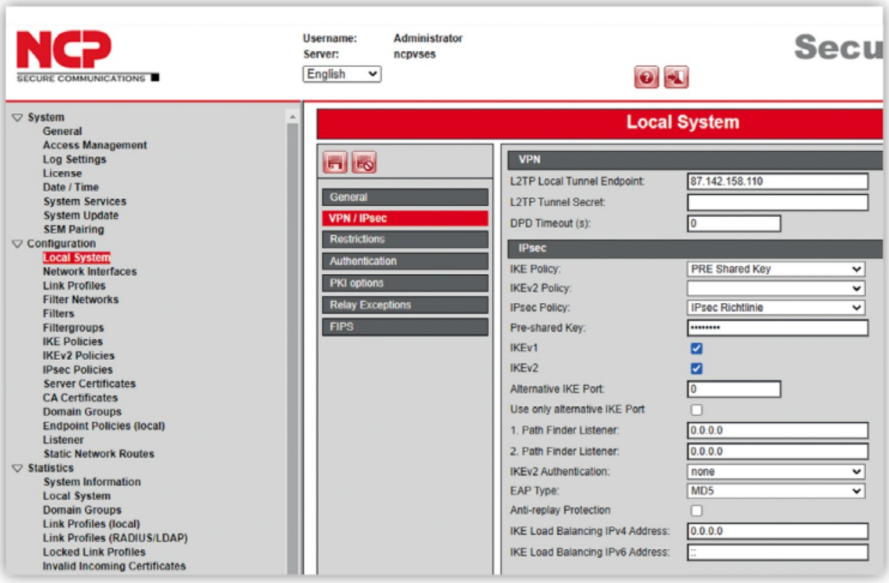
Testreihe VPN-Gateways, Teil 6: NCP

Skalierbares VPN

Mit dem Secure Enterprise VPN Server bietet NCP eine Softwarelösung für VPN-Gateways an, die flexibel einsetzbar ist und sich aufgrund guter Skalierbarkeit auch für große Unternehmen eignet. Dem VPN-Client hat NCP eine intelligente Firewall und einen VPN-Fallback-Mechanismus spendiert.

Im letzten Teil der LANline-Testreihe zu VPN-Gateways steht NCPs Softwarelösung Secure Enterprise VPN Server auf dem Prüfstand. Die VPN-Lösung ist in zwei Varianten erhältlich: Zum einen lässt sich die Software auf Windows-Servern (WS2019, WS2016, WS2012R2) und auf Linux-Servern (unter anderem Debian und Red Hat) installieren, die damit zu VPN-Gateways werden. Zum anderen bietet NCP mit dem Virtual Secure Enterprise VPN Server eine vorkonfigurierte virtuelle Appliance an, die sich schnell in Betrieb nehmen lässt. Sie unterstützt die Virtualisierungsplattformen VMware ESXi, Microsoft Hyper-V und Debian KVM. Eine zentrale Verwaltung großer Umgebungen ist mit dem NCP Secure Enterprise Management Server (SEM) möglich.

NCPs VPN-Gateways unterstützen die gängigen VPN-Protokolle und -Verschlüsselungsverfahren, darunter IPSec-VPNs im Tunnel- und Transport-Modus, SSL-VPNs sowie L2TP-VPNs. Auch eine zum international anerkannten Standard FIPS-140-2 Standard (Federal Information Processing Standard) kompatible VPN-Verschlüsselung steht zur Verfügung. Bei hohen Anforderungen an die Verfügbarkeit lassen sich die VPN-Gateways per Failsafe-Funktion durch ein Backup-System absichern. Es ist zudem möglich, mehrere VPN-Server zum ausfallsicheren Load-Balancing-Verbund zusammenzuschalten. Die VPN-Gateways sind im Zusammenspiel mit SEM mandantenfähig. SEM unterstützt auch Endpoint Security für die zentral verwalteten Endgeräte. Für die Benutzerverwaltung lassen sich Authentifizierungssysteme wie Radius, LDAP oder Microsofts Active Directory nutzen. Eine Integration mit PKI- und OTP-Lösungen (Public Key Infrastructure, One-Time Password) ist ebenso möglich wie eine Zwei-Faktor-Authentisierung via SMS.



Die Verwaltung des NCP Secure Enterprise VPN Servers erfolgt über die lokale Web-Konsole oder über eine zentrale Management-Software.

Den VPN-Software-Client bietet NCP für Windows, Linux, macOS, iOS und Android an. NCP- Clients finden sich als OEM-Lösung auch in den VPN-Portfolios anderer Hersteller. In den VPN-Client hat NCP eine intelligente Firewall integriert. Mit der „Friendly Net Detection"-Funktion erkennt der Client automatisch, in welchem Netzwerktyp sich ein Anwender gerade befindet, und aktiviert die dafür passenden Firewall-Regeln. Eine Hotspot-Login-Funktion wiederum stellt sicher, dass Benutzer Anmeldungen an Hotspots nur mit aktivierten Schutzmechanismen durchführen können. Mit der Home-Zone-Funktion dürfen Anwender lokal angeschlossene Netzwerkgeräte wie Drucker nutzen, der Zugriff auf das Internet ist aber ausschließlich über den VPN-Tunnel möglich. Eine weitere nützliche Client-Funktion ist NCPs „Path Finder"- Technik. Sie stellt automatisch eine Verbindung über IPSec/HTTPS her, wenn sich der VPN-Client hinter einer Firewall befindet, die IPSec-Traffic über Port 500 und UDP-Encapsulation nicht zulässt. Hilfreich ist zudem das Logbuch des VPN-Clients, das umfangreiche Informationen für die Fehlersuche liefert.

Den LANline-Test führten wir mit dem NCP Virtual Secure Enterprise VPN Server durch. Zunächst legten wir im Virtual Center auf einem ESXi-Test-Cluster eine neue VM-Hülle für die virtuelle VPN-Appliance an und konfigurierten sie gemäß NCP-Vorgaben für ein Debian-Linux-Betriebssystem. Dann verbanden wir die von NCP bereitgestellte ISO-Datei mit der VM-Hülle und schalteten die VM ein. Beim Hochfahren bootete sie automatisch von der ISO-Datei, und wir richteten den

VPN-Server mittels Setup-Dialog ein. Der Administrator gibt unter anderem IP-Adresse und Name der Appliance sowie die DNS- und Zeit-Server an. Die Basisinstallation dauerte nur wenige Minuten.

In produktiven Umgebungen wird das VPN-Gateway oft in einer DMZ zwischen zwei Firewalls platziert, die die Verbindungen zwischen dem internen Netz und dem Internet schützen. Für den Test standen keine zusätzlichen Firewalls zur Verfügung. Deshalb installierten wir die VPN-Appliance im selben IP-Subnetz, in dem sich der DSL-Router mit der Internetanbindung befand. Es handelte sich um einen normalen Endkunden-DSL-Anschluss. Die IP-Adresse des DSL-Routers trugen wir auf dem VPN-Server als Default-Gateway ein.

Sobald die Installation der VPN-Appliance abgeschlossen war, konnten wir von einem Admin-Rechner aus per Web-Browser auf die lokale Verwaltungskonsole des Systems zugreifen. Die Kommunikation erfolgt über den TCP-Port 20112. Für die Verwaltung größerer Umgebungen bietet NCP einen eigenen Management-Server an, mit dem sich die VPN-Gateways und -Clients von zentraler Stelle aus konfigurieren, aktualisieren und überwachen lassen. Im Test beschränkten wir uns auf die Web-Konsole für die lokale Verwaltung der virtuellen Appliance. Erfahrene Administratoren haben zudem die Möglichkeit, das System über die Kommandozeile zu bedienen. Ein Assistent für eine automatisierte VPN-Einrichtung ist in der lokalen Web-Konsole nicht vorhanden. Über den Hilfe-Button lässt sich aber immerhin die lokal verfügbare Dokumentation öffnen, die alle Konfigurationsoptionen ausführlich beschreibt.

Für den LANline-Test konfigurierten wir per Web-Konsole ein IPSec-VPN für IKEv1, das einen Pre-Shared Key verwendete. Der Administrator legt im VPN-Menü unter anderem die Namen und Passwörter der VPN-Benutzer fest, ebenso die aus dem Internet erreichbare VPN-IP-Adresse sowie die Verschlüsselungsalgorithmen. Dann speichert er die Settings in einer IPSec-Richtlinie. Im Menü mit den Domain Groups ist der Pre-Shared Key ebenfalls zu hinterlegen. Hier trägt der Administrator unter anderem ein, aus welchem IP-Adressbereich die VPN-Clients beim Verbindungsaufbau eine IP-Adresse zugewiesen bekommen. Wir richteten einen Pool mit der ID 1 ein, der von 192.168.200.20 bis .50 reichte.

Die Web-Konsole bietet umfassende Konfigurationsmöglichkeiten, um beispielsweise spezielle Routing-Anforderungen abzubilden, Firewall-Regeln zu definieren oder einen Syslog-Server einzurichten. Wenn ein Management-Server vorhanden ist, lässt sich die virtuelle Appliance über das Menü SEM-Pairing in die zentrale SEM-Konsole integrieren. Die lokale Verwaltung via Web-GUI ist dann nicht mehr möglich. Beim Setup der virtuellen VPN-Appliance hatten wir den DSL-Router als Default-Gateway eingetragen. Um vom Internet aus den Zugriff auf das VPN-Gateway zu ermöglichen, mussten wir auf dem DSL-Router Port-Forwarding für das IPSec-VPN via UDP-Port 500 einrichten.

Um Remote-Zugriffe per VPN-Tunnel zu testen, installierten wir den VPN-Client auf zwei Windows-10-Notebooks. NCP empfiehlt, Antivirenprogramme vor der Installation des VPN-Clients vom Rechner zu entfernen, da deren Filtertreiber zu Problemen führen können. Sobald der VPN-Client aufgespielt ist, kann man die AV-Software wieder installieren. Der Client verfügt über eine grafische Oberfläche, die auch einen Test-Button enthält, der eine Verbindung zu einem von NCP gehosteten VPN-Gateway aufbaut. Dies klappte mit beiden Notebooks auf Anhieb. Die VPN-Konfiguration lässt sich in eine Datei exportieren, die der Administrator dann auf anderen Rechnern importieren kann. Mit dem SEM-Server lassen sich Profile von zentraler Stelle aus auf die VPN-Clients ausrollen.

Wir konfigurierten die VPN-Clients mit denselben Einstellungen, die wir auf dem VPN-Gateway in der IPSec-Richtlinie vorgenommen hatten. Die ersten Verbindungsversuche schlugen jedoch fehl. Der VPN-Client konnte das VPN-Gateway zwar erreichen, die Verbindung wurde aber abgelehnt. Wie sich nach kurzer Fehlersuche herausstellte, hatte bei der Konfiguration des VPN-Gateways noch ein Link-Profil gefehlt. Anschließend konnten wir uns mit dem ersten Testnotebook erfolgreich mit dem VPN-Gateway verbinden und auf die Rechner im Testnetz zugreifen. Als wir mit dem zweiten Notebook eine VPN-Verbindung aufbauen wollten, klappte dies ebenfalls zunächst nicht. In der NCP-Dokumentation fanden wir nach kurzer Suche den Hinweis, dass auf dem VPN-Gateway im Authentication-Menü ein Haken bei Multi User Profile gesetzt sein muss. Sobald dies erfolgt war, konnten wir mit beiden Notebooks gleichzeitig eine VPN-Verbindung zum NCP-Gateway aufbauen und die Ressourcen des Testnetzes aus der Ferne nutzen. Der Test mit einem Android-Handy und dem mit Zehn-Tage-Testlizenz erhältlichen NCP Secure Android Client verlief ebenfalls erfolgreich: Nachdem wir den VPN-Client mit den Einstellungen für unser VPN-Profil konfiguriert hatten, konnten wir uns über das Mobilfunknetz mit dem LANline-Testnetz verbinden.

Tested by LANline IT • Network • Datacenter

NCP Virtual Secure Enterprise VPN Server

https://www.ncp-e.com

- ✓ Flexibel einsetzbare VPN-Softwarelösung, die als virtuelle Appliance schnell startbereit ist
- ✓ Gute Skalierbarkeit inklusive Support für Failsafe- und Load-Balancing-Konfigurationen
- ✓ Leistungsfähige VPN-Client-Software mit integrierter Firewall und automatischer SSL-VPN-Fallback-Funktion
- ✗ In der lokalen Web-Konsole kein Assistent für die VPN-Einrichtung

Fazit

Mit dem Secure Enterprise VPN Server bietet NCP eine flexibel einsetzbare Softwarelösung an, die sich auch für größere Unternehmen eignet. Integrierte Firewall-Funktionen sorgen für ein hohes Sicherheitsniveau. Vermisst haben wir lediglich einen Assistenten für die VPN-Einrichtung. Preise sind auf Anfrage direkt bei NCP oder NCP-Partnern erhältlich.

Christoph Lange/wg