

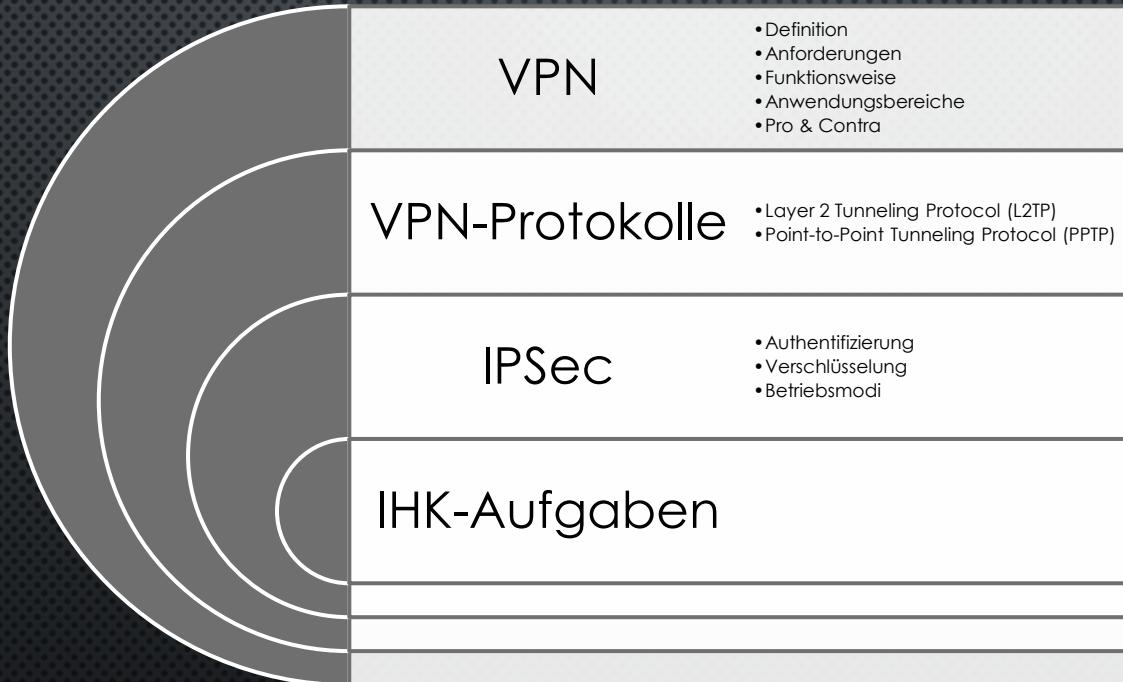
VPN + IPSec

VIRTUAL PRIVATE NETWORKS

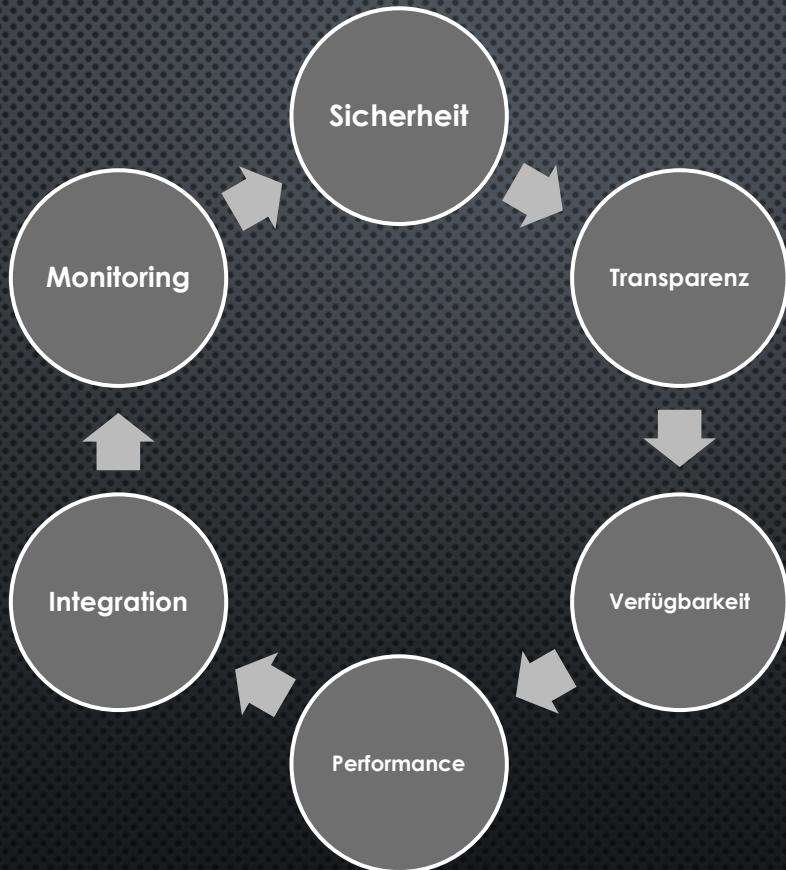


ipssec 

VIRTUAL PRIVATE NETWORKS - AGENDA

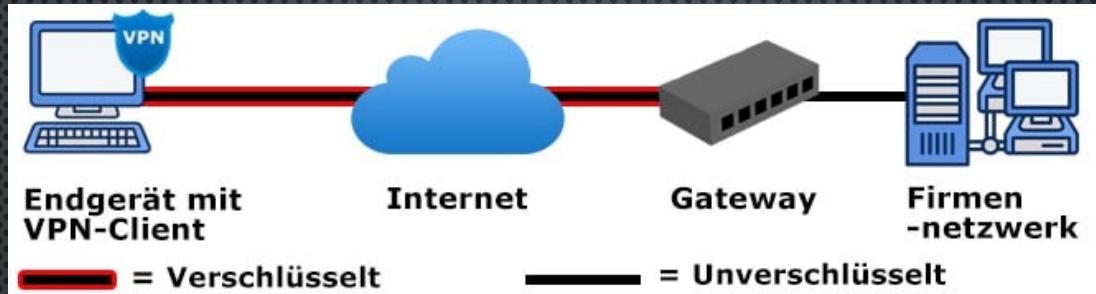


VPN - ANFORDERUNGEN



VPN - ANWENDUNGSBEREICHE

End-to-Site



Vorteile

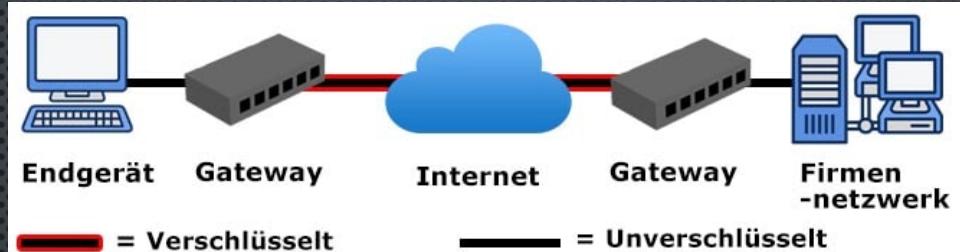
- Der Außendienstmitarbeiter braucht **keine zusätzliche Hardware**.
- Es wird nur ein VPN-Gateway benötigt, somit werden **Kosten reduziert**.
- Niemand im LAN bzw. WLAN des Endgerätes kann den Datenverkehr abfangen.
- Alle Geräte im Firmennetzwerk und der VPN-Client können problemlos **miteinander kommunizieren**.

Nachteile

- Das Gerät (z.B. Notebook) muss einen **VPN-Client (Software)** installiert haben.
- Ab dem Gateway ist der Datenverkehr des VPN-Clients im Firmennetzwerk **unverschlüsselt**.

VPN - ANWENDUNGSBEREICHE

Site-to-Site



Vorteile

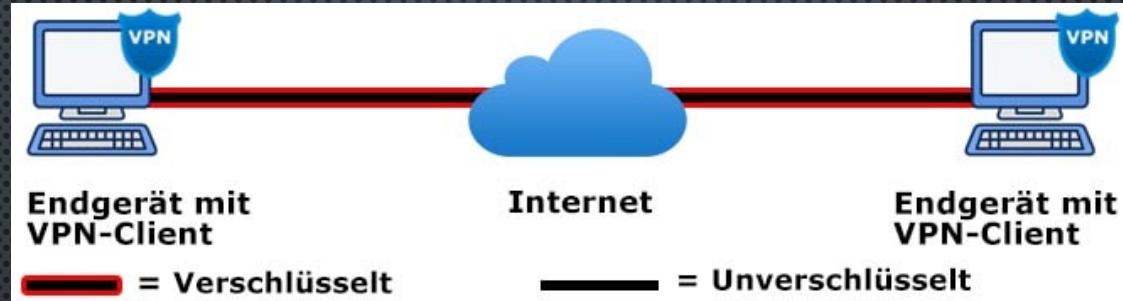
- Sämtliche Geräte im Netzwerk brauchen nicht konfiguriert zu werden.
- An das Netzwerk lassen sich ganz einfach, ohne Konfiguration weitere Geräte anschließen.
- Es können schnell & einfach weitere VPN-Gateways (weitere Standorte) hinzugefügt werden.

Nachteile

- Es wird weitere Hardware benötigt – VPN-Gateway.
- Der Datenverkehr des Endgerätes ist innerhalb seines LANs nicht verschlüsselt. Ebenso der Datenverkehr innerhalb des Firmennetzwerkes. Ausschließlich zwischen den Gateways wird verschlüsselt.

VPN - ANWENDUNGSBEREICHE

End-to-End



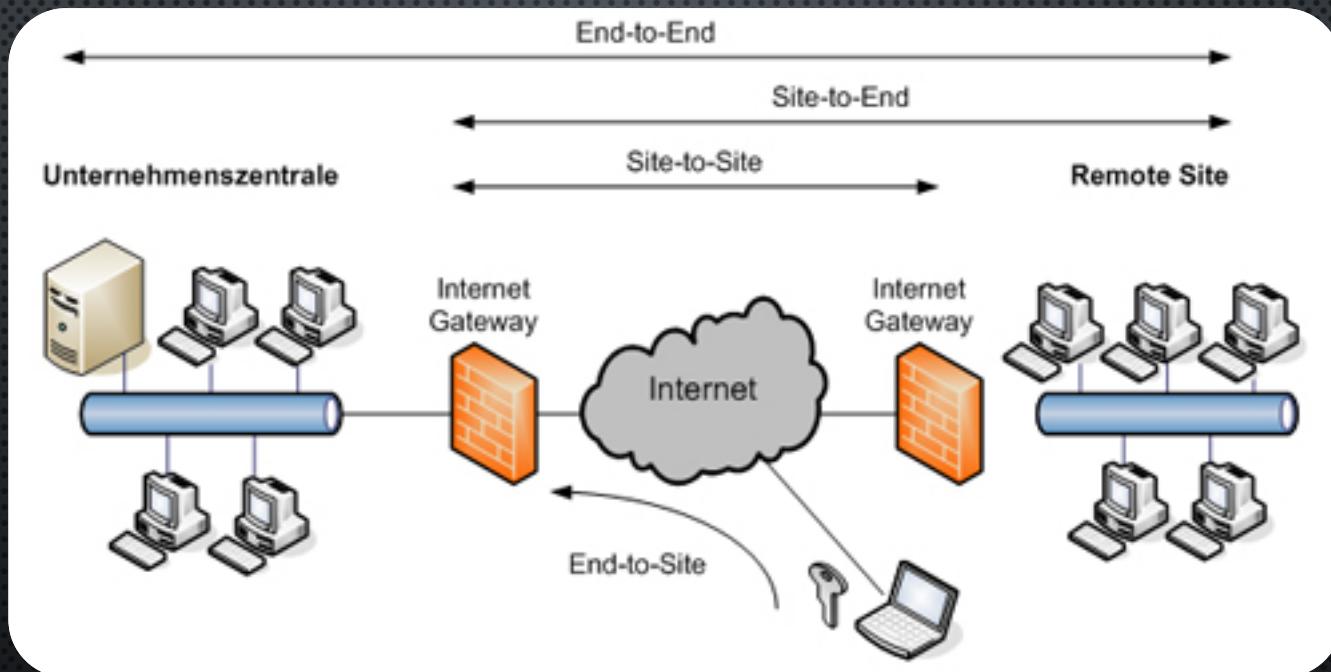
Vorteile

- Es wird keine zusätzliche Hardware benötigt.
- Die komplette Verbindung zwischen beiden Endgeräten ist verschlüsselt. Niemand sonst im LAN kann den Datenverkehr abfangen.
- Niemand im LAN bzw. WLAN der Endgeräte kann den Datenverkehr abfangen.

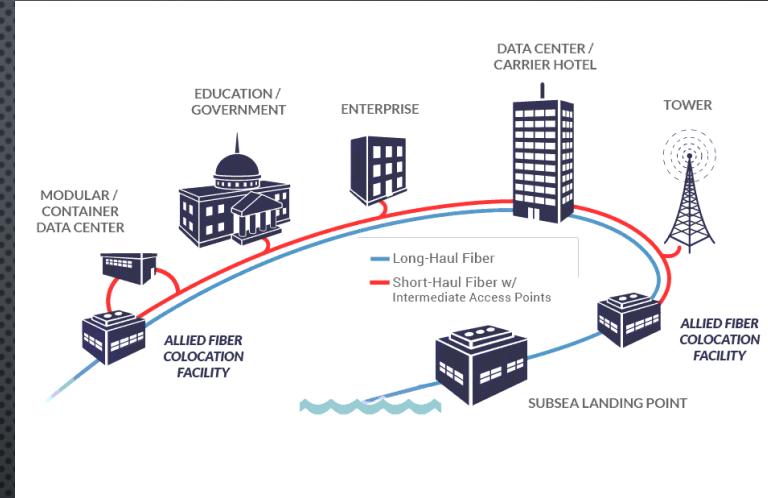
Nachteile

- Beide Endgeräte müssen einen VPN-Client installiert haben.
- Möchte eines der Endgeräte auf ein anderes im jeweils anderen Netzwerk zugreifen, geht dies nur über den VPN-Client des Partners (nur über den VPN-Endpunkt). Das Gerät muss also eingeschaltet sein.

VPN - ANWENDUNGSBEREICHE



VPN – ALTERNATIVEN

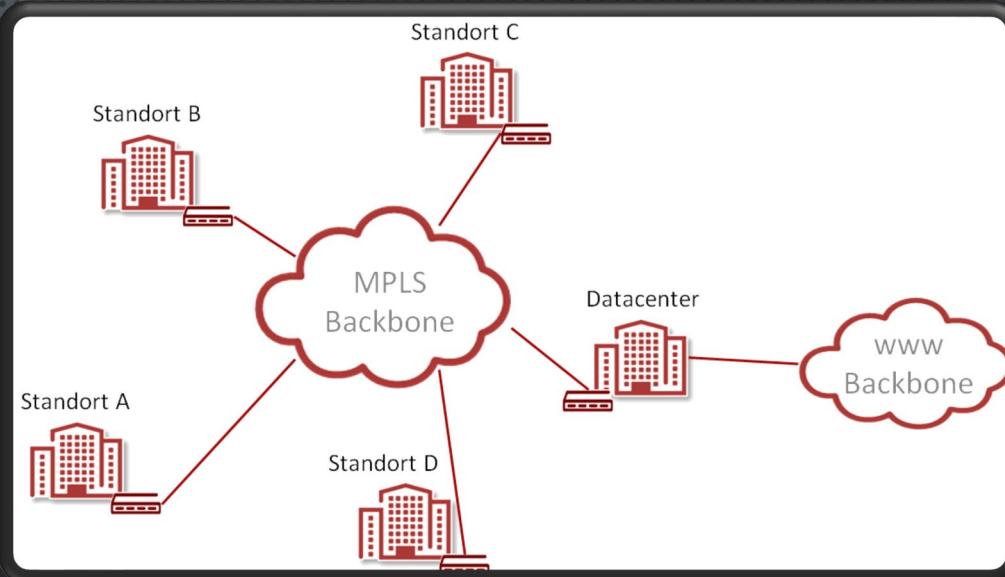


Die Kosten für die Miete liegen je nach Wettbewerbssituation pro Meter und Jahr bei ca. 1,20 €

VPN – ALTERNATIVEN

Multiprotocol Label Switching (MPLS)

| Bandbreite | Einrichtungskosten (einmalig) | | | Monatliche Kosten | | |
|-----------------------------|-------------------------------|-------------|-------------|-------------------|-------------|-------------|
| | 24 Monate | 36 Monate | 60 Monate | 24 Monate | 36 Monate | 60 Monate |
| 2 Mbit/s | 199,00 € | 99,00 € | 0,00 € | ab 139,00 € | ab 129,00 € | ab 119,00 € |
| 4 Mbit/s | 199,00 € | 99,00 € | 0,00 € | ab 219,00 € | ab 209,00 € | ab 199,00 € |
| 8 Mbit/s | 349,00 € | 249,00 € | 149,00 € | ab 399,00 € | ab 379,00 € | ab 369,00 € |
| 10 Mbit/s | 349,00 € | 249,00 € | 149,00 € | ab 579,00 € | ab 539,00 € | ab 499,00 € |
| 20 Mbit/s - 1 Gbit/s | auf Anfrage | auf Anfrage | auf Anfrage | ab 699,00 € | ab 649,00 € | ab 599,00 € |



Mit MPLS lässt sich jeder Anwendung eine differenzierte Dienstgüte zuordnen.

VPN – PRO & CONTRA

Pro

- Kostengünstig

- Sicher

- Flexibel

Contra

- Abhängig von der Verfügbarkeit anderer Netzwerke

- Performance

- Aufwand zu Erhaltung der Sicherheit

VPN – PROTOKOLLE

| Eigenschaften | PPTP | L2TP | IPsec |
|--|----------|------|-------|
| Authentifizierung | Ja | Ja | Nein |
| Unterstützung von NAT | Ja | Ja | Nein |
| Multiprotokollfähigkeit | Ja | Ja | Nein |
| Dynamische Zuweisung von Tunnel-IP-Adressen | Ja | Ja | N/A |
| Verschlüsselung | begrenzt | Nein | Ja |
| Public Key Infrastructure | Nein | Nein | Ja |
| Überprüfung der Authentizität von Paketen | Nein | Nein | Ja |
| Unterstützung Multicast | Ja | Ja | Nein |



Vertraulichkeit



Authentizität



Integrität

VPN – IP SEC (IP SECURITY PROTOCOL)

- IP Sec – „IP Security“
- Entwickelt in 1998 von der IETF (Internet Engineering Task Force)
- Ursprünglich für IPv6
- Sicherheitsarchitektur für IP – Netze
- Arbeitet auf OSI – Layer 3
- Gewährleistet Vertraulichkeit und Integrität

VPN – IP SEC (IP SECURITY PROTOCOL)

Authentifizierung

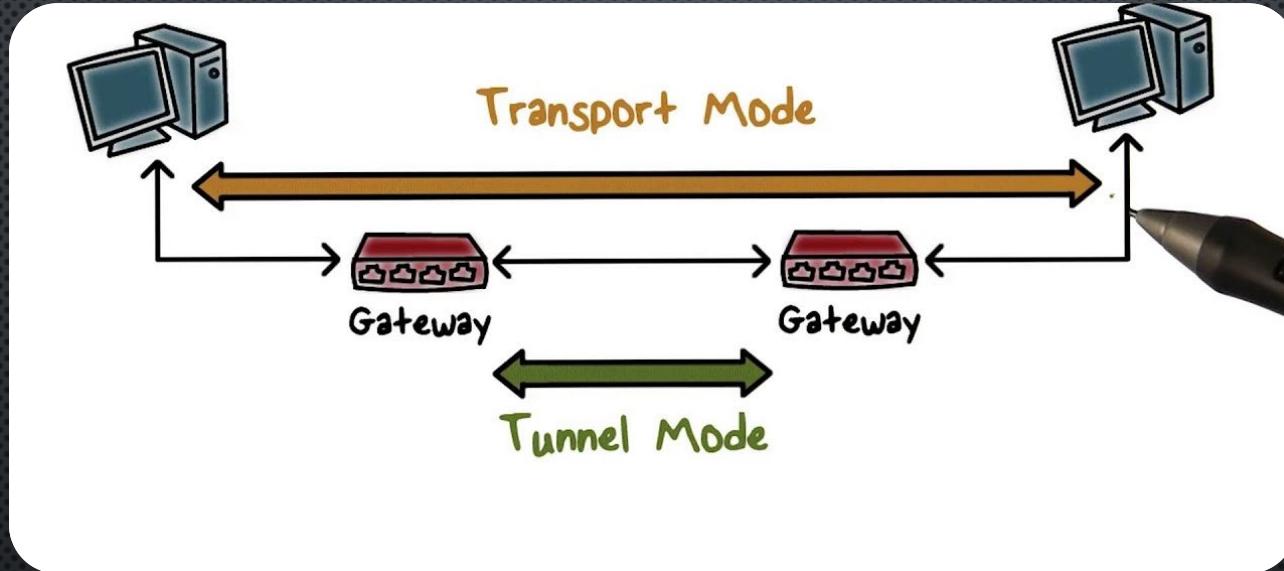
- PSK (Pre Shared Key)
- IKEv2 (Internet Key Exchange Protocol)
 - Diffie-Hellmann-Verfahren (Verwendung von X.509 Zertifikaten)
 - UDP Port 500

VPN – IP SEC (IP SECURITY PROTOCOL)

Sicherheit

- AH – Authentication Header
 - Datenintegrität
 - Datenaauthenzität
 - Keine Verschlüsselung
- ESP – Encapsulating Security Payload
 - Funktionalität des AH - Protokolls
 - Verschlüsselung der Pakete (z.B. AES,...)

UNTERSCHIEDE TRANSPORT- TUNNELMODUS



Der Tunnelmodus kann bei allen VPN-Anwendungen eingesetzt werden. In der Hauptsache aber, wenn zwei Netzwerke über ein unsicheres Netzwerk miteinander verbunden werden sollen. Will man nur zwei Rechner miteinander verbinden, dann verwendet man den Transportmodus. Der Transportmodus kann aber nur bei einer Host-to-Host-Verbindung verwendet werden.

AH - AUTHENTICATION HEADER

Authentication Header (AH) sorgt innerhalb von IPsec (VPN) für die Authentizität der zu übertragenen Daten und die Authentifizierung des Senders. Mit AH kann man "nur die Integrität und Echtheit" der Daten sicherstellen. Die Nutzdaten werden nicht verschlüsselt und sind damit für jeden lesbar.

AH wird selten verwendet, weil "nur Integrität" meist nicht ausreicht. In der Regel möchte man die Daten noch verschlüsseln, um sie vor fremdem Zugriff zu schützen. Neben Authentication Header (AH) gibt es auch noch Encapsulating Security Payload (ESP). Beide können gemeinsam oder alleine genutzt werden. Im Unterschied zu Authentication Header verschlüsselt Encapsulating Security Payload die Daten.

ESP - ENCAPSULATING SECURITY PAYLOAD

Encapsulating Security Payload (ESP) sorgt innerhalb von IPsec (VPN) für die Authentisierung, Integrität und Vertraulichkeit der IP-Pakete. Im Unterschied zu Authentication Header (AH) werden die Nutzdaten verschlüsselt übertragen. Während AH "nur die Integrität und Echtheit" der Daten sicherstellen kann, erhöht ESP die Datensicherheit in Abhängigkeit des gewählten Verschlüsselungsalgorithmus. Deshalb wird in der Regel ESP und nicht AH verwendet. ESP sorgt für die Vertraulichkeit der Kommunikation. Die Pakete werden verschlüsselt. Zusätzlich schützt eine Integritätssicherung vor Manipulation.

Authentication Header (AH)

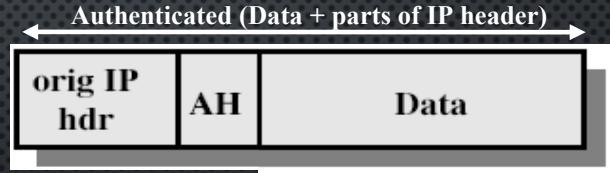
Hiermit bekommt jedes Paket eine digitale Signatur zugewiesen, wodurch Ihr Netzwerk und Ihre Daten vor Störungen durch Dritte geschützt werden. Dies bedeutet, dass der Inhalt eines Datenpakets nicht geändert werden kann, ohne dies festzustellen und ermöglicht auch die Identitätsüberprüfung zwischen den beiden Enden einer Verbindung.

Original IP Paket:



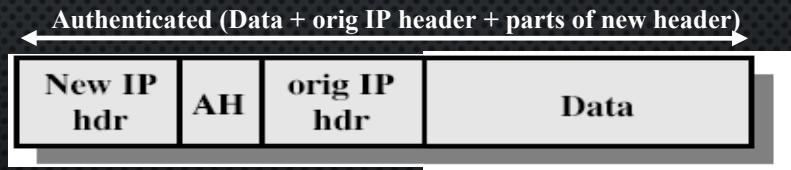
Transport Modus:

- Nur Data und Teile des Headers sind authentifiziert



Tunnel Modus:

- Das ganze Paket ist authentifiziert und Teile des neuen Headers



Encapsulating Security Payload (ESP)

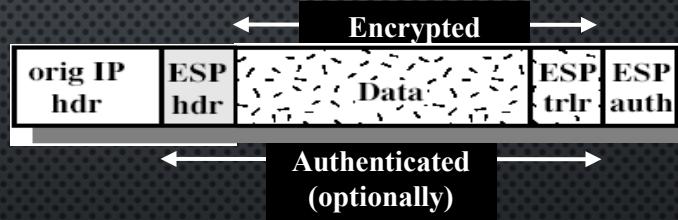
Während der AH die Manipulation eines Pakets verhindert, stellt das ESP sicher, dass die Informationen im Paket verschlüsselt sind und nicht gelesen werden können. Ein ESP-Header, ein Trailer und eine Authentifizierungsblockierung werden verwendet, um die komplette Nutzlast eines Pakets zu verschlüsseln.

Original IP Paket:



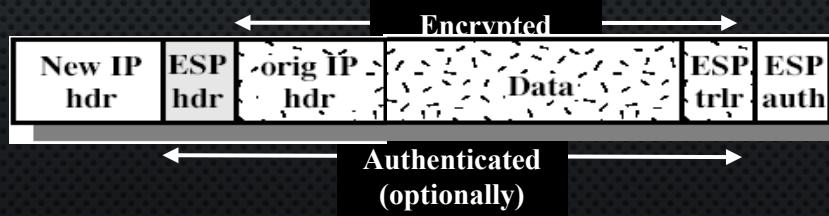
Transportmodus:

- Nur Data ist verschlüsselt & authentifiziert



Tunnel Modus:

- Das ganze Paket ist verschlüsselt & authentifiziert



VOR- UND NACHTEILE VON IPSEC

Vorteile

Da IPSec auf Netzwerkebene arbeitet, müssen Änderungen nur am Betriebssystem und nicht an einzelnen Anwendungen vorgenommen werden.

IPSec ist im Betrieb vollständig unsichtbar und daher die ideale Wahl für ein VPN.

Die Verwendung von AH und ESP garantiert ein Höchstmaß an Sicherheit und Datenschutz.

Nachteile

IPSec ist komplizierter als alternative Sicherheitsprotokolle und schwieriger zu konfigurieren.

Für IPSec sind sichere öffentliche Schlüssel erforderlich. Wenn Ihr Schlüssel kompromittiert ist oder Sie über ein schlechtes Schlüsselmanagement verfügen, können Probleme auftreten.

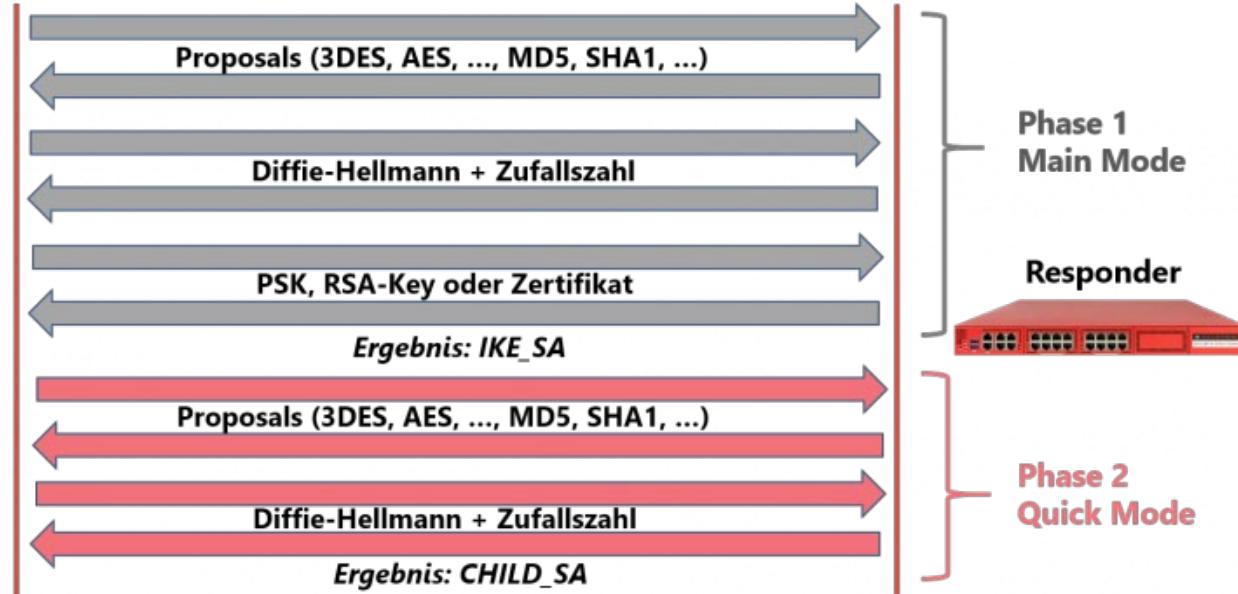
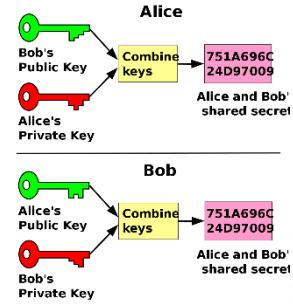
Für die Übertragung kleiner Pakete kann IPSec eine ineffiziente Methode zum Verschlüsseln von Daten darstellen.

VPN – IP SEC (IP SECURITY PROTOCOL)

Verbindungsauftbau IKE

1. Sender sendet Vorschläge für Authentisierungs- und Verschlüsselungsalgorithmen
2. Empfänger wählt den sichersten Algorithmus und teilt dies dem Sender mit
3. Beide berechnen den privaten Schlüssel
4. Sender sendet seinen öffentlichen Schlüssel
5. Empfänger sendet seinen öffentlichen Schlüssel
6. Mit privatem Schlüssel: Authentifizierung mit Zertifikat oder PSK

Anschließend Wiederholung der Schritte (verschlüsselt),
eine SA (Security Association) wird angelegt



VPN – IP SEC (IP SECURITY PROTOCOL)

SA – Security Association

Vereinbarung zwischen den kommunizierenden Partnern mit Inhalt:

1. Identifikation mit Zertifikat oder PSK
2. Verwendeter Schlüsselalgorithmus
3. Sender – IP
4. Empfänger – IP
5. TTL für Authentifizierung
6. TTL für IPSec – Schlüssel

IHK AUFGABEN

c) Zwischen den vier Standorten der GeoData AG wird ein VPN eingerichtet.

ca) Nennen Sie den Verbindungstyp.

GH2
S17

2 Punkte

ca) 2 Punkte

Site-to-Site (LAN-to-LAN)

cb) Es wird IPsec als Protokoll verwendet.

Nennen Sie den Verbindungsmodus.

GH2
S17

2 Punkte

cb) 2 Punkte

Tunnelmodus

cc) Die Datenübermittlung im VPN ist durch Authentifizierung abgesichert.

Erläutern Sie, was bei der Datenübertragung im VPN durch Authentifizierung sichergestellt werden soll.

GH2
S17

3 Punkte

cc) 3 Punkte

Identifizierung von autorisierten Nutzern und Prüfung, ob die gesendeten Daten aus der autorisierten Quelle stammen

IHK AUFGABEN

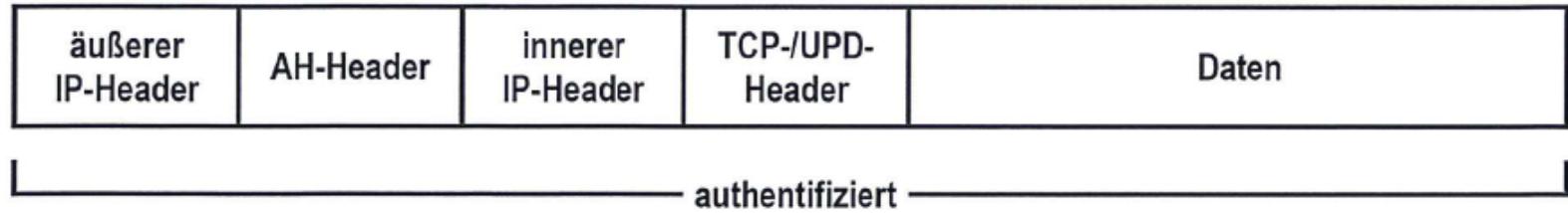
Die Außendienstmitarbeiter der RAVAG GmbH sollen sich von extern mit dem LAN der Zentrale Köln verbinden können.

- a) Ein Außendienstmitarbeiter soll über eine VPN-Verbindung an das Unternehmensnetz angebunden werden. Dazu wurde vom Administrator auf dem Notebook ein IPSec-Client installiert.
 - aa) Nennen Sie die Art des VPNs und den Namen der Schicht im OSI-Modell, auf dem die Verbindung aufgebaut wird. 2 Punkte

End-to-Site bzw. Tunnelmodus, Vermittlungsschicht bzw. Network-Layer (Schicht 3)

IHK AUFGABEN

- ab) Der Außendienstmitarbeiter soll mit seinem Notebook eine mit AH authentifizierte Verbindung zum VPN-Gateway in der Firma aufbauen. Das IP-Paket, das die Netzwerkschnittstelle des Notebooks verlässt, hat folgenden Aufbau:



Erläutern Sie, warum die Time-To-Live (TTL) im äußeren IP-Header nicht in die Prüfsumme im AH-Header einbezogen werden darf.

4 Punkte

- AH bildet einen Hashwert über das komplette IP-Paket.
- Wird die TTL einberechnet, verfälscht sich die Prüfsumme, da die TTL an jedem Router um 1 vermindert wird.

IHK AUFGABEN

ac) Die VPN-Verbindung wird über einen pre-shared key (PSK) authentifiziert.

Erläutern Sie, wie ein PSK zur Authentifizierung eingesetzt wird.

4 Punkte

- Sowohl auf dem Client als auch auf dem VPN-Gateway wird der PSK hinterlegt und verschlüsselt beim Verbindungsauftbau übermittelt.
- Stimmen der PSK des Clients mit dem des VPN-Gateways überein, wird die VPN-Verbindung aufgebaut.

ad) Die Authentifizierung durch pre-shared keys soll durch digitale Zertifikate abgelöst werden.

Nennen Sie drei Inhalte eines digitalen Zertifikats.

3 Punkte

- Aussteller
- Inhaber
- Gültigkeit
- Version
- Public Key des Inhabers
- Digitale Signatur der CA
- u. a.

IHK AUFGABEN

- ae) Ergänzen Sie die folgende Beschreibung, wie der VPN-Gateway die Gültigkeit des Client-Zertifikats überprüfen kann.

4 Punkte

Beschreibung:

Der VPN-Gateway entschlüsselt die digitale Signatur der CA mit dem public key der CA.

Der VPN-Gateway erhält den von der CA gebildeten Hashwert über das Zertifikat. Er vergleicht den Hashwert der CA mit dem von ihm gebildeten Hashwert. Stimmen die Hashwerte überein, ist das Zertifikat echt.

b) Die Administratoren bestellen eine Standleitung beim Provider. Die Verbindung hat folgende Spezifikationen:

Datentransferrate: 10 Mbit/s

Protokoll: Ethernet

Maximale Transfer Unit (MTU): 1.500 Byte

Maximale Länge Ethernetframe: 1.518 Byte

Als Schicht-3-Protokoll wird IPSec mit folgenden Werten verwendet:

Overhead Tunnelmodus: 20 Byte

- bc) Nachts werden die Daten aus den Baumärkten in die Zentrale übertragen. In der Filiale Köln werden 300 MiB Geschäftsdaten über eine mit IPSec gesicherte Ethernet-Verbindung abgerufen.

ESP-Header: 40 Byte

Berechnen Sie die minimale Übertragungsdauer bei einer Transferrate von 10 Mbit/s. Runden Sie das Ergebnis auf volle Sekunden. Der Rechenweg ist anzugeben.

TCP/IP Header: 40 Byte

6 Punkte

ba) Sie testen die funktionsfähige IPSec-Verbindung mit der Standard-MTU von 1.500 Byte. Dazu führen Sie einen ping mit den Parametern -f (don't fragment) und -l (Länge) aus:

```
ping -f -l 1500 www.vnet.de
```

Ping wird ausgeführt für www.vnet.de [85.100.20.17] mit 1500 Bytes Daten:

Paket müsste fragmentiert werden, DF-Flag ist jedoch gesetzt.

Ping-Statistik für 200.0.0.2:

Pakete: Gesendet = 4, Empfangen = 0, Verloren = 4
(100 % Verlust),

Erklären Sie, warum es zu einem Verlust von 100 % bei den gesendeten Paketen kommt.

3 Punkte

b) Die Administratoren bestellen eine Standleitung beim Provider. Die Verbindung hat folgende Spezifikationen:

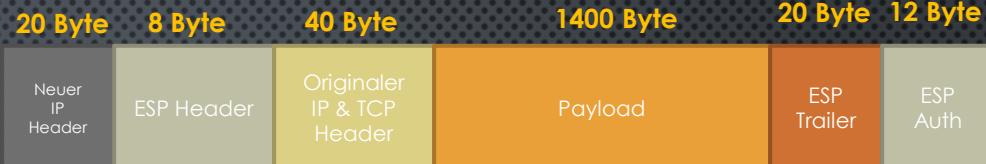
Datentransferrate: 10 Mbit/s
Protokoll: Ethernet
Maximale Transfer Unit (MTU): 1.500 Byte
Maximale Länge Ethernetframe: 1.518 Byte

Als Schicht-3-Protokoll wird IPSec mit folgenden Werten verwendet:

Overhead Tunnelmodus: 20 Byte
ESP-Header: 40 Byte
TCP/IP Header: 40 Byte

bc) Nachts werden die Daten aus den Baumärkten in die Zentrale übertragen. In der Filiale Köln werden 300 MiB Geschäftsdaten über eine mit IPSec gesicherte Ethernet-Verbindung abgerufen.

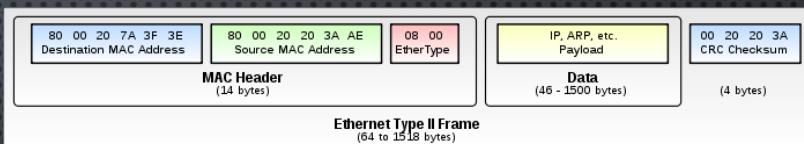
Berechnen Sie die minimale Übertragungsdauer bei einer Transferrate von 10 Mbit/s. Runden Sie das Ergebnis auf volle Sekunden. Der Rechenweg ist anzugeben.
6 Punkte



1500 Byte

Berechnung des max. Payloads:

$$\text{MTU (1.500 Byte)} - \text{20 Byte} - \text{40 Byte} - \text{40 Byte} = \underline{\underline{1.400 Byte}}$$



1. $300 \times 1024^2 = 314.572.800 \text{ Byte}$
2. $314.572.800 \text{ Byte} / 1.400 \text{ Byte} = 224.695 \text{ Pakete}$
3. $1.518 * 224.695 = 341.087.010 \text{ Byte}$
4. $341.087.010 \text{ Byte} * 8 = 2.728.696.080 \text{ Bit}$
5. $2.728.696.080 \text{ Bit} / 10 * 1000^2$

$$= 272,9 \text{ Sekunden} \rightarrow 273 \text{ Sekunden}$$

b) Die Administratoren bestellen eine Standleitung beim Provider. Die Verbindung hat folgende Spezifikationen:

Datentransferrate: 10 Mbit/s
Protokoll: Ethernet
Maximale Transfer Unit (MTU): 1.500 Byte
Maximale Länge Ethernetframe: 1.518 Byte

Als Schicht-3-Protokoll wird IPSec mit folgenden Werten verwendet:

Overhead Tunnelmodus: 20 Byte
ESP-Header: 40 Byte
TCP/IP Header: 40 Byte

ba) Sie testen die funktionsfähige IPSec-Verbindung mit der Standard-MTU von 1.500 Byte. Dazu führen Sie einen ping mit den Parametern -f (don't fragment) und -l (Länge) aus:

ping -f -l 1500 www.vnet.de

Ping wird ausgeführt für www.vnet.de [85.100.20.17] mit 1500 Bytes Daten:
Paket müsste fragmentiert werden, DF-Flag ist jedoch gesetzt.
Paket müsste fragmentiert werden, DF-Flag ist jedoch gesetzt.
Paket müsste fragmentiert werden, DF-Flag ist jedoch gesetzt.
Paket müsste fragmentiert werden, DF-Flag ist jedoch gesetzt.

Ping-Statistik für 200.0.0.2:

Pakete: Gesendet = 4, Empfangen = 0, Verloren = 4

(100 % Verlust), Die MTU ist zu groß, deswegen müsste das Paket fragmentiert werden, was allerdings nicht erlaubt ist.

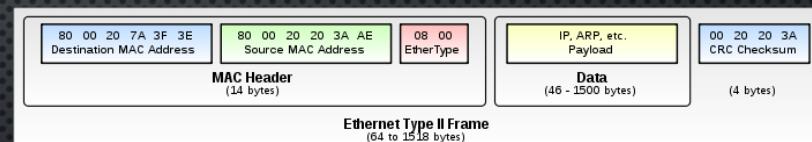
Erklären Sie, warum es zu einem Verlust von 100 % bei den gesendeten Paketen kommt. 3 Punkte

bb) Nennen Sie den ping-Befehl mit den optimalen Parametern, damit es zu keinem Paketverlust kommt! ping -f -l 1400



Berechnung des max. Payloads:

$$\text{MTU (1.500 Byte)} - \text{20 Byte} - \text{40 Byte} - \text{40 Byte} = \underline{\text{1.400 Byte}}$$



Wandeln Sie folgende MAC-Adresse in eine IPV6-Interface-ID um. (EUI64)
a0-23-ec-ff-fe-56 →

Es sollen 20 neue Arbeitsplatzrechner beschafft werden. Sie sind für die Hardwareausstattung der Geräte zuständig und sollen entscheiden, mit welchem der beiden zur Auswahl stehenden Netzteiltypen die Geräte ausgeliefert werden sollen.

Die Bauteile eines PCs benötigen 220 Watt

Der Strompreis liegt bei 28,8 Cent pro kWh

Laufzeit pro Jahr: 210 Tage

Laufzeit pro Tag: 8 Stunden

ba) Berechnen Sie die Stromkosten pro Jahr für Netzteiltyp A und Netzteiltyp B.

Der Rechenweg ist anzugeben. Das Ergebnis ist kaufmännisch zu runden.

6 Punkte

| | Netzteiltyp A | Netzteiltyp B |
|-----------------------|-----------------------------|----------------------------|
| | PowerMax Ex350WT (350 Watt) | Green EP300gt-C (300 Watt) |
| Preis: | 48 EUR | 39 EUR |
| 10-20 % Last @ 230 V | Wirkungsgrad: 58,3 % | Wirkungsgrad: 52,0 % |
| 20-40 % Last @ 230 V | Wirkungsgrad: 73,7 % | Wirkungsgrad: 67,0 % |
| 40-60 % Last @ 230 V | Wirkungsgrad: 86,6 % | Wirkungsgrad: 81,0 % |
| 60-100 % Last @ 230 V | Wirkungsgrad: 95,5 % | Wirkungsgrad: 91,5 % |
| Noise Level | 17,1 dB(A) | 27,5 dB(A) |

Es sollen 20 neue Arbeitsplatzrechner beschafft werden. Sie sind für die Hardwareausstattung der Geräte zuständig und sollen entscheiden, mit welchem der beiden zur Auswahl stehenden Netzteiltypen die Geräte ausgeliefert werden sollen.

Die Bauteile eines PCs benötigen 220 Watt

Der Strompreis liegt bei 28,8 Cent pro kWh

Laufzeit pro Jahr: 210 Tage

Laufzeit pro Tag: 8 Stunden

bb) Ermitteln Sie, welcher Netzteiltyp unter Einbeziehung des Kaufpreises und der Stromkosten bei einer Nutzungsdauer von vier Jahren für alle 20 Arbeitsplatzrechner die geringeren Kosten verursacht. Der Rechenweg ist anzugeben. Das Ergebnis ist kaufmännisch zu runden.

4 Punkte

| | Netzteiltyp A | Netzteiltyp B |
|-----------------------|-----------------------------|----------------------------|
| | PowerMax Ex350WT (350 Watt) | Green EP300gt-C (300 Watt) |
| Preis: | 48 EUR | 39 EUR |
| 10-20 % Last @ 230 V | Wirkungsgrad: 58,3 % | Wirkungsgrad: 52,0 % |
| 20-40 % Last @ 230 V | Wirkungsgrad: 73,7 % | Wirkungsgrad: 67,0 % |
| 40-60 % Last @ 230 V | Wirkungsgrad: 86,6 % | Wirkungsgrad: 81,0 % |
| 60-100 % Last @ 230 V | Wirkungsgrad: 95,5 % | Wirkungsgrad: 91,5 % |
| Noise Level | 17,1 dB(A) | 27,5 dB(A) |