Barracuda **NextGen Firewall F**

Skalowalne bezpieczeństwo przedsiębiorstwa

- ☑ **Security**
- ☐ Storage
- ☐ Application Delivery
- ☐ Productivity

Sieci korporacyjne z każdym dniem coraz bardziej się rozbudowują i stają się bardziej newralgiczne dla operacji biznesowych. Barracuda NextGen Firewall serii F to podstawowe narzędzie do **optymalizacji wydajności, bezpieczeństwa i dostępności korporacyjnych sieci WAN, nierzadko rozproszonych w wielu lokalizacjach.**

Przewaga Barracudy

Efektywne zarządzanie WAN
- Nadawanie priorytetów ruchu w WAN zależnie od aplikacji
- Inteligentne równoważenie uplink
- Inteligentna zmiana priorytetów ruchu w razie zaniku uplink

Gotowość do wdrożenia w przedsiębiorstwie
- Wiodące w branży centralne zarządzanie
- Optymalizacja WAN
- Globalne monitorowanie WAN przy użyciu Barracuda Earth

Skalowalne bezpieczeństwo
- Możliwość pracy w chmurze i bezpieczna wirtualizacja WAN
- Graficzny interfejs tunelowania VPN obsługiwany metodą drag-and-drop

O produkcie

- Rozbudowana zapora sieciowa nowej generacji
- Zaawansowane wykrywanie zagrożeń
- Wbudowane zabezpieczenia sieciowe i IDS/IPS
- Sieć VPN w topologii dynamic mesh site-to-site
- Sieć VPN Client-to-Site przez przeglądarkę (SSL VPN), klienty VPN w postaci aplikacji mobilnych i do komputerów stacjonarnych
- Pełna widoczność aplikacji i szczegółowa kontrola
- Inteligentna regulacja ruchu, w tym wybór operatora na podstawie aplikacji
- Ściśle zintegrowane funkcje jakości usługi (Quality of Service – QoS) i równoważenie łącza
- Centralne zarządzanie wszystkimi funkcjami
- Konfiguracja oparta na szablonach i rolach

Zintegrowane bezpieczeństwo nowej generacji

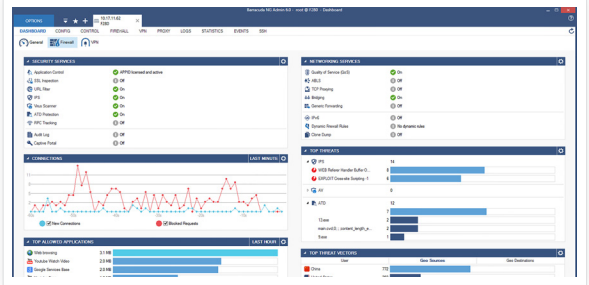
Barracuda NextGen Firewall serii F zaprojektowano i stworzono od podstaw tak, aby zapewnić wszechstronne możliwości zapory sieciowej nowej generacji. Filtrowanie i raportowanie treści w chmurze przenosi do chmury zadania wymagające dużej mocy obliczeniowej, co zwiększa efektywność wykorzystania zasobów i przepustowość. Seria F to idealne rozwiązanie dla dynamicznych organizacji, oparte na widoczności aplikacji, rozpoznawaniu tożsamości użytkowników i centralnym zarządzaniu.

Aktywność użytkowników znowu pod kontrolą

Wykorzystywane w pracy urządzenia mobilne, aplikacje Web 2.0, coraz większy stopień rozproszenia, rosnąca integracja z chmurą i zależność od umieszczonych w niej zasobów spowodowały, że sieci firmowe stały się nieprzejrzyste, a zarządzanie nimi – niemożliwe. Barracuda NextGen Firewall serii F przywraca kontrolę nad takimi sieciami. Ta zapora sieciowa rozszerza zabezpieczenia poza granice sieci, ułatwiając monitorowanie i regulowanie wszystkich działań, jakie wykonują urządzenia i użytkownicy sieci.

Pełna gotowość do wdrożenia w przedsiębiorstwie

Barracuda NextGen Firewall serii F spełnia wymagania organizacji pod względem dużej skalowalności oraz efektywnego zarządzania w rozproszonych sieciach. Zintegrowana optymalizacja WAN i wyspecjalizowane urządzenia centralnego zarządzania pozwalają organizacjom na zwiększenie dostępności systemu przy ograniczeniu czasu potrzebnego na administrowanie i obniżeniu kosztów.



Panel sterowania Barracuda NextGen Firewall F wyświetla informacje w czasie rzeczywistym i podsumowania działań w sieci organizacji.

Ostatnio testowałem jeden z tych wyspecjalizowanych produktów, aby zabezpieczyć sieć przed atakami Advanced Persistent Threat. Po miesiącu szeroko zakrojonego monitorowania okazało się, że Barracuda NextGen Firewall F chroni nasze infrastruktury na tyle dobrze, że możemy się skupić na faktycznych problemach związanych z działalnością przedsiębiorstwa. Wybór odpowiedniej zapory sieciowej pozwolił nam (i codziennie pozwala dalej) zaoszczędzić czas i pieniądze.

Dyrektor ds. informatyki
Związek Stowarzyszeń
Tureckich Izb Adwokackich

Specyfikacja techniczna

Zapora sieciowa

- Kontrola i przekazywanie Stateful Packet Inspection
- Pełne rozpoznawanie tożsamości użytkowników
- System wykrywania włamań i zapobiegania im (Intrusion Detection and Prevention System – IDS/IPS)
- Kontrola aplikacji i szczegółowe wymuszanie zasad działania aplikacji
- Przechwytywanie i rozszyfrowywanie aplikacji szyfrujących dane przy użyciu SSL/TLS
- Antywirus i filtrowanie treści w sieci w trybie jednoprzebiegowym
- Wymuszanie bezpiecznego przeszukiwania SafeSearch
- Obsługa YouTube dla Szkół
- Zabezpieczenie przed zwykłymi i rozproszonymi atakami odmowy usługi (DoS /DDoS)
- Zabezpieczenie przed spoofingiem i floodowaniem
- Zabezpieczenie przed spoofingiem i zaśmieczaniem tablicy ARP
- Filtrowanie na podstawie reputacji DNS
- Ponowne składanie strumienia TCP
- Transparentne proxy (TCP)
- NAT (SNAT, DNAT), PAT
- Dynamiczne reguły / wyzwalanie na podstawie timera
- Pojedyncza reguła obiektowa ustawiona dla routingu, mostkowania i mostkowania routowanego
- Wirtualne środowisko testowania reguł

Rozpoznawanie tożsamości użytkownika

- Agent serwera terminali
- Agent kontrolera domeny
- Uwierzytelnianie – obsługa x.509, NTLM, RADIUS, RSA SecurID, LDAP/LDAPS, Active Directory, TACACS+, SMS Passcode (VPN), lokalnej bazy danych uwierzytelniania
- Obsługa uwierzytelniania punktu dostępu WiFi

Wykrywanie włamań i zapobieganie im

- Ochrona przed exploitami, zagrożeniami i lukami bezpieczeństwa
- Ochrona przed nieprawidłowymi i pofragmentowanymi pakietami
- Zaawansowane techniki zapobiegania obchodzeniu zabezpieczeń i ukrywaniu ataków
- Automatyczne aktualizacje sygnatur

Optymalizacja ruchu

- Monitorowanie, agregacja łączy i bezpieczne przełączanie w razie awarii
- Dynamiczny routing
- Wybór operatora na podstawie aplikacji
- Kształtowanie ruchu i QoS
- Zmiana priorytetów przepływu na bieżąco
- Kompresja strumieni i pakietów
- Deduplikacja danych na poziomie pojedynczych bajtów
- Optymalizacja protokołu (SMBv2)

Zaawansowane wykrywanie zagrożeń

- Dynamiczna analiza złośliwych programów na żądanie (w środowisku sandbox)
- Dynamiczna analiza dokumentów z osadzonymi exploitami (PDF, Office itp.)
- Szczegółowa analiza kryminalistyczna złośliwego oprogramowania w postaci plików binarnych i zagrożeń (exploitów) sieciowych
- Obsługa różnych systemów operacyjnych (Windows, Android itp.)
- Elastyczna analiza złośliwego oprogramowania w chmurze

VPN

- Konfiguracja tunelowania VPN metodą drag & drop
- Bezpieczna sieć VPN site-to-site, client-to-site
- Sieć VPN w topologii dynamic mesh site-to-site
- Obsługa szyfrowania AES-128/256, 3DES, DES, Blowfish, CAST, różnych wersji Null Cipher
- Prywatne CA lub zewnętrzne PKI
- Certyfikat VPNC (podstawowa interoperacyjność)
- Routowanie ruchu z rozpoznawaniem aplikacji
- IPsec VPN / SSL VPN / TINA VPN/ L2TP / PPTP
- Kontrola dostępu do sieci
- Obsługa VPN dla urządzeń mobilnych z systemami iOS i Android

Wysoki poziom dostępności

- Aktywna-aktywna (wymaga zewnętrznego rozwiązania równoważenia obciążenia) lub aktywna-pasywna
- Transparentne przełączanie w razie awarii bez utraty sesji
- Powiadomienie sieciowe o przełączeniu w razie awarii
- Szyfrowana komunikacja HA

Opcje centralnego zarządzania

- Centrum sterowania Barracuda NextGen Control Center
  - Nieograniczona liczba zapór sieciowych
  - Obsługa korzystania z zasobów przez wielu użytkowników (multi-tenancy)
  - Obsługa zarządzania przez wielu administratorów i RCS

Usługi infrastruktury

- Serwer DHCP, relay
- Serwery proxy SIP, HTTP, SSH, FTP
- Obsługa SNMP and IPFIX
- Buforowanie DNS
- Brama SMTP i filtr antyspamowy
- Punkt dostępu Wi-Fi (802.11n) w wybranych modelach

Obsługiwane protokoły

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

Opcje pomocy technicznej

Barracuda Energize Updates

- Standardowa pomoc techniczna
- Aktualizacje oprogramowania układowego
- Aktualizacje sygnatur IPS
- Aktualizacje definicji kontroli aplikacji
- Aktualizacje filtrów sieciowych

Usługa natychmiastowej wymiany sprzętu

- Jednostka zastępcza wysyłana następnego dnia roboczego
- Pomoc techniczna 24x7
- Bezpłatna wymiana sprzętu na nowy po czterech latach

Opcje zabezpieczeń

- Zaawansowane wykrywanie zagrożeń
- NextGen Web Filter
- Ochrona przed złośliwym oprogramowaniem
- Subskrypcja usługi podstawowego dostępu zdalnego (Basic Remote Access) umożliwia zdalny dostęp przez przeglądarkę (SSL VPN) z kontrolą dostępu do sieci (NAC)
- Subskrypcja usługi rozszerzonego dostępu zdalnego (Premium Remote Access) umożliwia zdalny dostęp przez aplikację CudaLaunch dla urządzeń z systemem iOS i Android

PORÓWNANIE MODELI	F10	F18	F80	F180	F280	F380	F400 PODMODELE		F600 PODMODELE			F800 PODMODELE			F900 PODMODELE			F1000 PODMODELE		
							STD	F20	C10 C20	F10 F20	E20	CCC	CCF	CCE	CCC	CCE	CFE	CE0	CE2	CFE
POJEMNOŚĆ																				
Przepustowość zapory sieciowej [1]	300 Mb/s	1,0 Gb/s	1,35 Gb/s	1,65 Gb/s	3,0 Gb/s	3,8 Gb/s	5,5 Gb/s		16,3 Gb/s [6]			19,6 Gb/s [6]			22,2 Gb/s [6]			40 Gb/s [6]		
Przepustowość VPN [2]	85 Mb/s	190 Mb/s	240 Mb/s	300 Mb/s	1,0 Gb/s	1,2 Gb/s	1,2 Gb/s		2,3 Gb/s [6]			7,3 Gb/s [6]			7,8 Gb/s [6]			10 Gb/s [6]		
Przepustowość IPS [1]	60 Mb/s	400 Mb/s	500 Mb/s	600 Mb/s	1,0 Gb/s	1,4 Gb/s	2,0 Gb/s		5,0 Gb/s [6]			6,5 Gb/s [6]			7,1 Gb/s [6]			13 Gb/s [6]		
Liczba jednoczesnych sesji	2.000	80.000	80.000	100.000	250.000	400.000	500.000		2.100.000 [6]			2.500.000 [6]			4.000.000 [6]			10.000.000 [6]		
Nowe sesje (na sekundę)	1.000	8.000	8.000	9.000	10.000	15.000	20.000		115.000 [6]			150.000 [6]			160.000 [6]			250.000 [6]		
SPRZĘT																				
Wielkość urządzenia	Desktop mini	Desktop				1U montaż w stelażu									2U montaż w stelażu					
Ethernet z kablami miedzianymi 1 GbE	4x	4x	4x	6x	6x	8x	8x	8x	12x	8x	8x	20x	12x	12x	24x	16x	8x	16x	32x	16x
Światłowód SFP 1 GbE								4x		4x			4x				8x			16x
Światłowód SFP+ 10 GbE											2x			4x		4x	4x	4x	8x	8x
Zintegrowany switch				8-portowy	8-portowy															
Punkt dostępu Wi-Fi			●	●	●															
Zasilanie	Pojedyncze (zewn.)				Pojedyncze		Podwójne [7]		Pojedyncze [8]			Podwójne [7]								
FUNKCJE																				
Zapora sieciowa	●	●	●	●	●	●	●		●			●			●			●		
Kontrola aplikacji [3]	●	●	●	●	●	●	●		●			●			●			●		
IPS [3]	●	●	●	●	●	●	●		●			●			●			●		
Dynamiczny routing	●	●	●	●	●	●	●		●			●			●			●		
Wybór operatora na podstawie aplikacji	●	●	●	●	●	●	●		●			●			●			●		
VPN	●	●	●	●	●	●	●		●			●			●			●		
Przechwytywanie SSL		●	●	●	●	●	●		●			●			●			●		
Optymalizacja WAN		●	●	●	●	●	●		●			●			●			●		
Filtr sieci WWW		●	●	●	●	●	●		●			●			●			●		
Brama pocztowa i filtr antyspamowy				●	●	●	●		●			●			●			●		
NextGen Web Filter		Opcjonalnie	Opcjonalnie	Opcjonalnie	Opcjonalnie	Opcjonalnie	Opcjonalnie		Opcjonalnie			Opcjonalnie			Opcjonalnie			Opcjonalnie		
Ochrona przed złośliwym oprogramowaniem [4]		Opcjonalnie	Opcjonalnie	Opcjonalnie	Opcjonalnie	Opcjonalnie	Opcjonalnie		Opcjonalnie			Opcjonalnie			Opcjonalnie			Opcjonalnie		
Zaawansowane wykrywanie zagrożeń [4,5]		Opcjonalnie	Opcjonalnie	Opcjonalnie	Opcjonalnie	Opcjonalnie	Opcjonalnie		Opcjonalnie			Opcjonalnie			Opcjonalnie			Opcjonalnie		
Podstawowy dostęp zdalny			Opcjonalnie	Opcjonalnie	Opcjonalnie	Opcjonalnie	Opcjonalnie		Opcjonalnie			Opcjonalnie			Opcjonalnie			Opcjonalnie		
Rozszerzony dostęp zdalny [9]			Opcjonalnie	Opcjonalnie	Opcjonalnie	Opcjonalnie	Opcjonalnie		Opcjonalnie			Opcjonalnie			Opcjonalnie			Opcjonalnie		

[1] Zmierzono za pomocą dużych pakietów (MTU 1500)
[2] Przepustowość VPN przy użyciu AES128 NOHASH
[3] Wymaga subskrypcji Energize Updates.
[4] W tym protokoły FTP, poczty i WWW
[5] Wymaga subskrypcji ochrony przed złośliwym oprogramowaniem.
[6] Zmierzono przy użyciu portów światłowodowych 10GbE.
[7] Wewnętrzny podwójny zasilacz z funkcją hot swap
[8] Opcjonalny wewnętrzny podwójny zasilacz z funkcją hot swap
[9] Obejmuje subskrypcję Podstawowy dostęp zdalny.

Specyfikacje mogą ulec zmianie bez wcześniejszego powiadomienia.

Barracuda Networks i logo Barracuda Networks są zastrzeżonymi znakami towarowymi Barracuda Networks, Inc. w Stanach Zjednoczonych. Wszystkie pozostałe nazwy są własnością odpowiednich właścicieli.