# Barracuda NextGen Firewall F

Die Next-Generation Firewall für das Cloud-Zeitalter



Immer mehr Unternehmen machen die Public Cloud zu einem Bestandteil ihrer Netzwerke. Dadurch wandeln sich Firewalls vom reinen Perimeterschutz hin zum Dreh- und Angelpunkt der IT Kommunikation. Die Barracuda NextGen Firewall F wurde speziell für die **Optimierung der Leistung, Sicherheit und Verfügbarkeit moderner, verteilter Unternehmens-SD-WANs** entwickelt.

- **☑** Security
- □ Data Protection
- $\hfill\Box$  Application Delivery







# **Der Barracuda-Vorteil**

- Einfaches Preismodell ohne Lizenzgebühren pro Applikation, User oder Server.
- Unlimitiertes Site-to-Site und Client-to-Site VPN inklusive
- Flexibler Einsatz: als Hardware, Virtuelle Appliance oder in der Cloud
- Konfiguration und Lifecycle-Management über eine grafische Benutzeroberfläche ohne die Notwendigkeit eines Command Line Interface

# **Produktmerkmale**

- Volle User-/Group-Awareness
- Volle Application-Visibility und granulare Application-Control
- Advanced Threat Protection (inkl. Sandboxing)
- Integrierte Web-Security und IDS/IPS
- Integrierte SD-WAN Funktionalität
- Cloud-Ready Application-Based Provider Selection



# **Kompromisslose Sicherheit**

Barracuda Next-Generation Firewalls schützen das gesamte Unternehmensnetzwerk. Firewalling, IPS, URL-Filtering, dualer Virenschutz und Applikationskontrolle erfolgt verzögerungslos direkt im Datenfluss. Ressourcenintensivere Schutzmechanismen zur Abwehr von Ransomware durch Sandboxing erfolgen nahtlos integriert in der Cloud. Der Schutzumfang ist über alle Plattformen und Modelltypen identisch - egal ob Aussenstellen- oder High-End Modelle - maximale Sicherheit bleibt gewährleistet.



# Vollintegrierte SD-WAN Funktionalität

Das Cloud-Zeitalter stellt Unternehmen vor die Anforderung jede Niederlassung direkt und sicher mit der Cloud zu verbinden. Kostspielige Anbindungen aller Außenstellen an den zentralen Internetanschluss mittels MPLS werden durch kostengünstige Breitbandanschlüsse ersetzt. Barracuda NextGen Firewalls nutzen bis zu 24 Breitbandanschlüsse pro VPN Tunnel in die Cloud für bessere Bandbreite bei deutlich geringeren Kosten.





## Kräfte bündeln

Barracuda NextGen Firewalls kombinieren Next-Generation Security und SD-WAN Vernetzungsoptimierung in einem Produkt mit zentralem Management. Dadurch können Unternehmen alle Vorteile der Cloud sicher nutzen und den Zugriff in die Cloud von jedem Punkt des Netzwerks aus optimieren. Dank der niedrigen Leitungskosten und der effizienten Verwaltung lassen sich die Betriebskosten erheblich senken.



Das Dashboard der Barracuda NextGen Firewall F-Serie bietet Echtzeitinformationer und Zusammenfassungen aller Prozesse in einem Unternehmensnetzwerk.

### **Technische Angaben**

#### E Firewall

- · Stateful Packet Inspection und Forwarding
- · IP-lose Konfiguration mittels Named-Networks
- · Volle User-Identity Awareness
- · Intrusion Detection und Prevention (IDS/IPS)
- · Application Control und granulares Application Enforcement
- · Abfangen und entschlüsseln von SSL/ TLS verschlüsselten Anwendungen
- · Antivirus und Web-Filtering im Single-Pass Modus
- · Email-Security
- · SafeSearch-Enforcement
- · Google-Accounts-Enforcement
- Denial-of-Service Schutz (DoS/DDoS)
- · Spoofing und Flooding Schutz
- Schutz vor ARP Spoofing und Trashing
- · DNS Reputation Filter
- · TCP Stream Reassembly
- · Transparentes Proxying (TCP)
- · NAT (SNAT, DNAT), PAT
- Dynamische Regeln/zeitbasierte Trigger
- Finzelobiekt-Orientiertes Regelwerk für Routing, Bridging und Routed-Bridging
- · Virtuelle Regeltestumgebung

#### High Availability

- · Aktiv-Aktiv (nur mit externem Load Balancer) oder Aktiv-Passiv
- Transparentes Failover ohne Session-Verlust
- · Netzwerkbenachrichtigung bei Failover
- · Verschlüsselte HA-Kommunikation

#### │ Intrusion Detection und Prevention ⊕ Traffic Intelligence & SD-WAN

- Schutz vor Exploits, Bedrohungen und Schwachstellen
- · Schutz vor Packet Anomaly und Fragmentation
- Fortschrittlichste Anti-Evasion und Obfuscation Techniken
- · Automatische Signatur Updates

#### **Advanced Threat Protection**

- Dynamische, "on-demand" Analyse von Malware (Sandboxing)
- Dynamische Analyse von Dokumenten mit eingebetteten Exploits (PDF, Office, usw.)
- · Detailierte Forensik für Malware Binaries und Web-Bedrohungen (Exploits)
- · Unterstützung für mehrere Betriebssysteme (Windows, Android, usw.) 🗣 VPN
- Botnet- und Spyware-Schutz
- · TypoSquatting und Link-Protection für E-Mail

### **Zentrale Management-Optionen** über NextGen Control Center

- · Unlimitierte 7ahl an Firewalls
- Mandantenfähig
- · Multi-Administrator & RCS
- · Zero-Touch Deployment
- Pool-Lizenz Management
- · Template & Repositorybasiertes Management
- REST API

#### Unterstützte Protokolle

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

- · Zertifizierte Verschlüsselung (FIPS 140-2) Automatische VPN-Tunnel-Erstellung zwischen entfernten Spoke-Standorten basierend auf dem Anwendungstyp
- Dynamische Bandbreitenerkennung
- Performance-basierte Transportauswahl 🚚 Instant Replacement Service
- · Anwendungsorientiertes Traffic-Routing
- · Adaptives Session-Balancing über mehrere Uplinks hinweg
- · Traffic-Replikation (vorwärts gerichtete Fehlerkorrektur)
- · Application-based Provider Selection
- Anwendungsorientiertes Traffic-Routing (VPN)
- · Traffic-Shaping und QoS
- Integrierte Datendeduplizierung

- · VPN-Tunnel-Konfiguration per Drag-and-Drop
- · VPNC-zertifiziert (grundlegende Interoperabilität)
- · Network Access Control
- · VPN-Unterstützung für Mobilgeräte mit iOS und Android
- · Multi-Faktor Authentisierung für SSL VPN und CudaLaunch

## Infrastructure Services

- · DHCP-Server, Relay
- · SIP-, HTTP-, SSH-, FTP-Proxies
- SMTP-Gateway & IPFIX Unterstützung
- · DNS Cache

· WLAN (802.11n)-Access Point für ausgewählte Modelle

## **Support Optionen**

#### **♦** Barracuda Energize Updates

- · Standardmäßiger technischer Support
- Firmware-Updates
- · IPS-Signaturen-Updates
- Application Control Definitionsupdates
- · Web-Filter-Updates

- · Austauschgeräteversand innerhalb eines Werktags
- Technischer 24-Stunden-Support
- Alle vier Jahre gratis Hardware Refresh

# **Zusätzliche Optionen**

· Advanced Threat und Malware Protection kombiniert den Schutz gegen Malware und Viren mit dem Sandboxing von Advanced Threat Protection wodurch auch Netzwerk-Angriffe, Zero-Dav-Malware-Exploits und anderer Advanced Malware wie Ransomware keine Bedrohung mehr darstellen.

- · Total Protect kombiniert die Hardware Appliance mit Energize Updates, Application Control, IPS, Web Filter, Malware Protection, E-Mail Security, Warranty Extension, und 8x5 Standard Support.
- · Total Protect PLUS kombiniert die Hardware Appliance mit Energize Updates, Application Control, IPS, Web Filter, Email Security, Advanced Threat und Malware Protection, Advanced Remote Access und 24x7 Support.

EINSTIEGS- UND BRANCH OFFICE MODELLE	F18		F8x MODELLE		F1 MOI	F200	
		F80	F82.DSLA	F82.DSLB	F180	F183	F280
LEISTUNG							
Firewall-Durchsatz <sup>1</sup>	1.0 Gbps		1.35 Gbps		1.65	Gbps	3.0 Gbps
VPN-Durchsatz <sup>2</sup>	190 Mbps	240 Mbps			300	1.0 Gbps	
IPS-Durchsatz <sup>3</sup>	400 Mbps	500 Mbps			600	1.0 Gbps	
NGFW-Durchsatz <sup>4</sup>	300 Mbps	400 Mbps			550	800 Mbps	
Gleichzeitige Sessions	80,000	80,000			100	250,000	
Neue Sessions/s	8,000	8,000			9,0	10,000	
HARDWARE							
Formfaktor	Desktop	Desktop	Desktop	Desktop	Desktop	Desktop	Desktop
Kupfer-Ethernet-NICs	4x1 GbE	4x1 GbE	4x1 GbE	4x1 GbE	6x1 GbE	6x1 GbE	6x1 GbE
Glasfaser-SFP -NICs	-	-	1x1 GbE	1x1 GbE	-	2x1 GbE	-
Integrierter Switch	-	-	-	-	8-Port	-	8-Port
Integriertes Modem	-	-	DSL Annex A, RJ11	DSL Annex B, RJ45	-	-	-
WLAN Access Point	-	•	•	•	•	•	•
Stromversorgung	Single Extern	Single Extern	Single Extern	Single Extern	Single Extern	Single Extern	Single Extern
FEATURES							
Firewall	•	•	•	•	•	•	•
Application Control	•	•	•	•	•	•	•
IPS	•	•	•	•	•	•	•
Dynamic Routing	•	•	•	•	•	•	•
Application-based Provider Selection	•	•	•	•	•	•	•
Client-to-Site & Site-to-Site VPN (unlimitiert)	•	•	•	•	•	•	•
SSL Interception	•	•	•	•	•	•	•
SD-WAN	•	•	•	•	•	•	•
Web Filter	•	•	•	•	•	•	•
Zero-Touch Deployment	•	•	•	•	•	•	•
Advanced Threat und Malware Protection	Optional	Optional	Optional	Optional	Optional	Optional	Optional
Total Protect	Optional	Optional	Optional	Optional	Optional	Optional	Optional
Total Protect PLUS	Optional	Optional	Optional	Optional	Optional	Optional	Optional

MID-RANGE MODELLE	F380	F400 MODELLE				F600 MODELLE				
MID-RANGE MODELLE	F360	STD	F20	C10	C20	F10	F20	E20		
LEISTUNG										
Firewall-Durchsatz <sup>1</sup>	3.8 Gbps	5.5 (	Gbps			16.3 Gbps				
VPN-Durchsatz <sup>2</sup>	1.2 Gbps	1.2 Gbps			2.3 Gbps					
IPS-Durchsatz <sup>3</sup>	1.4 Gbps	2.0 Gbps		5.0 Gbps						
NGFW-Durchsatz <sup>4</sup>	1.0 Gbps	1.2 Gbps		4.6 Gbps						
Gleichzeitige Sessions	400,000	500,000		2,100,000						
Neue Sessions/s	15,000	20,000		115,000						
HARDWARE										
Formfaktor		1U Rackmount		1U Rackmount						
Kupfer-Ethernet-NICs	8x1 GbE	8x1 GbE	8x1 GbE	12x1 GbE	12x1 GbE	8x1 GbE	8x1 GbE	8x1 GbE		
Glasfaser-SFP -NICs	-	-	4x1 GbE	-	-	4x1 GbE	4x1 GbE	-		
Glasfaser-SFP+-NICs	-	-	-	-	-	-	-	2x10 GbE		
Stromversorgung	Single Intern	Single Intern	Dual Hot Swap	Single Intern	Dual Hot Swap	Single Intern	Dual Hot Swap	Dual Hot Swap		
FEATURES										
Firewall	•	•	•	•	•	•	•	•		
Application Control	•	•	•	•	•	•	•	•		
IPS	•	•	•	•	•	•	•	•		
Dynamic Routing	•	•	•	•	•	•	•	•		
Application-based Provider Selection	•	•	•	•	•	•	•	•		
Client-to-Site & Site-to-Site VPN (unlimitiert)	•	•	•	•	•	•	•	•		
SSL Interception	•	•	•	•	•	•	•	•		
SD-WAN	•	•	•	•	•	•	•	•		
Web Filter	•	•	•	•	•	•	•	•		
Zero-Touch Deployment	•	•	•	-	-	-	-	-		
Advanced Threat und Malware Protection	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional		
Total Protect	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional		
Total Protect PLUS	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional		

LEISTUNG Firewall-Durchsatz <sup>1</sup>	ссс	CCF 30 Gbps	CCE	ссс	CCE	CFE	CE0	CE2	CFE		
Firewall-Durchsatz <sup>1</sup>											
					35 Gbps			40 Gbps			
VPN-Durchsatz <sup>2</sup>		7.5 Gbps			9.3 Gbps			10 Gbps			
IPS-Durchsatz <sup>3</sup>		8.3 Gbps			11.3 Gbps			13 Gbps			
NGFW-Durchsatz <sup>4</sup>	7.0 Gbps			8.0 Gbps			10.2 Gbps				
Gleichzeitige Sessions	2,500,0000			4,000,000			10,000,000				
Neue Sessions/s	180,000			190,000			250,000				
HARDWARE											
Formfaktor	1U Rackmount			1U Rackmount			2U Rackmount				
Kupfer-Ethernet-NICs	24x1 GbE	16x1 GbE	16x1 GbE	32x1 GbE	16x1 GbE	8x1 GbE	16x1 GbE	32x1 GbE	16x1 GbE		
Glasfaser-SFP -NICs	-	8x1 GbE	-	-	-	8x1 GbE	-	-	16x1 GbE		
Glasfaser-SFP+-NICs	-	-	4x10 GbE	-	8x10 GbE	8x10 GbE	4x10 GbE	8x10 GbE	8x10 GbE		
Stromversorgung	Dual Hot Swap			Dual Hot Swap			Dual Hot Swap				
FEATURES											
Firewall	•	•	•	•	•	•	•	•	•		
Application Control	•	•	•	•	•	•	•	•	•		
IPS	•	•	•	•	•	•	•	•	•		
Dynamic Routing	•	•	•	•	•	•	•	•	•		
Application-based Provider Selection	•	•	•	•	•	•	•	•	•		
Client-to-Site & Site-to-Site VPN (unlimitiert)	•	•	•	•	•	•	•	•	•		
SSL Interception	•	•	•	•	•	•	•	•	•		
SD-WAN	•	•	•	•	•	•	•	•	•		
Web Filter	•	•	•	•	•	•	•	•	•		
Advanced Threat und Malware Protection	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional		
Total Protect	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional		
Total Protect PLUS	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Optional		

Alle Performance-Zahlen werden unter optimierten Bedingungen gemessen, sind als "bis zu" Werte zu betrachten und können je nach Systemkonfiguration und Infrastruktur variieren:

1 Firewall-Durchsatz gemessen mit großen UDP-Paketen (MTU1500), bidirektional über mehrere Ports; Falls vorhanden mit 10Gbps-Ports gemessen.

2 VPN-Performance basiert auf Barracuda TINA VPN-Protokoll, 1415 Byte UDP-Pakete mit AES128 NOHASH, bidirektional mit BreakingPoint-Traffic-Generator; Falls vorhanden mit 10Gbps-Ports gemessen.

3 IPS-Durchsatz gemessen mit großen UDP-Paketen (MTU1500) und über mehrere Ports.

4 NGFW-Durchsatz wird mit IPS, Application Control und Web Filter aktiviert, basierend auf BreakingPoint Realworld-IPS-Enterprise-Traffic-Mix, bidirektional über mehrere Ports hinweg gemessen. Falls vorhanden mit 10Gbps-Ports gemessen.



# Protecting People, Businesses, and Brands

Available today for Office 365, and coming soon to other platforms.







# Barracuda Sentinel

Al for Real-Time Spear Phishing and Cyber Fraud Defense



