ZSL
Zentrum für Schulqualität
und Lehrerbildung
Baden-Württemberg

Networking Academy

VPN and IPsec Concepts

Ursprünglicher Autor der Folien:
Michael Krüger
Carl-Benz-Schule BBS Technik Koblenz
mich@elkrueger.de

Andreas Grupp
Andreas.Grupp@fbu-rpt.de

Carina Haag
haag.c@lanz.schule

Tobias Heine
tobias.heine@springer-schule.de

Uwe Thiessat
uwe.thiessat@gbs-sha.de

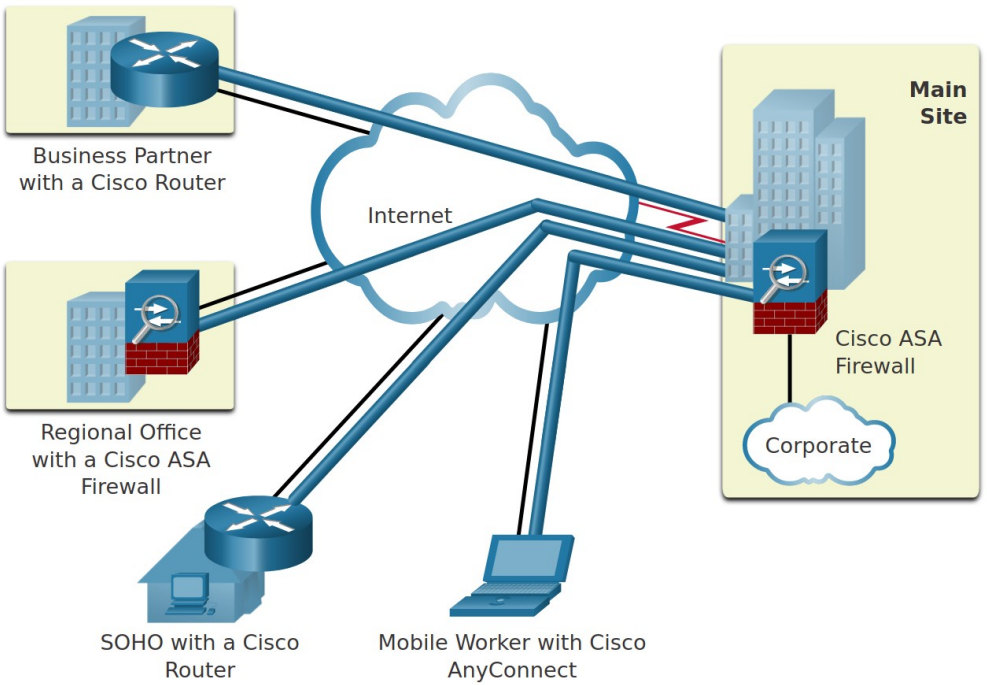
Ziel des Kapitels

Ziel: Site-To-Site und Remote-Access-Verbindungen mit VPNs und IPSEC absichern.

- **VPN Technology**
  → Vorteile, die VPNs bieten
  (Tobi)
- **Types of VPNs**
  → Verschiedene VPN-Arten
  (Tobi)
- **IPsec**
  → Verwendung von IPsec, um Netzwerkverkehr abzusichern
  (Carina)

Virtual Private Network (VPN)

- **Virtual ...**
  ... weil die Daten über ein öffentliches Netzwerk geleitet werden, aber so aussehen, als ob sie von einem internen Netzwerk kommen
- **Private …**
  … weil die Daten verschlüsselt übertragen werden



VPN-Technnologie – Vorteile von VPNs

Kosteneinsparung

- Günstige private Breitbandverbindung kann mit genutzt werden. Keine eigenen Leitungen notwendig.

Sicherheit

- Fortgeschrittene Kryptographie- (in IPsec und SSL) und Authentifizierung-Protokolle werden genutzt um die Daten zu schützen.

Skalierbarkeit

- Nutzung des Internets: dadurch können z. B. neue Nutzer implementiert werden ohne dass zusätzliche Infrastruktur benötigt wird

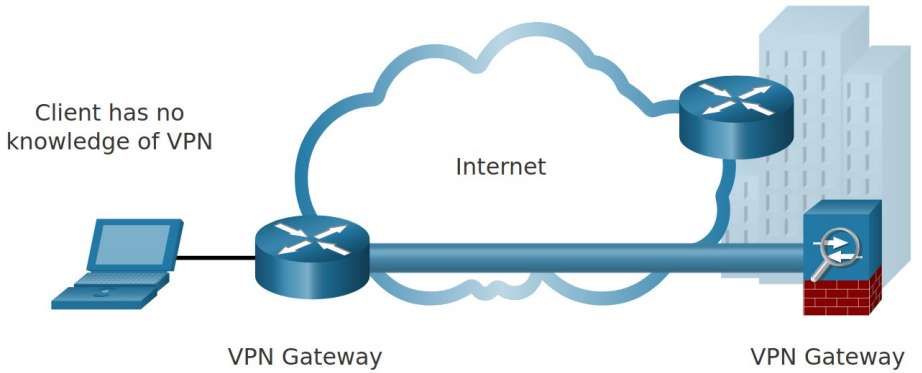
Kompatibilität

- VPNs funktionieren über alle WAN-Verbindungen (DSL, Kabel, Mobilfunk, …)

VPN-Technnologie

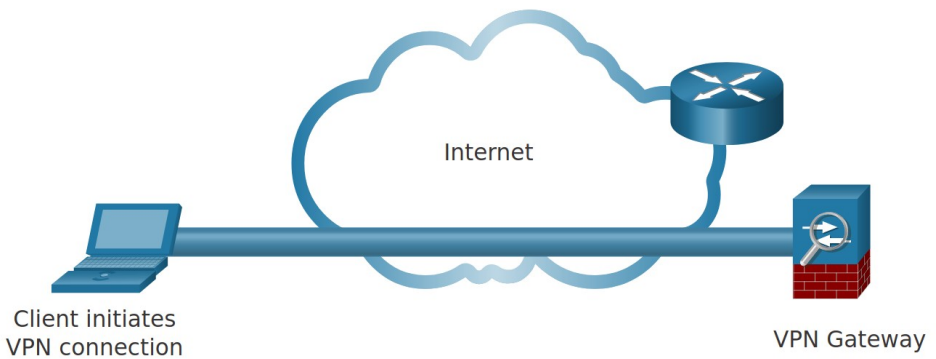
Site-to-Site-VPN

- Router baut Verbindung auf
- Clients bekommen nichts vom VPN mit, sondern senden Daten an Router



Remote-Access-VPN

- Client baut VPN-Verbindung auf
- Entweder durch VPN-Software oder auf Betriebssystem-Ebene konfiguriert

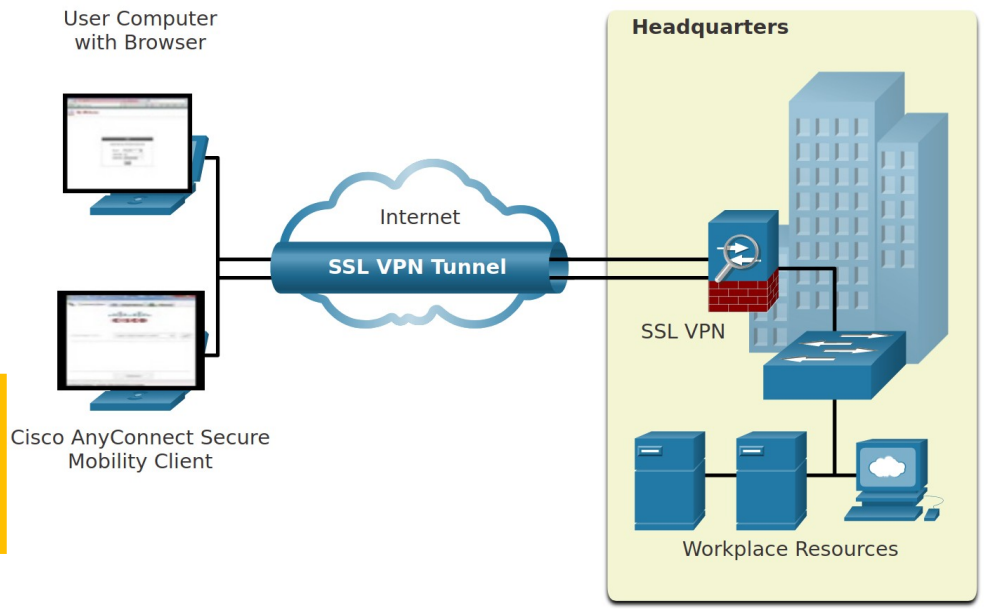


VPN-Technnologie – Enterprise und Provider

- Enterprise-VPNs für weltweit agierende Großunternehmen
  - Site-to-site
    - IPsec VPN
    - GRE over IPsec
    - Cisco Dynamic Multipoint Virtual Private Network (DMVPN)
    - IPsec Virtual Tunnel Interface (VTI)
    - [auch OpenVPN, Wireguard, …aber nicht im Material genannt]
  - Remote Access VPNs
    - Client-based IPsec VPN
    - * Clientless SSL connection (z.B. im Browser)
- Service-Provider-Managed VPNs für ISPs
  - Multiprotocol Label Switching (MPLS) auf Layer 2 oder 3
  - Früher (Legacy): Frame Relay, Asynchronous Transfer Mode ATM

Arten von VPNs – Remote-Access via IPsec oder SSL

- * „Clientless VPN connection“ – über Browser mit HTTPS
  - Nutzt SSL (bzw. Nachfolge-Technologie TLS bzw. SSL/TLS)
  - Browserbasiert
  - Wird genutzt wenn schnelle Implementierung im Fokus
- Client-based VPN connection – über VPN-Software / OS
  - i. d. R wird ein eigener Client benötigt z.B. Cisco AnyConnect Secure Mobility Client
  - Wird benutzt wenn höchste Sicherheit im Fokus



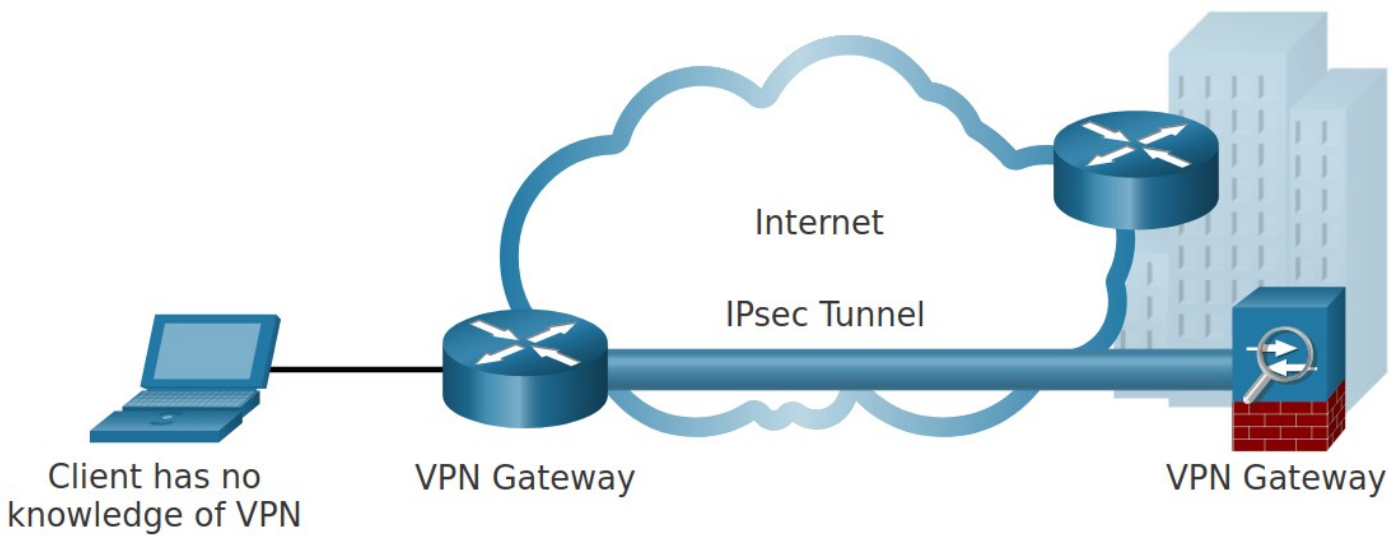
* Anmerkung: Cisco betrachtet hier SSL als VPN-Technologie, auch wenn der Vergleich etwas hinkt. Es wird kein Netzwerk aufgebaut.

Gegenüberstellung

Feature	IPsec	SSL
Applications supported	**Extensive** - All IP-based applications are supported.	**Limited** - Only web-based applications and file sharing are supported.
Authentication strength	**Strong** - Uses two-way authentication with shared keys or digital certificates.	**Moderate** - Using one-way or two-way authentication.
Encryption strength	**Strong** - Uses key lengths from 56 bits to 256 bits.	**Moderate to strong** - With key lengths from 40 bits to 256 bits.
Connection complexity	**Medium** - Because it requires a VPN client pre-installed on a host.	**Low** - It only requires a web browser on a host.
Connection option	**Limited** - Only specific devices with specific configurations can connect.	**Extensive** - Any device with a web browser can connect.

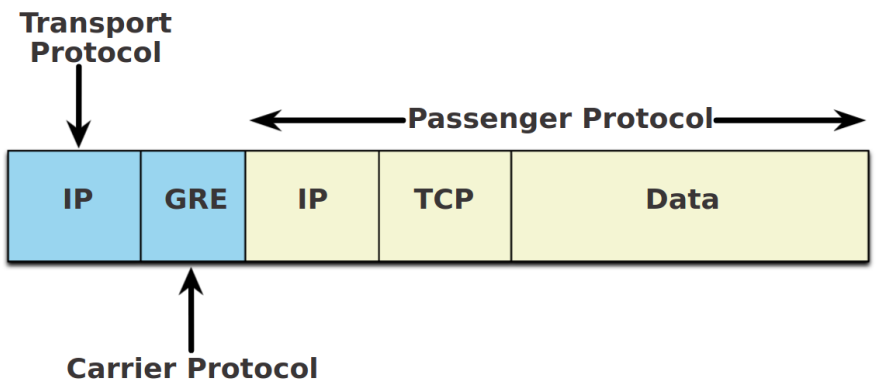
Arten von VPNs – Site-to-site IPsec

- Site-to-site VPNs werden oft über IPsec aufgebaut
- VPN-Gateway bei Zweigstelle baut Verbindung „nach Hause“ auf
  - „Nach Hause“ kann Cisco ASA in der Zentrale sein
- Client merkt nicht, dass ein VPN aufgebaut ist
  - Client sieht sich nativ im Firmennetz

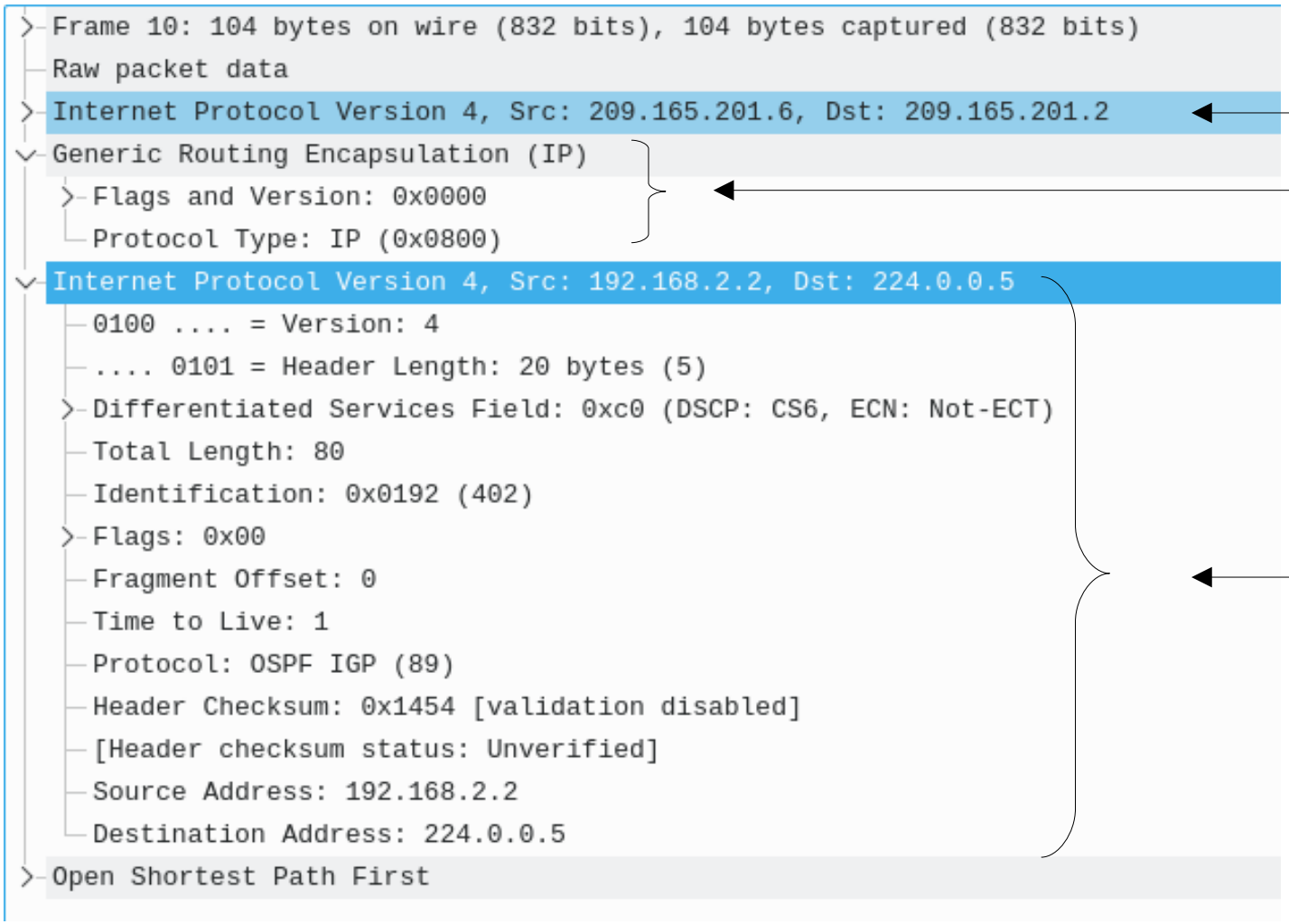


Arten von VPNs – GRE over IPsec

- Site-to-site VPNs mit IPsec können nur **Unicast-Traffic** übertragen
- **Problem für Routingprotokolle** → Kommunikation via Multicast!
- **Abhilfe:** Carrier-Protokoll Generic Routing Encapsulation (GRE)
  - Beliebige Protokolle werden als Daten innerhalb von GRE weitergeleitet (Beispiel: IP-Multicast)
  - GRE kann über beliebige Protokolle transportiert werden (z.B. IP)
  - Demzufolge mit GRE ein IP-Multicast-in-IP-Unicast-Tunnel möglich



Arten von VPNs – GRE over IPsec



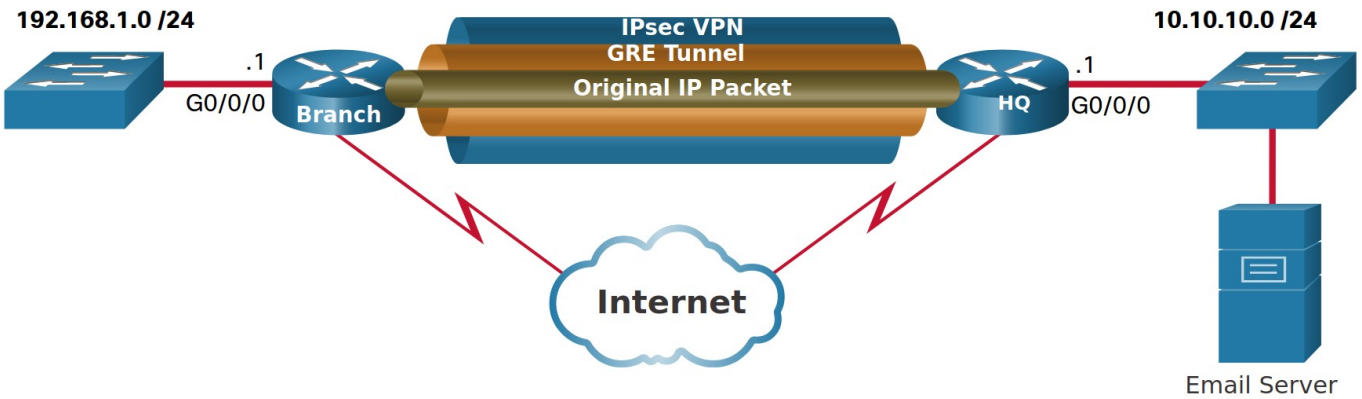
Transport-Protocol

Carrier-Protocol

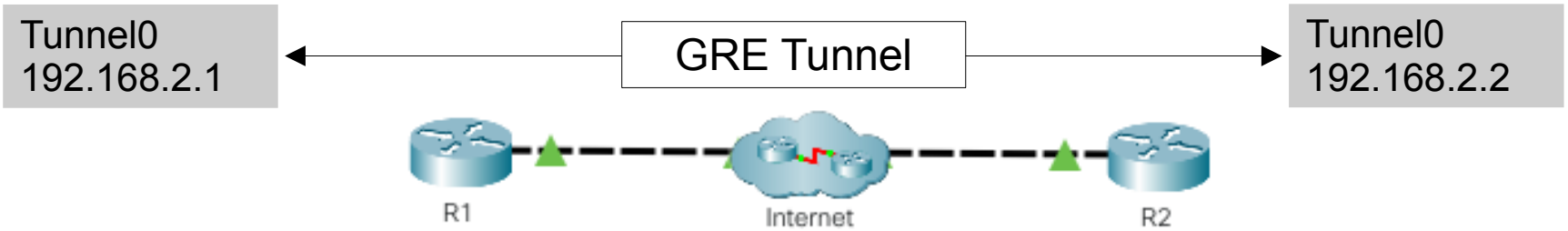
Transport-Protocol

Arten von VPNs – GRE over IPsec

- GRE unterstützt **keine Verschlüsselung** → IPsec muss her
  - **„Sandwich“:** IP(Multicast) in GRE in IPsec(Unicast)



Exkurs – GRE-Tunnel konfigurieren



Über den Tellerrand geschaut:

- Im CCNAv7-Curriculum sind keinerlei Konfigurationsbefehle enthalten, auch wenn diese fürs Verständnis hilfreich sind.
- Auf den folgenden Folien wird beispielhaft eine zusätzliche GRE-Konfiguration (ohne IPsec) dargestellt.
- Packettracer-Umgebung als Ausgangssituation im Moodle-Kurs

Exkurs – GRE-Tunnel konfigurieren

Tunnel0
192.168.2.1

GRE Tunnel

Tunnel0
192.168.2.2

G0/0/0:
209.165.201.2/30
Lo0:
192.168.10.1/24
Lo1:
192.168.11.1/24

G0/0/0:
209.165.201.6/30
Lo0:
192.168.20.1/24
Lo1:
192.168.21.1/24

```
R1(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.2
R1(config)#interf g0/0/0
R1(config-if)#ip address 209.165.201.2 255.255.255.252
R1(config-if)#no shut
R1(config-if)#interf lo0
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#interf lo1
R1(config-if)#ip address 192.168.11.1 255.255.255.0
```

R2 ebenfalls entsprechend konfigurieren

Exkurs – GRE-Tunnel konfigurieren

Tunnel0
192.168.2.1

GRE Tunnel

Tunnel0
192.168.2.2

OSPF konfigurieren:
- Prozess-ID: 1
- Router-ID: 1.1.1.1
- alle Lo-Netzwerke
- g0/0/0 → passive interf.

OSPF konfigurieren:
- Prozess-ID: 1
- Router-ID: 2.2.2.2
- alle Lo-Netzwerke
- g0/0/0 → passive interf.

```
R1(config)#router ospf 1
R1(config-router)#router-id 1.1.1.1
R1(config-router)#passive-interface g0/0/0
R1(config-router)#network 192.168.10.0 0.0.0.255 area 0
R1(config-router)#network 192.168.11.0 0.0.0.255 area 0
R1(config-router)#exit
R1(config)#
```

R2 ebenfalls entsprechend konfigurieren

Exkurs – GRE-Tunnel konfigurieren

Tunnel0
192.168.2.1

GRE Tunnel

Tunnel0
192.168.2.2

GRE konfigurieren:
- Tunnel0:
- IP: 192.168.2.1
- Ausgangs-Interface g0/0/0
- Ziel-Adresse: 209.165.201.6
- OSPF ergänzen (Tun0-Net)

GRE konfigurieren:
- Tunnel0:
- IP: 192.168.2.2
- Ausgangs-Interface g0/0/0
- Ziel-Adresse: 209.165.201.2
- OSPF ergänzen (Tun0-Net)

```
R1(config)#interface Tunnel0
R1(config-if)#tunnel mode gre ip
R1(config-if)#ip address 192.168.2.1 255.255.255.0
R1(config-if)#tunnel source g0/0/0
R1(config-if)#tunnel destination 209.165.201.6
R1(config-if)#exit
R1(config)# router ospf 1
R1(config-router)#network 192.168.2.0 0.0.0.255 area 0
```

R2 ebenfalls entsprechend konfigurieren

Exkurs – GRE-Tunnel konfigurieren

Tunnel0
192.168.2.1

GRE Tunnel

Tunnel0
192.168.2.2

GRE konfigurieren:
- Tunnel0:
- IP: 192.168.2.1
- Ausgangs-Interface g0/0/0
- Ziel-Adresse: 209.165.201.6
- OSPF ergänzen (Tun0-Net)

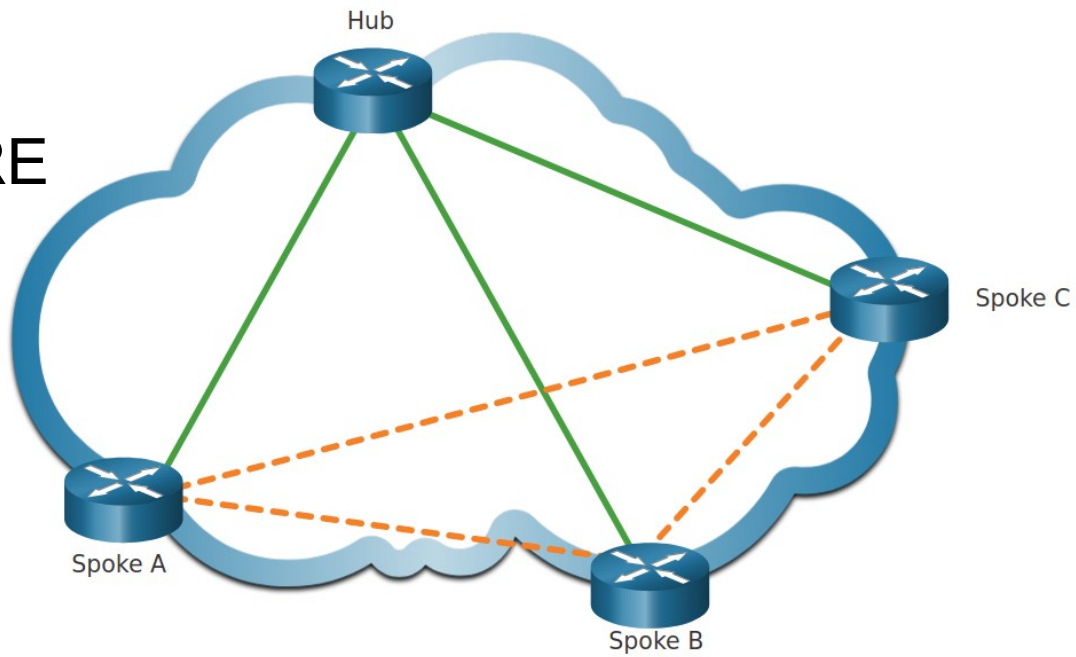
GRE konfigurieren:
- Tunnel0:
- IP: 192.168.2.2
- Ausgangs-Interface g0/0/0
- Ziel-Adresse: 209.165.201.2
- OSPF ergänzen (Tun0-Net)

Konfig prüfen auf R1:

```
R1#sh ip interf brief
R1#sh ip route
R1#sh ip protocols
R1#sh ip ospf neighbor
R1#ping 192.168.2.2
R1#traceroute 209.165.201.6 → Anzahl Hops?
R1#traceroute 192.168.2.2 → Anzahl Hops?
```

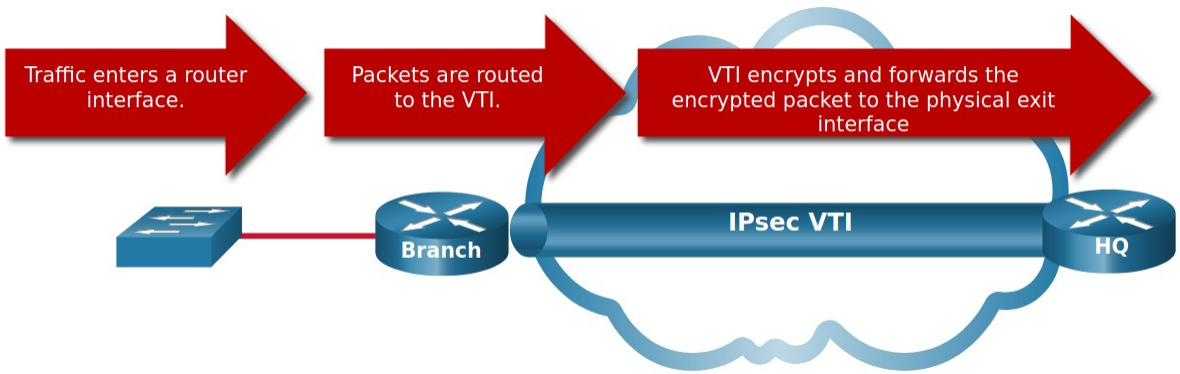
Arten von VPNs – Cisco DMVPN

- **Cisco Dynamic Multipoint VPN** (DMVPN) unterstützt Verbindungen zwischen Zweigstellen
- Baut auf IPsec auf bzw. nutzt IPsec
- Nicht nur „Hub (Nabe) to Spoke (Speiche)“, sondern auch „Spoke to Spoke“
- Verbindungsaufbau zwischen Branches dynamisch mit mGRE
  - mGRE = Multipoint GRE
  - Ein mGRE-Interface untertützt mehrere IPsec-Tunnel
  - Keine zusätzliche Konfiguration nötig



Arten von VPNs – IPsec Virtual Tunnel Interface

- IPsec alleine erzeugt kein neues Interface → Policy-based VPN
  - Was über den Tunnel geht, entscheidet die Policy
- IPsec VTI
  - Es wird ein neues Interface erzeugt (mit IP, Subnetz, …)
  - Pakete werden in dieses virtuelle Tunnelinterface geroutet
  - Die Pakete werden dann verschlüsselt über das konfigurierte physische Interface weitergeleitet
  - Vorteil: das VTI kann in ACLs / Firewallregeln genutzt werden



Arten von VPNs – MPLS auf Providerebene

- Frühere WAN-Lösungen wie Leased Lines, Frame Relay und ATM wurden durch Multiprotocol Label Switching (MPLS) ersetzt
- Provider gibt jedem Paket ein Label, sobald es ankommt
- Gelabelte Pakete gehen entlang von Label Switched Paths (LSP)
- Zwei Arten von MPLS-VPNs
  - Layer 3 MPLS VPN: Der Provider weiß von den Standorten und IP-Routen des Kunden; er routet dessen Pakete durch sein eigenes MPLS-Netzwerk
  - Layer 2 MPLS VPN: Der Provider bietet dem Kunden einen „Virtual Private LAN Service“ (VPLS); der Kunde sieht ein Ethernet-LAN, das technisch über MPLS realisiert wird. Es gibt kein Routing, sondern die Router sind alle im gleichen „LAN“ – ein Ethernet multiaccess LAN mit allen Remote-Standorten.

IPSec | „*Security Architecture for the Internet Protocol*“

- Offener IETF-Standard (RFC 2401-2412) | Schützt von Layer 4 bis Layer 7
- IPSec ist ein Framework bzw. eine Protokoll-Suite und ist damit flexibel und lässt sich mit unterschiedlichen Sicherheitstechnologien kombinieren:

Und jetzt im Detail ...

IPSec Protocol Encapsulation

Für die Encapsulation stehen drei Protokolle zur Verfügung:

Authentication Header (AH) bietet Authentifizierung und Integrität, jedoch keine Verschlüsselung der Daten und damit keine Vertraulichkeit → *IP Protocol 51*

Encapsulation Security Payload (ESP) stellt neben Authentifizierung und Integrität auch Vertraulichkeit bereit und verschlüsselt die Nutzdaten *(Klassiker)* → *IP Protocol 50*

Verwendung von beiden Protokollen hintereinander ist sehr selten.

IPSec - Transportmodus

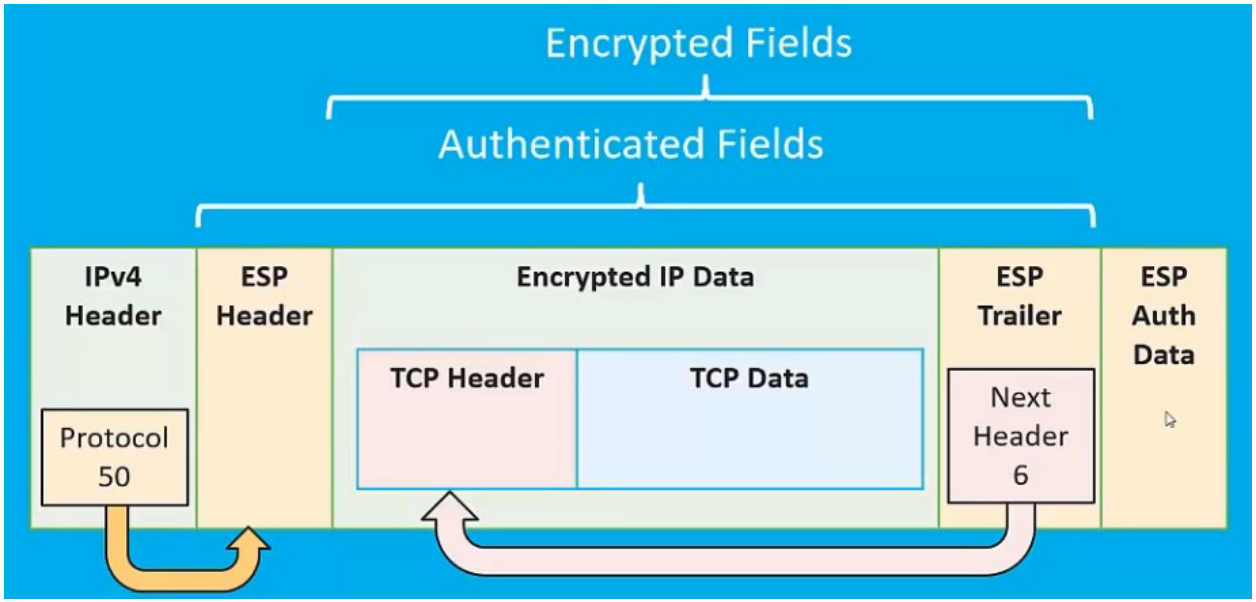
Für ESP oder AH stehen zwei Modi zur Verfügung:

Video

(1) Transportmodus

- Original IP-Header bleibt erhalten, nur Nutzdaten werden verschlüsselt
- Nutzung bei Host-to-Host-Verbindungen
- Nachteil: Nicht NAT/PAT-fähig, da kein Layer 4 / keine Portnummern
  Abhilfe bspw. NAT Traversal (NAT-T)
- Vorteil: Geringerer Overhead als bei Tunnelmodus

Beispiel Transport-modus mit ESP



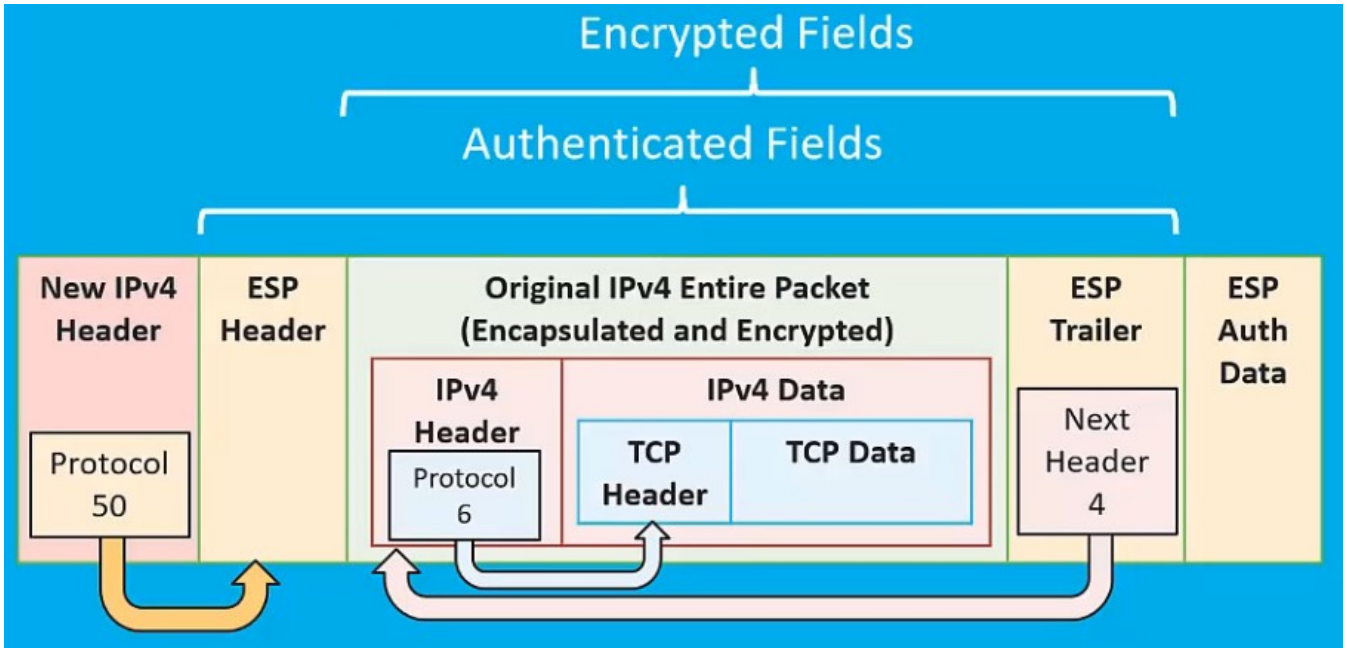
IPSec - Tunnelmodus

Video

(2) Tunnelmodus

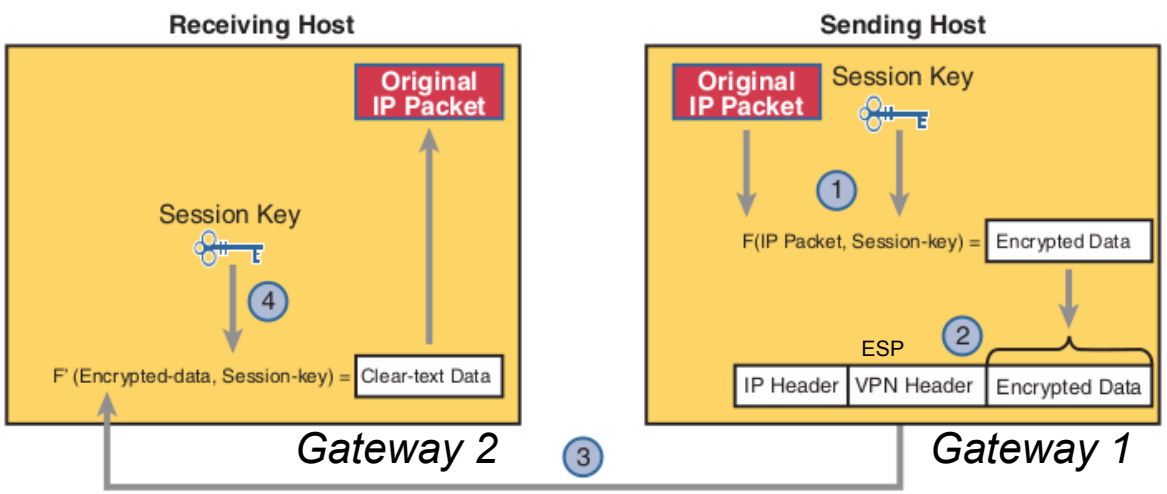
- Gesamtes IP-Paket ist als Nutzlast eingepackt
- Übliche Nutzung Site-to-Site
- Vorteil: Nur Router müssen IPSec implementieren, nicht Endgeräte
- Nachteil: Mehr Overhead als Transportmode

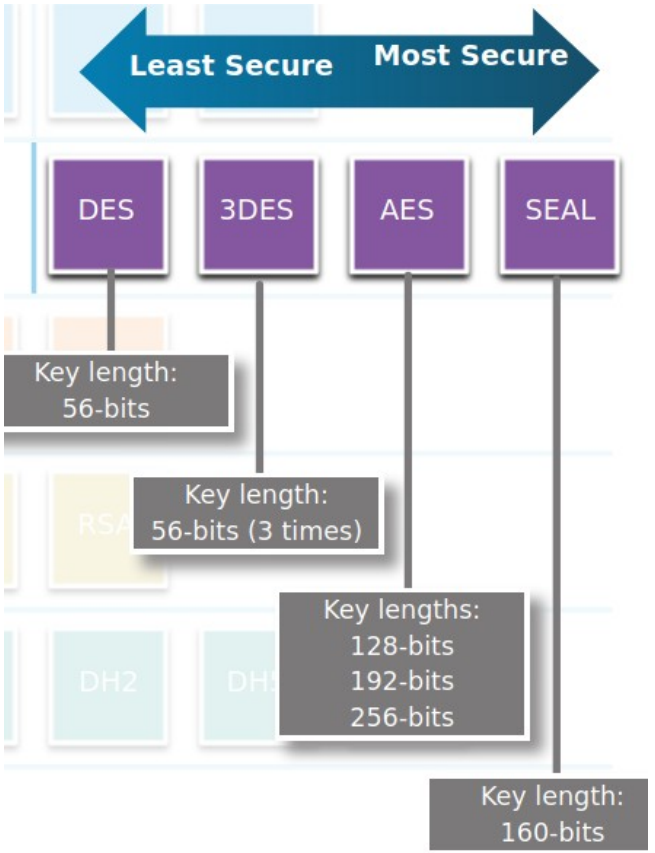
Beispiel Tunnel-modus mit ESP



Confidentiality / Vertraulichkeit

- Symmetrische Verschlüsselung (ESP)
- Mittels des IKE (Internet Key Exchange) wird u.a. der symmetrische Algorithmus ausgehandelt und weitere Verb.parameter
- SEAL ist eine Stromverschlüsselung *(Bit für Bit)*

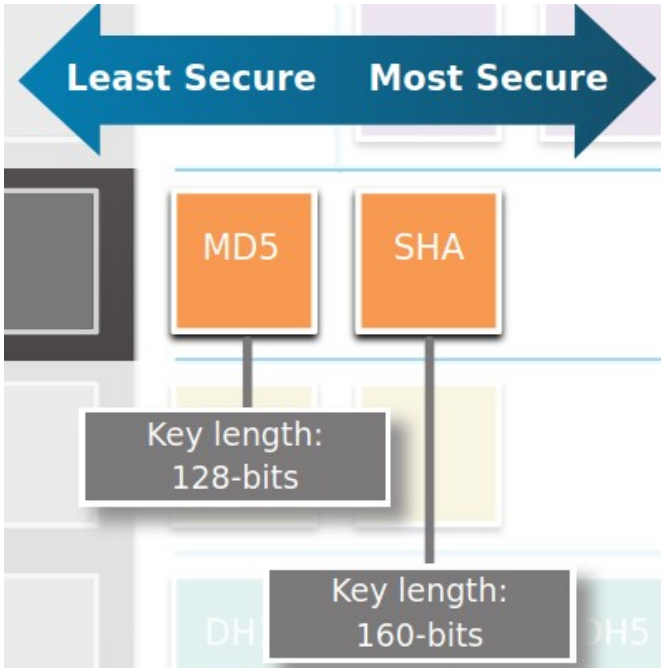




Bildquelle: Odom, W. (2020) CCNA 200-301 Official Cert Guide, Volume 2. Cisco Press

Integrität

- Mittels Hashing + symm. Schlüssel wird eine Art Prüfsumme erzeugt
- Hashed Message Authentication Code (HMAC) mit mind. SHA-256 wird empfohlen
- Kann bei ESP optional über ein zusätzliches Header-Feld hinzugefügt werden




```
|                               |  Pad Length   | Next Header   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Integrity Check Value-ICV   (variable)                |
~                                                               ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

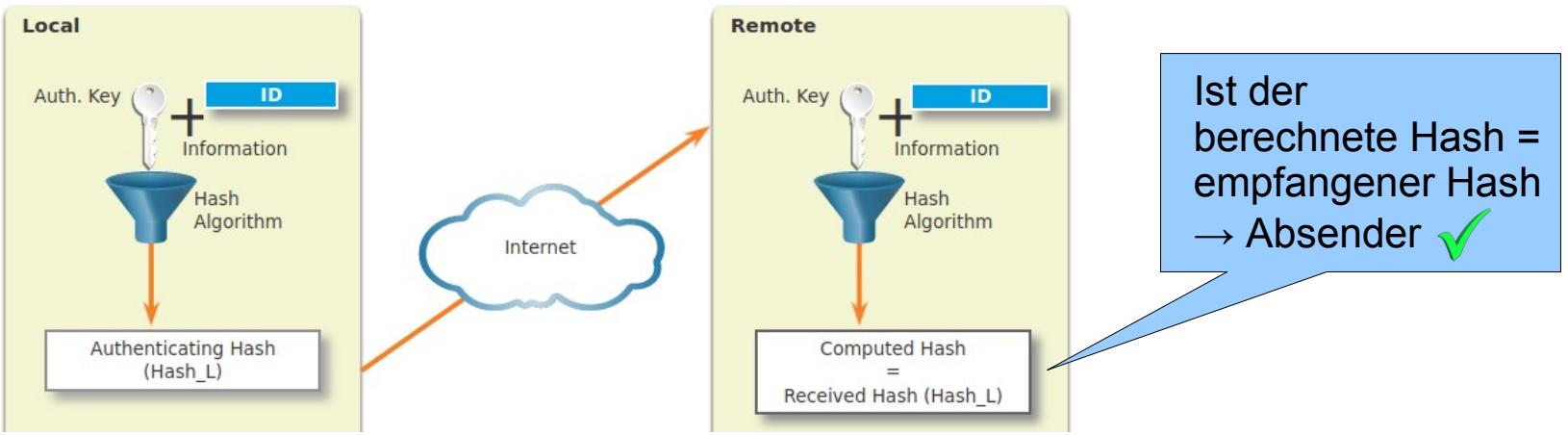
Figure 1. Top-Level Format of an ESP Packet

Quelle: https://tools.ietf.org/html/rfc4303

Authentifizierung - Pre-Shared-Secret Key (PSK)

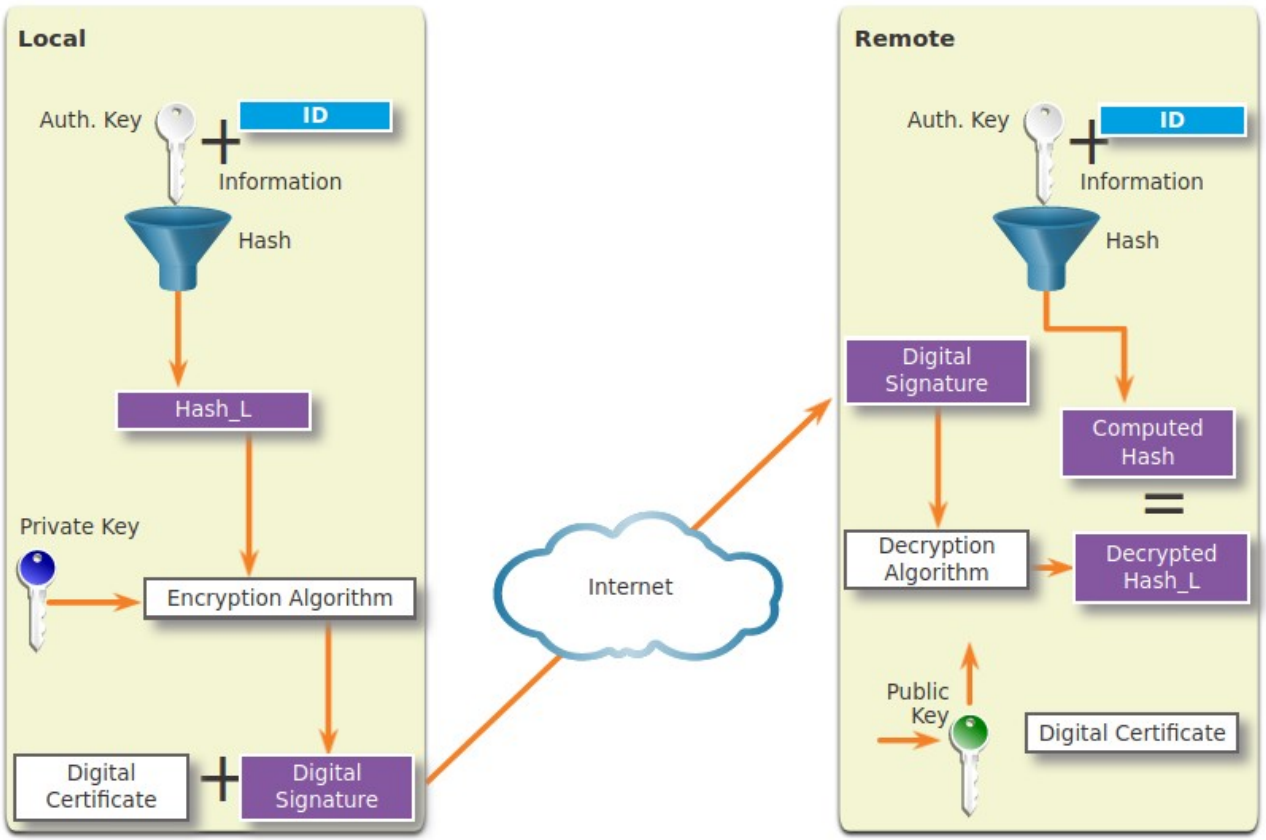
Authentifizierung der Kommunikationspartner über **Pre-Shared-Secret Key (PSK)** oder **RSA Authentifizierung**

PSK:
vorher vereinbarter Schlüssel (Zeichenfolge) wird mit weiteren Informationen kombiniert, gehasht und anschließend gesendet; für jeden IPSec-Peer muss ein PSK konfiguriert werden



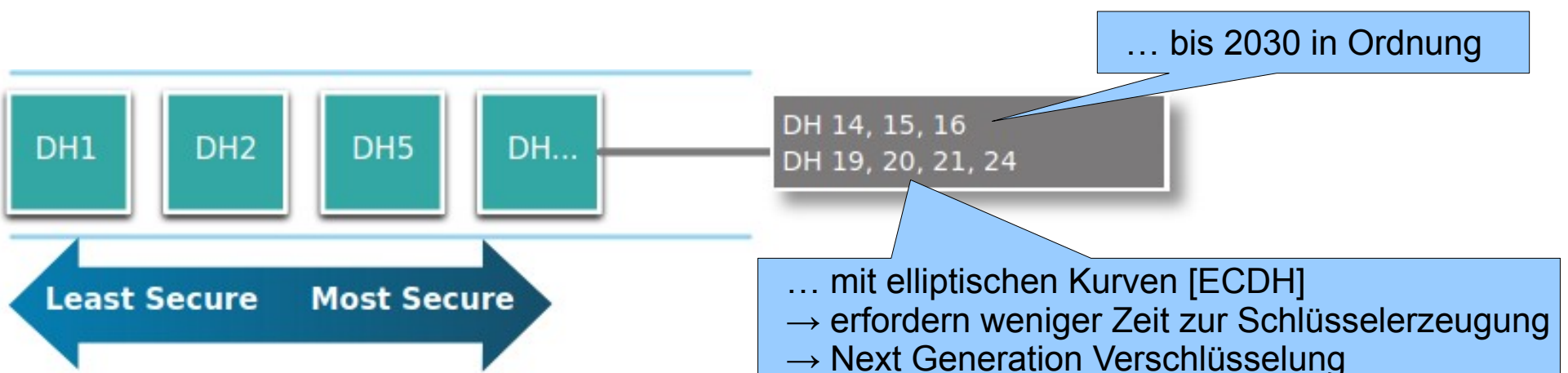
Authentifizierung - RSA

RSA: Zertifikat und Digitale Signatur werden übertragen. Digitale Signatur (verschlüsselter Hashwert) wird mittels Public Key entschlüsselt und überprüft.



Secure Key Exchange mit Diffie-Hellman

- Ermöglicht Kommunikationspartnern ...
  - über eine unverschlüsselte Verbindung
  - durch Austausch einiger Informationen
  - getrennt voneinander einen gemeinsamen und geheimen Schlüssel zu erzeugen
  - der aber nie über das Netz übertragen wurde
- Grunds. je höher die DH-Gruppennr. desto höher die Schlüsselstärke



Modulabschluss

- 8.1.5 Quiz – VPN Technology
- 8.2.8 Quiz – Types of VPN
- 8.3.9 Qiz - IPsec
- Module Quiz – VPN and IPsec Concepts – 8.4.2

Fragen ...