

## 2N02 Aufbau eines VPNs mit IPsec

Andreas Aurand  
Compaq Solution and Service Center

### Agenda

- IPsec Konfiguration unter IOS
  - Konfiguration der ISAKMP Protection Suite
  - Konfiguration der IPsec Protection Suite
- "Cisco VPN Client"-Verbindungen
  - ISAKMP Authentifizierung über Pre-Shared Keys
- "Windows 2000 L2TP"-Verbindung
  - ISAKMP Authentifizierung über RSA Signaturen
  - Per-User Konfiguration

## Konfiguration der ISAKMP Protection Suite

Festlegung der Sicherheitsservices, die innerhalb der ISAKMP SA eingesetzt werden müssen.  
Die Protection Suite wird unter IOS auch als **ISAKMP Policy** bezeichnet.

## Konfiguration der ISAKMP Protection Suite

### **crypto isakmp policy #**

**encryption** *des* | *3des*

⇒ Verschlüsselungsalgorithmus

**hash** *sha* | *md5*

⇒ Hashfunktion

**group** *1* | *2* | *5*

⇒ Diffie-Hellman-Gruppe

**authentication** *pre-share* | *rsa-sig* | *rsa-encr*

⇒ Authentifikation der Partner

- Bei mehreren Policy-Einträgen sendet der Initiator alle Vorschläge zum Partner.
- Der Responder wählt aus diesen Vorschlägen den ersten passenden Eintrag aus.

## Konfiguration der ISAKMP Protection Suite

### # show crypto isakmp policy

#### Protection suite of priority 10

encryption algorithm: Three key triple DES  
hash algorithm: Secure Hash Standard  
authentication method: Pre-Shared Key  
Diffie-Hellman group: #2 (1024 bit)  
lifetime: 86400 seconds, no volume limit

#### Protection suite of priority 20

encryption algorithm: Three key triple DES  
hash algorithm: Secure Hash Standard  
authentication method: Rivest-Shamir-Adleman Signature  
Diffie-Hellman group: #2 (1024 bit)  
lifetime: 40000 seconds, no volume limit

#### Default protection suite

encryption algorithm: DES - Data Encryption Standard (56 bit keys).  
hash algorithm: Secure Hash Standard  
authentication method: Rivest-Shamir-Adleman Signature  
Diffie-Hellman group: #1 (768 bit)  
lifetime: 86400 seconds, no volume limit

## Konfiguration der IPsec Protection Suite

Festlegung der Sicherheitservices, die innerhalb der IPsec SA eingesetzt werden müssen.

Festlegung, ob die Schlüssel manuell oder über ISAKMP/IKE erzeugt und verwaltet werden.

## Schlüsselverwaltung über ISAKMP/IKE

### ▪ Definition der „crypto map“

```
crypto map name sequence-number ipsec-isakmp
```

```
set peer ip-address1
```

⇒ IP-Adresse des Partners

```
set transform proposal1 [ proposal2 ... ]
```

⇒ Sicherheitsprotokoll

```
match address access-list
```

⇒ Festlegung der zu schützenden Pakete

### ▪ Zuweisung der „crypto map“ zu einem Interface

```
interface xxx
```

```
crypto map name [ redundancy standby-name ]
```

↙ HSRP und IPsec  
ab V12.2(8)T

- Die Auswertung der Sequenzen - d.h. der Vergleich der anstehenden Datenpakete gegen die Access-Listen - erfolgt in der Reihenfolge der Sequenznummern.

## „match address“-Eintrag

- Festlegung, welche Pakete zu schützen sind
  - **permit**: Datenpakete werden über IPsec geschützt
  - **deny**: Pakete ohne IPsec über den normalen Routing-Pfad
- Adressen immer **aus Sicht der ausgehenden Schnittstelle**
- **!!! Access-Listen auf beiden Partnern immer spiegelbildlich definieren !!!**
- **"any"-Adressen** bei „permit“-Einträgen **vermeiden**
  - Ansonsten werden auch Routing- und Multicastdaten verschlüsselt
  - **IPsec gilt nur für Unicast-Daten**
    - **GRE Tunnel** zur Verschlüsselung von **Multicast-Daten** verwenden
- Pro "permit"-Eintrag in der Access-Liste eine outbound und inbound SA

## Transform-Set definieren

```
crypto ipsec transform-set Name2 transform1 [ transform2 ... ]
  mode tunnel | transport
!
crypto ipsec transform-set Name1 transform1 [ transform2 ... ]
  mode tunnel | transport
!
crypto map ... ...
  set transform-set Name1 [ Name2 ... ]
```

Bei mehreren *Transforms* muss der Partner alle Sicherheitsmechanismen unterstützen.

Bei mehreren Einträgen wählt der Partner immer den ersten passenden Eintrag aus.

```
crypto ipsec transform-set ESP-DES esp-des esp-sha-hmac
  mode tunnel
!
crypto ipsec transform-set AH-MD5 ah-md5-hmac
  mode transport
!
crypto map ... ...
  set transform-set ESP-DES AH-MD5
```

## Unterstützte Sicherheitsmechanismen

### ▪ ESP

Sicherheitsmechanismus	IOS-Name
RFC 2410 - Null Encryption	esp-null
RFC 2405 - DES-CBC Algorithmus	esp-des
RFC 2451 - Triple DES Algorithmus	esp-3des
RFC 2403 - Authentifikation mit MD5 als HMAC	esp-md5-hmac
RFC 2404 - Authentifikation mit SHA1 als HMAC	esp-sha-hmac

- Advanced Encryption Standard (AES) in einem der nächsten IOS Releases

### ▪ AH

Sicherheitsmechanismus	IOS-Name
RFC 2403 - Authentifikation mit MD5 als HMAC	ah-md5-hmac
RFC 2404 - Authentifikation mit SHA1 als HMAC	ah-sha-hmac

## HSRP und IPsec (ab IOS V12.2(8)T)

- **HSRP Standby Adresse als IPsec Tunnel Endpunkt Adresse**
  - IPsec SAs gehen immer vom aktiven Router aus
  - Stateless Failover
    - Bei Ausfall des aktiven Routers muss Standby die IPsec SAs neu aufbauen
- **Reverse Route Injection (RRI)**
  - Erzeugt automatisch einen Routing Eintrag für die IPsec Proxies
    - Statische Crypto Map: Die Destination-Adressen der "permit"-ACLs
    - Dynamische Crypto Map: Das Subnets/Host, das der Partner schützt
  - Automatische Übernahme in die dynamischen Routing-Protokolle

```
crypto ipsec transform-set ESP-3DES esp-3des esp-sha-hmac
crypto dynamic-map DYNMAP-VPNclients 10
set transform-set ESP-3DES
reverse-route
interface Ethernet0
ip address 16.37.176.187 255.255.255.0
standby ip 16.37.176.30
standby name LAN
crypto map ETH_redundancy LAN
```

Aufbau eines VPNs mit IPsec 11

Andreas Aurand

## L2TP und VPN Client

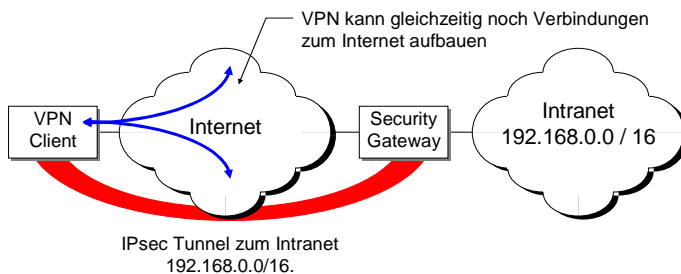
## L2TP vs. Cisco VPN Client

	L2TP	VPN Client
Implementation	L2TPv2: RFC 2661	Cisco Unity Implementation
ISAKMP-Authentifizierung	RSA-Signaturen	RSA-Signaturen Pre-Shared Keys
Benutzer-Authentifizierung	PPP Authentication (CHAP, PAP, EAP)	Cisco IPsec XAUTH
Übertragung der VPN Parameter	PPP Authorization	Cisco IPsec Mode Config Policy Push
IPsec Mode	Transport Mode	Tunnel Mode
Split Tunnel	immer aktiv (außer Filter gesetzt)	standardmäßig ausgeschaltet
Richtung	ein- und ausgehend	nur eingehend

- Komponenten, die **VPN Client-Funktionalität** unterstützen
  - VPN Client für Windows, Linux, Solaris, MAC
  - IOS V12.2(4)YA für Cisco 806, 826, 827, 828, 1700, uBR905, uBR925 (Easy VPN Client)
  - PIX V6.2
  - VPN 3002 Hardware Client und VPN 3000 Software Client

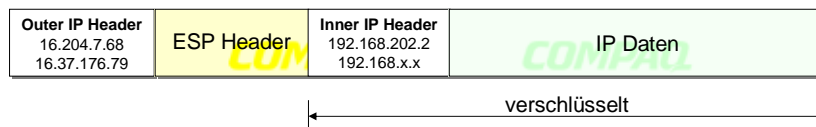
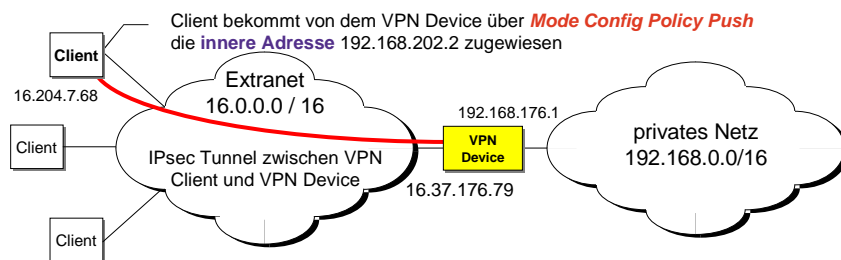
## Split Tunnel

- Client kann **zur gleichen Zeit Intranet- und Internet-**Verbindungen herstellen.
- Stellt Sicherheitsrisiko dar, da Angriffe aus dem Internet in das Intranet möglich sind.

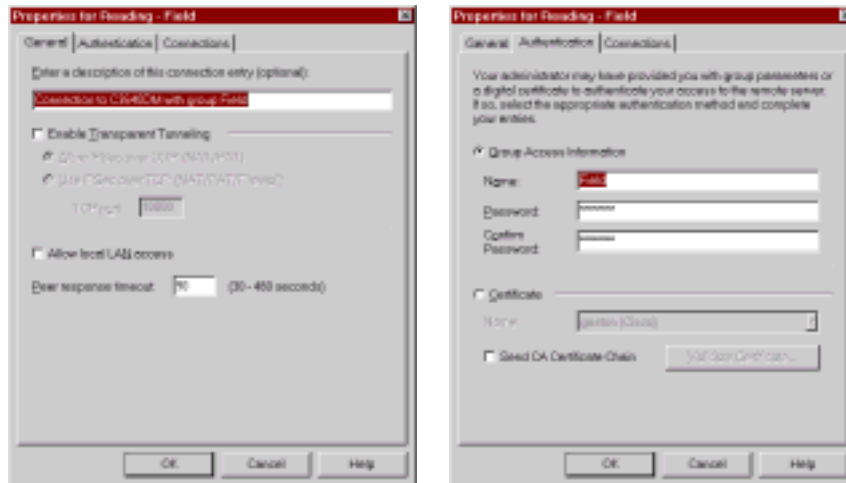


# VPN Client Konfiguration unter Windows

## Cisco VPN Client Verbindung



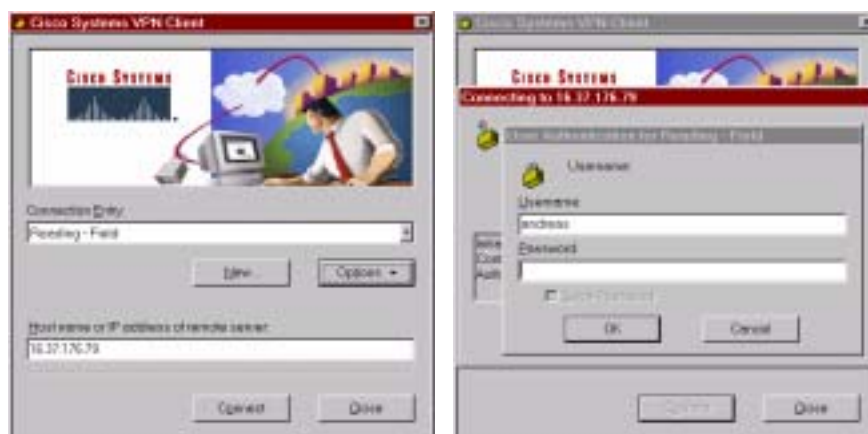
## VPN Client Konfiguration



Aufbau eines VPNs mit IPsec 17

Andreas Aurand

## VPN Client Verbindungsaufbau



Aufbau eines VPNs mit IPsec 18

Andreas Aurand

## IOS Konfiguration für VPN Client Verbindungen

## VPN Client Konfiguration unter IOS

```
hostname c3640dm
crypto isakmp policy 10
  encr 3des
  authentication pre-share
  group 2
crypto isakmp client configuration group default
  key 12345678
  dns 16.41.91.242
  wins 16.41.91.242
  pool VPNclients
  acl 100
crypto ipsec transform-set ESP-3DES esp-3des esp-sha-hmac
crypto dynamic-map DYNMAP-VPNclients 10
  set transform-set ESP-3DES
  reverse-route
crypto map ETH client authentication list VPNclient
crypto map ETH client configuration address respond
crypto map ETH isakmp authorization list IKE
crypto map ETH 1000 ipsec-isakmp dynamic DYNMAP-VPNclients
```

Verwendet, falls die vom Client angegebene Gruppe nicht passt

Pre-Shared Key für die IPsec Authentifizierung

Split-Tunnel Konfiguration

Authentifizierung des Benutzers über Cisco XAUTH Erweiterung

Abfrage von Parametern (z.B. Pre-Shared Key) für die ISAKMP SA über AAA

## VPN Client Konfiguration unter IOS

```

aaa new-model
aaa group server radius FRS
  server 16.204.7.96 auth-port 1812 acct-port 1813
aaa authentication login VPNclient local group FRS
aaa authorization network IKE group FRS local
username andreas password c
username hugo password c
interface FastEthernet0/0
  ip address 16.37.176.79 255.255.255.0
  crypto map ETH
interface FastEthernet0/1
  ip address 192.168.176.1 255.255.255.0
ip local pool VPNclients 192.168.200.1 192.168.200.254
ip local pool VPNclients-Engineering 192.168.201.1 192.168.201.254
ip local pool VPNclients-Field 192.168.202.1 192.168.202.254
access-list 100 permit ip 192.168.0.0 0.0.255.255 any log-input
ip radius source-interface FastEthernet0/0
radius-server host 16.204.7.96 auth-port 1812 acct-port 1813 key ABC
  
```

Username/Passwort für lokale Authentifizierung des Benutzers

## Group-Einträge auf dem Radius-Server

- Password für den Zugriff auf den Radius-Server ist immer "cisco"

```

Field Auth-Type := Local, Password := "cisco", Service-Type == Outbound-User
  Service-Type = Outbound-User,
  Cisco-AVPair = "ipsec:key-exchange=ike",
  Cisco-AVPair = "ipsec:tunnel-password=12345678",
  Cisco-AVPair = "ipsec:inacl=100",
  Cisco-AVPair = "ipsec:addr-pool=VPNclients-Field",
  Cisco-AVPair = "ipsec:dns-servers=16.41.91.242 16.37.147.242",
  Cisco-AVPair = "ipsec:wins-servers=16.41.91.242 16.37.147.242"

Engineering Auth-Type := Local, Password := "cisco", Service-Type == Outbound-User
  Service-Type = Outbound-User,
  Cisco-AVPair = "ipsec:key-exchange=ike",
  Cisco-AVPair = "ipsec:tunnel-password=87654321",
  Cisco-AVPair = "ipsec:inacl=100",
  Cisco-AVPair = "ipsec:addr-pool=VPNclients-Engineering",
  Cisco-AVPair = "ipsec:dns-servers=16.41.91.242 16.37.147.242",
  Cisco-AVPair = "ipsec:wins-servers=16.41.91.242 16.37.147.242"
  
```

Pre-Shared Key

Pre-Shared Key

## IPsec-Informationen vom Router

```
c3640dm# show ip route
      16.0.0.0/24 is subnetted, 1 subnets
C       16.37.176.0 is directly connected, FastEthernet0/0
C       192.168.176.0 is directly connected, FastEthernet0/1
      192.168.202.0/32 is subnetted, 1 subnets
S       192.168.202.2 [1/0] via 0.0.0.0, FastEthernet0/0
S*      0.0.0.0/0 [1/0] via 16.37.176.64
```

Über **reverse-route** Eintrag hinzugefügt

```
c3640dm# show crypto isakmp peer
Peer: 16.204.7.68
Configuration:
  Refcount: 3, Configured Address: 192.168.202.2, State: allocated, Attributes: REQUEST
  XAUTH: user unknown   FLAGS: (Need xauth on next phase 1) (xauth done)
  last_locker: 0x61611D20, last_last_locker: 0x61611D20
  last_unlocker: 0x615E4A98, last_last_unlocker: 0x615E4A98

Group Policy :
  group name      = Field
  pre-shared key  = 12345678
  address pool    = VPNclients-Field
  default domain =
  acl             = 100
  idletime        = 0
  maxtime         = 0
  dns primary     = 16.41.91.242
  dns secondary  = 16.37.147.242
  wins primary    = 16.41.91.242
  wins secondary  = 16.37.147.242
```

## IPsec-Informationen vom Router

```
c3640dm# show crypto map
Crypto Map "ETH" 1000 ipsec-isakmp
  Dynamic map template tag: DYNMAP-VPNclients

Crypto Map "ETH" 1010 ipsec-isakmp
  Peer = 16.204.7.68
  Extended IP access list
    access-list permit ip host 16.37.176.79 host 192.168.202.2
    dynamic (created from dynamic map DYNMAP-VPNclients/10)
  Current peer: 16.204.7.68
  Security association lifetime: 4608000 kilobytes/3600 seconds
  PFS (Y/N): N
  Transform sets={ ESP-3DES, }
  Reverse Route Injection Enabled

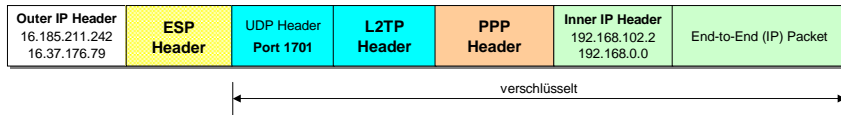
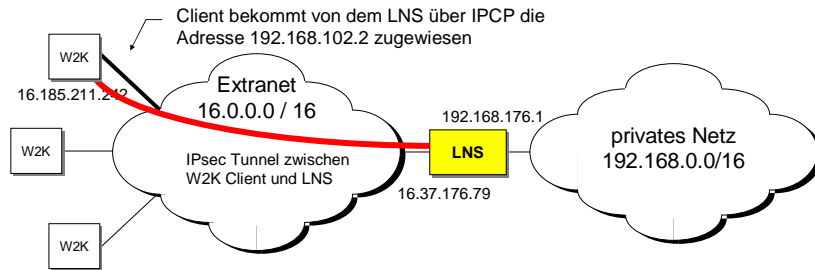
Crypto Map "ETH" 1020 ipsec-isakmp
  Peer = 16.204.7.68
  Extended IP access list
    access-list permit ip 192.168.0.0 0.0.255.255 host 192.168.202.2
    dynamic (created from dynamic map DYNMAP-VPNclients/10)
  Current peer: 16.204.7.68
  Security association lifetime: 4608000 kilobytes/3600 seconds
  PFS (Y/N): N
  Transform sets={ ESP-3DES, }
  Reverse Route Injection Enabled
  Interfaces using crypto map ETH:
    FastEthernet0/0
```

Direkter Datentransfer zwischen VPN Client und Router

Zugriff vom VPN Client auf das interne Netzwerk



## L2TP zwischen W2K Client und Router



## L2TP Konfiguration unter Windows 2000

# L2TP Konfiguration

**Netzwerkverbindungs-Assistent**

**Netzwerkverbindungstyp**  
 Sie können den Typ der zu erstellenden Netzwerkverbindung wählen. Die Wahl sollte der Netzwerkkonfiguration und Ihren Bedürfnissen entsprechen.

- In ein privates Netzwerk einwählen**  
 Stellt Verbindung über eine Telefonleitung (Modem oder ISDN) her.
- In das Internet einwählen**  
 Stellt Internetanschluss über eine Telefonleitung (Modem oder ISDN) her.
- Verbindung mit einem privaten Netzwerk über das Internet herstellen**  
 Stellt VPN-Verbindung oder Tunnel durch das Internet her.
- Eingehende Verbindungen akzeptieren**  
 Andere Computer können über eine Telefonleitung, das Internet oder ein direktes Kabel eine Verbindung zu diesem Computer herstellen.
- Direkt mit anderem Computer verbinden**  
 Stellt Verbindung über seriellen, parallelen oder Infrarotanschluss her.

**Netzwerkverbindungs-Assistent**

**Öffentliches Netzwerk**  
 Windows kann gewährleisten, dass die Verbindung mit dem öffentlichen Netzwerk zuerst hergestellt wird.

Windows kann eine Anfangsverbindung mit dem Internet oder einem anderen öffentlichen Netzwerk automatisch wählen, bevor die virtuelle Verbindung hergestellt wird.

- Keine Anfangsverbindung automatisch wählen
- Automatisch diese Anfangsverbindung wählen:

# L2TP Konfiguration

**Netzwerkverbindungs-Assistent**

**Zieladresse**  
 Geben Sie den Namen oder die Adresse des Zielnetzwerks ein.

Geben Sie den Hostnamen oder die IP-Adresse des Computers oder Netzwerks ein, zu dem eine Verbindung hergestellt werden soll.

Hostname oder IP-Adresse (z.B. microsoft.com oder 123.45.6.78):

**Netzwerkverbindungs-Assistent**

**Fertigstellen des Assistenten**

Geben Sie einen Namen für die Verbindung an:

Klicken Sie auf "Fertig stellen", um diese Verbindung zu erstellen und im Ordner "Netzwerk- und DFU-Verbindungen" zu speichern.

Markieren Sie im Ordner "Netzwerk- und DFU-Verbindungen" eine Verbindung. Klicken Sie auf "Datei" und dann auf "Eigenschaften", um die Verbindung zu bearbeiten.

Verknüpfung auf dem Desktop hinzufügen

## Authentifizierung über Signaturen

## Zertifikat unter Windows 2000 anfordern

Microsoft Certificate Services - Microsoft Internet Explorer provided by Compaq Computer Corporation

Address <http://ipsecpp.fns.cpqcorp.net/certreq/certreq.asp>

**Certificate Template:**  
[IPSEC (Offline request)]

**Identifying Information For Offline Template:**

Name: [schloepfel@lab.de]  
E-Mail: [ ]  
Company: [Andreas Aurand]  
Department: [FFIS-LAB]  
City: [ ]  
State: [ ]  
Country/Region: [DE]

**Key Options:**

CSP: [Microsoft Base Cryptographic Provider v1.0]

Key Usage:  Exchange  Signature  Both  
Key Size: [512] Min: 204 Max: 1024 (current key size: 512, 3025)

Create new key set  
 Set the container name  
 Use existing key set  
 Enable strong private key protection  
 Mark keys as exportable  
 Export keys to file  
File name: [d:\temp\key]  
 Use local machine store  
You must be an administrator to generate a key in the local machine store.

## Lokales RSA-Schlüsselpaar erzeugen

- Für die Kommunikation mit der CA verwenden die Router das „**Simple Certificate Enrollment Protocol - SCEP**“
  - Certificate Authorities von Verisign, Entrust, Microsoft unterstützen SCEP
    - MS Certificate Servers benötigt CEP-Erweiterung aus dem Resource Kit
  - Zertifikate gelten nur für einen bestimmten Zeitraum
    - **Korrekte Zeit** auf den Routern ist wichtig (**NTP verwenden**)
- **Erzeugen der RSA-Schlüssel auf dem lokalen Router**

```
c3640dm(config)# hostname c3640dm
c3640dm(config)# ip domain-name reo-lab.de
c3640dm(config)# crypto key generate rsa general-key
The name for the keys will be: c3640dm.reo-lab.uk
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys ...

00:23:23: %SSH-5-ENABLED: SSH 1.5 has been enabled
```

## Anforderung des CA-Zertifikats

- **Definition der Trustpoint CA**

```
ip host mpdepp.frs-lab.de 16.204.7.75
crypto ca trustpoint MSCertServFRS
  enrollment mode ra
  enrollment url http://mpdepp.frs-lab.de:80/certsrv/mscep/mscep.dll
  usage ike
  serial-number
  ip-address none
  password xxx
  crl best-effort
```

↙ Falls definiert, gilt das Zertifikat nur für diese Adresse
- **Änderungen in IOS V12.2(8)T**
  - Mehrere Certificate Authorities unterstützt
  - Unterschiedliche RSA-Schlüsselpaare für die einzelnen CAs

## Anforderung des CA-Zertifikats

### ▪ Anforderung des Zertifikats der Certificate Authority

```
c3640dm(config)# crypto ca authenticate MSCertServFRS
```

```

Certificate has the following attributes:
Fingerprint: 1FF8BA6C 3C49A981 A5F772C7 64F3C690
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.

```

### ▪ Überprüfung des Zertifikats



## Registrierung des lokalen RSA-Schlüssels

```
c3640dm(config)# crypto ca enroll MSCertServFRS
```

```

% Start certificate enrollment ..
% The subject name in the certificate will be: c3640dm.reo-lab.uk
% The serial number in the certificate will be: 17651273
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.
Fingerprint: A0BB0FEF 2ECDBC26 ED87E49C F234E944
00:27:54: %CRYPTO-6-CERTRET: Certificate received from Certificate Authority

```

```
c3640dm# show crypto key mypubkey rsa
```

```
c3640dm# show crypto key pubkey-chain rsa
```

```
c3640dm# show crypto ca certificates
```

```
c3640dm# show crypto ca trustpoints
```

```
c3640dm# show crypto ca crls
```

## ISAKMP Authentifizierung über Signaturen

```

hostname c3640dm
ip domain-name reo-lab.uk
ip host mpdepp.frs-lab.de 16.204.7.75
crypto ca trustpoint MSCertServFRS
  enrollment mode ra
  enrollment url http://mpdepp.frs-lab.de:80/certsrv/mscep/mscep.dll
  usage ike
  serial-number
  ip-address none
  password xxx
  crl best-effort
crypto ca certificate chain MSCertServFRS
certificate ca 1D34B7A3E70E718F431768F1248E759E
  3082030C 308202B6 A0030201 0202101D 34B7A3E7 0E718F43 1768F124 8E759E30
  quit
certificate ra-encrypt 6124F79B000000000003
  86F70D01 01050500 304D310B 30090603 55040613 02444531 17301506 0355040A
  quit
certificate ra-sign 6124F2C1000000000002
  86F70D01 01050500 304D310B 30090603 55040613 02444531 17301506 0355040A
  quit
certificate 1A9A74520000000000056
  86F70D01 01050500 304D310B 30090603 55040613 02444531 17301506 0355040A
  quit
ntp server 16.37.176.9
ntp server 16.37.176.13

```

Zertifikate werden automatisch durch die "crypto ca authenticate" und "crypto ca enroll" Kommandos eingetragen (im DER-Format)

Zertifikate haben nur eine bestimmte Gültigkeit. Zeit auf dem Router muss korrekt sein

Aufbau eines VPNs mit IPsec 37

Andreas Aurand

## Per-User Konfiguration des Virtual-Access Interface

## L2TP und IPsec Konfiguration (ab V12.2(4)T)

```

vpdn-group W2K-Clients
  accept-dialin
  protocol l2tp
  virtual-template 1
  l2tp security crypto-profile W2K-Clients
  no l2tp tunnel authentication
  source-ip 16.37.176.79
!
interface Virtual-Template1
  no ip address
  ip access-group BlockAll in
  ppp authentication chap W2K-Clients
  ppp authorization W2K-Clients
  ppp accounting W2K-Clients
!
crypto isakmp policy 20
  encr 3des
  group 2
!
crypto ipsec transform-set ESP-Transport esp-3des esp-sha-hmac
  mode transport
!
crypto map ETH 100 ipsec-isakmp profile W2K-Clients
  set transform-set ESP-Transport
!
interface FastEthernet0/0
  ip address 16.37.176.79 255.255.255.0
  crypto map ETH
!
interface FastEthernet0/1
  ip address 192.168.176.1 255.255.255.0
  ip access-list extended BlockAll
  deny ip any any

```

Ab IOS V12.2(4)T: *Securing L2TP using IPsec (RFC 3193)*

Authentifizierung des Benutzers über PPP CHAP

Zuweisung von Interface-spezifischen Parametern

Aufbau eines VPNs mit IPsec 39

Andreas Aurand

## Per-User Konfiguration

```

aaa new-model
aaa group server radius FRS
  server 16.204.7.96 auth-port 1812 acct-port 1813
aaa authorization network default group FRS
aaa authorization network W2K-Clients group FRS
aaa authentication ppp W2K-Clients group FRS
aaa accounting network W2K-Clients wait-start group FRS
aaa configuration config-username c3640-w2kpool password df9434dvj
!
ip radius source-interface FastEthernet0/0
radius-server host 16.204.7.96 auth-port 1812 acct-port 1813 key ABC
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 44 include-in-access-req
!
time-range allow-http
  periodic weekdays 18:00 to 23:59
  periodic weekdays 0:00 to 7:59
!
time-range allow-sap
  periodic weekdays 8:00 to 18:00
!
interface Loopback0
  ip address 192.168.100.1 255.255.255.0
!
interface Loopback1
  ip address 192.168.101.1 255.255.255.0
!
interface Loopback2
  ip address 192.168.102.1 255.255.255.0

```

Für Download der lokalen Adress-Pools vom Radius-Server notwendig

Username/Password für das Download der lokalen Adress-Pools

IP Unnumbered Adressen für das Virtual-Access Interface

Aufbau eines VPNs mit IPsec 40

Andreas Aurand

## User-Einträge auf dem Radius-Server

```

andreas Auth-Type := Local, Password := "c", Service-Type==Framed-User, Framed-Protocol==PPP
  CHAP-Password = c,
  Service-Type = Framed-User,
  Framed-Protocol = PPP,
  Framed-IP-Address = 192.168.99.1,
  Framed-Routing = None,
  Cisco-AVPair = "lcp:interface-config#1 = ip address 192.168.99.2 255.255.255.252",
  Cisco-AVPair = "lcp:interface-config#2 = ppp timeout idle 120",
  Cisco-AVPair = "lcp:interface-config#3 = ppp ipcp dns 16.41.91.242",
  Cisco-AVPair = "lcp:interface-config#4 = ppp ipcp wins 16.41.91.242",
  Cisco-AVPair = "ip:route#1=50.104.7.0 255.255.255.0 192.168.99.1",
  Cisco-AVPair = "ip:inacl#1=permit ip host 192.168.99.1 host 192.168.176.1",
  Cisco-AVPair = "ip:inacl#2=permit ip host 192.168.99.1 host 192.168.176.2",
  Cisco-AVPair = "ip:inacl#3=permit ip 20.1.1.0 0.0.0.255 192.168.176.0 0.0.0.255"

Marketing Auth-Type := Local, Password == c, Service-Type==Framed-User, Framed-Protocol==PPP
  CHAP-Password = c,
  Service-Type = Framed-User,
  Framed-Protocol = PPP,
  Cisco-AVPair = "lcp:interface-config#1 = ip unnumbered loopback0",
  Cisco-AVPair = "lcp:interface-config#2 = ppp ipcp dns 16.41.91.242",
  Cisco-AVPair = "lcp:interface-config#3 = ppp ipcp wins 16.41.91.242",
  Cisco-AVPair = "ip:addr-pool=W2K-Marketing",
  C. = "ip:inacl#1=permit tcp 192.168.100.0 0.0.0.255 host 192.168.56.7 range 3000 3030 time-range allow-sap",
  C. = "ip:inacl#2=permit tcp 192.168.100.0 0.0.0.255 any eq 8086 time-range allow-http"

```

Aufbau eines VPNs mit IPsec 41

Andreas Aurand

## User-Einträge auf dem Radius-Server

```

Engineering Auth-Type := Local, Password := "c", Service-Type==Framed-User, Framed-Protocol==PPP
  Chap-Password = c,
  Service-Type = Framed-User,
  Framed-Protocol = PPP,
  Cisco-AVPair = "lcp:interface-config#1 = description -- L2TP Client Engineering --",
  Cisco-AVPair = "lcp:interface-config#2 = ip unnumbered loopback1",
  Cisco-AVPair = "ip:addr-pool=W2K-Engineering",
  Cisco-AVPair = "ip:inacl#1=permit ip 192.168.101.0 0.0.0.255 any",
  Cisco-AVPair = "ip:inacl#2=deny ip any any"

Field Auth-Type := Local, Password := "c", Service-Type == Framed-User, Framed-Protocol == PPP
  Chap-Password = c,
  Service-Type = Framed-User,
  Framed-Protocol = PPP,
  Cisco-AVPair = "lcp:interface-config#1 = description -- L2TP Client Field --",
  Cisco-AVPair = "lcp:interface-config#2 = ip unnumbered loopback2",
  Cisco-AVPair = "ip:addr-pool=W2K-Field",
  Cisco-AVPair = "ip:inacl#1=permit tcp 192.168.102.0 0.0.0.255 host 192.168.56.7 eq telnet",
  Cisco-AVPair = "ip:inacl#2=deny ip any any"

c3640-w2kpool Auth-Type := Local, Password := "df9434dvj", NAS-IP-Address == 16.37.176.79
  Service-Type = Outbound-User,
  Cisco-AVPair = "ip:pool-timeout=3600",
  Cisco-AVPair = "ip:pool-def#1=W2K-Marketing 192.168.100.2 192.168.100.254",
  Cisco-AVPair = "ip:pool-def#2=W2K-Engineering 192.168.101.2 192.168.101.254",
  Cisco-AVPair = "ip:pool-def#3=W2K-Field 192.168.102.2 192.168.102.254"

```

Aufbau eines VPNs mit IPsec 42

Andreas Aurand

## IP- und L2TP-Informationen vom Router

### c3640dm# show ip local pool

Pool	Begin	End	Free	In use	
W2K-Marketing	192.168.100.2	192.168.100.254	253	0	(dynamic, 3598m. left)
W2K-Engineering	192.168.101.2	192.168.101.254	253	0	(dynamic, 3598m. left)
W2K-Field	192.168.102.2	192.168.102.254	252	1	(dynamic, 3598m. left)

Pools werden dynamisch vom  
Radius-Server geladen

### c3640dm# show vpdn

```
L2TP Tunnel and Session Information Total tunnels 1 sessions 1
LocID RemID Remote Name State Remote Address Port Sessions VPDN Group
51730 6 schlaeppel.em est 16.185.211.242 1701 1 W2K-Clients
LocID RemID TunID Intf Username State Last Chg Fastswitch
2 1 51730 Vi1 Field est 00:01:49 enabled
```

### c3640dm# show ip access-list

```
Extended IP access list BlockAll
deny ip any any
Extended IP access list Virtual-Access1#21 (per-user)
permit tcp 192.168.102.0 0.0.0.255 host 192.168.56.7 eq telnet (32 matches)
deny ip any any (69 matches)
```

Automatisch vom Router  
angelegt

## IPsec-Informationen vom Router

### c3640dm# show crypto map

```
Crypto Map "ETH" 100 ipsec-isakmp
No matching address list set.
Current peer: 0.0.0.0
Security association lifetime: 4608000 kilobytes/3600 seconds
PFS (Y/N): N
Transform sets={ESP-Transport,}
```

```
Crypto Map "ETH" 110 ipsec-isakmp
Peer = 16.185.211.242
Extended IP access list
access-list permit udp host 16.37.176.79 host 16.185.211.242 port = 1701
Current peer: 16.185.211.242
Security association lifetime: 4608000 kilobytes/3600 seconds
PFS (Y/N): N
Transform sets={ ESP-Transport, }
Interfaces using crypto map ETH:
FastEthernet0/0
```

"Crypto Map"-Eintrag für den Client legt  
IOS automatisch an

### c3640dm# show crypto engine connection active

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
1	FastEthernet0/0	16.37.176.79	set	HMAC_SHA+3DES_56_C	0	0
2000	FastEthernet0/0	16.37.176.79	set	HMAC_SHA+3DES_56_C	0	130
2001	FastEthernet0/0	16.37.176.79	set	HMAC_SHA+3DES_56_C	96	0

## Accounting Records auf dem Radius-Server

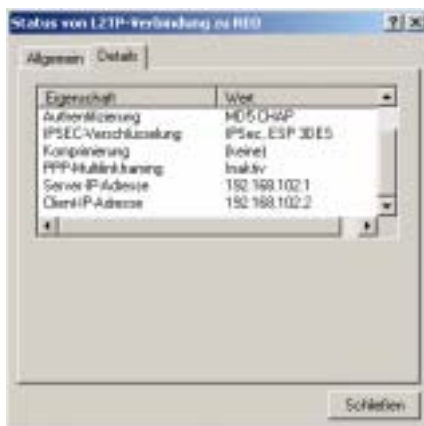
### Start Record

```
Wed Mar 27 15:07:18 2002
Acct-Session-Id = "00000002"
Attr-67 = "\00016.37.176.79"
Attr-66 = "\00016.185.211.242"
Attr-82 = "\000W2K-Clients"
Attr-64 = "\000\000\000\003"
Attr-90 = "\000schlaeppel.emea.cpqcorp.net"
Attr-91 = "\000c3640dm"
Framed-Protocol = PPP
Framed-IP-Address = 192.168.102.2
Acct-Authentic = RADIUS
User-Name = "Field"
Acct-Status-Type = Start
NAS-Port = 1
NAS-Port-Type = Virtual
Service-Type = Framed-User
NAS-IP-Address = 16.37.176.79
Event-Timestamp = "Mar 27 2002"
NAS-Identifizier = "c3640dm.reo-lab.uk"
Acct-Delay-Time = 0
Client-IP-Address = 16.37.176.79
Timestamp = 1017238038
```

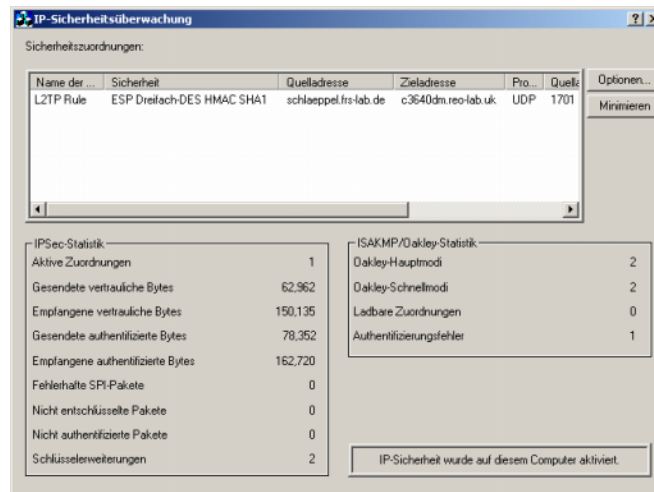
### Stop Record

```
Wed Mar 27 15:34:49 2002
Acct-Session-Id = "00000002"
Attr-67 = "\00016.37.176.79"
Attr-66 = "\00016.185.211.242"
Attr-82 = "\000W2K-Clients"
Attr-64 = "\000\000\000\003"
Attr-90 = "\000schlaeppel.emea.cpqcorp.net"
Attr-91 = "\000c3640dm"
Framed-Protocol = PPP
Framed-IP-Address = 192.168.102.2
User-Name = "Field"
Acct-Session-Time = 1656
Acct-Input-Octets = 57994
Acct-Output-Octets = 126722
Acct-Input-Packets = 779
Acct-Output-Packets = 934
Acct-Terminate-Cause = Admin-Reset
Acct-Authentic = RADIUS
User-Name = "Field"
Acct-Status-Type = Stop
Service-Type = Framed-User
NAS-IP-Address = 16.37.176.79
Event-Timestamp = "Mar 27 2002"
NAS-Identifizier = "c3640dm.reo-lab.uk"
Client-IP-Address = 16.37.176.79
Timestamp = 1017239689
```

## W2K Informationen über L2TP-Verbindung



## W2K Informationen über IPsec Sas



Aufbau eines VPNs mit IPsec 47

Andreas Aurand

## Links

- **Radius Server**
  - <http://www.freeradius.org/>
  - <http://www.radiusvms.com/>
- **Liste von Radius Attributen**
  - <http://www.freeradius.org/rfc/attributes.html>
- **IPsec für L2TP auf Windows 2000 ausschalten (*ProhibitIPsec*)**
  - <http://support.microsoft.com/default.aspx?scid=kb;en-us;Q240262>
  - <http://support.microsoft.com/default.aspx?scid=kb;en-us;Q258261>
- **L2TP Tunnel Authentication für Windows 2000 einschalten**
  - <http://www.netarc.jp/discussion/vpn-talk/old/msg00567.html>
- **Cisco VPN und Security Informationen**
  - <http://www.cisco.com/go/safe>
  - [http://www.cisco.com/warp/customer/471/top\\_issues/vpn/vpn\\_index.shtml](http://www.cisco.com/warp/customer/471/top_issues/vpn/vpn_index.shtml)
  - <http://www.cisco.com/warp/public/779/largeent/learn/technologies/VPNs.html>

Aufbau eines VPNs mit IPsec 48

Andreas Aurand

# Fragen ?

