



netfence VPN Connectors

Virtual Private Network (VPN)-Technologie ist mittlerweile zum de facto Standard für Remote Access in Unternehmensnetzen geworden. Administratoren sehen sich mit stetig steigenden Anforderungen an die Sicherheit, Zuverlässigkeit und Administrierbarkeit der eingesetzten Fernzugriffslösung konfrontiert.

VPN Client Software muss sichere Authentizierung und starke Verschlüsselung gewährleisten sowie zentrale Security Policies ermöglichen. Zugleich soll sie leicht ausrollbar und für den Endanwender einfach zu verwenden sein. Der VPN-Fernzugriff soll von jedem Netzwerk aus und für alle gängigen Internetanbindungen möglich sein. Dial-up-, Breitband- und Wireless-Zugänge müssen problemlos ohne zusätzlichen Konfigurationaufwand unterstützt werden.

Beim Fernzugriff über das Internet auf ein Unternehmensnetz muss die eingesetzte VPN Client Software bestmöglichen Schutz des mobilen Endgerätes gegen Attacken aus dem Internet gewährleisten, da das Gerät gleichzeitig mit dem nicht vertrauenswürdigen Internet und dem Unternehmensnetz verbunden ist. netfence VPN Connectors entspricht diesen hohen Anforderungen mit zwei Varianten der

Client Software, dem netfence Smart Connector und netfence Secure Connector, die beide eine Stateful Inspection Firewall enthalten. Beide Varianten bieten sicheren Verbindungskomfort und dieselben zentralisierten Wartungs- und Managementvorteile, die alle netfence Produkte auszeichnen.

Personal Firewall

Die Personal Firewall der VPN Clients hat viele ihrer Sicherheitsfeatures von ihrem großen Bruder in der netfence gateway übernommen. Dank einer übersichtlichen Benutzeroberfläche ist sie für den Benutzer einfach zu handhaben, bietet aber andererseits auch Features für den professionellen Anwender. Dazu gehören detaillierte Echtzeit-überwachung des Verbindungsstatus, Langzeit-Cache für alle Netzwerkaktivitäten und Angriffsversuche, Regeleditor, virtueller Firewall-Regeltester sowie Paketlogs zur Datenverkehrsanalyse. Der Standardbenutzer wird nur mit einfachen Popup-Warnhinweisen und einer Statusanzeige der gerade aktiven Anwendungen konfrontiert. Angriffe werden automatisch gemeldet und bis zur Quelladresse zurückverfolgt. Alle späteren ähnlichen Attacken von derselben Adresse können vom Benutzer durch einen Klick im Popup automatisch blockiert werden.

Features & Benefits

➤ **Unbegrenzte Connectivity**

Die Kombination der Vorteile von IPsec und SSL-VPN ermöglicht NAT Traversal und HTTPS/SOCKS Proxy-Kompatibilität.

➤ **Automatische Reconnects**

Volle Roaming Unterstützung durch on-the-fly IP reassignment

➤ **Sicherheit ohne Kompromisse**

- Starke zweistufige Authentizierung, AES256 und 3DES Verschlüsselung mit Smartcard und USB Token Support.
- Volle Unterstützung externer PKIs, sowie von X.509v3 Policy Feldern.

➤ **Integrierte Personal Firewall**

Die enthaltene Personal Firewall schafft zusätzliche Desktop-Sicherheit.

➤ **Zentrales VPN Policy Management**

VPN Policies werden Anwendern/Gruppen zugewiesen und automatisch vom netfence gateway abgerufen. Im netfence Secure Connector sind auch die Regelsätze der Personal Firewall inkludiert.

➤ **Multiplattform VPN-Client**

VPN Client für Windows 2000/XP, MacOS X, Linux.

netfence VPN Connectors

Während andere Anbieter für die Bewerkstelligung von NAT-Tauglichkeit einfache UDP-Encapsulierungstechniken verwenden, bietet netfence Client VPN die Wahl zwischen UDP, TCP oder einer kombinierten UDP/TCP (hybriden) Encapsulierung. Durch TCP-Encapsulierung wird auch HTTPS und SOCKS Proxy-Kompatibilität erreicht.

Die Personal Firewall erweitert den Schutz des Endgerätes des mobilen Users und des damit verbundenen Firmennetzes. Die Personal Firewall verwendet Stateful Inspection-Technologie und setzt auf der Netzwerktreiberebene an, um das System des mobilen Benutzers gegen Angriffe aus dem Internet zu schützen. Zusätzlich wird der Benutzer von autonomen Verbindungen ins Internet benachrichtigt und kann diese zukünftig unterbinden. Der Schutz erstreckt sich auch auf die Anwendungsebene. Der Netzzugang kann auf vertrauenswürdige Anwendungen eingeschränkt werden. Diese Anwendungen werden nicht nur am Namen erkannt, sondern bei Bedarf auch zusätzlich durch ihre digitalen Signaturen (MD5-Hash).

netfence Smart Connector

netfence Smart Connector Client VPN ist Software, die auf der Seite des Benutzers zur Errichtung einer authentizierten und abhörsicheren VPN-Verbindung mit einem netfence gateway erforderlich ist. netfence Client VPN schützt den Datenaustausch durch Verwendung des IPsec-Protokolls. Der Verbindungsaufbau wird mit einer starken zweistufigen Authentizierung auf Basis von Passwörtern und digitalen x.509 Zertifikaten abgesichert. Die eingeschränkte Connectivity des nativen IPsec wird von netfence durch den Einsatz einer intelligenten Encapsulierungsmethode wesentlich verbessert. Damit können VPN Datenströme auch über dazwischenliegende NAT-Geräte fließen.

Der netfence Smart Connector kombiniert somit alle Sicherheitsvorteile von etablierter IPsec-VPN-Technologie mit den für mobile Benutzer so wichtigen Connectivity-Vorteilen einer auf Secure Socket Layer (SSL) basierenden VPN-Technologie.

Sichere Kommunikationskanäle etabliert der netfence Smart Connector aus jeder Netzwerk-umgebung heraus, gleichgültig ob klassisches Ethernet, oder schon seltenes Tokenring, Einwahl per Modem oder UMTS/GPRS-Mobiltelefon oder über Wireless LAN Anbindung. netfence Smart Connector VPN ist für eine breite Palette verschiedener Desktop-Plattformen verfügbar und arbeitet mit serverseitig vorgegebenen Sicherheits-einstellungen:

- Der Split Tunnel Mode ermöglicht Internetzugang auch bei aktivem VPN.
- Exklusiver Netzwerkzugang (ENA) gewährleistet, dass bei aktivem VPN sämtlicher Internetverkehr nach aussen und nach innen blockiert ist.

- Durch serverseitige Zuweisung von VPN-Netzwerkrouen in Kombination mit ENA kann sämtlicher Internetverkehr zur Filterung durch zentrale netfence gateways in den VPN-Tunnel geleitet werden (Mit Ausnahme des Netzverkehrs, der nötig ist, um die VPN-Verbindung selbst aufrechtzuerhalten). Die integrierte Personal Firewall wird vom User selbst verwaltet.

netfence Secure Connector

Der netfence Secure Connector bietet neben der gesamten Funktionalität des netfence Smart Connectors zusätzliche Features, die es ermöglichen beim Start der Verbindung Scripts auszuführen (z.B. Starten eines Anti-Viren-Updates, etc.) oder die Registry auf eine gültige Signatur der Applikationen (aktive, wie passive) zu prüfen.

Die Personal Firewall verwendet zwei unabhängige Regelsätze. Solange es keine aktive VPN-Verbindung gibt, ist der lokale Regelsatz des Benutzers aktiv. Sobald eine VPN-Verbindung aufgebaut ist, wird ein serverseitig gehaltener Regelsatz an den VPN Client übertragen und aktiviert. Der Benutzer kann weder die darin enthaltenen Regeln verändern, noch die Firewall deaktivieren. Ausserdem kann ein modifizierter lokaler Regelsatz durch einen serverseitig gehaltenen Standard-Regelsatz ersetzt werden. Eine beschädigte oder beeinträchtigte Firewall führt dazu, dass die VPN Verbindung gar nicht erst betrieben werden kann (Posture Assessment).

Damit hat der Administrator des netfence gateways das sicherheitsrelevante Verhalten des Zugreifers vollständig im Griff.

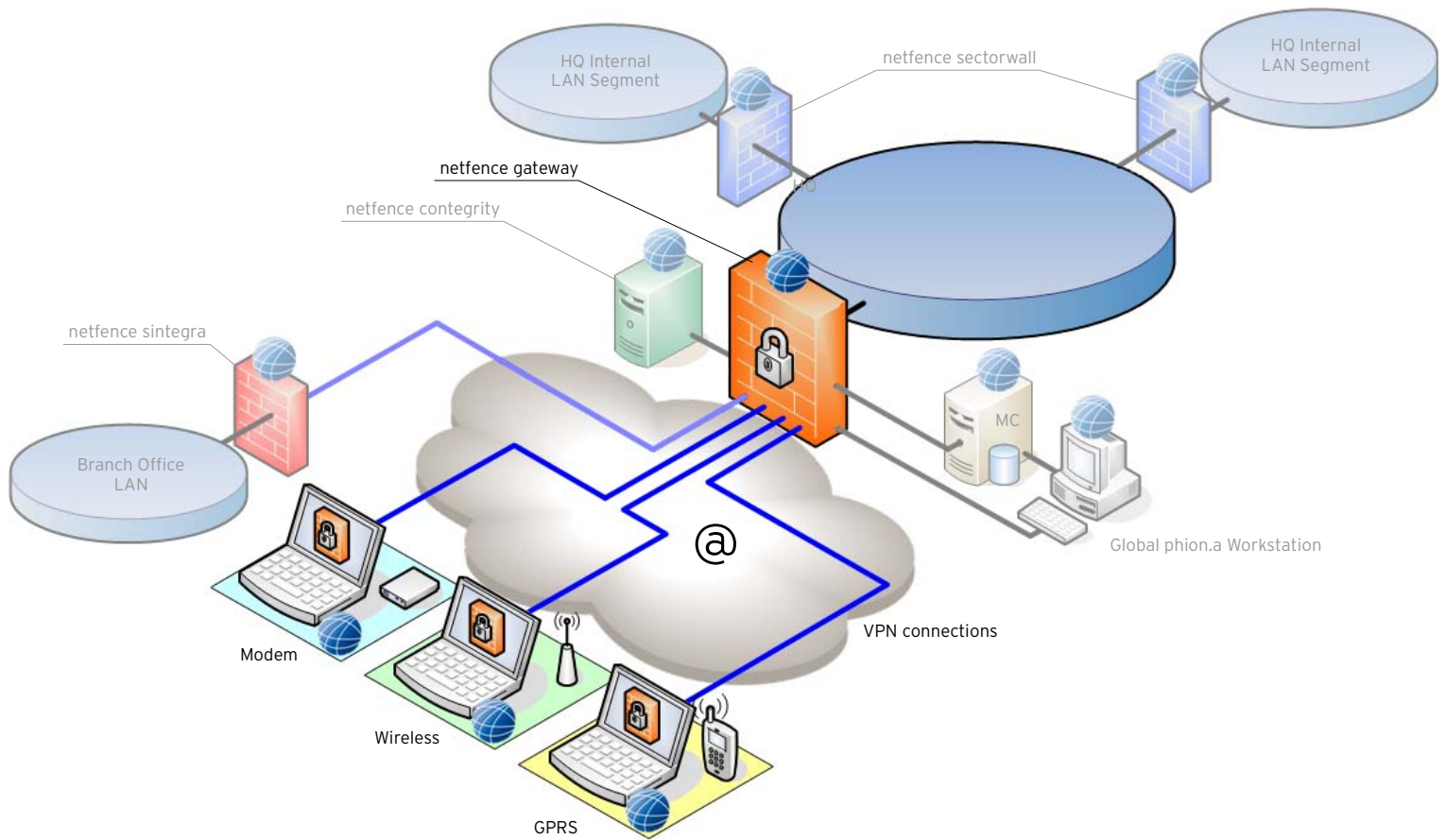
Wartung und zentrales Management

Zeitsparende und damit kostengünstige Wartung der netfence VPN Client Software, leistungsfähiges zentrales Konfigurationsmanagement des VPN Clients und der Personal Firewall sowie integrierte Tools zur Fehlerbeseitigung, mit deren Hilfe Benutzer Diagnoserports erstellen können, sind essenzielle Faktoren für den breiten Einsatz von VPN im Unternehmen.

Die VPN-Sicherheitsrichtlinien werden zentral am netfence gateway definiert und nach erfolgter starker zweistufiger Authentizierung an den Klienten übertragen. Um sicherzustellen, dass ausschließlich autorisierte VPN Clients VPN-Zugang erhalten, benötigt jeder Client ein gültiges, von der Zertifizierungsstelle (CA) am netfence gateway ausgestelltes, digitales x.509 Zertifikat. Zudem werden noch Benutzer und Zugangscode überprüft (lokal am Gateway oder externe RADIUS, NT, LDAP oder SecurID-Authentizierung). Alternativ lassen sich auch Zertifikate anderer PKIs verwenden. Deren Policy Extensions können dazu verwendet werden, den User mit Gruppenpolicies zu verknüpfen.

Softwareupdates können während einer aktiven VPN-Verbindung von einem sicheren Downloadbereich am netfence gateway heruntergeladen werden.

Client Security und Connectivity für höchste Ansprüche



tergeladen werden. Mit einstellbaren Popup-Hinweisen kann der Benutzer nach erfolgter Herstellung der VPN-Verbindung über Downloads oder sonstige News informiert werden. Die Popups können auch so konfiguriert werden, dass sie das jeweilige Unternehmenslogo zeigen, um den Identifikationsstandards des Unternehmens zu entsprechen.

Digitale Benutzerzertifikate können problemlos am Gateway regelmäßig getauscht werden. Der betroffene Anwender kann sein altes Zertifikat noch für einen weiteren VPN-Zugang verwenden. Nach erfolgreicher Herstellung der Verbindung wird das alte Zertifikat am Anwenderrechner einfach durch das neue ersetzt. Um die Diagnose von Client-Netzwerkproblemen zu erleichtern, bietet der VPN Client ein Diagnose-Log sowie die Möglichkeit zur Erzeugung eines vollständigen Systemreports an, der bei Bedarf per E-Mail oder Fax an den netfence gateway Administrator zur weiteren Analyse übermittelt werden kann. Das netfence gateway verfügt zusätzlich zu den Protokolldateien für jeden VPN Client über eine Kurzeithistorie, die Auskunft über die letzten 5 Zugriffsversuche gibt. Darin enthalten sind wertvolle Informationen über Tunnelmodus, Art und Version des Betriebssystems und des VPN Clients sowie den Grund für das etwaige Scheitern eines Zugriffsversuchs.

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

Cryptography	netfence Smart Connector	netfence Secure Connector
AES (128-bit)	Yes	Yes
AES (256-bit)	No	Yes
3DES and DES	Yes	Yes
CAST and BLOWFISH	Yes	Yes
Authentication only (null encryption)	Yes	Yes
SHA-1 and MD5 hashing	Yes	Yes

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

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

Personal firewall	netfence Smart Connector	netfence Secure Connector
Application control	Yes	Yes
NetBIOS protection	Yes	Yes
DoS attack protection	Yes	Yes
AutoBlock	Yes	Yes
Registry check	No	Yes
Local rule set check	No	Yes
Executable scripts	Yes	Yes
Local Offline rule set	Yes	Yes
VPN Online rule set	No	Yes

User Authentication	netfence Smart Connector	netfence Secure Connector
Strong 2-factor authentication	Yes	Yes
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	Yes	Yes
Microsoft Certificate Management (Crypto API)	Yes	Yes
USB/Smartcard support***	Yes	Yes
RADIUS user database****	Yes	Yes
LDAP user database****	Yes	Yes
NT user database****	Yes	Yes
RSA SecurID user database****	Yes	Yes
Local user database****	Yes	Yes
Microsoft domain logon support (Pre-logon)	Yes	Yes

Management	netfence Smart Connector	netfence Secure Connector
Central management of VPN configuration	Yes	Yes
VPN diagnostic log	Yes	Yes
VPN system diagnostics report	Yes	Yes
VPN status monitoring	Yes	Yes
Attack access cache	Yes	Yes
Packet log (capture)	No	Yes
VPN groups	Yes	Yes
Server-held local Offline rule sets	No	Yes
Server-held VPN Online rule sets	No	Yes
Silent Client Setup	Yes	Yes

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



* Involves in particular routes, WINS and DNS-Adressen, IP address and network mask, domain and 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

Affiliations & Partnerships

