LANCOM Techpaper

LANCOM High Scalability VPN (HSVPN)

Um vertrauliche Daten innerhalb des Netzwerks sicher auszutauschen, werden Unternehmensstandorte, Filialen, Home-Offices und mobile Mitarbeiter über die bewährte Verschlüsselungstechnologie IPSec-VPN miteinander vernetzt. Hierbei wird ein verschlüsselter Datentunnel durch das öffentliche Internet aufgebaut, sodass ein sicheres privates Netzwerk entsteht, auf das ausschließlich Befugte zugreifen können. Dabei müssen in den meisten Fällen mehrere logisch getrennte Netze (VLANs) für verschiedene Unternehmensanwendungen an den unterschiedlichen Tunnelendpunkten bereitgestellt werden – bei großen Multi-Service-IP-Netzwerken führt dies zu einer nicht zu unterschätzenden Komplexität. Statt für jede Anwendung eine eigene Infrastruktur und verschiedene Internetzugänge zu verwenden, empfiehlt sich der Einsatz von Netzwerkvirtualisierung. Je nach zugrundeliegender Infrastruktur finden dazu verschiedene Verfahren Anwendung, die sich in einer Art "Evolution" mit unterschiedlichen Stärken und Schwächen entwickelt haben. Diese werden in diesem Techpaper beschrieben.

Drei Verfahren der standortübergreifenden Netzwerkvirtualisierung

Multi-PPTP-over-IPSec (Tunnel-in-Tunnel)

In vielen Netzwerkszenarien ist es gängig, mehrere logische Netze isoliert voneinander zu verwalten (Advanced Routing & Forwarding, ARF). Damit eine echte Ende-zu-Ende-Netzvirtualisierung über IPSec-VPN möglich wird, müssen zwischen den VPN-Gateways PPTP- oder L2TP-Tunnel innerhalb eines IPSec-Tunnels aufgebaut werden, die völlig unabhängig vom IP-Adressraum der zu übertragenden

Netze sind. Mit dem PPTP- bzw. L2TP-Protokoll bieten sich Protokolle an, die schon lange als Tunneltechniken etabliert sind. Ähnlich wie bei VLAN im LAN wird für jeden ARF-Kontext ein PPTP-Tunnel aufgebaut, der die korrespondierenden VLANs der Standorte durch einen IPSec-Tunnel hindurch getrennt übermittelt (siehe Abbildung 1). Die im Layer 2 vorhandene VLAN-Information wird verwendet, um die Netzwerke an die einzelnen PPTP-Tunnel anzubinden, die wiederum in einem gemeinsamen IPSec-VPN-Tunnel über das Internet übertragen werden. Somit wird eine vollständige Virtualisierung von Netzwerksegmenten über das gesamte Unternehmensnetzwerk ermöglicht.

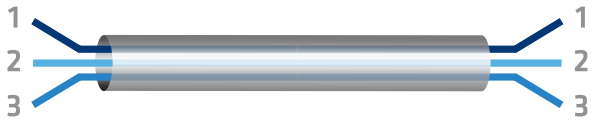

Abb. 1: Multi-PPTP-over-IPSec (Tunnel-in-Tunnel)

Dieses Verfahren nutzt nur einen IPSec-VPN-Tunnel zur Übertragung mehrerer getrennter Netze. Gleichzeitig erzeugt dieses Verfahren durch die Schachtelung der Tunnel jedoch einen nicht unerheblichen Overhead in den Datenpaketen. Die VPN-Gateways an beiden Tunnelendpunkten werden zusätzlich belastet, da sie jedes Datenpaket mehrfach ver- und entpacken müssen und somit auch die Routing-Tabelle häufiger durchlaufen, was wiederum eine entsprechende Rechenleistung erfordert.

Vorteile: Nur soviele IPSec-Tunnel wie Standorte angebunden werden, dadurch geringere Last auf den VPN-Gateways durch IPSec-Verhandlungen und Rekeyings.
Nachteile: Reduzierte MTU durch Tunnel-in-Tunnel-Schachtelung. Ineffizienter Paketransport, da jedes Paket zweimal ein- und ausgepackt werden muss.

IPSec per Network (Multi-VPN)

IPSec-VPN ist die bewährte, sichere Methode, den Übertragungsweg zwischen Standorten über das Internet zu virtualisieren. IPSec bietet jedoch keinerlei Möglichkeiten, Netzwerke, die logisch voneinander getrennt wurden (z. B. mit VLAN und ARF), durch einen IPSec-Tunnel weiterzuleiten und dabei die logische Trennung der Netze beizubehalten. Um dieses Problem zu umgehen, kann für jedes definierte Netz ein separater IPSec-VPN-Tunnel pro IP-Netz aufgebaut werden (siehe Abbildung 2).

Abb. 2: IPSec per Network (Multi-VPN)

Diese einfache Architektur erfordert eine hohe CPU-Leistung an beiden Tunnel-Endpunkten, da pro Netz je eine IPSec-Aushandlung stattfinden muss. Gleichzeitig müssen die zugrundeliegenden IPSec-Gateways in der Lage sein, die geforderte Anzahl an parallelen IPSec-VPN-Tunneln aufzubauen: Die Anzahl der zu terminierenden VPN-Tunnel ist die Anzahl der Netze mal die Anzahl der Standorte.

Vorteile: Die Übertragung ist sehr effizient, da die MTU maximiert ist und Pakete im Router nur einmal ein- und ausgepackt werden müssen.
Nachteile: Hohe Belastung der VPN-Endpunkte durch IPSec-Verhandlungen und Rekeyings. Daraus resultierend dauert es auch entsprechend lange, die Tunnel initial oder im Fail-Over-Fall aufzubauen.

LANCOM High Scalability VPN (HSVPN)

Bei der Variante "IPSec per Network" wurde insbesondere der Durchsatz optimiert, da die Variante "Multi-PPTP-over-IPSec" bei diesem relativ ineffizient war. Dort lag der Fokus auf der Trennung der Datenströme. Eine effiziente Netzvirtualisierung via IPSec-VPN sollte aber generell die Anzahl der zum Einsatz kommenden Tunnel – IPSec oder PPTP – möglichst gering halten und dabei die zur Verfügung stehende MTU möglichst groß wählen. Dies geschieht in einem weiteren Optimierungsschritt mit dem Namen LANCOM High Scalability VPN (HSVPN), bei dem die Anzahl der IPSec-Tunnel wieder reduziert wird.

Vergleich der Anzahl aufgebauter Tunnel bei den vorgestellten Verfahren

- ☐ Multi-PPTP-over-IPSec
  Anzahl Standorte * Anzahl ARF * PPTP/L2TP +
  Anzahl der Standorte * IPSec
- ☐ IPSec per Network
  Anzahl Standorte * Anzahl ARF * IPSec
- ☐ LANCOM High Scalability VPN (HSVPN)
  Anzahl Standorte * IPSec

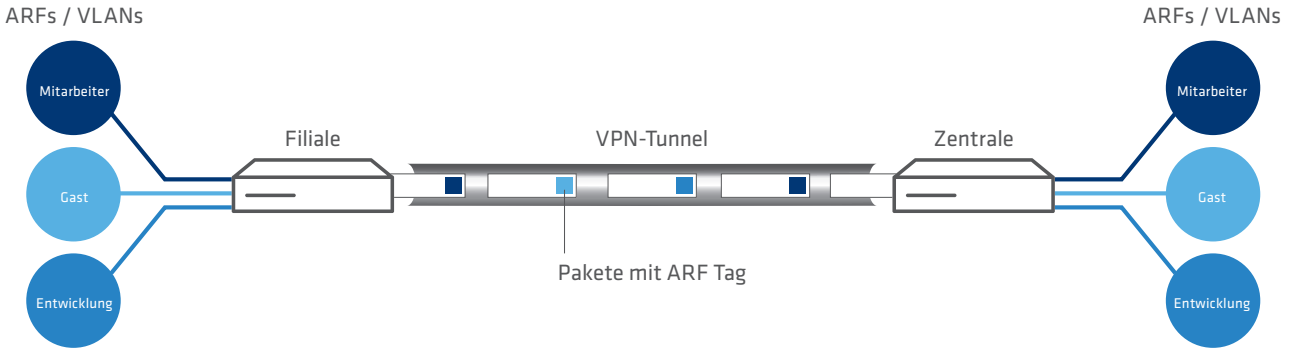

Abb. 3: LANCOM High Scalability VPN (HSVPN)

Es gilt zu beachten, den Übertragungsweg innerhalb des IPSec-Tunnels und des Routers effizienter zu gestalten als bei Multi-PPTP-over-IPSec. Hierbei wird den einzelnen ESP-Paketen ein sog. Trailer angehängt der ein Routing-Tag in verschlüsselter Form enthält, ähnlich wie es das VLAN-Tag (IEEE 802.1Q) im Ethernet Frame macht. Diese Kennzeichnung erlaubt eine parallele Übertragung logisch getrennter IP-Datenpakete, auch ohne zusätzliche innere Tunnel: Das annehmende VPN-Gateway erkennt anhand des Trailers des ankommenden IP-Datenpakets, zu welchem ARF-Kontext es zugehörig ist und leitet es in diesem an die entsprechende Zieladresse weiter (siehe Abbildung 3).

LANCOM HSVPN ist aus Verschlüsselungssicht ein modernes IPSec auf Basis von standardkonformem IKEv2 und bietet somit exakt dieselbe Sicherheit wie IKEv2. Zudem ist es nicht auf zentrale Verwaltungsinstanzen angewiesen und arbeitet als unabhängiges dezentrales System. Genau wie bei den anderen Verfahren verändert sich die benötigte Verschlüsselungsleistung nicht. Jedes Paket wurde und wird nur einmal verschlüsselt.

Vorteile: Die Last ist geringer, da nur ein Tunnel pro Filiale benötigt wird. Dadurch müssen insgesamt weniger Tunnel aufgebaut und verwaltet werden (Rekeyings). Gleichzeitig muss auch weniger Last beim Pakettransport aufgewendet werden, da die Pakete nicht durch mehrere Tunnel geschleift werden und nicht mehrfach ein- und ausgepackt werden müssen.

Dieses Verfahren ist zwar nicht herstellerübergreifend verfügbar, die eingesetzten Technologien basieren aber auf dem Standard IPSec und erben damit auch die Sicherheit dieses Verfahrens. Die Netztrennung durch die angefügten Trailer ist bei deutlich geringerem Overhead genauso effizient und sicher wie die Trennung durch einen inneren Tunnel.

Zusammenfassung

Je komplexer eine Netzwerkinfrastruktur ist, desto mehr sollte bei der Planung und Umsetzung insbesondere der standortübergreifenden Übertragungswege ein passendes Netzwerkvirtualisierungs-Verfahren gewählt werden. Dabei empfiehlt sich grundsätzlich der Ansatz, die Anzahl der zum Einsatz kommenden Datentunnel gering zu halten, ohne auf die strikte Trennung der Routing-Kontexte und die Sicherheit eines modernen IPSecs zu verzichten. Genau dies wird mit LANCOM High Scalability VPN erreicht.