Barracuda **NextGen Firewall F**

Il Firewall di nuova generazione per l'era del Cloud

- ☑ **Security**
- ☐ Data Protection
- ☐ Application Delivery

Le reti aziendali sono sempre più grandi e più complesse, nonché sempre più cruciali per i principali processi aziendali. Barracuda NextGen Firewall F-Series è uno strumento essenziale per **ottimizzare le prestazioni, la sicurezza e la disponibilità delle moderne reti WAN aziendali geograficamente distribuite.**

Il vantaggio Barracuda

Gestione efficace della WAN
- Attribuzione di priorità al traffico in base all'applicazione in tutta la WAN
- Bilanciamento intelligente dell'uplink
- Revisione intelligente delle priorità del traffico in caso di perdita dell'uplink

Preparazione dell'azienda
- Gestione centralizzata leader nel settore
- Ottimizzazione della WAN
- Monitoraggio globale della WAN con Barracuda Earth

Sicurezza scalabile
- Abilitazione al cloud e virtualizzazione sicura della WAN
- Interfaccia grafica per il tunnel VPN con funzione di trascinamento

In primo piano

- Potente firewall per reti di nuova generazione
- Advanced Threat Protection (incl. sandboxing)
- Sicurezza Web e IDS/IPS integrati
- Mesh dinamico VPN da sito a sito
- VPN da client a sito tramite browser (SSL VPN), apps per dispositivi portatili e client VPN desktop
- Visibilità totale delle applicazioni e controllo granulare
- Regolazione intelligente del traffico, con selezione del provider in base all'applicazione
- Qualità del servizio (QoS) e bilanciamento del link strettamente integrati
- Gestione centralizzata di tutte le funzionalità
- Configurazione basata su modelli e su ruoli

Sicurezza di nuova generazione integrata

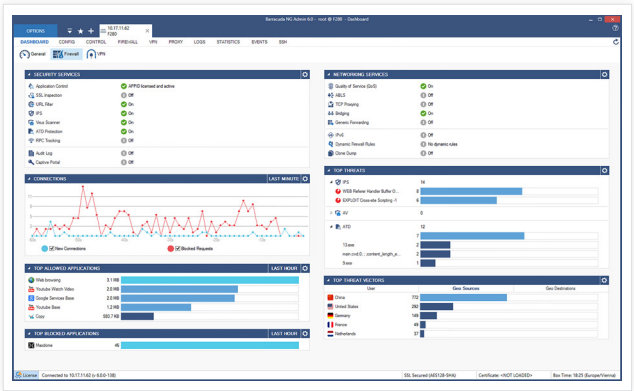
Barracuda NextGen Firewall F-Series è stato progettato sin dall'inizio e realizzato in modo da offrire funzionalità firewall di nuova generazione complete. Filtraggio dei contenuti in hosting nel cloud e segnalazione delle attività che impegnano molta potenza elaborativa al cloud per ottenere maggiore efficienza e produttività dalle risorse. Basato sulla visibilità delle applicazioni, la conoscenza dell'identità degli utenti, la prevenzione delle intrusioni e la gestione centralizzata, F-Series è la soluzione ideale per le aziende dinamiche di oggi.

Preparazione reale della rete

Barracuda NextGen Firewall F-Series soddisfa i requisiti delle aziende in materia di scalabilità di massa ed efficienza nella gestione tra reti distribuite. L'ottimizzazione della WAN e le appliance di gestione centralizzata dedicate integrate permettono alle organizzazioni di incrementare la disponibilità dei sistemi, contenendo i costi di gestione e i tempi di amministrazione.

Riprendere il controllo delle attività degli utenti

Barracuda NextGen Firewall F-Series restituisce il controllo di reti complicate e rese ingestibili dall'azione di dispositivi portatili, dalle applicazioni Web 2.0 e dall'aumento della dispersione geografica, dell'integrazione e della dipendenza da risorse basate sul cloud. Estende la copertura della sicurezza oltre i confini della rete e facilita il monitoraggio e la regolazione di tutte le operazioni eseguite dalla rete e dai suoi utenti.



Il dashboard di Barracuda NextGen Firewall F-Series fornisce informazioni e riepiloghi in tempo reale degli eventi in corso in una rete aziendale.

Di recente ho provato uno di questi prodotti dedicati per la protezione dalle minacce persistenti avanzate. Dopo un mese di monitoraggio intensivo abbiamo riscontrato che Barracuda NextGen Firewall F protegge talmente bene le nostre infrastrutture da lasciarci liberi di dedicarci ai veri problemi aziendali. Inoltre, la scelta del firewall giusto ci permette di risparmiare ogni giorno tempo e denaro.

CIO dell'Unione delle associazioni forensi turche

Specifiche Tecniche

Firewall
- Ispezione e inoltro di stateful packet
- Conoscenza completa dell'identità degli utenti
- Sistema di rilevamento e prevenzione delle intrusioni (IDS/IPS)
- Controllo ed esecuzione granulare delle applicazioni
- Intercettazione e decrittazione della applicazioni SSL/TLS crittografate
- Antivirus e filtraggio Web in single pass mode
- Esecuzione di SafeSearch
- Rafforzamento dei Google Account
- Protezione dagli attacchi di tipo denial-of-service (DoS /DDoS)
- Protezione da attacchi basati su spoofing e flooding
- Protezione da spoofing ARP e trashing
- Filtri di attendibilità per i DNS
- Riassemblaggio del flusso TCP
- Proxy trasparenti (TCP)
- NAT (SNAT, DNAT), PAT
- Regole dinamiche/attivazione di timer
- Regole orientate agli oggetti univoche impostabili per routing, bridging e bridging con routing
- Ambiente di test delle regole virtuale

Conoscenza dell'identità degli utenti
- Agente Terminal Server
- Agente del Domain Controller
- Autenticazione: supporto di x.509, NTLM, RADIUS, RSA SecurID, LDAP/LDAPS, Active Directory, TACACS+, SMS Passcode (VPN), database di autenticazione locale
- Supporto dell'autenticazione con access point WiFi

Rilevamento e prevenzione delle intrusioni
- Protezione contro exploit, minacce e vulnerabilità
- Protezione da anomalie e frammentazione dei pacchetti
- Tecniche anti-evasione e offuscamento avanzate
- Aggiornamenti automatici delle firme

Ottimizzazione del traffico
- Monitoraggio di link, aggregazione e failover
- Routing dinamico
- Selezione del provider in base all'applicazione
- Adattamento del traffico (Traffic Shaping) e QoS
- Revisione istantanea delle priorità del flusso
- Compressione per streaming e pacchetti
- Deduplica dei dati a livello di byte
- Ottimizzazione protocollo (SMBv2)

Protezione avanzato delle minacce
- Analisi dinamica, on-demand dei programmi malware (sandbox)
- Analisi dinamica dei documenti con exploit incorporati (PDF, Office, ecc.)
- Analisi dettagliata sia di malware costituito da codice binario che da minacce basate sul Web (exploit)
- Supporto per vari sistemi operativi (Windows, Android, etc.)
- Protezione contro Botnet e Spyware
- Analisi del malware flessibile nel cloud

Alta disponibilità
- Modello attivo-attivo (richiede un sistema di bilanciamento del carico esterno) o attivo-passivo
- Failover trasparente senza perdita della sessione
- Notifica di rete del failover
- Comunicazione HA crittografata

Servizi di infrastruttura
- Server DHCP, relay
- Proxy SIP, HTTP, SSH, FTP
- Supporto per SNMP e IPFIX
- Cache DNS
- Gateway SMTP e filtro SPAM
- Access point Wi-Fi (802.11n) su alcuni modelli

VPN
- Configurazione del tunnel VPN mediante funzioni di trascinamento
- Sicurezza della VPN da sito a sito e da client a sito
- VPN mesh da sito a sito dinamica
- Supporto di AES-128/256, 3DES, DES, Blowfish, CAST, cifre nulle
- Autorità di certificazione (CA) privata o infrastruttura a chiave pubblica (PKI) esterna
- Certificazione VPNC (interoperabilità di base)
- Routing del traffico sensibile all'applicazione
- IPsec VPN / SSL VPN / TINA VPN/ L2TP / PPTP
- Controllo dell'accesso alla rete
- Supporto VPN per dispositivi portatili con iOS e Android

Opzioni di gestione centralizzata
- Barracuda NextGen Control Center
  - Firewall illimitati
  - Supporto dell'architettura multi-tenant
  - Supporto di più amministratori e RCS

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

Opzioni di supporto

Barracuda Energize Updates
- Supporto tecnico standard
- Aggiornamenti del firmware
- Aggiornamenti delle signatures IPS
- Aggiornamento delle definizioni di controllo delle applicazioni
- Aggiornamenti di Web Filter

Servizio di Instant Replacement
- Spedizione dell'unità sostitutiva entro il giorno lavorativo successivo
- Supporto tecnico 24 ore su 24, 7 giorni su 7
- Aggiornamento hardware gratuito ogni 4 anni

Opzioni di sicurezza

- Protezione avanzato delle minacce eseguito sulla base del tipo di file con Advanced Malware protection e Sandboxing nel cloud
- Malware Protection
- L'abbonamento con accesso remoto avanzato permette l'accesso remoto tramite l'app CudaLaunch per dispositivi con Windows, macOS, iOS e Android

CONFRONTO MODELLI	F18	F80	F180	F280	F380	F400 MODELLI		F600 MODELLI			F800 MODELLI			F900 MODELLI			F1000 MODELLI		
						STD	F20	C10 C20	F10 F20	E20	CCC	CCF	CCE	CCC	CCE	CFE	CE0	CE2	CFE
CAPACITÀ																			
Velocità firewall [1,2]	1.0 Gbps	1.35 Gbps	1.65 Gbps	3.0 Gbps	3.8 Gbps	5.5 Gbps		16.3 Gbps [6]			30.0 Gbps [6]			35 Gbps [6]			40 Gbps [6]		
Velocità VPN [2,3]	190 Mbps	240 Mbps	300 Mbps	1.0 Gbps	1.2 Gbps	1.2 Gbps		2.3 Gbps [6]			7.5 Gbps [6]			9.3 Gbps [6]			10 Gbps [6]		
Velocità IPS [2]	400 Mbps	500 Mbps	600 Mbps	1.0 Gbps	1.4 Gbps	2.0 Gbps		5.0 Gbps [6]			8.3 Gbps [6]			11.3 Gbps [6]			13 Gbps [6]		
Sessioni concorrenti	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]		
Nuove sessioni/s	8,000	8,000	9,000	10,000	15,000	20,000		115,000 [6]			180,000 [6]			190,000 [6]			250,000 [6]		
HARDWARE																			
Fattore di forma	Desktop				1U Rack Mount												2U Rack Mount		
NIC in rame da 1GbE	4x	4x	6x	6x	8x	8x	8x	12x	8x	8x	24x	16x	16x	32x	16x	8x	16x	32x	16x
NIC SFP in fibre da 1GbE							4x		4x			8x				8x			16x
NIC SFP in fibre da 10GbE										2x			4x		8x	8x	4x	8x	8x
Switch integrato			8-porte	8-porte															
Wi-Fi Access Point		●	●	●															
CARATTERISTICHE																			
Firewall	●	●	●	●	●	●		●			●			●			●		
Controllo applicazioni [3]	●	●	●	●	●	●		●			●			●			●		
IPS [3]	●	●	●	●	●	●		●			●			●			●		
Routing Dinamico	●	●	●	●	●	●		●			●			●			●		
Selezione del provider in base all'applicazione	●	●	●	●	●	●		●			●			●			●		
VPN	●	●	●	●	●	●		●			●			●			●		
SSL Interception	●	●	●	●	●	●		●			●			●			●		
Ottimizzazione WAN	●	●	●	●	●	●		●			●			●			●		
Web Filter	●	●	●	●	●	●		●			●			●			●		
Gateway Mail & Spam Filter			●	●	●	●		●			●			●			●		
Malware Protection [4]	Opzionale	Opzionale	Opzionale	Opzionale	Opzionale	Opzionale		Opzionale			Opzionale			Opzionale			Opzionale		
Protezione avanzato delle minacce [4]	Opzionale	Opzionale	Opzionale	Opzionale	Opzionale	Opzionale		Opzionale			Opzionale			Opzionale			Opzionale		
Accesso Remoto Avanzato	Opzionale	Opzionale	Opzionale	Opzionale	Opzionale	Opzionale		Opzionale			Opzionale			Opzionale			Opzionale		

[1] Misurate con pacchetti grandi (MTU1500)
[2] Throughput dello chassis mediante porte multiple
[3] Velocità VPN utilizzando AES128 NOHASH
[4] È richiesto l'abbonamento a Energize Updates.
[5] Include protocolli E-Mail, FTP e Web
[6] Misurazione effettuata con porte in fibra 10GbE

Specifiche soggette a variazioni senza preavviso.