderním“ hrozbám. Zároveň řídí přístup k síti a filtruje emailový a webový provoz, ochranu proti pokročilým hrozbám

Řízení webového provozu | Možnost nastavení politik pro přístup k aplikacím dle uživatelů a skupin, šířky pásma, času a dalších kritérií integrované s LDAP / Active Directory. Politiky lze vynutit na celé aplikace nebo pouze na jejich určité funkce (např. zakázat pouze Facebook games).

Control Center | Barracuda nabízí (volitelně) centrální management konzoli pro správu jednoho či stovky firewallů, která umožní nastavování pravidel, politik, instalaci aktualizací a softwarových záplat nebo granulární delegování administrativních práv dle oddělení či pozici nebo správu certifikátů (X.509, SSH, VPN). Nabízí přehledné reporty a integrovaný kontrolní systém revizí pro snadné auditování.



Optimalizace WAN Barracuda NG Firewall nabízí možnost optimalizace WAN pomocí komprese a dekomprese dat, optimalizace provozu TCP, akcelerace protokolů a deduplikaci dat. Nabízí inteligentní up-link balancing a failover. WAN provoz může být účinně komprimován až o 95%, což výrazně sníží nároky na šířku pásma.

Zabezpečený vzdálený přístup Barracuda NG Firewall nabízí site-to-site a client-to-site VPN. S využitím SSL a IPSec protokolů nabízí jednoduchý a bezpečný vzdálený přístup. Barracuda vyvinula proprietární rozšíření protokolu IPsec nazvaný TINA (Transport Independent Network Architecture) s cílem dosažení vyšší rychlosti, lepší konektivity a stability VPN.

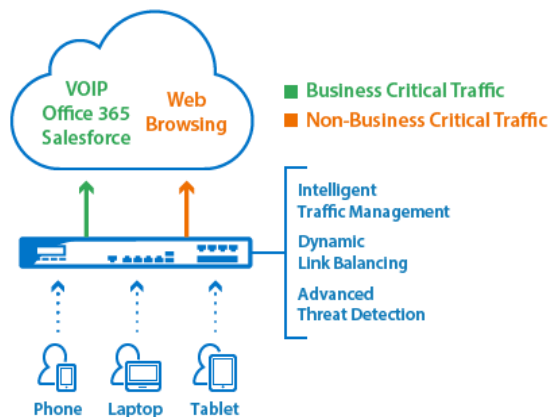
NGFW podpora pro O365 – Barracuda NG Firewall dokáže přímo rozpoznat aplikaci O365 a přidělit jí například garantovanou šířku pásma, či nastavit směrování traffic přes jiného ISP.

SANDBOX - Advanced Threat Detection Barracuda ATD nabízí bezpečnou emulaci podezřelého systému a zkoumá jeho chování. Porovnává podezřelé soubory s hash databází a pokud není soubor znám, je spuštěn v emulačním prostředí pro posouzení, zda se jedná o maligní soubor. Barracuda využívá oceňovanou next-generation sandbox technologii od společnosti LastLine. Tento sandbox využívá „full-system emulation“, který nabízí podrobnosti o chování podezřelého objektu. Pokud je soubor shledán škodlivým, je odeslán log do NG Firewallu, který automaticky provede karanténu napadeného subjektu a upozorní administrátora.



Klíčové vlastnosti

- ✓ Centrální správa
- ✓ Optimalizace WAN provozu
- ✓ VPN technologie TINA
- ✓ Flexibilní možnosti nasazení
- ✓ Plná funkcionalita pro všechny modely (AV, ATD, IPS, URL filter, Aplikační FW)
- ✓ Směrování na základě aplikací
- ✓ Podpora pro O365
- ✓ Ochrana ověřením v SANDBOX Advanced Threat Detection
- ✓ Možnosti nasazení: HW, Virtual, Azure, AWS, vCloud Air, Google Cloud Platform



Modely:

- F18
- F80
- F180
- F280
- F380
- F400
- F600
- F800
- F900
- F1000



Přehled klíčových funkcí a vlastností modelů

Vlastnosti Firewallu

- Neomezený počet uživatelů
- Intrusion Prevention (IPS)
- Transparentní proxy (TCP)
- Anti-virus & Web filtering; DDoS protection
- Správa pomocí Control Center
- Možnosti rozšíření
 - Advanced Threat Detection (**sandbox**)
 - Malware Protection
 - Premium Remote Access (aplikace pro iOS, Android, PC (Win, Mac))

Optimalizace provozu

- Agregace a sledování spojení, Fail-Over
- Dynamické směrování
- Application-based provider selection
- Traffic shaping & QoS
- On-the-fly prioritizace provozu
- Kompresce WAN (Stream a paket komprese)

Služby infrastruktury

- DHCP, HTTP, SSH, FTP proxy
- SMTP gateway a spam filter, DNS Cache
- WiFi (802.11b/g) na vybraných modelech
- Autentizace x.509, NTLM, RADIUS, RSA SecurID, LDAP/LDAPS, Active Directory, TACACS+, SMS passcode, lokální autentizace, WiFi AP podpora autentizace

Detekce a prevence vniknutí

- Ochrana proti exploitům, hrozbám a zranitelnostem
- Ochrana proti packet anomaly and fragmentation

- Automatická aktualizace signatur
- Ochrana proti vniknutí a mlžícím technikám

Podporované protokoly

- IPv4 IPv6
- BGP/OSFP/RIP
- VoIP (H.323, SIP, SCCP [skinny])
- RPC protokoly (ONC-RPC, DCE-RPC)
- 802.1q VLAN

VPN

- Drug & Drop konfigurace VPN tunelu
- Site-to-site, Client-to-site VPN
- IPSec, SSL, TINA, PPTP/L2TP (IPsec)
- Podpora AES-128/256, 3DES, DES
- Soukromé CA nebo externí PKI
- IPsec VPN klient pro Windows, Mac, Linux
- Application-aware intelligence pro stránky
- VPN throughput používá AES 128 NOHASH
- iOS a Android VPN (Network Access Control)

Vysoká dostupnost

- Active-active (vyžaduje externí load balancer) nebo active-passive
- Notifikace failover
- Transparentní failover bez ztráty spojení
- Šifrovaná HA komunikace

Možnosti rozšíření bezpečnosti

- Advanced Threat Detection
- Barracuda NG SSL VPN a NAC
- Malware Protection

Firewall

- Stavová inspekce paketů

- Intrusion Prevention and Detection systems (IPS/IDS)
- Application Control
- Zachycení a dešifrace SSL/TLS šifrovaných aplikací
- Antivirus & Web Filtering
- Ochrana proti DDoS/DoS
- Filtrování reputace DNS
- Transparentní proxy (TCP)
- NAT (SNAT, DNAT), PAT
- Dynamická pravidla, časové triggerry
- Testování ve virtuálním prostředí
- Ochrana proti DDoS

Advanced Threat Detection

- Dynamický, on-demand analýza podezřelých souborů (sandboxing)
- Dynamická analýza dokumentů (PDF, MS Office atd.)
- Detailní forenzní analýza

Možnosti podpory

- Energize Updates
 - Standardní technická podpora
 - Updaty firmwaru
 - Definice řízení pro více než 800 aplikací
- Instant Replacement Support
 - Náhradní jednotka odeslaná next business day
 - 24x7 technická podpora

Nárok na nový HW každé 4 roky

Model	F18	F80	F180	F280	F380	F400	F600	F800	F900	F1000
Kapacita										
Propustnost firewallu	1 Gbps	1,35 Gbps	1,65 Gbps	3 Gbps	3,8 Gbps	5,5 Gbps	16,3 Gbps	19,6 Gbps	35 Gbps	40 Gbps
Propustnost VPN	190 Mbps	240 Mbps	300 Mbps	1 Gbps	1,2 Gbps	1,2 Gbps	2,3 Gbps	7,3 Gbps	9,3 Gbps	10 Gbps
Propustnost IPS	400 Mbps	500 Mbps	600 mbps	1 Gbps	1,4 Gbps	2 Gbps	5 Gbps	6,5 Gbps	11,3 Gbps	13 Gbps
Současná spojení	80.000	80.000	100.000	250.000	400.000	500.000	2,1 mil	2,5 mil	4 mil	10 mil
Nová spojení/s	8.000	8.000	9.000	10.000	15.000	20.000	115.000	150.000	190.000	250.000
Hardware										
Rozměry hardwaru	Desktop	Desktop	Desktop	Desktop	1U	1U	1U	1U	1U	2U
Ethernet rozhraní	4 x 1GbE	4 x 1GbE	6 x 1GbE	6 x 1GbE	8x1GbE	8x1GbE	8/12	12/20	8/32	16/32
1Gb fiber (std/max)	-	-	-	-	-	0/4	0/4	0/4	0/8	0/16
10Gb fiber	-	-	-	-	-	-	0/2	0/4	0/8	4/8
Integrovaná Wi-Fi	-	ano	ano	ano	-	-	-	-	-	-
Integrovaný Switch	-	-	8-port	8-port	-	-	-	-	-	-
Vlastnosti										
Firewall	ano	ano	ano	ano	ano	ano	ano	ano	ano	ano
IPsec VPN	ano	ano	ano	ano	ano	ano	ano	ano	ano	ano
Application control	ano	ano	ano	ano	ano	ano	ano	ano	ano	ano
IPS	ano	ano	ano	ano	ano	ano	ano	ano	ano	ano
WAN Optimalizace	ano	ano	ano	ano	ano	ano	ano	ano	ano	ano
VPN	ano	ano	ano	ano	ano	ano	ano	ano	ano	ano
Zachycení SSL	ano	ano	ano	ano	ano	ano	ano	ano	ano	ano
Web Filter	ano	ano	ano	ano	ano	ano	ano	ano	ano	ano
Spam filtr & Mail Gateway	-	-	ano	ano	ano	ano	ano	ano	ano	ano
Advanced Threat Detection	volitelný	volitelný	volitelný	volitelný	volitelný	volitelný	volitelný	volitelný	volitelný	volitelný
Malware Protection	volitelný	volitelný	volitelný	volitelný	volitelný	volitelný	volitelný	volitelný	volitelný	volitelný
Remote Access	-	volitelný	volitelný	volitelný	volitelný	volitelný	volitelný	volitelný	volitelný	volitelný

NG Firewally jsou také dostupné v podobě virtuální appliance pro VMware, XenServer, KVM a Hyper-V.



BARRACUDA NG FIREWALL

Modely:

F18
F80
F180
F280
F380
F400
F600
F800
F900
F1000