Technical Paper

high security remote access

Filialvernetzung

Stand August 2014

Haftungsausschluss

Die in diesem Dokument enthaltenen Informationen können ohne Vorankündigung geändert werden und stellen keine Verpflichtung seitens der NCP engineering GmbH dar. Änderungen zum Zwecke des technischen Fortschritts bleiben der NCP engineering GmbH vorbehalten.

Warenzeichen

Alle genannten Produkte sind eingetragene Warenzeichen der jeweiligen Urheber.

Anforderungen an eine sichere und effiziente Vernetzung von Zweigstellen mit der Firmenzentrale

Ein Site-to-Site VPN verbindet Netzwerke miteinander und wird bei der Zweigstellenanbindung oder Filialvernetzung eingesetzt. Meist handelt es sich um die Verbindung der Netzwerke von Niederlassungen mit dem Netzwerk der Firmenzentrale. Aber ebenso kommunizieren Maschinen mit dem zentralen Gateway, also die Machine-to-Machine (M2M)-Vernetzung. Zum Einsatz kommen VPN Gateways die eine Verbindung zum Internet herstellen und die IP-Nutzdaten über das Internet verschlüsseln, authentisieren und tunneln. Das am häufigsten verwendete VPN-Protokoll für diese Art von Verbindungen ist IPsec.
Der Artikel behandelt Aspekte der Zweigstellenanbindung, die oftmals nicht unmittelbar bei der Planung oder dem Ausbau von Site-to-Site VPNs beachtet werden, aber häufig Probleme verursachen.

Vernetzungsarten

Bei der Vernetzung von Zweigstellen gibt es zwei Arten der Anbindung: Vermaschte und sternförmige Netzwerke. Vermaschte Netzwerke sind so aufgebaut, dass die Filialen nicht nur mit der Zentrale, sondern auch untereinander vernetzt sind. Bei der sternförmigen Vernetzung läuft auch die Anbindung der Filialen untereinander ausschließlich über ein zentrales VPN Gateway. Unternehmen müssen deshalb eine höhere Latenzzeit bei der Kommunikation zwischen den einzelnen Zweigstellen hinnehmen. Vorteilhaft wirkt sich jedoch aus, dass bei einer sternförmigen Vernetzung IT-Administratoren über ein zentrales Monitoring das Netzwerk immer im Griff haben. Dies ermöglicht das Lokalisieren von Verbindungsstörungen zwischen den einzelnen Zweigstellen schnell und in Echtzeit. Voraussetzung hierfür ist ein zentrales VPN Management System. Treten hingegen in einem vermaschten Netzwerk Verbindungsstörungen innerhalb der Querverbindungen auf, ist das „Orten" wesentlich schwieriger. Bei einer Vernetzung von beispielsweise 100 Filialen ist das Netzwerk nur mit stark erhöhtem Aufwand in den Griff zu bekommen.

Hohe Verfügbarkeit

Je nachdem welche Zweigstellen eingebunden werden, unterscheiden sich die Verfügbarkeitskriterien. So muss bei ausfallkritischen Zweigstellen, wie beispielsweise Bankfilialen und deren Geldautomaten oder Kassensystemen von Einzelhandelsketten, zu jeder Zeit eine hohe Verfügbarkeit gewährleistet sein. Deshalb unterstützen professionelle VPN-Systeme mehrere Backup-Mechanismen.
Eine grundlegende Voraussetzung, um überhaupt Backups durchführen zu können, ist die Überwachung der VPN-Verbindung. Eine Methode der Verbindungsüberwachung ist DPD (Dead Peer Detection - RFC). Des Weiteren sollte das VPN Gateway in der Filiale alternative Media-Typen (Übertragungswege) zur Einwahl ins Internet beherrschen. Die VPN-Lösung muss entsprechend intelligent sein und automatisch erkennen, wenn eine Verbindungsstörung mit einer Gegenstelle vorliegt. Das VPN Gateway baut dann automatisch die Standardverbindung ab und einen alternativen Backup Link auf. Inzwischen gibt es VPN Softwarelösungen die unbegrenzt Backup-Verbindungen

unterstützen. Der begrenzende Faktor ist in diesem Fall die Anzahl an unterstützten Media-Typen der Hardware.

Zentrales Management

Voraussetzung für eine effektive Vernetzung von Filialen ist ein zentrales VPN Management System. Selbst bei nur wenigen Zweigstellen ist der Aufwand einer Administration vor Ort meist unverhältnismäßig. Im M2M-Bereich ist das sogar oft nur schwer möglich.
Ein zentrales VPN Management automatisiert die Verwaltung der Remote/Filial VPN-Gateways. Je mehr VPN relevante Systeme in das zentrale Management eingebunden sind, desto einfacher und überschaubarer wird es für Administratoren. Neben Konfigurations- und Software-Update-Management kommen hier noch in Frage: das Management der Verteilung digitaler Software- oder Hardwarezertifikate (CA), die LDAP-Konsole für das Identitäts- und Rechte-Management sowie die Sicherheitsüberprüfung der Endgeräte (Network Access Control/Endpoint Security).

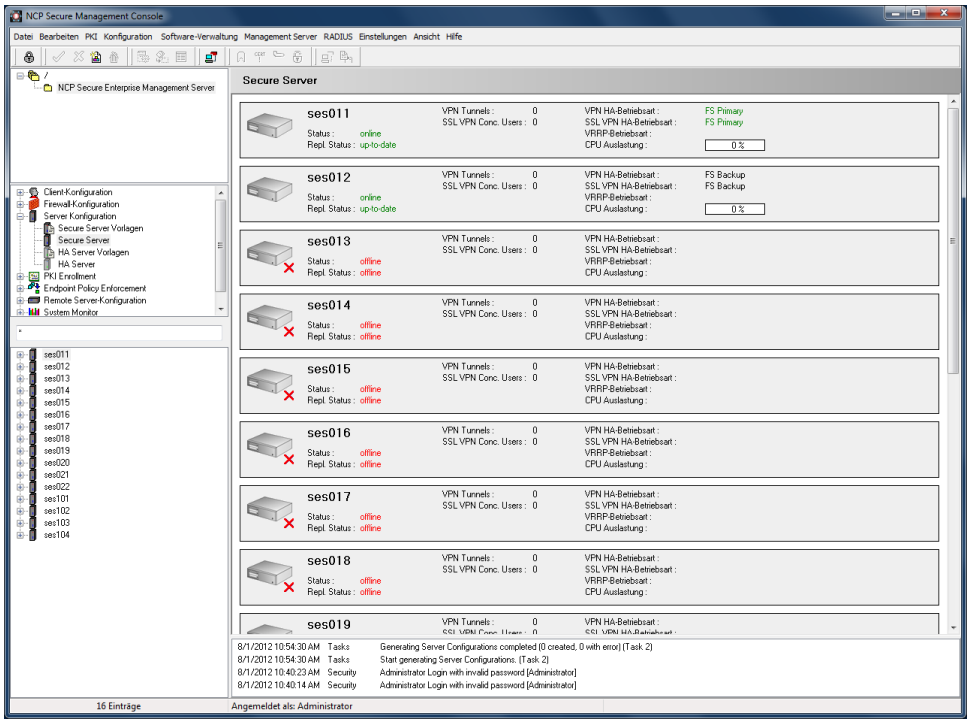

Bild 1: Multiple VPN Management Konsole

Ein VPN-System sichert sämtliche Datentransfers im verschlüsselten Tunnel. Doch schon die Einwahl ins Internet muss abgeschottet sein, denn das ist der häufigste Angriffspunkt von Hackerattacken. Es geht also darum, wie sich die Filialen gegenüber dem zentralen Gateway authentisieren. Zum einen besteht die Möglichkeit dies über Preshared Keys zu regeln, zum anderen über Zertifikate. Aus Sicherheitsgründen sind zertifikatsbasierte Lösung vorzuziehen, da hier Zertifikate angepasst werden können, d.h. alte Zertifikate können gesperrt und neue verteilt werden. Hier gilt es nun das Zertifikats-Handling zu organisieren, d.h. ist ein Zertifikat abgelaufen, sollte das VPN Management über entsprechende Automatismen verfügen, neue Zertifikate anzufordern und zu verteilen.

Eine weitere Sicherheitsanforderung wird manchmal übersehen. Die Firewall darf ausschließlich IPsec-Verbindungen zulassen. Üblicherweise verfügen Filialen über einen DSL Router zur Verbindung ins Internet. Dieser schottet das VPN Gateway entsprechend ab. Manche VPN Gateways unterstützen auch PPPoE als Media-Typ. Daher können diese direkt zur DSL-Einwahl verwendet werden. Ein DSL Router ist nicht notwendig. Auch in diesem Fall darf die Firewall nur IPsec-Verbindungen durchlassen. Zur Wartung des VPN Gateways in der Filiale ist auch eine direkte Einwahl via ISDN denkbar – nicht über das Internet.

Maskieren

Eine aus Administratorsicht berechtigte Forderung ist häufig, dass er von der Zentrale bzw. von ihrem Management System Zugriff auf jedes einzelne Filial-Endgerät hat. Auf der anderen Seite ist es einfacher, die IP-Netze der Filiale außen vor zu lassen und bei der Verbindung zur Zentrale zu maskieren, d.h. hinter einer Adresse zu verstecken. Diese beiden Forderungen bilden in sich aber einen Widerspruch.
Müssen Administratoren transparent auf die Filialen zugreifen, ist es unumgänglich, dass jedes Filial-Netz einen eigenen, eindeutigen IP-Adressbereich bekommt (falls nicht schon vorhanden). Was aber gleichzeitig bedeutet, dass alle installierten Router und Endgeräte entsprechend neu konfiguriert werden müssten. In kleinen, überschaubaren Netzwerken mag dies noch zu handhaben sein, jedoch in größeren Netzwerkumgebungen ist der Aufwand für IT-Administratoren enorm. Der Administrator muss dafür Sorge tragen, dass entsprechende Routen auf Zentralseite bekannt gemacht werden. Manche VPN Gateways machen bei aufgebauter Verbindung die Routinginfomationen dynamisch bekannt.
Ist der transparente Zugriff nicht zwingend erforderlich, bietet sich an, mittels Network Address Translation (NAT) die IP-Adressen zu „maskieren". D.h. die IP-Adresse wird umgewandelt in eine VPN Tunnel IP-Adresse, welche der Host bzw. das zentrale VPN Management System erkennt und automatisch der jeweiligen Zweigstelle zuordnet, nicht aber den Endgeräten. Vom Konfigurations- und Rollout-Aufwand resultiert daraus eine erhebliche Erleichterung.

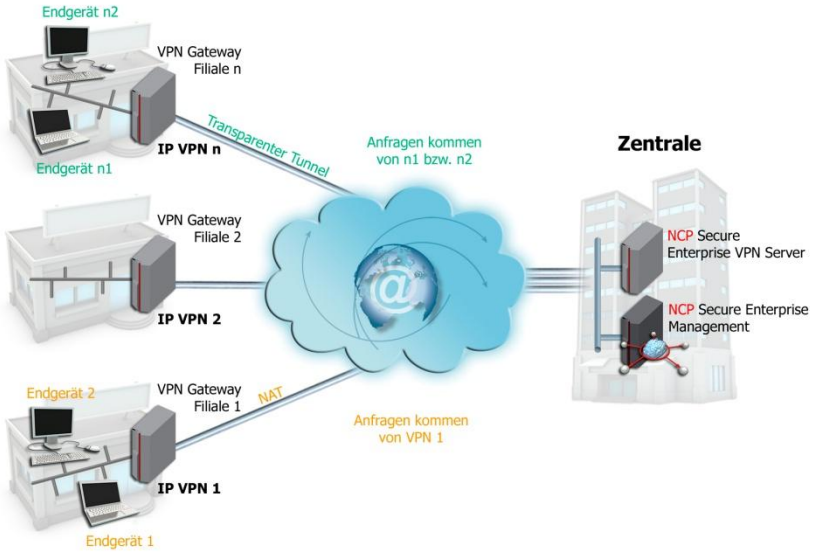

Bild 2: Maskieren (NAT) oder transparenter Filialnetzzugriff

Unternehmen müssen sich dementsprechend zwischen „Maskieren" und dem Zugriff auf alle Endgeräte - mit erhöhtem Administrationsaufwand in den Filialen - entscheiden. Ein Mischbertrieb ist natürlich auch möglich.

Fragmentierung und Maximum Transmission Unit (MTU)
Ein weiteres Problem, das es zu umschiffen gilt, ist die Größe der Datenpakete bei der Kommunikation über unterschiedliche Internet-Einwahltypen. DSL erlaubt beispielsweise eine Größe von 1492 Byte. Nun kommt es aber häufig vor, dass die Größe der VPN-Datenpakete, die vom Filial-VPN Gateway via DSL an einen Router geschickt werden, diese 1492 Byte überschreiten. Die Folge: die VPN-IPsec Datenpakete werden standardmäßig fragmentiert. Allerdings wirkt sich diese Fragmentierung auf IP-Ebene nachteilig aus, da die fragmentierten IPsec-Pakete von vielen Routern nicht zugelassen werden. Mit dem Ergebnis, dass Daten nicht weitergeleitet werden und es deshalb zu Datenverlusten kommt. Dieses Problem lässt sich umgehen, indem eine sogenannte Pre-Fragmentierung durchgeführt wird. Dabei werden nicht die IPsec-Pakete fragmentiert, sondern die Fragmentierung der Datenpakete wird bereits vor dem Tunneling vorgenommen und erst danach wird der IPsec Tunnel Header aufgesetzt. Somit werden, für die Internet Router/Firewall „zugelassene", nicht fragmentierte Datenpakete verschickt.
Inzwischen bieten professionelle VPN-Lösungen mit der Methode des dynamischen Heruntersetzens der MTU eine wesentlich intelligentere Vorgehensweise. Denn diese VPN-Gateways sind in der Lage, bei TCP-Verbindungen die Paketgröße vor dem Verbindungsaufbau automatisch der vorgegebenen Größe anzupassen.

DSL-Zwangstrennung
Die bekannte DSL-Zwangstrennung spielt für viele Site-to-Site VPNs keine Rolle. Jedoch gibt es durchaus Szenarios, bei welchen in „Hauptverkehrszeiten" eine permanente Verbindung gewährleistet sein muss. Die DSL-Zwangstrennung wird von vielen Providern automatisch 24 Stunden nach dem ersten Verbindungsaufbau durchgeführt. Daher sollte bei solch einer VPN-Installation darauf geachtet werden, dass die VPN Gateways über eine Funktion verfügen, mit der sich der Zeitpunkt der DSL-Zwangstrennung vom Administrator selbst festlegen lässt.

Zweigstellenstruktur entscheidet
Die oben diskutierten Punkte sollten grundsätzlich bei Site-to-Site VPN Installationen beachtet werden. Oft sind es Kleinigkeiten, welche die seit Jahren praktizierte Zweigstellenanbindung häufig schwierig machen. Grundsätzlich leisten viele VPN Gateways einfache Standardvernetzungen, doch gerade bei Administrations- und Verwaltungs-Tools trennt sich die Spreu vom Weizen.