



netfence gateways

netfence gateways sind speziell entwickelte Security Server, die neue Maßstäbe in Bezug auf Sicherheit, Connectivity und Management in Unternehmensnetzwerken setzen.

Mit Hilfe eines bewährten Schnellinstallationsverfahrens wird handelsübliche Intel-Serverhardware in weniger als vier Minuten zu einem netfence Firewall- und VPN-Gateway. Das leistungsfähige Betriebssystem von netfence, das phionOS*, sichert das reibungslose Zusammenspiel von Networking und Routing mit modernster Firewalling- u. VPN-Technologie. netfence gateways sind das Resultat der Evolution von traditionellen Security Gateways, hin zu intelligenten Traffic Managern, die Unternehmen zu Sicherheit und gleichzeitig signifikant besserer Verfügbarkeit ihrer digitalen Kommunikationswege bei deutlich niedrigeren Betreiberkosten

verhelfen.

netfence gateways vereinen Gigabit-Firewalling, modernste VPN Technologie, Content Security mit Intrusion Prevention zur Abwehr von Angriffen, SPAM- und URL-Filter, Schutz gegen DDoS/DoS-Attacken sowie Bandbreitenmanagement mit Standard Application Gateway-Funktionalität. netfence gateways können auch als SMTP Mail Router, DNS-Server oder HTTP Proxy eingesetzt werden, um Infrastrukturen sowohl auf Netzwerk- als auch auf Anwendungsebene zu schützen und zu verstärken.

Firewall

Die Firewall-Komponente von netfence ist mit allen im Unternehmensbereich relevanten Funktionen ausgestattet und verwendet durchgängig modernste Stateful und Deep-Level Inspection-Technologie, um Firmennetzwerke nachhaltig vor Angriffen von außen und

Features & Benefits

- **Multifunktions-Sicherheitslösung**
Gigabit-fähige Stateful und Deep-Level Inspection Firewall, VPN, SPAM-Filter, Intrusion Prevention, URL-Filter, Bandbreitenmanagement.
- **Hervorragendes Echtzeit- und Langzeit Reporting**
Stellt grafische Informationen zu Nutzungsverhalten, Performance und Auslastung zur Verfügung und ermöglicht die proaktive Überwachung von sicherheitsrelevanten Ereignissen.
- **Hervorragendes Preis-Leistungs-Verhältnis**
Durch Koppelung mit phionOS stellt netfence eine echte Software Appliance dar.
- **Intelligentes Traffic Management**
Redundante, mit NAT und Proxy kompatible VPN-Tunnel, Multi-Provider-Installationen, Breitband Internetverbindungen mit dynamischen IPs.
- **Umfassende Networking-Fähigkeiten**
802.1q VLAN Tagging, Trunking, Policy Routing, Tokenring-Unterstützung, integrierter OSPF Router.
- **High Availability**
Regelmässige Synchronisation der bestehenden Sessions zwischen den HA Partnern für unterbrechungsfreie Übernahmen.
- **Policy Management**
Komplettes Policy Management für skalierbare VPN Client-Projekte PKI kompatibel (Unterstützung für X.509v3 Policy-Extensions)
- **Umfassendes Management und Skalierbarkeit**
netfence Connectivity Gateways verfügen über herausragende Managementfähigkeiten, die das sichere und effiziente Management selbst mehrerer tausend Gateways und Remote VPN Clients ermöglichen.
- **Remote Access**
Management erfolgt auf SSL-Protokoll-Basis mit starker zweistufiger Authentisierung und 3DES/AES Verschlüsselung. Jedes netfence System ist durch ein eigenes digitales x.509 Zertifikat mit 1024-bit RSA-Schlüssel identifizierbar.
- **Zu den Managementfähigkeiten zählen:**
 - Auf phion.a GUI basierendes Konfigurationsmanagement einschließlich OS Management.
 - Umfassendes Eventing mit Benachrichtigung (UDP, eMail, SNMP)
 - Echtzeitverwaltung von phion OS und Gateway-Serviceaktivitäten.
 - Multiadministratorfähiges Management.
 - Flexible, mandantenfähige, rollenbasierende Administrationsmodelle.
 - VPN-Technologie mit Connection Intelligence gewährleistet zentralisiertes Remote Management auch mit dynamischen IP-Adressen.

* phionOS basiert auf einem optimierten und gehärteten Linux Betriebssystem, das um eine leistungsstarke und sichere Managementschicht erweitert wurde.

innen zu schützen. netfence gateways bieten pro Firewall-Regel die Wahl zwischen leistungsfreundlichem Stateful-Packetfiltering oder transparentem Applikationsproxying für zusätzlichen Schutz vor Angriffen auf der TCP-Stack- und Applikationsebene. netfence gateways bringen ungeahnte Flexibilität und Sicherheit für moderne Netzwerkinfrastrukturen durch folgende Features:

- Voll integrierte wartungsfreundlichen Lösung mit optimiertem phionOS Betriebssystem, für erhöhte Security und Connectivity und optimales Preis-Leistungs-Verhältnis im Gigabit-Bereich als herkömmliche Appliance-Lösungen.
- Routet alle gängigen IP-Protokolle, überwacht den ARP-Verkehr an allen aktiven Netzwerkschnittstellen.
- Umfassender Schutz vor DoS-Attacken inkl. SYN Flood, Flood Ping, Port/Address Range Scans.
- Intrusion Prevention durch musterbasierte Datenstromanalyse pro Firewallregel einstellbar.
- NAT, Port Address Translation (PAT) zur Absicherung interner oder nicht routbarer Netzwerke.
- Routing oder vollständig überwachter Bridging-Betriebsmodus.
- Hochverfügbare Firewall durch kontinuierliche Synchronisierung der bestehenden Sessions zwischen den HA Partnern.

phionOS

phionOS verwandelt ein gehärtetes, und optimiertes Linux-Betriebssystem mittels zusätzlicher struktureller Komponenten in ein vollständig gemanagtes Betriebssystem. Aufgrund der Bündelung mit phionOS besitzt jedes netfence gateway alle Managementvorteile einer echten Appliance, jedoch ohne deren typische Nachteile. Anzahl oder Art der verfügbaren Netzwerkschnittstellen sowie Gerätekosten bestimmt der Anwender selbst. Das innovative Schnellinstallationsverfahren von netfence benötigt weniger als vier Minuten, um ein neues Gateway auf Intel-Hardware aufzusetzen und in Betrieb zu nehmen. Das gleiche gilt für die Wiederinbetriebnahme nach einem Hardwareausfall. phionOS ist in allen netfence gateways enthalten und verfügt über folgende Kernfeatures:

- Umfassende Networking- und Routing-Fähigkeiten zur Unterstützung von Multi-Provider-Installationen oder redundanten Routingpfaden.
- Eigene Host-Firewall zum Schutz der netfence gateways vor unbefugtem Zugriff / Attacken.
- VLAN-Support zur Unterstützung der Integration der Security in bestehende Netzwerke.
- High Availability für maximale Zuverlässigkeit und fehlertoleranten Betrieb.
- Überwachung des gesamten Systemzustands und Echtzeitüberwachung von Aktivitäten.
- Unterstützung von dynamischer IP-Adressenzuweisung die zur Breitband-Anbindung kleinerer Zweigstellen an das Internet verwendet wird.
- Managementfunktionen auf GUI-Basis zur Systemüberwachung und vollständigen Konfiguration von netfence gateways sind sowohl in-band als auch über dedizierte Netzwerkschnittstellen

verfügbar.

- Serielle Schnittstellen sowie Command Line Interface stehen ebenfalls zur Verfügung.

Virtual Private Network (VPN)

Neben einer Firewall auf Basis modernster Technologie bieten netfence gateways auch eine VPN-Lösung, die den Einsatz von VPN Technologien auf höchstem Niveau ermöglicht, z.B. zur Standortvernetzung, zur Sicherung von Wireless LANs mit IPsec-Technologie oder zur Anbindung von mobilen Mitarbeitern.

Der integrative Charakter des phionOS stellt sicher, dass der gesamte VPN-Datenverkehr nach der Entschlüsselung oder vor der Verschlüsselung für sämtliche Standort-Verbindungen durch die Firewall zusätzlich gefiltert wird. netfence gateways erreichen dadurch eine verbesserte granulare Zugangskontrolle an den Tunnelendpunkten und machen somit die konsequente Durchsetzung von Sicherheitsvorgaben möglich. netfence Tunneltechnologie mit Traffic Intelligence lässt flexible, zuverlässige und kostengünstige globale VPN-Architekturen Realität werden durch:

- Unterstützung redundanter VPN Gateways,
- Konfiguration mehrerer Gateways für einen beliebigen Tunnel mit transparenter Verbindungsübernahme.
- Lastverteilung über mehrere VPN-Tunnel (jede Kombination aus Standleitung, Internet über DSL oder Standleitung und/oder Frame Relay möglich) je nach Protokoll oder Zieladresse. Das Zusammenspiel von Firewall- und Routing-Fähigkeiten des phionOS ermöglicht damit Kostenreduktion und sorgt für hohe VPN-Verfügbarkeit.
- Enkapsulierungstechnologie ermöglicht die Kombination der Sicherheit von IPsec und der Connectivity eines SSL-basierten VPN in einem Produkt.
- Unterstützung von Breitband-Internetzugang mit dynamischen IP-Adressen (xDSL, ISDN, Kabel).
- Umfassende Remote Access VPN-Unterstützung. Flexible, starke zweistufige Benutzer-Authentifizierung mit Unterstützung für integrierte Windows Domänenanmeldung (Pre-logout) und serverseitig administrierbare VPN Client Firewall zur Sicherung aller Tunnelendpunkte.
- Vollständiges zentrales Management aller VPN Client Einstellungen.

Content Security

- Intrusion Prevention
Moderne Firewalls schützen Ihr Netz sowohl auf Netzwerk- als auch auf Anwendungsebene. Aus diesem Grund enthält die integrierte Firewall auch umfassende Mechanismen zur Erkennung und zur Abwehr von auf Anwendungsprotokollen basierenden Attacken auf die Serverressourcen des Unternehmensnetzes. Um dieses wirksam vor Angriffen zu schützen, durchsucht das gateway den Datenstrom nach Mustern zur Ausnutzung von Sicherheitslücken. Werden solche Muster gefunden, wird die Verbindung instantan abgebrochen. Somit wird der Angriff unterbunden, noch bevor er den Server

Firewall	
Stateful packet forwarding	Yes, per rule
Transparent proxying mode (TCP)	Yes, per rule
Inline graphical packet analyser	Yes
NAT (src, dst, nets), PAT	Yes
Policy based NAT	Yes, per rule
Protocol support	IPv4, ARP
Gigabit performance	Yes
Object oriented ruleset	Yes
Virtual rule sets	Yes
Virtual rule test environment	Yes
Redirection to local application	Yes
Realtime connection status	Yes
Historical access caches	Yes
Event triggered notification	Yes
Load balancing for protected servers	Yes
Multipath load balancing	Yes
Dynamic rules with timer triggered deactivation	Yes, per rule
Bridging mode / Routing mode	Yes
Virtual IP (proxyARP) support	Yes
User Authentication	Yes
RPC protocol support	ONC-RPC, DCE-RPC
VoIP support	H.323, SIP, SCCP (skinny)

Network Attack Protection	
Active ARP handling	Yes
Inline Intrusion prevention	Yes
Attack patterns configurable	Yes, unlimited
DoS and DDoS protection	Yes
SYN attack protection	Yes
Reverse routing path check	Yes
ICMP flood ping protection	Yes, by size and rate limit
Malformed packet check	Yes

Routing, Networking	
Ethernet support	Yes (10/100/1000Mbit)
Tokenring support	Yes (4/16Mbit)
Max number of physical interfaces	16
802.1q VLAN support	Yes, up to 4096
xDSL support	PPPoE, PPTP (multi-link)
DHCP client support	Yes
ISDN support	EuroISDN (syncppp, rawip)
Link monitoring	Yes (DHCP, xDSL, ISDN)
Policy routing support	Yes
Ethernet channel bonding	Yes
Multiple networks on interface, IP aliases	Yes
Configurable MTU size	Yes, per route
IPinIP and GRE tunnels	Yes
Integrated OSPF router	Yes

Traffic Management	
Maximum overall bandwidth	Yes, per interface
Number of traffic bands	8 per interface (Sys, A-G)
On-the-fly reprioritisation	Yes, via firewall status GUI
Ingress Shaping	Yes, per interface

Central User Authentication	
Supported services	VPN, FW, HTTP/FTP/SSH proxy
External database types	Microsoft NTLM, RADIUS, RSA SecurID, LDAP/LDAPS, Microsoft Active Directory

High Availability	
Hot standby mode	Yes
Network notification on failover	Yes
Key-based authentication	Yes
Encrypted HA communication	Yes
Transparent Failover without session loss	Yes
Provider/Link Failover	Yes

VPN	
Encryption	AES, 3DES, DES, Null
Private CA	Yes, up to 4096bit RSA
External PKI support	Yes
x.509v3 policy extensions	Fully recognised
Certificate revokation	OCSF, CRL
Site-to-site VPN	Yes
Star (hub and spoke) VPN network topology	Yes
Client VPN*	Yes
Microsoft domain logon (Pre-logon)	Yes
Strong user authentication	Yes
Replay protection	Yes
NAT traversal	Yes
HTTPS and SOCKS proxy compatible	Yes
Redundant VPN gateways	Yes
Native IPSEC for 3rd party connectivity	Yes
PPTP/L2TP (IPSec)	Yes, client VPN only
OSPF via VPN	Yes

System Management	
In-band management	Yes, all functions available
Dedicated management interface	Yes
Serial interfaces	Management and/or console
Central management interface	Yes
All management via VPN tunnel	Yes
SSH based access	Yes
Management Centre compatible	Yes
System maintenance fully GUI based	Yes
Command line interface (CLI) available	Yes

Logging/Monitoring/Accounting	
System health, activity monitoring	Yes
Monitoring of network environment	Yes
Dynamic routing table updates	Yes
FW connection monitoring	Yes
Human readable log files	Yes
Active event notification	UDP/email/SNMP trap
Realtime accounting and reporting	Yes, 10 sec interval
Syslog streaming	Yes

Additional functions	
Multi-domain capable DNS server	Yes, fully GUI configurable
DHCP relay and server	Yes
GUI-based DHCP server management	Yes
NTP4 time server and client	Yes
SMTP gateway	Yes
SPAM mail filtering	Yes
GUI-based mail spool queue management	Yes
Caching HTTP proxy (based on squid)	Yes
FTP & SSH gateway	Yes
Accounting for additional functions	Yes

Administration	
Multiple Administrators	Yes, role based
Key-based authentication	Yes
Passphrase authentication	Yes
Strong authentication	Yes
SSL-based Windows-GUI access	Yes, AES128
Access control lists (ACL)	Yes
Configuration management	GUI/MC
Software updates	GUI/MC
Network misconfiguration protection	Yes

