6 Cisco IPsec Grundkonfiguration

Cisco IPSec Einsatzscenarien

- Peer-to-Peer VPN
- VPN Server (Einwahl durch VPN Cients)
- DMVPN (Dynamic Multipoint VPN)

Grundsätzliche Konfigurationsschritte

1. Interessanten Verkehr definieren (Crypto ACL)
2. IKE Phase I Parameter konfigurieren (ISAKMP Policy, Identity, Key)
3. IKE Phase II Parameter konfigurieren (IPsec Transform Set, Crypto Map)
4. IPsec aktivieren (Referenz auf eine Crypto Map im Interface Subconfiguration Mode)

6.1 Interessanten Verkehr definieren (Crypto ACL)

Eine **Crypto ACL** ist eine extended ACL, die angibt welcher Datenverkehr via IPsec gesichert übertragen werden soll (permit) und welcher Datenverkehr nicht (deny). Diese ACL muß spiegelverkehrt beim Remote Peer konfiguriert sein (nicht bei VPN Server oder DMVPN).
Das Schlüsselwort any darf innerhalb der Crypto ACL nicht verwendet werden.

6.2 IKE Phase I Parameter (ISAKMP Policy, Identity, Key)

ISAKMP policy
bezeichnet IKE Phase I Konfigurationssätze, von denen beliebig viele konfiguriert werden können (alledings mit unterschiedlicher Priorität, die nur lokale Bedeutung hat). 2 Kommunikationspartner müssen mindestens eine übereinstimmende Policy haben.
In der Policy werden folgende Konfigurationen für IKE Phase I vorgenommen:

- Verschlüsselungsalgorithmus: z.B. DES, 3DES, ...
- Hashalgorithmus: MD5 oder SHA
- Authentifikation: Pre-Shared Key (lokales Passwort) oder RSA (zu erzeugen)
- Diffie-Hellman Gruppe: 1, 2 oder 5 (1 = 768 bit, 2 = 1024 bit, 5 = 1536 bit)
- Lebensdauer der ISAKMP SA in Sekunden (default = 86400 = 24h)

```
(config)# crypto isakmp policy 10
(config-isakmp)# encryption 3des
(config-isakmp)# hash md5
(config-isakmp)# authentication pre-share
(config-isakmp)# group 2
(config-isakmp)# lifetime 86400
```

Identity
Festlegung, ob die locale IP-Adresse in den Authenfikations-Prozess mit einbezogen wird (default-Einstellung. Wird in der running-config nicht angezeigt).
Andere Möglichkeit: Hostname.
Die One-Way Hash Funktion wird also über den Pre-Shared-Key und die IP-Adresse (oder den Hostname) durchgeführt.

```
(config)# crypto isakmp identity address
```

Key (pre-shared key)
Konfiguration eines Pre-Share Keys (local konfiguriertes Authentifikations-Passwort), dabei wird die IP-Adresse des Remote-Peer mit angegeben, wenn die Identity entsprechend konfiguriert wurde. Ansonsten wird der Hostname mit angegeben.
Der Key muß identisch auf dem Remote Peer gesetzt werden.

```
(config)# crypto isakmp key geheim address 192.168.1.1
```

6.3 IKE Phase II Parameter (IPsec Transform Set, Crypto Map)

Transform Set
Konfiguration der Parameter zur Aushandlund der IPsec SA durch ein IPsec Transform Set, das wird innerhalb einer Crypto Map referenziert wird.
Mit dem Transform Set wird festgelegt, welche IPsec-Protokolle (AH und/oder ESP) mit welche Verschlüsselungsmethoden für die IPsec SA verwendet werden sollen.

Möglichkeiten:

Authentication	*Encryption*
ah-md5-hmac ah-sha-hmac	esp-des esp-3des esp-null
esp-md5-hmac esp-sha-hmac	

Nach diesem "übergeordnet Kommando" gelangt man in den Crypto Transform Subconfiguration Mode wo man den IPsec Modus festlegen kann (Tunnel, Transport). Dabei ist der Tunnelmodus die default-Einstellung und wird nicht in der Running-Config angezeigt.

```
(config)# crypto ipsec transform-set mytset esp-md5-hmac esp-3des
(cfg-crypto-tran)# mode tunnel
```

Crypto Map
Eine Crypto Map fasst die verschiedenen IPsec Konfigurationen zu einem Profil mit weiteren Einstellung zusammen. Folgend das wichtigste:

- Crypto ACL (match address acl-nummer)
- IP Adresse des Remote Peers (nicht notwendig bei dynamscher Crypto Map)
- Die Parmeter für die IPsec SA (transform set)
- PFS (Perfect Forward Secrecy: während IKE Phase II wird ein neuer Diffie-Hellman Key Exchange durchgeführt)
- Die Lebensdauer der IPsec SA.

Es können mehrer Crypto Maps erzeugt werden (z.B. falls mehrere Peer-to-Peer IPsec Verbindungen benötigt werden, eine pro Verbindung), die durch ihre Sequenz-Nummer unterschieden werden.

```
(config)# crypto map mymap 10 ipsec-isakmp
(config-crypto-m)# match address 101
(config-crypto-m)# set peer 192.168.1.1
(config-crypto-m)# set transform-set mytset
(config-crypto-m)# set pfs group2
(config-crypto-m)# set security-association lifetime seconds 86400
```

6.4 IPsec aktivieren

An der Tunnel-End Schinttstelle durch Referenzierung der Crypto Map.

```
(config-if)# crypto map mymap
```

6.5 Troubleshooting IPsec

Wenn im laufenden Betrieb von IPsec Änderungen an der Konfiguration vorgenommen werden sollten zuerst die bestehenden SAs gelöscht werden.

clear crypto sa

Troubleshooting Commands

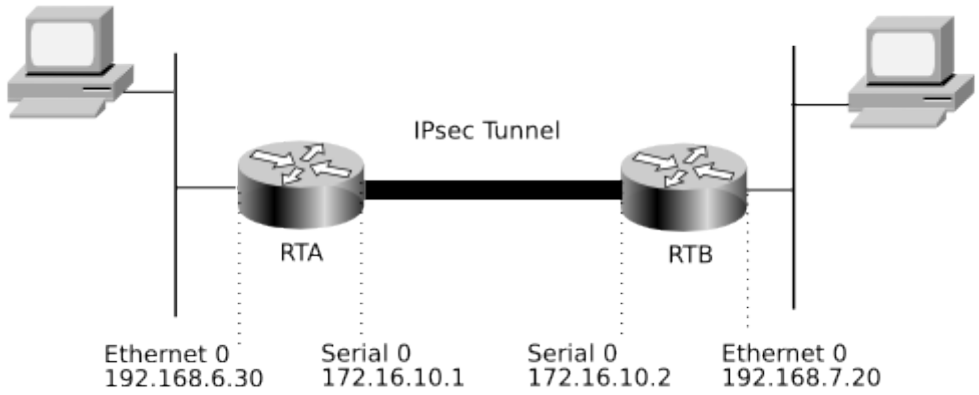
show running-config

show crypto isakmp policy
show crypto isakmp sa

show crypto ipsec transform-set
show crypto map
show crypto ipsec sa
show crypto ipsec security-association lifetime

debug crypto isakmp

7 LAB: Peer-to-Peer VPN




```
!
hostname RTA
!
crypto isakmp policy 8
 hash md5
 authentication pre-share
 group 5
 lifetime 43200
crypto isakmp key cisco address 172.16.10.2
!
crypto ipsec transform-set NEIGH ah-md5-hmac esp-3des
!
crypto map TEST 1 ipsec-isakmp
 set peer 172.16.10.2
 set security-association lifetime seconds 43200
 set transform-set NEIGH
 set pfs group5
 match address 100
!
interface Ethernet0
 ip address 192.168.6.30 255.255.255.0
!
interface Serial0
 ip address 172.16.10.1 255.255.255.0
 crypto map TEST
!
!
ip route 192.168.7.0 255.255.255.0 172.16.10.2
!
access-list 100 permit ip 192.168.6.0 0.0.0.255   \
          192.168.7.0 0.0.0.255
!
end
```

```
!
hostname RTB
!
crypto isakmp policy 12
 hash md5
 authentication pre-share
 group 5
 lifetime 43200
crypto isakmp key cisco address 172.16.10.1
!
crypto ipsec transform-set TRSET ah-md5-hmac esp-3des
!
crypto map CRMAP 1 ipsec-isakmp
 set peer 172.16.10.1
 set security-association lifetime seconds 43200
 set transform-set TRSET
 set pfs group5
 match address 100
!
interface Ethernet0
 ip address 192.168.7.20 255.255.255.0
!
interface Serial0
 ip address 172.16.10.2 255.255.255.0
 clockrate 4000000
 crypto map CRMAP
!
ip route 192.168.6.0 255.255.255.0 172.16.10.1
!
access-list 100 permit ip 192.168.7.0 0.0.0.255  \
          192.168.6.0 0.0.0.255
!
end
```