



Remote-Working mit IPSec

1

Kosten sparen mit den Remote-Working-Lösungen von ZyXEL

2

Produktivität steigern mit den Remote-Working-Lösungen von ZyXEL

3

Flexible Arbeitsbedingungen für Mitarbeiter schaffen



Teleworker müsste man sein

Sicherer Remote-Access mit vielen Vorteilen

Mehr denn je ist das Thema Remote-Access in aller Munde! Die Wirtschaftskrise hat gezeigt, daß ständige Verfügbarkeit und intelligente Kostenreduktion immer wichtiger werden. Virtual-Private-Networks (VPNs) ermöglichen es, diesen Anforderungen gerecht zu werden und helfen, neue Einkommensquellen für das Unternehmen zu erschliessen.

„ständige Verfügbarkeit“ – der Anspruch der heutigen Geschäftswelt

Veränderte Bedingungen der Arbeitsumgebung, neue Kommunikationsmittel und stetig steigende Erwartungen der Konsumenten führen zu einer wachsenden Nachfrage nach umfassenden Remote-Access-Lösungen. Immer mehr Firmen beschäftigen Teleworker, die ihr Home-Office nutzen. Verschiedene Einflussfaktoren werden Teleworking in Zukunft weltweit noch populärer machen:

Einflussfaktor Business

Produktivität und Kostenminimierung - wichtiger denn je

Moderne Unternehmen können Wettbewerbsvorteile durch Produktivitätssteigerung und Kostenminimierung erzielen. Diese Vorteile werden mit Hilfe von Technologien erreicht, die den Mitarbeitern ermöglichen, orts- und zeitunabhängig zu arbeiten. Sinkende Kranken- und Fehlzeiten sind die Folge.

In Krisenzeiten müssen Kostenstrukturen verändert werden. Hohe

Mieten für Bürogebäude und hohe Betriebskosten belasten kleine und mittlere Unternehmen enorm. Eine Möglichkeit, hier Kosten einzusparen, ist, die Anzahl der Teleworker zu erhöhen. So lassen sich Kosten für Büroausstattung und Kommunikationsmittel reduzieren.

Einflussfaktor Mensch

Mehr Flexibilität und bessere Work-Life-Balance

Work-Life-Balance ist ein wunderbar motivierender Faktor, wenn es um Firmentreue und Mitarbeiterbindung geht. Heutzutage erwarten Mitarbeiter immer häufiger flexible und ihren Bedürfnissen angepasste Arbeitszeiten. Moderne Firmen können diesen Wünschen durch Teleworking entsprechen und sich so das Gütesiegel „familienfreundlich“ erwerben. Sie müssen auch nicht mehr auf ihre hochqualifizierten weiblichen Mitarbeiter verzichten, wenn diese sich in der Familienplanung befinden. Letztendlich werden durch mehr Flexibilität und Kontrolle über die Arbeitszeit Leistungsbereitschaft und Eigenverantwortung erhöht.

Einflussfaktor Umwelt

Umweltfreundlichkeit

Die Geschäftswelt wird mehr und mehr mit dem wachsenden Druck der globalen Erwärmung und anderer Umweltthemen konfrontiert. Daher suchen Unternehmen „grüne Lösungen“ zur Minimierung der Umweltbelastung. Teleworking verringert das Verkehrsaufkommen und den Smog und senkt gleichzeitig die laufenden Kosten für Bürogebäude. Dies wiederum bedeutet weniger Verkehrsaufkommen und Luftverschmutzung.



Vorteile für Unternehmen, Mensch und Umwelt

Unternehmen

- sinkende Gebäude- und Betriebskosten
- höhere Motivation und Produktivität der Mitarbeiter
- größtmögliche Flexibilität

Mensch

- flexible Arbeitsbedingungen - und zeiten für Mitarbeiter
- ausgezeichnete Work-Life-Balance
- Einsparpotential bei Reise- und Anfahrtskosten

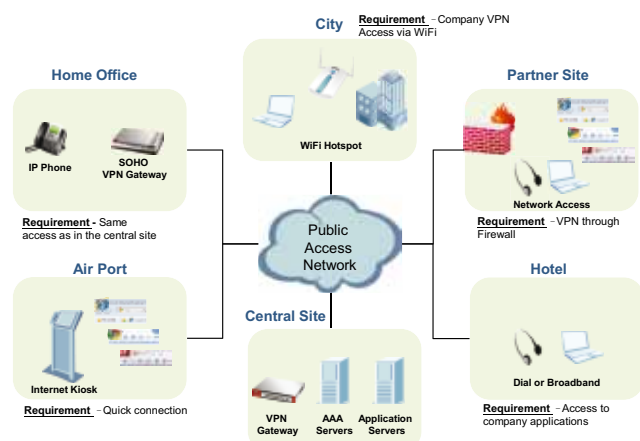
Umwelt

- Verringerung des CO₂-Ausstosses
- weniger Stau während der Stosszeiten
- reduzierte Schadstoffbelastung durch Arbeitsverkehr/
positive Auswirkung auf die Umwelt

Warum ist eine sichere Verbindung notwendig?

Unternehmen bemerken einen steigenden Bedarf an flexiblen Arbeitsplätzen für Teleworker, Filialen, Geschäftspartner und Kunden. Sie alle benötigen, unabhängig vom Standort, Zugang zu Firmendaten und erwarten einen einfachen und absolut sicheren Access zu den notwendigen Netzwerk-Ressourcen – von überall, zu jeder Zeit und mit jedem Gerät. Wie kann also ein Unternehmen

einen garantiert sicheren Zugang bereitstellen, ohne unerwünschte Zuhörer? Entscheidend ist ein sicherer, immer verfügbarer und kosteneffizienter Remote-Access. Aus diesem Grund nutzen die meisten Unternehmen Virtual-Private-Networks (VPNs), um eine sichere Verbindung garantieren zu können.



Grafik: Sicherer Remote-Access via VPN ist ein weitverbreitetes Bedürfnis



Sichere Verbindungsarten - Virtual-Private-Networks (VPNs)

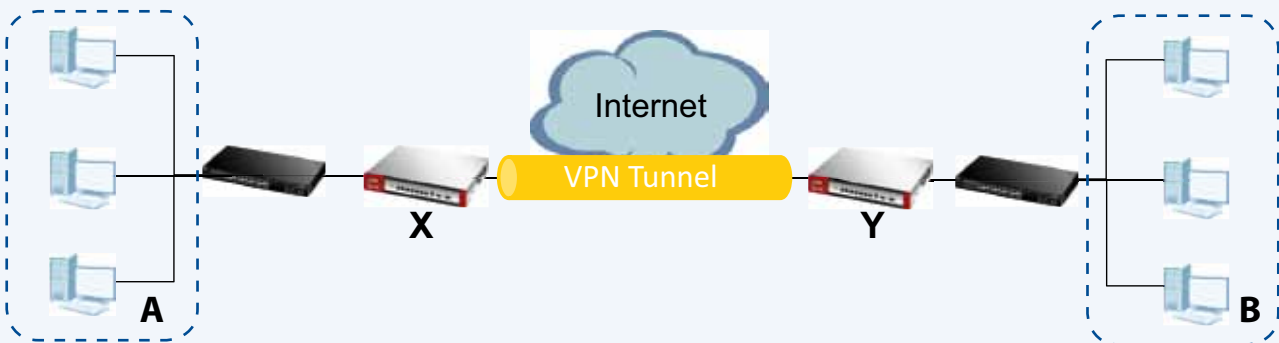
Ein Virtual-Private-Network (VPN) gewährleistet die sichere Kommunikation zwischen Standorten ohne den Aufwand einer Standleitung. Ein sicheres VPN ist eine Kombination aus Tunneling, Verschlüsselung, Authentifizierung, Zugangskontrolle und Auditing. Es wird verwendet, um den Datenfluss über das Internet oder ein anderes unsicheres Netzwerk, das TCP/IP verwendet, zu leiten. Virtual-Private-Networks (VPNs) sind die richtige Lösung für den

verlässlichen und sicheren Remote-Access zur Firmenzentrale. Durch die wachsende Breitband-Abdeckung und die starke Zunahme von mobilen Geräten gewinnt Teleworking immer mehr an Bedeutung. VPN stellt eine sichere, schnelle und kostengünstige Lösung hierfür dar. Prinzipiell gibt es zwei übliche Methoden, um Remote-Access VPNs einzurichten: IPSec und SSL. Beide haben ihre bedürfnisabhängigen Vorteile.

IPSec VPNs

Internet-Protocol-Security (IPSec) ist ein Standards-basiertes VPN und bietet flexible Lösungen für sicheren Datenfluss über ein öffentliches Netz wie das Internet. IPSec arbeitet mit standardisierten Verschlüsselungstechniken, die Vertraulichkeit, Daten-Integrität und Authentifizierung auf IP-Ebene gewährleisten. Die Verbindun-

gen werden mit einer auf dem Benutzer-Desktop vorinstallierten VPN-Client Software aufgebaut. Diese Technik ist in erster Linie für Desktops geeignet, die von Unternehmen verwaltet werden. Im Folgenden wird ein IPSec-VPN-Tunnel schematisch dargestellt.



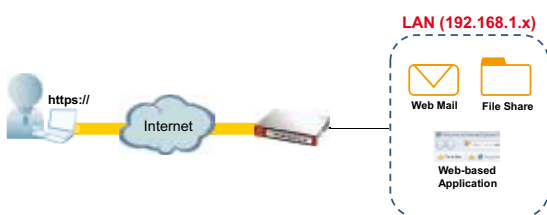
Grafik: Das VPN-Tunnel verbindet die Firewall (X) mit dem Remote (Peer)-IPSec-Router (Y). Diese Router verbinden dann das lokale Netzwerk (A) mit dem Remote-Netzwerk (B).

SSL VPNs

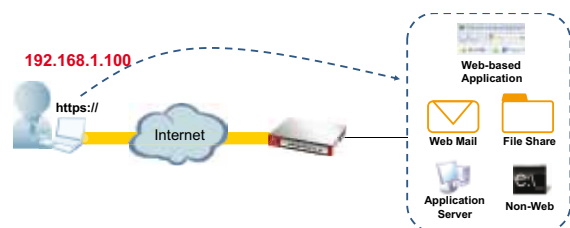
Ein Secure-Socket-Layer-Virtual-Private-Network (SSL VPN) verwendet SSL, um einen VPN-Netzwerk-Zugang für Remote-User zu schaffen. Wenn SSL (das Secure-Socket-Layer-Protokoll) benutzt wird, ist keine Security-Software-Installation notwendig. Remote-

User können Internet Explorer oder einen anderen Standard-Web-Browser verwenden. Es gibt zwei Modi eines SSL VPN Netzwerk-Zugangs: ReverseProxy und Full-Tunnel.

Reverse-Proxy-Modus



Full-Tunnel-Modus



Warum IPSec VPN?

IPSec vs SSL VPNs

IPsec und SSL VPN haben beide individuelle Vorteile. Es stellt sich also nicht die Frage, welche Methode „besser“, sondern vielmehr, welche geeigneter für das jeweilige Netzwerk ist. Die folgende Matrix stellt die Unterschiede zwischen IPSec und SSL VPN dar.

	IPSec VPN	SSL VPN
Netzwerkumgebung und Gerät		
Verbindungsart	fixe Verbindung	flüchtige (temporäre) Verbindung
Kosten	hoher Fixanteil/geringer variabler Anteil	mässiger Fixanteil/hoher variabler Anteil
Skalierbarkeit	Einfach zu installieren und zu skalieren	serverseitig zu skalieren
Gerätetyp	in Besitz und Verwaltung des Unternehmens	verwaltet oder nicht verwaltet
User		
Aussenstelle oder Filiale	✓	-
mobile Mitarbeiter	✓	✓
Geschäftspartner	✓	✓
Kunden	✓	✓
Anwendungen und Inhalt		
unterstützte Anwendungen	Alle IP-basierten Services	Web-fähige Anwendungen, File-Sharing, E-mail

Unter gewissen Bedingungen ist IPSec VPN jedoch besser geeignet als SSL VPN. IPSec VPN ist optimal für den Punkt-zu-Punkt-Zugang, wenn ein Unternehmen eine permanente Verbindung zwischen zwei Standorten benötigt, wie zum Beispiel zwischen einer Filiale

und der Unternehmenszentrale. Die Methode bewährt sich im Einsatz für eine begrenzte Anzahl von Benutzer-Desktops, die vom Unternehmen verwaltet werden.

ZyXEL hat die Lösung

ZyXEL hat eine umfassende IPSec VPN Lösung für Remote-Working entwickelt, die das Arbeiten in Büroumgebung von einem Home Office oder einem alternativen Arbeitsort aus ermöglicht. Die ZyWALL UTM Firewall von ZyXEL ist das ideale Gerät für diese Anforderung.

Zusätzlich kann das intelligente ZyWALL VPN unterbrochene Tunnel wiederherstellen und so eine sichere Verbindung aufrechterhalten.

IPSec VPNS

Layer 3 Encryption between Gateway-to-Gateway or Gateway-to-Remote client.

