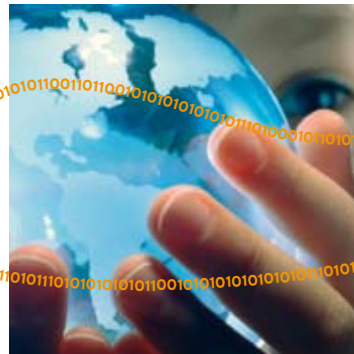


That's what we call Unified Threat Management

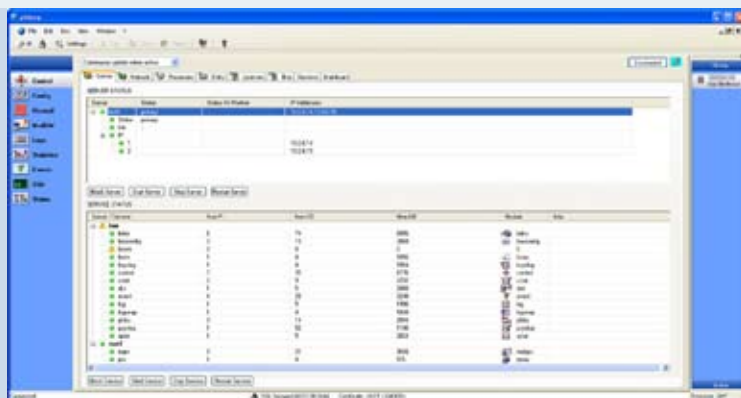
## ➤ netfence gateways



**Effective Perimeter Security is a combination of Firewall, Content Security and intelligent Mail Security. phion netfence integrates all these tasks in one Management and efficiently protects your Corporate Communication from various enemies such as Hacker attacks, Viruses, Worms, Spyware, Disgruntled employees, human error (e.g. your provider), natural disasters, etc.**

### Features & Benefits

- **Multi-Purpose Protection Platform**
- **Powerful Real-Time & Historical Reporting Capabilities**
- **Outstanding Cost-Performance Ratio**
- **Intelligent Traffic Management**
- **Extensive Networking Capabilities**
- **High Availability**



netfence gateways integrate gigabit-performance firewall, cutting-edge technology VPN, intrusion prevention, DDos/DoS protection, and intelligent application selective bandwidth and multipath management with other critical application gateway functionality.

A netfence gateway may also act as a fully fledged SMTP mail router, DNS server, or HTTP proxy thereby protecting and strengthening your infrastructures both on the network and the application security level.

### Firewall

netfence's full-featured firewall component uses state-of-the-art stateful and deep level inspection based technology to provide thorough protection against external and internal attacks on your IT resources. netfence gateways offer a per-rule choice between performance friendly standard stateful packet forwarding or transparent application proxying for extra protection against attacks staged at the TCP stack and application level. netfence gateways provide added flexibility and security for today's networks through:

- Fully integrated and easy to maintain solution with optimised phionOS providing a higher level of security and connectivity than loosely coupled software based solutions and better cost-performance ratio in the gigabit domain than specialised appliance solutions.
- Routes all commonly used IP protocols, monitors ARP activity on all active network interfaces.

- Supports extensive DoS and attack mitigation features including SYN flood, flood ping, port/address range scans.
- Pattern based intrusion prevention with data stream filtering on a per rule basis.
- NAT and port address translation (PAT) to shield internal or non-routable networks.
- Routing or fully-inspected bridging mode of operation.
- High availability firewall through continuous synchronisation of existing sessions between HA partners.

### Content Security

State-of-the-art firewalls protect your network both at the network level and at the application level. This is why the integrated firewall also includes extensive mechanisms for the recognition of and defence against application-protocol-based attacks on the server resources of your company's network. netfence gateways provide effective intrusion prevention by scanning traffic for known exploit patterns and terminating the connection instantaneously in case of a match.

Thus the protocol exploit is intercepted before it may ever reach and harm your server. In addition netfence gateways provide transparent redirection of network traffic into local application gateways such as a SMTP mail router, a HTTP proxy or a local DNS server for extra protocol protection.



www.phion.com

# netfence gateways

Unwanted mails have become a serious problem for corporate networks. A spam filter integrated into the SMTP mail gateway of netfence gateway helps to regain control over mail traffic by identifying spam mails. Spam filter definitions may be set very easily by both administrator and mail user.

A netfence gateway may be equipped with an URL filter that works together with the HTTP proxy.

Web content filtering allows administrators to consequently enforce and maintain the corporate security policies. Better control of Internet access protects networks from unwanted content and increases the productivity of employees.

All Web and SMTP-Mail traffic may be scanned for viruses and other malware by means of a separate fully integrated AV scanning service. phion netfence gateway thus can stop viruses and malicious code already at the network perimeter.

## WAN Optimisation

netfence gateway's unique traffic intelligence is effected by the integrative nature of phionOS. Powerful routing features such as policy routing in combination with continual smart monitoring of the network environment make intelligent traffic routing possible.

In combination with firewall functionality, bandwidth-management and VPN true traffic intelligence is available turning arbitrary IP-communication structures into highly failsafe networks. Multi-provider setups for Internet link redundancy and protocol based load balancing over multiple links for maximum cost-efficiency and top reliability is netfence's daily business. Thus netfence offers optimisation of connection costs through a high availability design that extends from the link layer all the way to the application level.

netfence gateways allow defining a traffic management scheme for each network interface on your netfence gateway. This means you define the maximum permissible bandwidth for inbound (ingress) and outbound traffic on the interface as well as eight traffic bands which each are allotted a certain percentage of the maximum bandwidth. Within the firewall rule set you may assign traffic to each of these bands based on IP address or network protocol information. This means your critical applications are always guaranteed a fixed minimum amount of bandwidth.

## Virtual Private Network (VPN)

In addition to a state-of-the-art stateful inspection firewall netfence gateways are also a full-featured VPN solution facilitating advanced VPN deployments such as cross-linking the company locations, securing wireless LANs with IPsec technology or linking mobile workers.

The integrated nature of the phion OS underlying netfence warrants that VPN traffic is routinely inspected after decryption or prior to encryption for all site-to-site traffic. With netfence VPN traffic is fully firewalled and thus gives you more granular access control at the tunnel endpoints for a more thorough

enforcement of your security policies. Using netfence's cutting edge tunnel technology with traffic intelligence flexible, reliable and cost-efficient global VPN security architectures become a reality due to:

- Redundant VPN gateway support.
- Configure multiple gateways for a given tunnel with automated fail-over when a gateway becomes unreachable.
- Protocol or address based load balancing over several VPN-tunnels (any combination of leased lines, internet via DSL or leased line and/or frame relay) due to an interplay of firewall and routing capabilities of the phionOS. This helps reducing costs and provides superior VPN high availability.
- Leading encapsulation technology combines the security of IPsec and the connectivity of SSL based VPN in one product.
- Support for broadband internet access with dynamic IP addresses (xDSL, ISDN, Cable).
- Extensive remote access VPN support, flexible and strong 2-factor user authentication including support for Windows domain logons (pre-logon) and a server-side managed VPN client firewall to secure all tunnel endpoints.
- Complete central policy management for client VPN.

## Management and phionOS

By adding additional structural components, phionOS transforms a hardened and optimised Linux OS into a fully managed operating system. Since netfence software comes bundled with its own optimised operating system phionOS, it provides all the management advantages of a genuine appliance without annoying hardware limitations on number or type of available network interfaces. netfence's proven speed install procedure takes less than 4 minutes to get a new gateway up and running or to restore it to its previous state after a server hardware failure. phionOS provides many of the core features of the netfence gateway and is part of all netfence products:

- Extensive networking and routing capabilities to support multi-provider set-ups or redundant routing paths.
- Separate host firewall protecting netfence gateways from unauthorized access attempts and attacks.
- VLAN support to facilitate integration of security into existing networks.
- High availability for maximum reliability & fault tolerant operation.
- Health-monitoring and real-time activity accounting.
- Support for dynamic IP address assignment commonly used to connect branch offices to the internet (broadband).
- GUI based management functions providing overall control and complete configuration of the netfence gateway are available in-band or via dedicated network interfaces.
- Serial interfaces and a command line interface are provided.

Beside the phion.a GUI Management every netfence gateway can be managed through netfence Management Centres. These allow enterprises to manage even thousands of netfence gateways at lowest costs.

# That's what we call Unified Threat Management

Firewall	
Stateful packet forwarding	✓ per rule
Transparent proxying mode (TCP)	✓ per rule
Inline graphical packet analyser	✓
NAT (src, dst, nets), PAT	✓
Policy based NAT	✓ per rule
Protocol support	IPv4, ARP
Gigabit performance	✓
Object oriented ruleset	✓
Virtual rule sets	✓
Virtual rule test environment	✓
Redirection to local application	✓
Realtime connection status	✓
Historical access caches	✓
Event triggered notification	✓
Load balancing for protected servers	✓
Multipath load balancing	✓
Firewall-to-Firewall compression (stream & packet compr.)	✓
Dynamic rules with timer triggered deactivation	✓ per rule
Bridging mode / Routing mode (mixed)	✓
Virtual IP (proxyARP) support	✓
User Authentication (x.509, Microsoft NTLM, RADIUS, RSA SecurID, LDAP/LDAPS, Microsoft Active Directory)	✓
RPC protocol support	ONC-RPC, DCE-RPC
VoIP support	H.323, SIP, SCCP (skinny)
Network Attack Protection	
Active ARP handling	✓
Inline Intrusion prevention	✓
Behaviour-based IPS option (P2P, IM, Skype)	✓
Attack patterns configurable	✓ unlimited
SYN / DoS / DDoS attack protection	✓
Reverse routing path check	✓
ICMP flood ping protection	✓ by size and rate limit
Malformed packet check	✓
Routing, Networking	
Ethernet support	✓ (10/100/1000Mbit)
Max number of physical interfaces	32
802.1q VLAN support	✓ up to 4096
xDSL support	PPPoE, PPTP (multi-link)
UMTS/EDGE/HSDPA	Appliance-based only
DHCP client support	✓
ISDN support	EuroISDN (syncppp, rawip)
Link monitoring	✓ (DHCP, xDSL, ISDN)
Policy routing support	✓
Ethernet channel bonding	✓
Multiple networks on interface, IP aliases	✓
Configurable MTU size	✓ per route
IPinIP and GRE tunnels	✓
Integrated OSPF/RIP router	
Traffic Management	
Maximum overall bandwidth	✓ per interface
Number of traffic bands	✓
On-the-fly reprioritisation	✓ via firewall status GUI
Ingress Shaping	✓ per interface
Central User Authentication	
Supported services	VPN, FW, HTTP/FTP/SSH proxy
External database types	MS* NTLM, RADIUS, RSA SecurID, LDAP/LDAPS, MS Active Directory
High Availability	
Standby mode	Active-Active**, Active-Passive
Network notification on failover	✓
Key-based authentication	✓
Encrypted HA communication	✓
Transparent Failover without session loss	✓
Provider/Link Failover	✓

VPN	
Encryption	AES-128/256, 3DES, DES, Null
Cryptohardware acceleration	✓ **
Private CA	✓ up to 4096bit RSA
External PKI support	✓
x.509v3 policy extensions	Fully recognised
Certificate revocation	OCSP, CRL
Site-to-site VPN	✓
Star (hub and spoke) VPN network topology	✓
Client VPN***	✓
Microsoft domain logon (Pre-logon)	✓
Strong user authentication	✓
Replay protection	✓
NAT traversal	✓
HTTPS and SOCKS proxy compatible	✓
Redundant VPN gateways	✓
Native IPSEC for 3rd party connectivity	✓
PPTP/L2TP (IPSec)	✓ client VPN only
OSPF via VPN	✓

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

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

Additional functions	
Multi-domain capable DNS server	✓ fully GUI configurable
GUI-based DHCP server management	✓
NTP4 time server and client	✓
SMTP/POP3 gateway	✓
SPAM mail filtering	✓
GUI-based mail spool queue management	✓
Caching HTTP proxy (based on squid)	✓
FTP & SSH gateway	✓
Accounting for additional functions	✓

Supported Platforms	
Standard	Intel x86
Crossbeam****	X-Series, C2, C6
Sun	Sun Fire 4200

\* MS = Microsoft  
 \*\* only with load balancer  
 \*\*\* check back for crypto hardware compatibility list  
 \*\*\*\* check back for compatibility list

## netfence Product family

	needs	purpose		solution		management
customer requirements	Comprehensive UTM protection of the critical resources and processes of a company	<b>Perimeter Security</b>	appliances	<b>netfence gateways</b>	central	<b>netfence Management Centre &amp; netfence reporter</b>
	Protection against undesired content such as SPAM, manipulated emails and web pages, worms, viruses etc.	<b>Content Security</b>		<b>netfence contegrity</b>		
	UTM protection and high level of availability for remote sites	<b>Secure Connectivity</b>		<b>netfence sintegra</b>		
	UTM protection and high level of availability for micro offices			<b>netfence edge</b>		
	Protection against internal threats and misuse	<b>Internal Security</b>		<b>netfence sectorwall</b>		
	Unrestricted connectivity and policy enforcement	<b>Endpoint Security</b>	VPN	<b>netfence VPN Connectors</b>		
	UTM protection for industrial environments	<b>Industrial Security</b>	specialists	<b>netfence industrial</b>		
	UTM protection for SMBs	<b>UTM protection for single locations</b>		<b>netfence M</b>	direct	<b>phion.a</b>

## Contact information

Headquarters	<b>phion AG</b>
	Eduard-Bodem-Gasse 1
	6020 Innsbruck
	AUSTRIA
	Phone +43 (0)508 100
	Fax +43 (0)508 100 20
	Mail office@phion.com

**netfence**  
your  
**network**

	 <b>Austria</b>	 <b>Germany</b>	 <b>Italy</b>	 <b>Switzerland</b>
Regional Offices	<b>phion Sales Office Vienna</b>	<b>phion AG</b>	<b>phion AG</b>	<b>phion Swiss GmbH</b>
	Mooslackeng. 15-17 / Top 2042	Humboldtstr. 12	Via Borgogna 2	Sempacherstrasse 15
	1190 Vienna	85609 Dornach / Munich	20122 Milan	8044 Zurich
	AUSTRIA	GERMANY	ITALY	SWITZERLAND
	Phone +43 (0)508 100	Phone +49 (0)89 9449 0240	Phone +39 346 8664 420	Phone +43 (0)508 100
	Fax +43 (0)508 100 20	Fax +49 (0)89 9449 0110	Fax +39 0362 476 863	Fax +43 (0)508 100 20
	Mail office@phion.com	Mail office@phion.com	Mail office@phion.com	Mail office@phion.com

