VPN auf Cisco-Router

Internet Key Exchange (IKE) Phase 1

Gegenseitige Authentifizierung der Peers: eine bidirektionale Security Association (SA)

1. ISAKMP aktivieren (Internet Security Association and Key Management Protocol)

```
ROUTER(config)# crypto isakmp enable
```

2. ISAKMP-Policy

```
ROUTER(config)# crypto isakmp policy 1            (1 = priority)
ROUTER(config-isakmp)# authentication pre-share
ROUTER(config-isakmp)# encryption aes 256         (des | 3des | aes 128 | aes 192 | aes 256)
ROUTER(config-isakmp)# group 5                    (Diffie-Hellman: group 1 | 2 | 5)
ROUTER(config-isakmp)# hash sha                   (sha | md5)
ROUTER(config-isakmp)# lifetime 3600              (eine Stunde)
```

3. Pre-Shared Key und Username (= IP-Adresse)

```
ROUTER(config)# crypto isakmp key XXXX address 1.2.3.4    (IP-Adresse des Gegenübers)
```

Das Passwort muss für alle Tunnnel gleich sein!

IKE Phase 2

IPSec-Tunnel aushandeln: zwei unidirektionale Security Associations (SAs)

1. Interesting Traffic mit ACL

```
ROUTER(config)# ip access-list extended VPNTRAFFIC
ROUTER(config-ext-nacl)# permit ip QUELLE1 ZIEL1
ROUTER(config-ext-nacl)# permit ip QUELLE2 ZIEL2
```

Für jeden Tunnel wird eine eigene ACL benötigt.

2. Transform-Set: confidentiality / integrity algorithms

```
ROUTER(config)# crypto ipsec transform-set MYSET esp-aes 256 esp-sha-hmac
```

3. Crypto-Map: Verknüpfung von Interesting Traffic, Peer, Transform-Set

```
ROUTER(config)# crypto map MYMAP 10 ipsec-isakmp (eine Map kann mehrere Sequenznummern haben)
ROUTER(config-crypto-map)# match address VPNTRAFFIC
ROUTER(config-crypto-map)# set peer 1.2.3.4      (IP-Adresse des Gegenübers)
ROUTER(config-crypto-map)# set transform-set MYSET

ROUTER(config)# crypto map MYMAP 20 ipsec-isakmp (eine Map kann mehrere Sequenznummern haben)
...
```

Mehrere Tunnel teilen sich eine Map mit unterschiedlichen Sequenznummern.

4. Crypto-Map an Interface hängen

```
ROUTER(config)# interface S2/0
ROUTER(config-if)# crypto map MYMAP
```

Diagnose

IKE Phase 1

```
ROUTER# debug crypto isakmp
ROUTER# show crypto isakmp policy
ROUTER# show crypto isakmp sa
```

IKE Phase 2

```
ROUTER# debug crypto ipsec
ROUTER# show crypto ipsec sa
ROUTER# show crypto ipsec transform-set
ROUTER# show crypto map
```