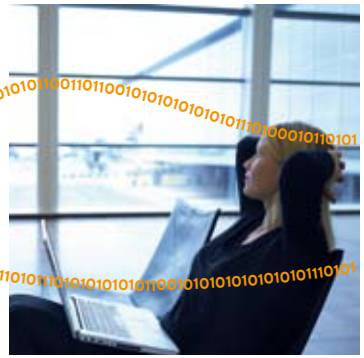


Client security and connectivity for highest demands

## netfence VPN Connectors



To meet the requirements of today's connectivity, comprehensive solutions are required that not only enforce endpoints to be compliant, but also guarantee the up-to-date health status & performance of end point's Antivirus, Antispam, etc. netfence VPN Connectors meet these requirements by offering an integrated personal firewall, unrestricted connectivity and central security policy implementation.

### Features & Benefits

- Multiplatform VPN client
- Integrated Personal Firewall
- Strong two-stage Authentication and Encryption
- Automatic Reconnection & Roaming support
- Implementation of global security policies
- Central Management



### netfence Smart/Secure Connector

**netfence Smart Connector** is the software required at the client end to establish an authenticated and secure VPN communication with a netfence gateway. netfence VPN client software achieves security by using the IPSec protocol and strong 2-factor authentication based on passwords and digital x.509 certificates. phion has improved the rather limited connectivity provided by raw IPSec by a novel encapsulation technique that immunises VPN data streams against intermittent NAT devices. netfence client VPN thus combines all the security advantages of standard IPSec VPN technology with the connectivity advantages of secure-socket-layer (SSL) based VPN technology required by road warriors.

netfence client VPN can be used to establish secure communication lines in any network environment, be it plain ethernet, legacy tokenring LANs, dial-up including UMTS/GPRS cell-phones, or wireless. netfence Smart Connector VPN is available for a wide variety of desktop platforms and operates with policies enforced by server-side configuration (integrated Personal Firewall is maintained by the user himself):

- Split tunnel mode allows access to the Internet even while VPN is active.
- Exclusive network access (ENA) warrants that all internet traffic is blocked when VPN is active.
- Server-side assignment of VPN client network routes in combination with ENA can be used to force all internet traffic into the VPN tunnel for processing by the central netfence gateway (except for network traffic required to keep the VPN connection itself up).

The **netfence Secure Connector** advanced client provides several features in addition to the features of the Smart Connector. These features allow executing scripts on connection start (e.g. to start an anti-virus update, etc.) or scanning the registry for valid application signatures (active as well as passive applications).

The personal firewall uses two independent rule sets. At times when there is no VPN connection active a personalised private ruleset is active. As soon as a VPN connection is established a server-side held ruleset is transferred to the VPN client and activated. The end user may not alter the security policies stated therein nor deactivate the Personal Firewall Posture assessment is automatically integrated as subsequent VPN communication requires an active firewall to work.

This gives the netfence gateway administrator full control over the behaviour of the remote access client.

### Personal Firewall

netfence's personal firewall has inherited many of its security features from its big brother integrated into the netfence gateway. This means that while remaining easy to handle for the average user due to an intuitive frontend enterprise grade features are readily available for the more experienced user. These entail detailed real time connection state monitoring, historical activity and attack access cache, rule editor, virtual firewall rule tester as well as packet capture logs for traffic analysis. Pop-up alerts and compact in and out connection status on the applica-



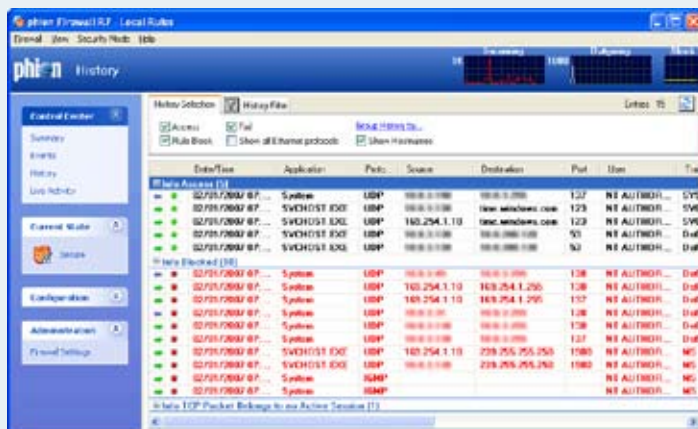
www.phion.com

# netfence VPN Connectors

tion level in realtime are the only elements the standard user is confronted with. Attacks are always automatically traced back to their source IPs. All subsequent similar attacks from this source may be blocked automatically by a single click of the user on the alert pop-up.

While many other vendors use a simple UDP encapsulation technology to achieve NAT traversal capability phion offers a choice of UDP, TCP or a combination of both (hybrid) encapsulation. TCP encapsulation paves the way for HTTPS and SOCKS proxy compatibility.

Both types of VPN client offer an integrated enterprise grade personal firewall for extra protection of the mobile user's computer and cutting edge encapsulation for HTTPS and SOCKS proxy compatibility. The Personal Firewall uses stateful inspection technology and operates at the network driver level to shield a mobile user's system from outside attacks and unnoticed connection attempts from and to the internet. Integrated application control technology limits network-access to trusted applications. Applications are recognised not only by their names but optionally also by unique digital signatures and must be approved (MD5 hash).

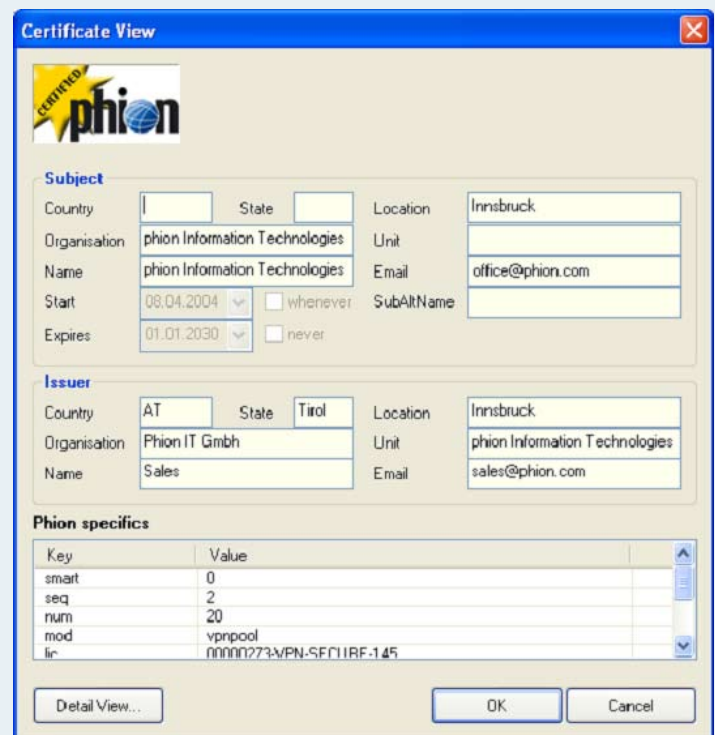


## Central management

Time and thus cost-efficient maintenance of VPN client software, powerful central configuration management of VPN client and firewall settings as well as integrated trouble-shooting tools by help of which mobile users may generate diagnostic reports are key factors for successful widespread VPN usage throughout an enterprise.

netfence VPN policies are centrally defined at the netfence gateway and transferred to the client upon successful strong 2-factor authentication. To ensure that only authorised VPN clients are allowed VPN access each client requires a valid digital x.509 certificate issued by the CA on the netfence gateway and successful validation (locally on the gateway or mediated by the gateway via RADIUS, NT, LDAP or SecurID authentication). Alternatively, certificates from other PKIs may be used. Their

policy extensions allow linking the user with group policies. Client software updates may be obtained when VPN is active from a secure download area on the netfence gateway. Customisable notification pop-ups upon successful VPN connection establishment may be used to inform remote users of new downloads or general news. The pop-ups can even be configured by the server administrator to display the company logo to conform to corporate ID standards. Digital user certificates are easily changed by an automatic update mode which grants the remote user one more VPN access with the obsolete certificate. After successful connection establishment the old certificate is simply replaced by the new one. To help diagnose client network problems each VPN client has been issued with diagnostic log support as well as the capability to generate a full system report that can be mailed or faxed to the netfence gateway administrator for further analysis. For each remote access client a short term access history is maintained at the netfence gateway that contains information about the last five access attempts. It provides valuable information such as type and version of the remote client's operating system and netfence VPN software as well as the reason for access failure.



# Client security and connectivity for highest demands

VPN	netfence Smart Connector	netfence Secure Connector
ESP	✓	✓
UDP encapsulation	✓	✓
TCP encapsulation	✓	✓
Hybrid encapsulation	✓	✓
DHCP-based parameter assignment*	✓	✓

Cryptography	netfence Smart Connector	netfence Secure Connector
AES (128-bit)	✓	✓
AES (256-bit)	-	✓
3DES and DES	✓	✓
CAST and BLOWFISH	✓	✓
Authentication only (null encryption)	✓	✓
SHA-1 and MD5 hashing	✓	✓

VPN Connection Intelligence	netfence Smart Connector	netfence Secure Connector
Redundant gateway support	✓	✓
NAT traversal	✓	✓
HTTPS proxy compatible	✓	✓
SOCKS4/5 proxy compatible	✓	✓
SSL handshake simulation	✓	✓

Security Features	netfence Smart Connector	netfence Secure Connector
Full server side control)	✓	✓
Split DNS	✓	✓
Split tunnel mode	✓	✓
Exclusive Network Access (ENA)	✓	✓
Driver level protection	✓	✓

Personal Firewall	netfence Smart Connector	netfence Secure Connector
Application control	✓	✓
NetBIOS protection	✓	✓
DoS attack protection	✓	✓
AutoBlock	✓	✓
Registry check	-	✓
Local rule set check	-	✓
Executable scripts	✓	✓
Local Offline rule set	✓	✓
VPN Online rule set	-	✓

User Authentication	netfence Smart Connector	netfence Secure Connector
Strong 2-factor authentication	✓	✓
Authentication requires	x.509** certificate & passphrase	x.509** certificate & passphrase
Max. RSA key length in x.509 certificate	2048-bit	2048-bit
External x.509 certificates	✓	✓
Microsoft Certificate Management (Crypto API)	-	✓
USB/Smartcard support***	-	✓
RADIUS user database****	✓	✓
LDAP user database****	✓	✓
NT user database****	-	✓
RSA SecurID user database****	✓	✓
Local user database****	✓	✓
Microsoft domain logon support (Pre-logon)	✓	✓

Management	netfence Smart Connector	netfence Secure Connector
Central management of VPN configuration	✓	✓
VPN diagnostic log	✓	✓
VPN system diagnostics report	✓	✓
VPN status monitoring	✓	✓
Attack access cache	✓	✓
Packet log (capture)	-	✓
VPN groups	✓	✓
Server-held local Offline rule sets	-	✓
Server-held VPN Online rule sets	-	✓
Silent Client Setup	✓	✓

Additional features	netfence Smart Connector	netfence Secure Connector
Embedded XP support	✓	✓
Remote VPN	✓	✓



\* Involves routes, WINS & DNS-Adressen, IP address and network mask, domain & firewall rule set.  
 \*\* x.509 digital certificate issued by phion netfence CA on netfence VPN Gateways.  
 \*\*\* For manufacturer with Microsoft Crypto Service Provider  
 \*\*\*\* Queried by netfence VPN server on behalf of client

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

## 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

	 Austria	 Germany	 Italy	 Switzerland
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

