Lucerne University of
Applied Sciences and Arts
HOCHSCHULE
LUZERN
Informatik
FH Zentralschweiz

NIS Labs
Networking+Services and
Information Security

Suurstoffi 41 b, CH-6343 Rotkreuz
T +41 41 757 68 64
www.hslu.ch

Informatik
Networking+Services and Information Security
Prof. Dr. Bernhard Hämmerli
T direkt +41 41 757 68 43
bernhard.haemmerli@hslu.ch

VPN

Dieses Dokument beinhaltet die Versuchsanleitung für die Durchführung des Laborversuches VPN im Labor Networking+Services. Bei Fragen zur Versuchsanleitung wenden Sie sich bitte direkt an das Laborpersonal.

Autoren: M.Rey, B. Freimann, K. Ivanov, M. Schröder
Version: 2.0
Letze Änderung: 22. Februar 2017

Laborbetreuung

Informatik
Networking+Services
Curdin Banzer

curdin.banzer@hslu.ch

Informatik
Networking+Services
Thomas Jösler

thomas.joesler@hslu.ch

Änderungsverzeichnis

Version	Datum	Status	Änderungen und Bemerkungen	Bearbeitet von
Nr. 1.0	08.05.12	Erledigt	Erstellung Dokument	M.Rey, B.Freimann, K.Ivanov, M.Schröder
Nr. 2.0	23.09.12	Erledigt	Überarbeitung	C.Di Battista, M. Schröder

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

In diesem Dokument werden folgende Abkürzungen verwendet:

Abkürzung	Beschreibung
AAA	Authentication Authorization Accounting
ASA	Adaptive Security Appliances
ASDM	Adaptive Security Device Manager
CLI	Command Line Interface
D-H Group	Diffie-Hellman Groups
DES	Data Encryption Standard
ESP	Encapsulating Security Payload
GRE	Generic Routing Encapsulation
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange
IOS	Internetwork Operating System Software
IPSec	Internet Protocol Security
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
L2TP	Layer 2 Tunneling Protocol
MD5	Message-Digest Algorithm 5
NAT	Network address translation
PAT	Port address translation
PFS	Perfect forward secrecy
PPTP	Point-to-Point Tunneling Protocol
SHA	Secure Hash Algorythm
SSH	Secure Shell
SSL	Secure Socket Layer
VPN	Virtual Private Network

Einleitung

Im Bereich der Netzwerktechnik verwenden wir den Ausdruck VPN häufig ohne richtiges Verständnis für das Thema an sich. Wir berichten beispielsweise, dass wir zu Hause eine VPN Verbindung mit der Schule eingerichtet haben. In diesen Fällen wissen wir ausreichend genau, was wir mit dem Ausdruck VPN meinen. Dagegen ist es äusserst schwierig, eine einheitliche Theorie des Themas zu entwickeln.

VPN ist heutzutage in der Arbeitswelt allgegenwärtig. Deshalb ist das Wissen, wie ein solches aufgebaut wird, unerlässlich, sei es in Verbindung mit Universitätsnetzwerken oder dem Remote Access auf den Server des eigenen Betriebes. VPN ist eine Lösung, um zwei verschiedene Netze sicher über das Internet zu verbinden. Dabei fungiert VPN wie ein Tunnel, der nur von Punkt A oder B betreten werden kann. Die Privatsphäre wird bei einer Verbindung mit VPN gross geschrieben.

Der folgende Versuch ist sehr interessant, weil das vermittelte Wissen für den Alltag sehr praktisch ist. Weiter ist VPN vom Transportmedium weitgehend unabhängig, daher bleibt es auch für die Zukunft relevant.

Wir behandeln verschiedene Funktionen des VPNs und wie diese konfiguriert werden. Ziel ist es, ein funktionierendes VPN einrichten zu können und zu wissen, was dafür nötig ist. Darauf aufbauend wird in die verschiedenen VPN Varianten, wie Site to Site und Remote Access, eingeführt. Gleichzeitig wird darauf eingegangen, wie man Fehler im VPN aufspürt und behebt.

Feedback

Mit Ihrer Mithilfe kann die Qualität des Versuches laufend den Bedürfnissen angepasst und verbessert werden.

Falls in diesem Versuchsablauf etwas nicht so funktioniert wie es beschrieben ist, melden Sie dies bitte direkt dem Laborpersonal oder erwähnen Sie es in Ihrem Laborbericht oder Protokoll. Die Geräte mit denen Sie den Laborversuch bestreiten, sind relativ teuer. Behandeln Sie diese mit der entsprechenden Umsicht. Die Syntax und die Ausgaben der einzelnen Befehle können je nach IOS-Version leicht verschieden sein. Bei Problemen wenden Sie sich bitte ebenfalls an das Laborpersonal.

Legende

In den Versuchen gibt es Passagen die mit den folgenden Zeichen markiert sind, diese werden hier erklärt.

Weiterführende Aufgaben. Dies sind Aufgaben, die nichts an den Versuchen ändern, aber ein vertieftes Wissen vermitteln.

Weiterführende Informationen. Dies sind Informationen, die nicht zur Ausführung der Versuche benötigt werden, aber bekannt sein sollten.

Dringend beachten. Was hier steht unbedingt merken oder ausführen.

Bemerkungen

Die Bezeichnung der Netzwerkschnittstelle kann unterschiedlich sein. Haben die Router 10/100Mbps-Port, dann werden die Interfaces mit FastEthernet bezeichnet. Sind es dagegen Gigabit Ports, dann sind es GigabitEthernet Interfaces.

Stellen Sie sicher, dass alle Firewalls und nicht benötigten Netzwerkinterfaces deaktiviert sind (Windows & Co).

1 Vorbereitung

Dieses Kapitel beschreibt die Vorbereitungsmassnahmen, die Sie zu Beginn des Laborversuches durchführen müssen.

1.1 Fragen zur Theorie

Beantworten Sie die folgenden Fragen richtig, können Sie den zugehörigen Theorieteil überspringen.

1. Was ist VPN?
2. Nutzen von VPN?
3. Wo wird es eingesetzt?
4. Was ist der Unterschied zwischen Site-to-Site VPN und Remote Access VPN?
5. Wie kann VPN gewährleisten, dass sich kein Sniffer zwischen den Peers befindet? Nennen Sie drei Mechanismen.
6. Was ist der Unterschied zwischen Tunnel- und Transport Mode?
7. Die folgenden Einstellungen werden wir an einem VPN Peer vornehmen. Erläutern Sie kurz die Begriffe und deren Aufgabe.

Peer-IP-Address	133.3.3.2
Local Network	172.16.0.0/24
Remote Network	10.0.0.0/24
IKE (ISAKMP Policy)	Authentication: Pre-shared key „cisco“ Encryption: 3DES Hash: SHA D-H Group: 1 Lifetime: 86400
IPsec	Encryption: 3DES Authentication: SHA PFS D-H Group: 1

Falls Sie die Begriffe gut kennen, dürfen Sie für Ihre Versuche andere Einstellungen auswählen (siehe Planungsblatt, Anhang B).

1.2 Theorie

- Frage 1 – 3: Lesen Sie Kapitel 8.6.3 auf Seite 840 vom Buch Computernetzwerke von A.S. Tanenbaum
- Frage 4 – 6: Lesen Sie Anhang A - Theorie
- Frage 7: Lesen Sie Anhang A.6 - IPSec

1.3 Materialiste

Für die Durchführung dieses Laborversuches benötigen Sie folgendes Material:

- 2x Cisco ASA 5505
- 2x Cisco Router mit 2 Fast oder GigabitEthernet-Schnittstellen
- 2x Workstations
- Diverse Kabel

2 Aufgabenstellung

Sobald man die Grundkonfiguration getätigt hat, führt man den Hauptversuch als Einstieg in VPN durch. Nach dem Hauptversuch stehen drei weitere unabhängige Versuche frei zur Auswahl. Diese drei Versuche wurden so konzipiert, dass jeweils nur wenig umgestellt und neukonfiguriert werden muss.

Falls Sie Terminologien begegnen die Sie nicht kennen, können Sie diese im Glossary Anhang C - VPN Glossary finden.

2.1 Troubleshooting

Nicht alles verläuft immer nach Plan. Das Kapitel 10 Troubleshooting umfasst mehrere Seiten, welche Ihnen helfen, die Probleme ohne Hilfe des Assistenten zu lösen. Auch wenn Sie alle Versuche ohne Probleme durchgeführt haben, schauen Sie sich das Kapitel 10 Troubleshooting an. Dies ist als Teil des Versuchs miteingeplant.

2.2 Hauptversuch Site-to-Site VPN

Site-to-Site ist eine direkte Verbindung zweier Netzwerke über zwei festinstallierte Cisco ASAs. Dazwischen wird das Internet mittels Loopback simuliert. Konfiguriert wird mit ASDM, einem von Cisco bereitgestelltem GUI.

Ziele

- Kennenlernen der graphische Benutzeroberfläche ASDM
- Eine Basis für das Verständnis von VPN aufbauen
- Ein Ping von Host A zu B ist möglich, obwohl diese in zwei nicht kompatiblen Netzen heimisch sind

2.3 Versuch 2: Internet over other Site (Hairpinning)

Anstatt direkt auf das Internet zuzugreifen, stellt Host A über die ASA Luzern eine VPN Verbindung mit Bern her, über die der gesamt Netzwerkverkehr läuft. Somit geht Host A über Bern ins Internet.

Ziele

- Ping von Host A über ASA von B zu Loopback
- Hairpinning anwenden können
- Einsatzmöglichkeiten von Hairpinning kennen

2.4 Versuch 3: Konfiguration mit Command-Line

Ein Site-to-Site Versuch mit unterschiedlichen Geräten. Eine der beiden ASAs wird durch einen Router ersetzt. Dieser wird mittels Kommandozeileneingabe konfiguriert.

Ziele

- VPN über Command-Line konfigurieren

- Befehle kennen lernen
- Zeigen, dass VPN auch mit anderen Geräten möglich ist

2.5 Versuch 4: Remote Access mit AnyConnect Client

Dieser Versuch zeigt, wie man einen Client Remote Access für mobile Mitarbeiter einrichten kann.

Ziele

- Remote Access von Host A zu Host B ist möglich (Remote Desktop)
- Client Software installieren
- Befugte User Accounts erstellen

3 Grundkonfiguration (30 min)

Verkabeln Sie die Geräte gemäss Abb. 1, verwenden Sie dazu gerade Kabel.

Starten Sie die ASA erst, sobald Teraterm/Putty läuft und die Geräte angeschlossen sind. Sie verpassen sonst die Aufforderung zum Einrichtungsassistenten, die Sie mit ***no*** umgehen müssen.

Löschen Sie die vorhandenen Konfigurationen:

```
ciscoasa> enable
Password: [enter drücken]
ciscoasa# wr erase
Erase configuration in flash memory? [confirm] [enter drücken]
[OK]
ciscoasa# reload
Proceed with reload? [confirm] [enter drücken]no
```

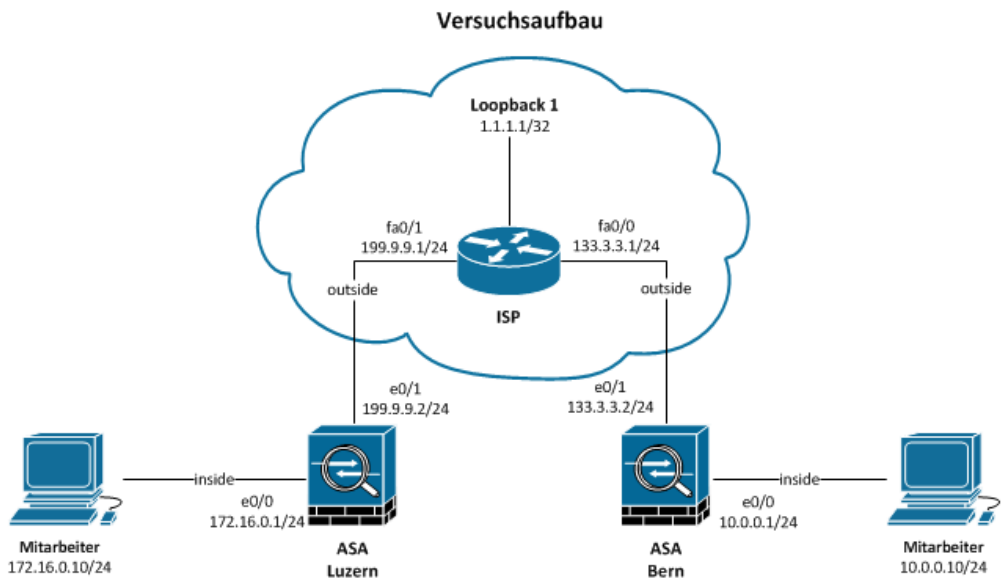

Abb. 1: Versuchsaufbau

3.1 Konfiguration Host

Konfigurieren Sie die Hosts gemäss Abb. 2. Beachten Sie, dass das Default Gateway jeweils das angeschlossene ASA ist.

Optional: Aktivieren Sie auf den Hosts den Web-Server. Er dient zu Testzwecken – eine Abwechslung zum Ping-Befehl.

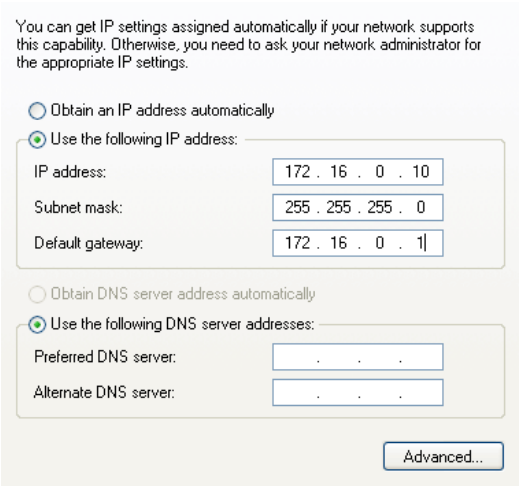

Abb. 2: Host Luzern

3.2 Konfiguration ASA Luzern, Bern

```
!--- 1. Interfaces
hostname Luzern
!--- entgegen anderen ASA Modellen hat die ASA 5505 einen eingebauten Switch
interface vlan 1
 !--- security-level ist ein Firewall-Feature
 nameif inside
 ip address 172.16.0.1 255.255.255.0
 no shutdown
 exit
interface vlan 2
 nameif outside
 ip address 199.9.9.2 255.255.255.0
 no shutdown
 exit
interface ethernet 0/0
 switchport access vlan 1
 no shutdown
 exit
interface ethernet 0/1
 switchport access vlan 2
 no shutdown
 exit
!--- 2. Default-Route
route outside 0.0.0.0 0.0.0.0 199.9.9.1
!--- 3. ICMP (Ping) erlauben
policy-map global_policy
 class inspection_default
  inspect icmp
  exit
 exit
!--- 4. Adaptive Security Device Manager (ASDM)
```

```
!--- Zugriff auf ASA über Browser erlauben
http server enable
http 172.16.0.0 255.255.255.0 inside
!--- Privilege der Stufe 15 erlaubt Ihnen die ganze Vollmacht
username cisco password cisco privilege 15
end
!--- speichert die Konfiguration
write memory
```

Konfigurieren Sie die ASA Bern analog zur ASA Luzern.

3.3 NAT

Öffnen Sie im Browser des Hosts Luzern die Adresse https://172.16.0.1. Installieren Sie ASDM. Username und Password ist wie konfiguriert ***cisco***. Loggen Sie sich ein und starten Sie den Device Manager.

Gehen Sie zu Configuration (oben) → Firewall (links) → NAT Rules. Fügen Sie folgende NAT Regel hinzu.

Konfigurieren Sie Bern analog.

Frage: Wofür braucht man diese Regel und warum benutzt man ein PAT?

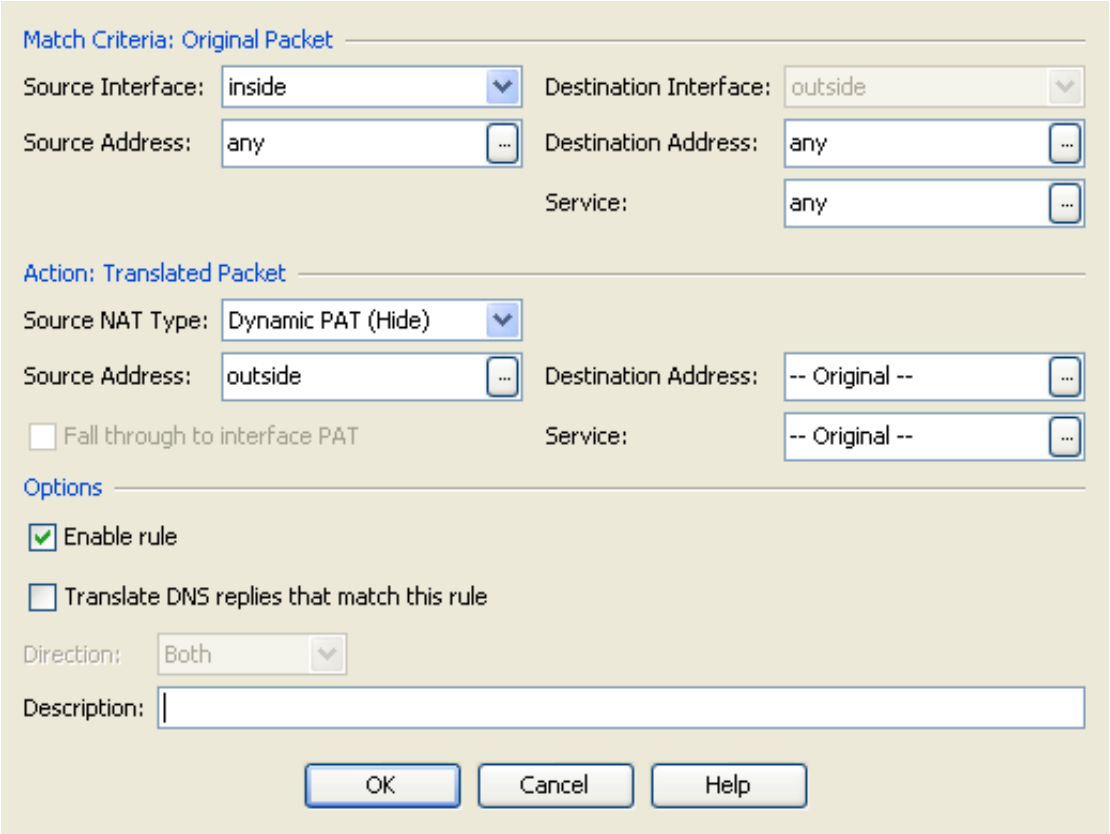

Abb. 3: NAT, der Host kann nun im Internet Surfen

Antwort: Das Internet routet keine privaten Adressen. ASA übersetzt die private Adresse in eine öffentliche Adresse. Werden mehrere private Adressen in nur eine öffentliche Adresse übersetzt, dann braucht man PAT (Layer 4), um auf dem Rückweg zu identifizieren, welcher Inhalt zu welcher privaten Adresse gehört.

3.4 Konfiguration Router ISP

```
!--- 1. Konsole
hostname ISP
!--- falsche Befehlseingabe ignorieren
no ip domain-lookup
line console 0
 !--- Befehlseingabe nicht durch Systemmeldungen unterbrechen
 logging synchronous
 exit
!--- 2. Interfaces
interface fastEthernet0/0
 ip address 133.3.3.1 255.255.255.0
 no shutdown
 exit
interface fastEthernet0/1
 ip address 199.9.9.1 255.255.255.0
 no shutdown
 exit
!--- das Internet
interface loopback 1
 ip address 1.1.1.1 255.255.255.255
 end
wr mem
```

3.5 Testen

Falls Sie Probleme haben, schauen Sie sich das Kapitel 10 Troubleshooting an.

1. Im ASDM gehen Sie zu Configuration → Device Setup (links) → Routing → Static Routes. Überprüfen Sie die Default-Route.

2. Im ASDM gehen Sie zu Configuration → Firewall → Service Policy Rules. Im Hauptfester klicken Sie auf inspection_default → Edit → Rule Actions. ICMP ist erlaubt.

3. Testen Sie alle Pings: Host Luzern – ASA Bern, Host Bern – ASA Luzern. Verzweifeln Sie nicht, wenn der inside Host das outside Interface von ASA nicht anpingen kann. Host Luzern kann Host Bern nicht anpingen, weil der ISP keinen Eintrag für das Netzwerk in der Routing Tabelle findet, und das Paket verwirft.

3.6 Kontrollfragen

- Was erzielt man mit dem Command ***nameif*** ?
- Was ist der Unterschied zwischen PAT und NAT?

4 Hauptversuch: Site-to-Site VPN (30 min)

ASDM bietet verschiedene Wizards, um beispielsweise auch Site-to-Site VPN einzurichten und diese auch leicht zu testen. Site-to-Site VPN verbindet zwei Netze, die an völlig verschiedenen Standorten über das Internet verbunden sind und zu einem Netz zusammengefasst werden können.
Um die ASDM Oberfläche und Site-to-Site VPN besser kennen zu lernen, wurde folgender Versuch aufgesetzt:

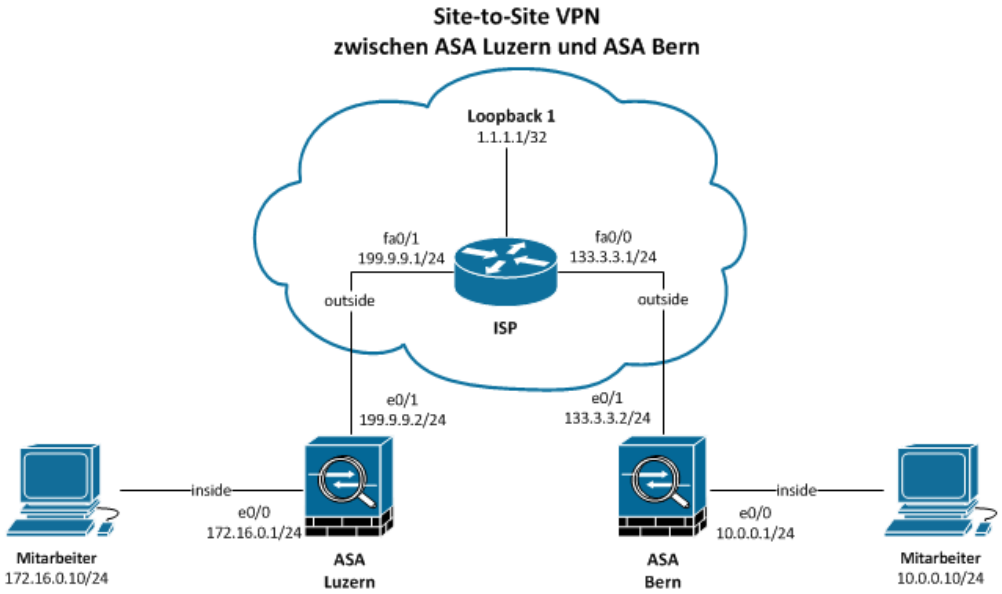

Abb. 4: Site-to-Site VPN zwischen ASA Luzern und ASA Bern

4.1 Planung

Peer-IP-Address	133.3.3.2
Local Network	172.16.0.0/24
Remote Network	10.0.0.0/24
IKE (ISAKMP Policy)	Authentication: Pre-shared key „cisco“ Encryption: 3DES Hash: SHA D-H Group: 1 Lifetime: 86400
IPsec	Encryption: 3DES Authentication: SHA PFS D-H Group: 1

4.2 Konfiguration ASA Luzern, Bern

ASA Luzern wird gemäss der folgenden Anleitung konfiguriert (ASA Bern analog). Den Wizard finden sie in der Menu-Leiste (oben) unter Wizards → VPN Wizards → Site-to-site VPN Wizard…

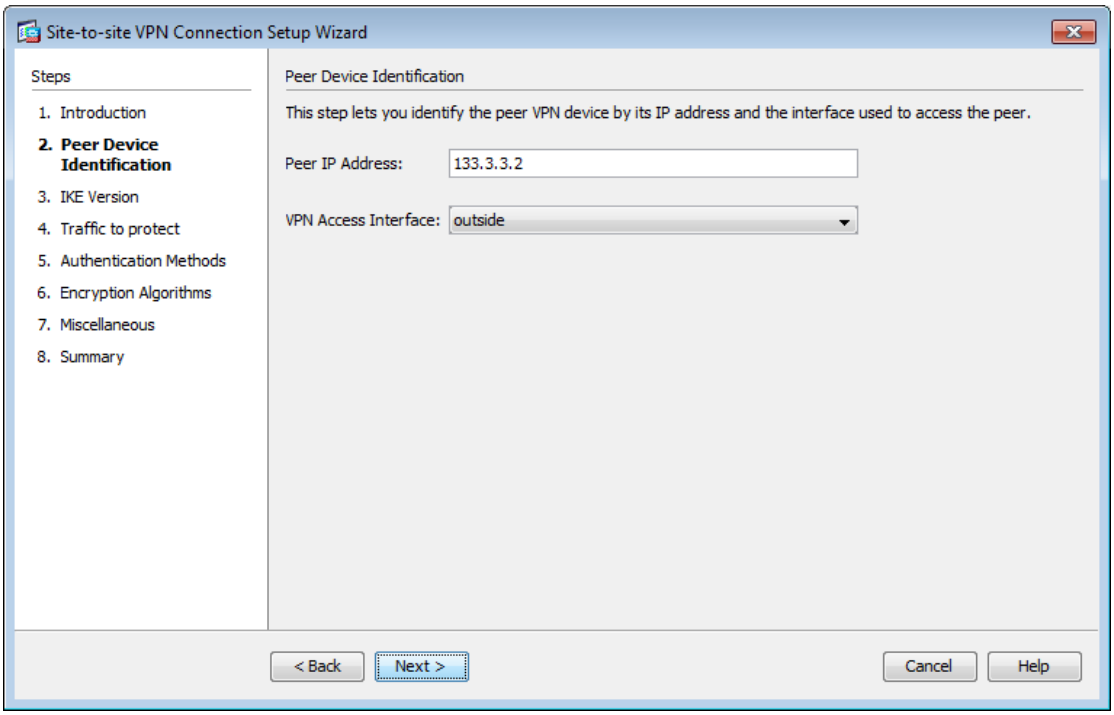

Abb. 5: Peer Device Identification

Die Peer IP Adresse ist die Adresse von ASA Bern (der Gegenstelle).

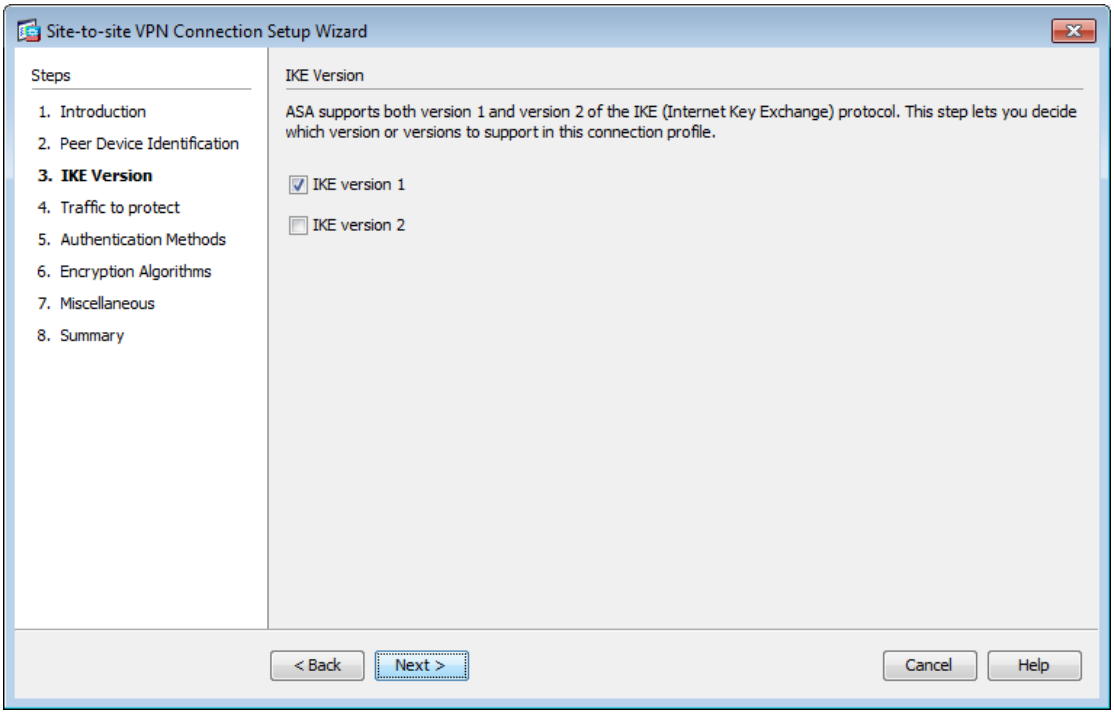

Abb. 6: IKE Version

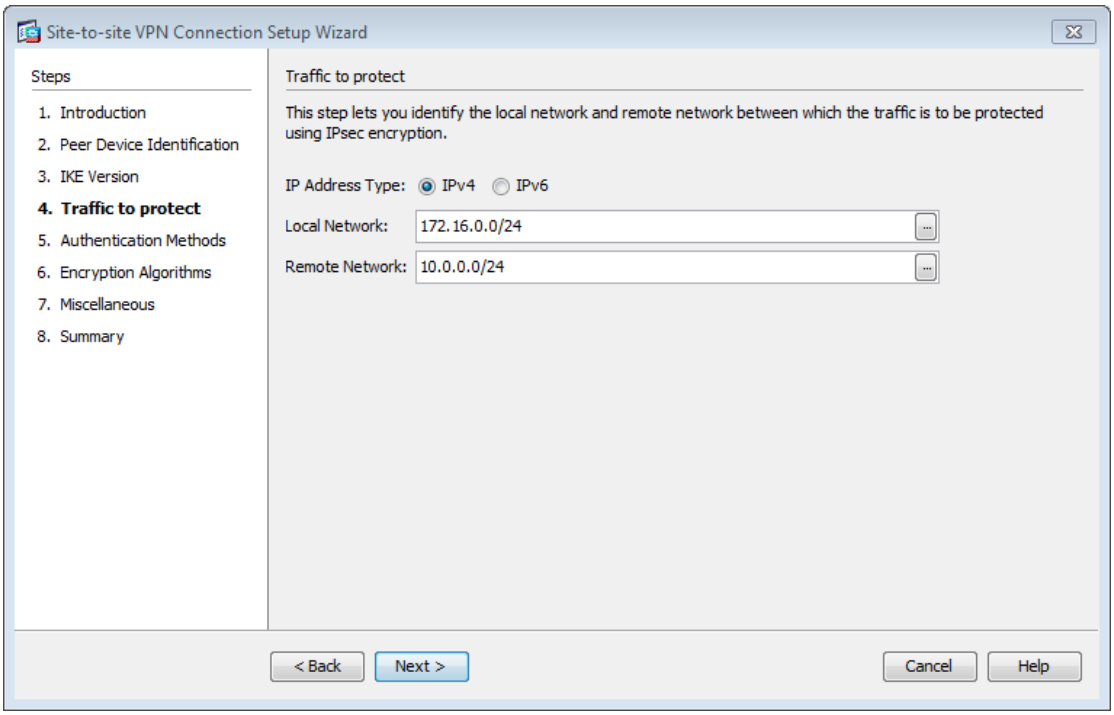

Abb. 7: Traffic to protect

Tragen Sie nun die beiden zu verbindenden Netze ein. In diesem Fall sind dies 172.16.0.0/24 und 10.0.0.0/24.

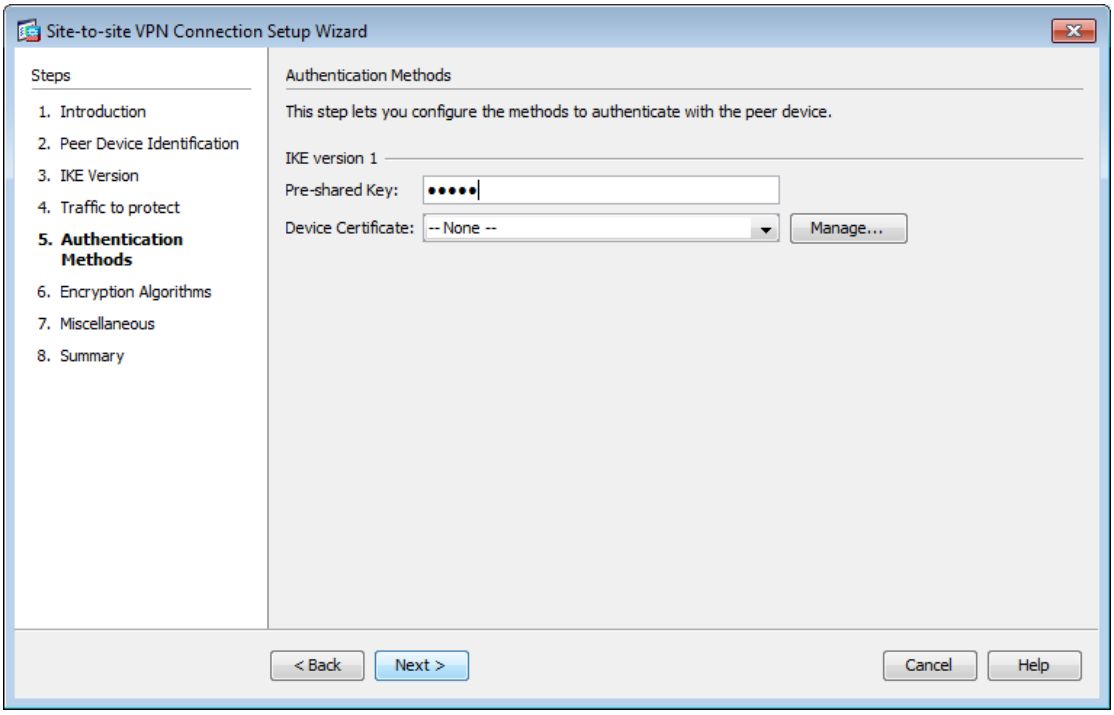

Abb. 8: Authentication Methods

Der Pre-shared Key muss auf beiden Seiten gleich sein (cisco).

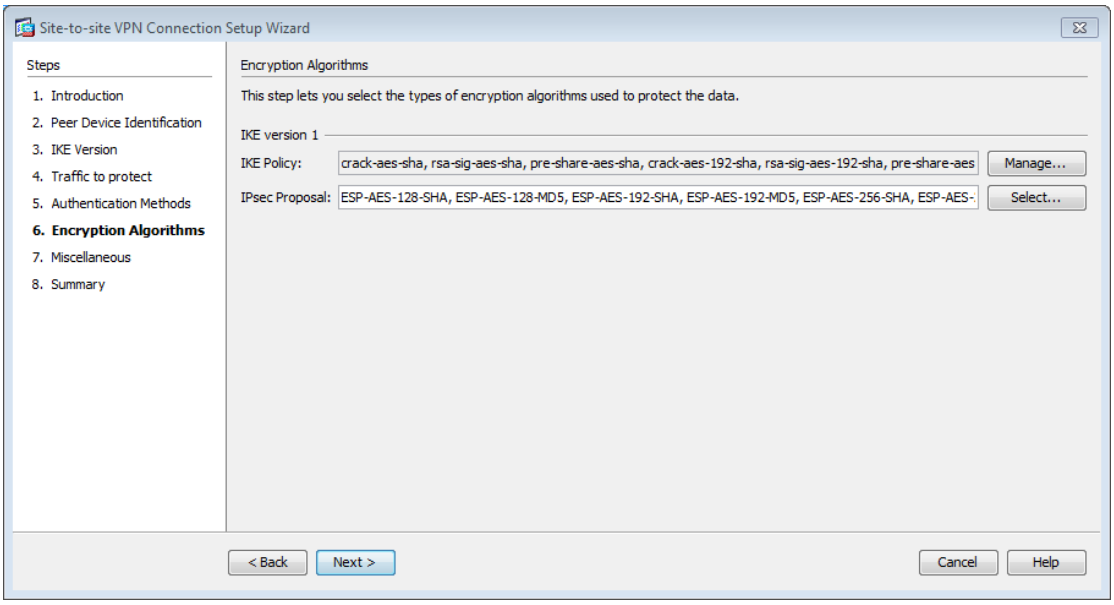

Abb. 9: Encryption Algorithmus

Belassen Sie die Verschlüsselung standardmässig.

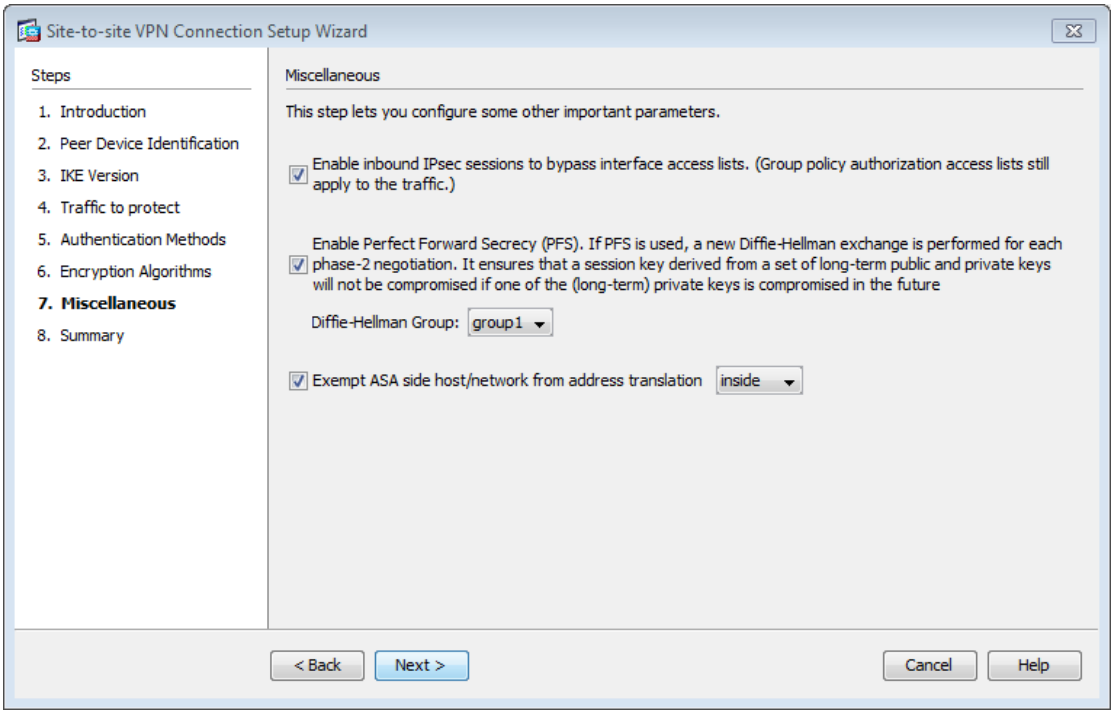

Abb. 10: Miscellaneous

Das letzte Häkchen erstellt automatisch eine NAT Regel. Falls das Ziel das Remote-Netzwerk ist, dann behalten Sie die private Adresse bei und übersetzen Sie diese NICHT in eine öffentliche Adresse.

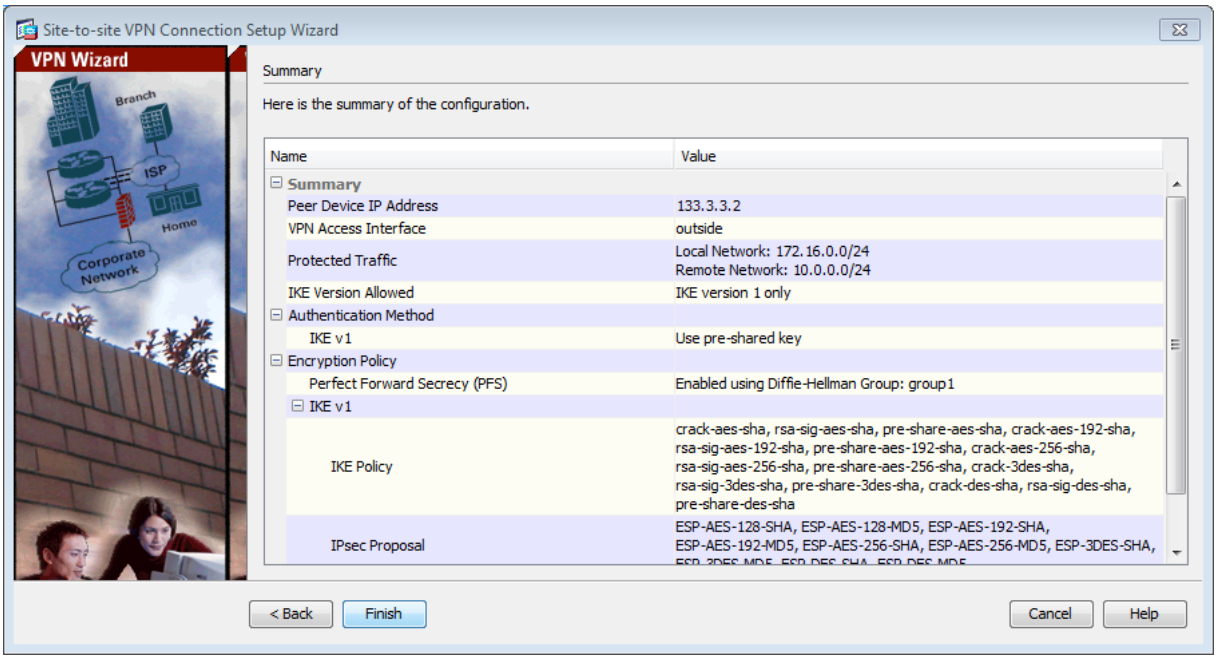

Abb. 11: Summary

Jetzt müssen Sie noch die in der Grundkonfiguration erstellte NAT Regel (any, any) in die 2. Position verschieben wie Abb. 12 dargestellt, da sie sonst eine zu hohe Priorität hat.

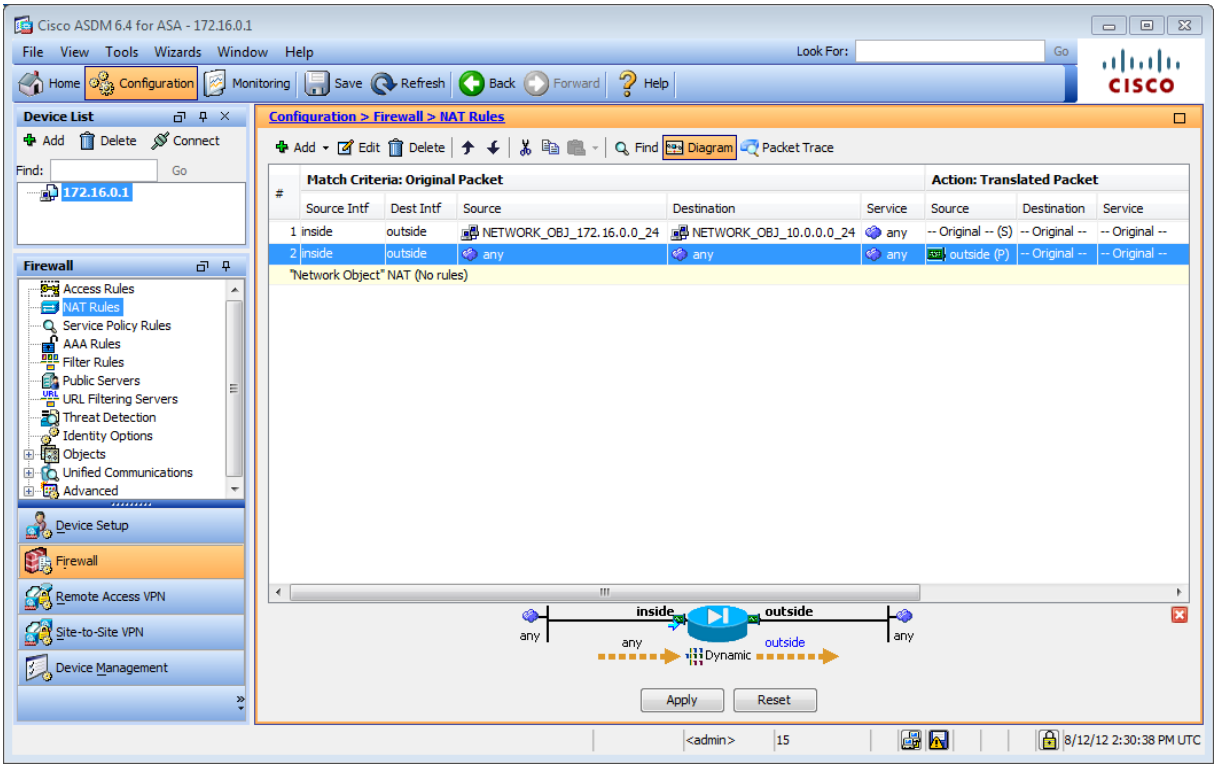

Abb. 12: NAT Regeln

Vergessen Sie nicht unten auf „Apply“ zu klicken, um die Änderungen zu bestätigen.

Die Konfiguration auf ASA Luzern ist abgeschlossen. Führen Sie den Wizard analog beim ASA Bern aus.

4.3 Testen

Falls Sie Probleme haben, schauen Sie sich das Kapitel 10 Troubleshooting an.

1. Durch die getätigten Konfigurationen sollte es Ihnen möglich sein, sowohl einen Host im 10.0.0.0/24 Netzwerk von Luzern aus, wie auch einen 172.16.0.0/24 Host von Bern anzupingen.

2. Versuchen Sie von Host 10.0.0.10 einen Ping zu 172.16.0.10 zu starten. Ist dieser Ping erfolgreich?

4.4 Kontrollfragen

- Wieso muss man die NAT Regel (any, any) der Grundkonfiguration in die 2. Position verschieben? Was geschieht wenn man Sie an der ersten Stelle belässt?
- Wie behandelt die ASA Luzern die IP-Pakete, welche nach zum Berner Subnet gehören? Erläutern Sie.

5 Versuch 2: Internet over other Site, Hairpinning (30 min)

Hairpinning, zu Deutsch Haarnadeln, bedeutet, dass ein Paket ohne Umweg über das gleiche Interface raus geht, wie es hinein gekommen ist. Während das Paket diese Haarnadelkurve nimmt, kann die ASA dem Paket eine neue Source und Destination Adresse geben (NAT) oder auch ein verschlüsseltes Paket entschlüsseln. In der Praxis kann ein Mitarbeiter somit sicher im Ausland im Internet surfen. Der gesamte Internetverkehr des Mitarbeiters geht verschlüsselt an die ASA in der Schweiz und von dort aus ins WWW.

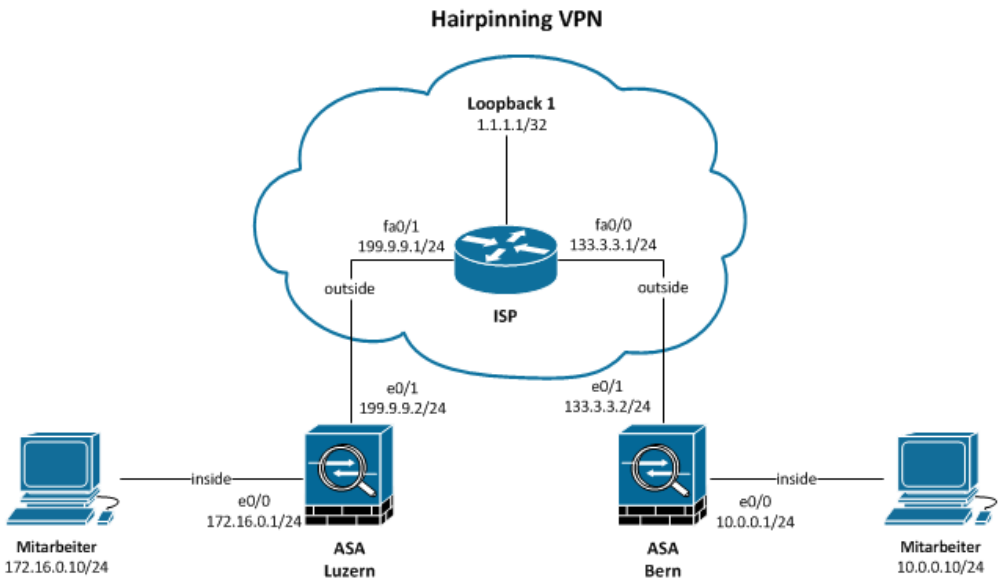

Abb. 13: Site-to-Site VPN zwischen ASA Luzern und ASA Bern, Hairpinning

Aufgabe: Konfigurieren Sie die Geräte oder überlegen Sie sich, wie der Host von ASA Luzern ins Internet über ASA Bern gelangt.

Hier eine Musterlösung:

5.1 Planung

Peer-IP-Address	133.3.3.2
Local Network	172.16.0.0/24
Remote Network	Any
IKE (ISAKMP Policy)	Authentication: Pre-shared key „cisco“ Encryption: 3DES Hash: SHA D-H Group: 1 Lifetime: 86400
IPsec	Encryption: 3DES Authentication: SHA PFS D-H Group: 1

5.2 Konfiguration ASA Luzern

Löschen Sie zuerst alle NAT und Site-to-Site Regeln.

Vergessen Sie nicht unten auf „Apply“ zu klicken, um die Änderungen zu bestätigen.

Die Konfiguration ist, bis auf einen Unterschied, genau gleich wie die im Kapitel 4.2 beschrieben. Im Wizard unter 4. Traffic to protect“ wird beim Remote Network, anstatt des Subnets der ASA Bern, any eingetragen.

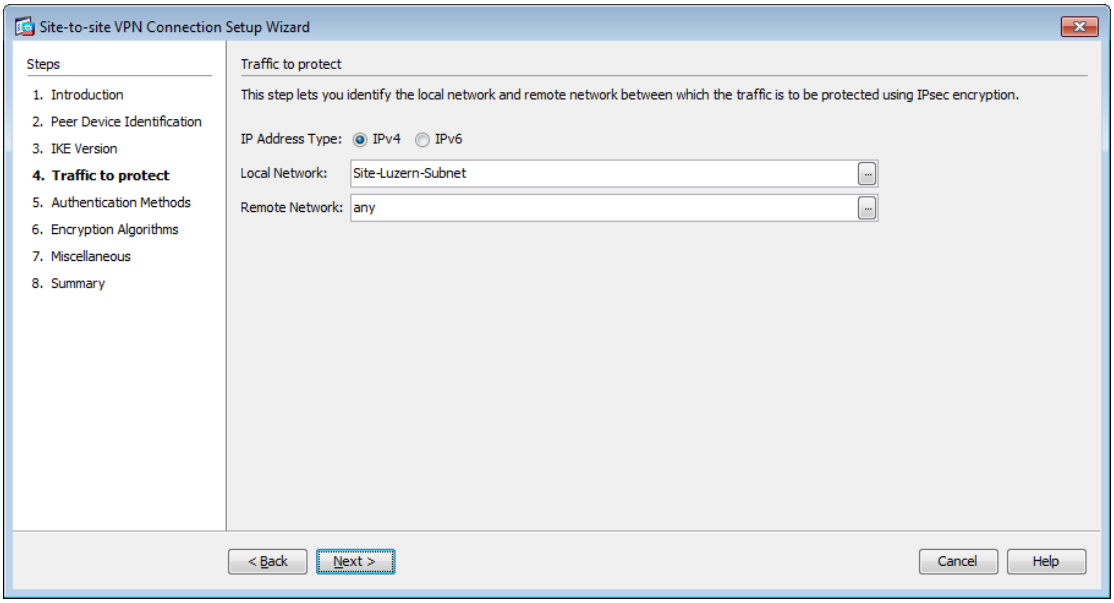

Abb. 14: ASA Luzern, Remote Network ändern

Vergessen Sie nicht die NAT Regel von der Grundkonfiguration zu erstellen. Beachten Sie dabei, dass sie an 2. Stelle aufgelistet wird.

5.3 Konfiguration ASA Bern

Löschen Sie zuerst alle NAT und Site-to-Site Regeln.

Die Konfiguration ist bis auf drei Unterschiede genau gleich, wie bei der Grundkonfiguration.

1. Im Wizard unter “4. Traffic to protect“ wird beim Local Network, anstatt des Subnets des ASA Luzern, any eingetragen.

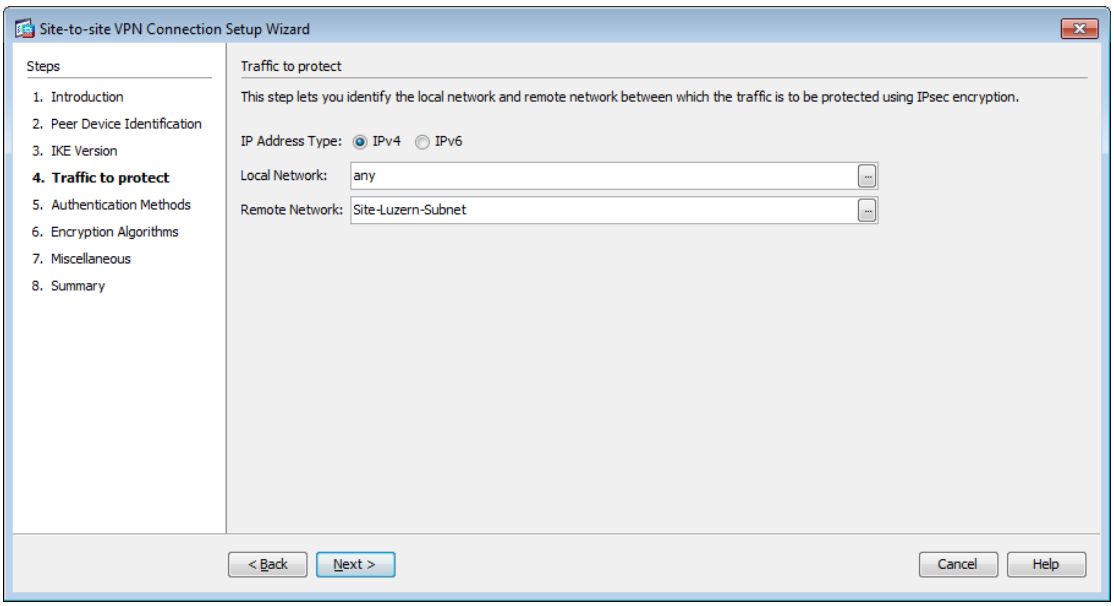

Abb. 15: ASA Bern, Local Network ändern

2. Zu der bereits vom Wizard erstellte NAT Regel muss noch eine Regel hinzugefügt werden. Diese sorgt dafür, dass der Verkehr vom Subnet Luzern, welcher nicht an Bern gerichtet ist, unverschlüsselt über die Static Route nach aussen geht. Die NAT Regel entspricht der Regel 2 im Bild unten, mit dem Source NAT Type Dynamic PAT.
3. Vergessen Sie nicht, die NAT Regel von der Grundkonfiguration zu erstellen. Beachten Sie dabei dass sie an 3. Stelle aufgelistet wird.

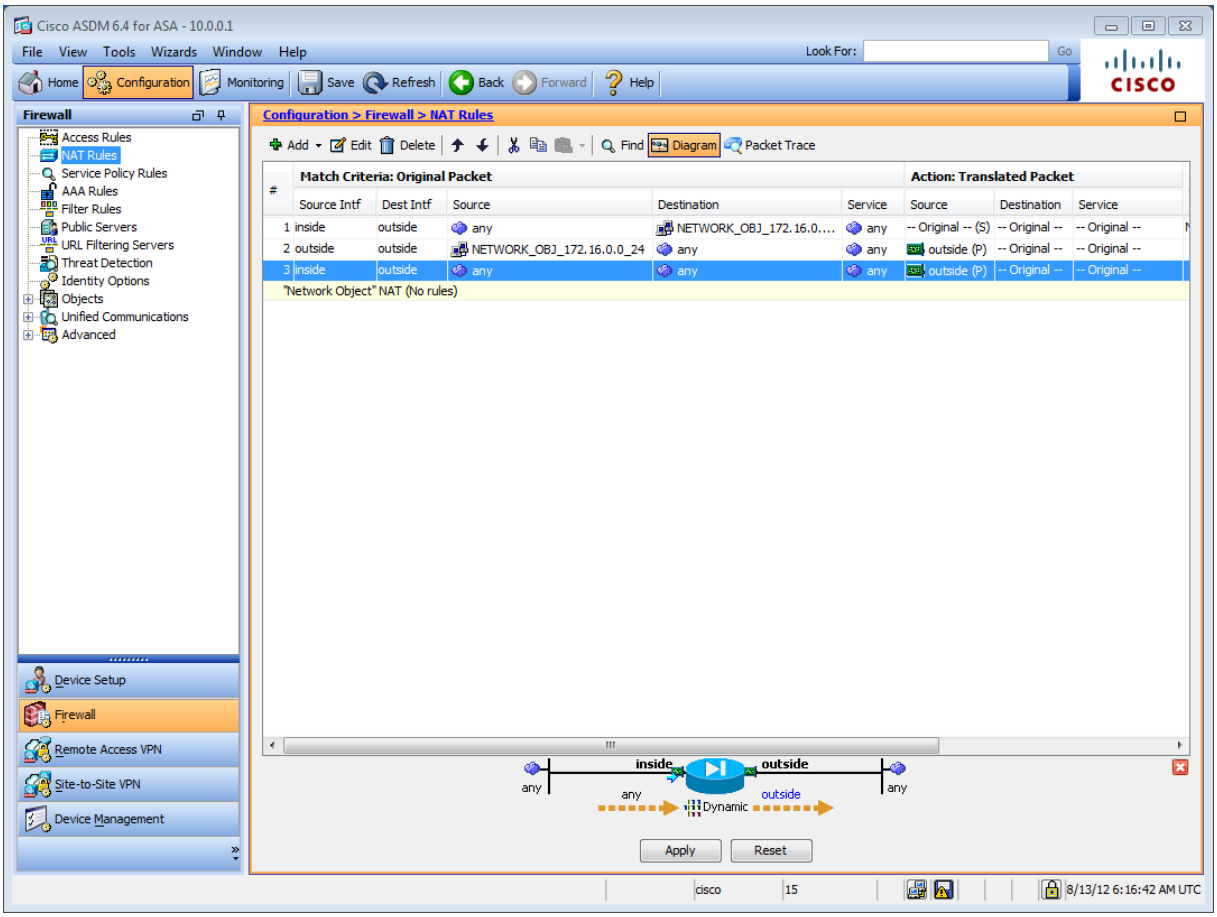

Abb. 16: Zwei zusätzliche NAT Regeln für Hairpinning

4. Unter Configuration → Device Setup → Interfaces, müssen unten beide Haken gesetzt werden. Die beiden Regeln erlauben den Hairpinning Netzwerkverkehr über das gleiche Interface.

Vergessen Sie nicht, unten auf „Apply“ zu klicken, um die Änderungen zu bestätigen.

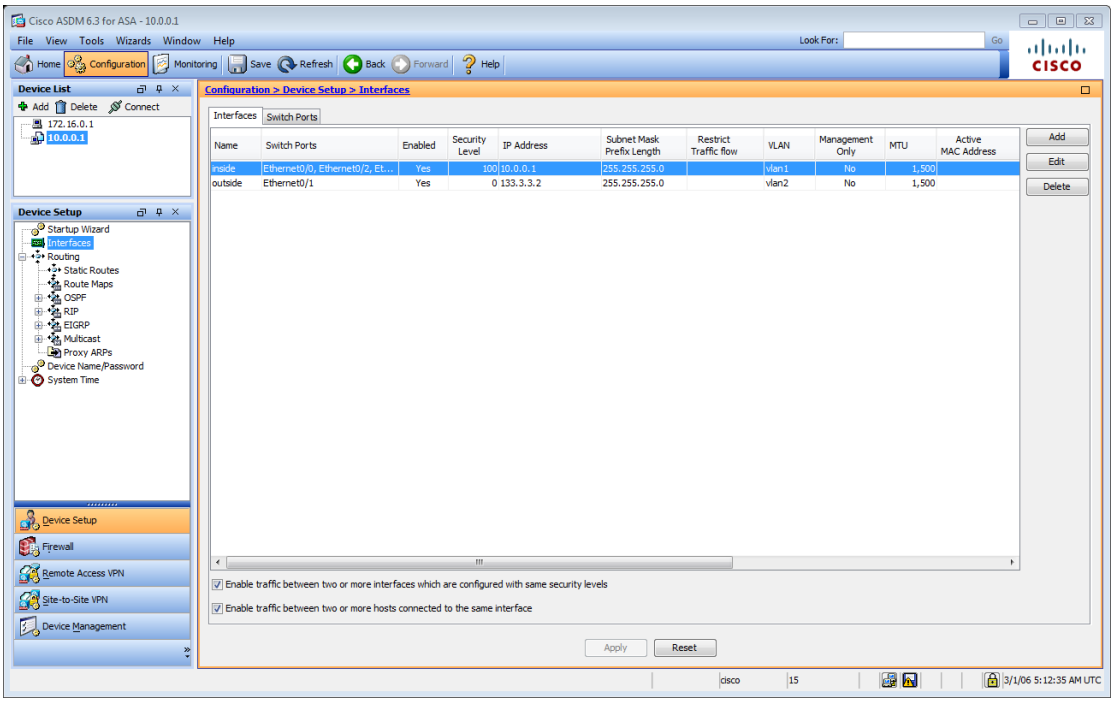

Abb. 17: Interface Regeln

5.4 Testen

Man schickt einen Ping vom Host Luzern an die Adresse 1.1.1.1 und wartet auf eine Antwort. Ob der Ursprung der Antwort auch wirklich vom Loopback kommt, wird am besten mit Wireshark überprüft (Siehe Kapitel 10 Troubleshooting).

5.5 Kontrollfrage

- Wieso wurde bei der Konfiguration von ASA Luzern (siehe Abb. 14) bei Remote Network anstatt Subnetz Bern, any eingetragen?

6 Versuch 3: Konfiguration mit Command-Line (30 min)

Wir ersetzten nun ASA Bern durch einen Router.

In diesem Versuch bauen Sie einen Site-to-Site VPN Tunnel zwischen ASA Luzern und dem Cisco Router Bern auf. Den Cisco Router werden Sie mittels Command-Line Interface konfigurieren.

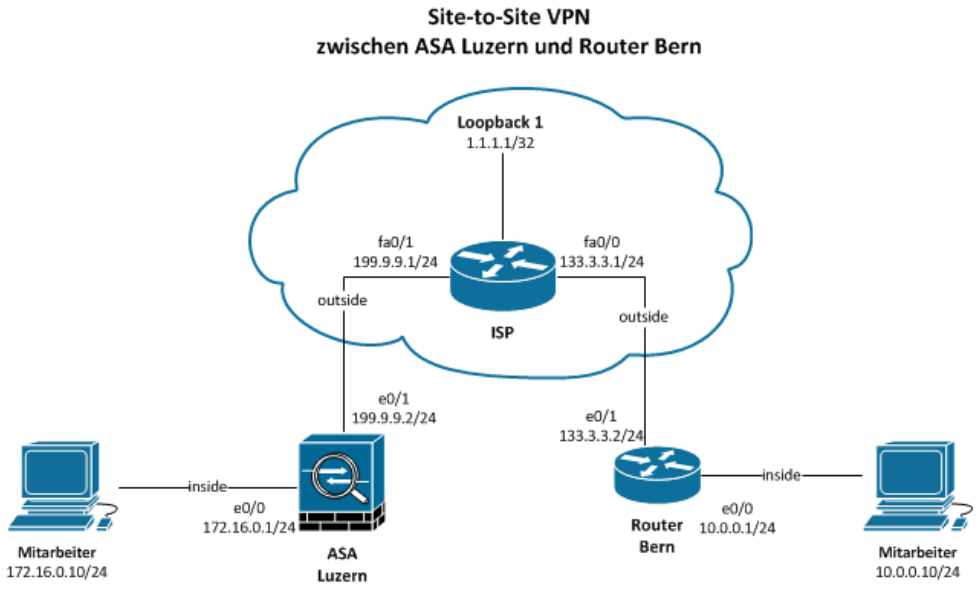

Abb. 18: Site-to-Site VPN zwischen ASA Luzern und Router Bern

6.1 Planung

Peer-IP-Address	199.9.9.2
Local Network	10.0.0.0/24
Remote Network	172.16.0.0/24
IKE (ISAKMP Policy)	Authentication: Pre-shared key „cisco“ Encryption: 3DES Hash: SHA D-H Group: 1 Lifetime: 86400
IPsec	Encryption: 3DES Authentication: SHA PFS D-H Group: 1

6.2 Konfiguration ASA Luzern

Vergessen Sie nicht die NAT und Site-to-Site Regeln von ASA Luzern zu löschen.

Die Konfiguration für ASA Luzern ist bis auf einen Unterschied genau gleich wie beim Hauptversuch.

Im Wizard unter "6. Encryption Algorithms“ (Abb. 19) wählen Sie nur die 3DES und SHA Verschlüsselung aus.

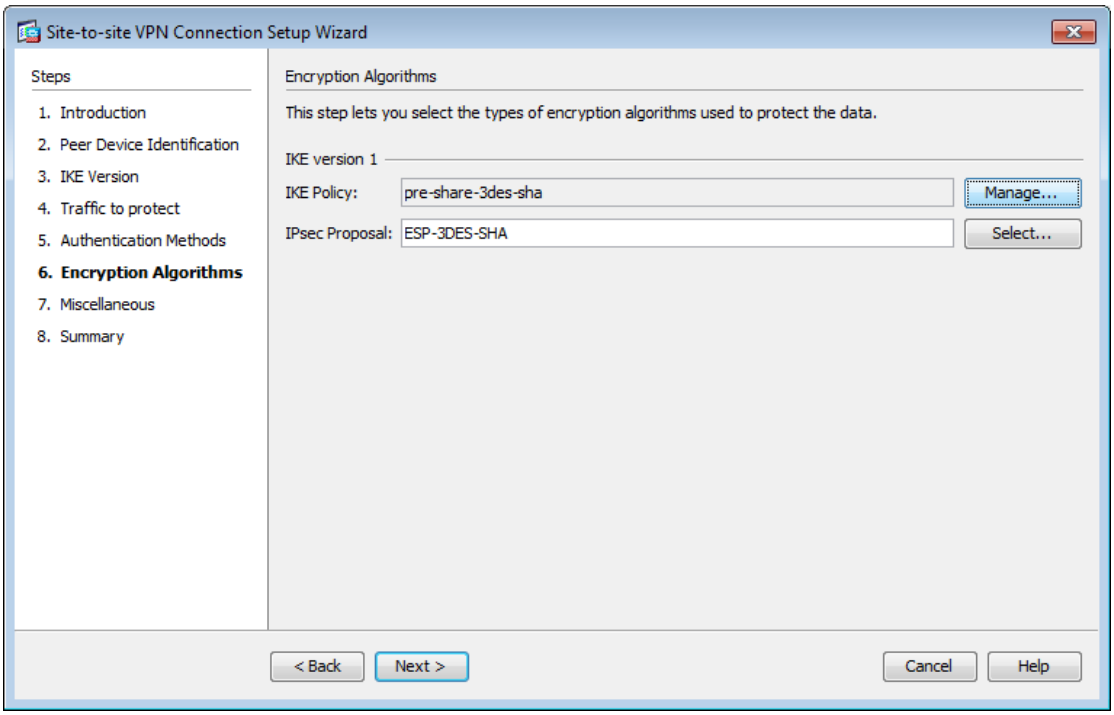

Abb. 19: Encryption Algorithms 3des-sha

6.3 Konfiguration Router Bern

Geben Sie die folgenden Befehle im globalen Konfigurationsmodus ein.

```
!--- 1. Konsole
hostname Bern
!--- falsche Befehlseingabe ignorieren
no ip domain-lookup
line console 0
 !--- Befehlseingabe nicht durch Systemmeldungen unterbrechen
 logging synchronous
 exit
!--- 2. Interfaces
interface fastEthernet 0/0
 ip nat inside
 ip address 10.0.0.1 255.255.255.0
 no shutdown
 exit
interface fastEthernet 0/1
 ip nat outside
 ip address 133.3.3.2 255.255.255.0
 no shutdown
 exit
!--- 3. Default Route
ip route 0.0.0.0 0.0.0.0 133.3.3.1
!--- 4. Network Address Translation (NAT)
!--- Wenn die erste Regel nicht zutrifft, dann wird die zweite Regel angewendet.
!---Reihenfolge (Sequence Number) anzeigen: show access-list 101
!--- Overload bedeutet Port Address Translation (PAT)
access-list 101 deny ip 10.0.0.0 0.0.0.255 172.16.0.0 0.0.0.255
access-list 101 permit ip 10.0.0.0 0.0.0.255 any
ip nat inside source list 101 interface fastEthernet 0/1 overload
!--- 5. Virtual Private Network (VPN)
!---  IKE (ISAKMP Policy)
```

```
crypto isakmp policy 1
 authentication pre-share
 encryption 3des
 group 1
 hash sha
 lifetime 86400
 exit
!--- Pre-shared key "cisco" der ASA zuweisen
crypto isakmp key cisco address 199.9.9.2
!--- IPSec 3DES Encryption and SHA Authentication Hash
crypto ipsec transform-set myset esp-3des esp-sha-hmac
 exit
!--- Alle Verbindungen zwischen Local- und Remote-Network erlauben.
access-list 100 permit ip 10.0.0.0 0.0.0.255 172.16.0.0 0.0.0.255
!--- Crypto Map setzt alles zusammen
crypto map mymap 1 ipsec-isakmp
 set peer 199.9.9.2
 !--- Perfect Forward Secrecy
 set pfs group1
 set transform-set myset
 match address 100
 exit
!--- ISAKMP Aktivieren, crypto map dem Interface zuweisen
interface fastEthernet 0/1
 crypto map mymap
 exit
```

6.4 Testen

Falls Sie Probleme haben, schauen Sie sich das Kapitel 10 Troubleshooting an.

Pingen Sie von Host Luzern erfolgreich Host Bern an. Leuchtet auf der ASA Luzern das VPN Lämpchen?

6.5 Kontrollfrage

- Wäre es möglich auch ASA Luzern durch einen Router zu ersetzen? Wenn ja, erstellen Sie eine Konfiguration.

7 Versuch 4: Remote Access mit AnyConnect Client (30 min)

Ziel in diesem Versuch ist es, die ASA so einzurichten, dass mobile Mitarbeiter mit Hilfe des Cisco AnyConnect Clients eine sichere Verbindung zum Firmennetzwerk herstellen können, egal wo sie sich im Moment befinden.

In diesem Szenario soll der externe IT-Mitarbeiter von seinem Laptop aus, mit Hilfe des Windows Remote Desktops, auf den PC eines technisch eher unbedarften Arbeitskollegen im Hauptsitz zugreifen können. Sie können auch eine Workstation verwenden, anstatt einen Laptop.

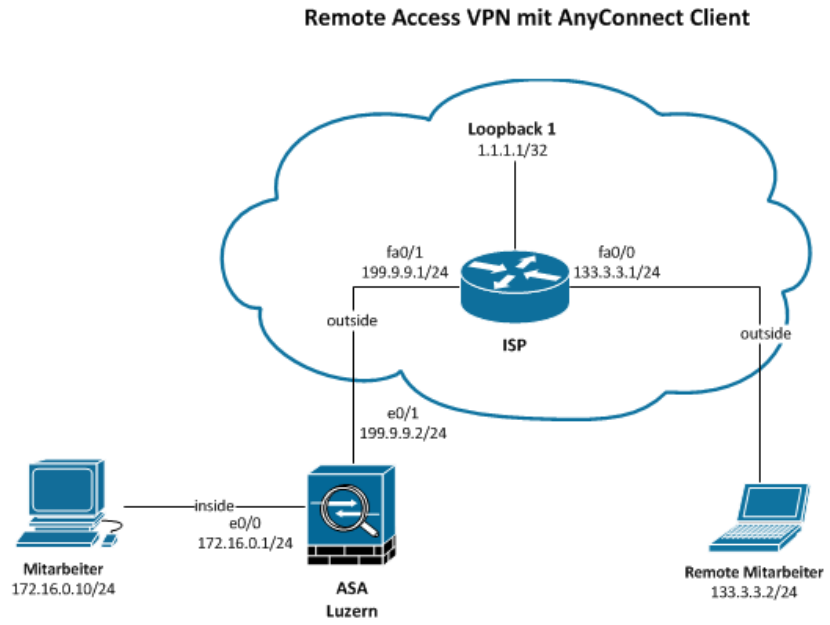

Abb. 20: Remote Access VPN mit Cisco AnyConnect Client

7.1 Planung

Local Network	172.16.0.0/24
Remote User	133.3.3.2/24
VPN Client Type	Cisco AnyConnect Client
VPN Protokoll	SSL
Client Authentification	Local Database
Address Pool Name	AnyConnect
Address Pool Settings • **Range** • **Subnetzmaske**	 192.168.0.10 – 192.168.0.20 255.255.255.0

7.2 Konfiguration ASA Luzern

Vergessen Sie nicht die NAT und Site-to-Site Regeln von ASA Luzern zu löschen.

Rufen Sie dazu den AnyConnect VPN Wizard auf.

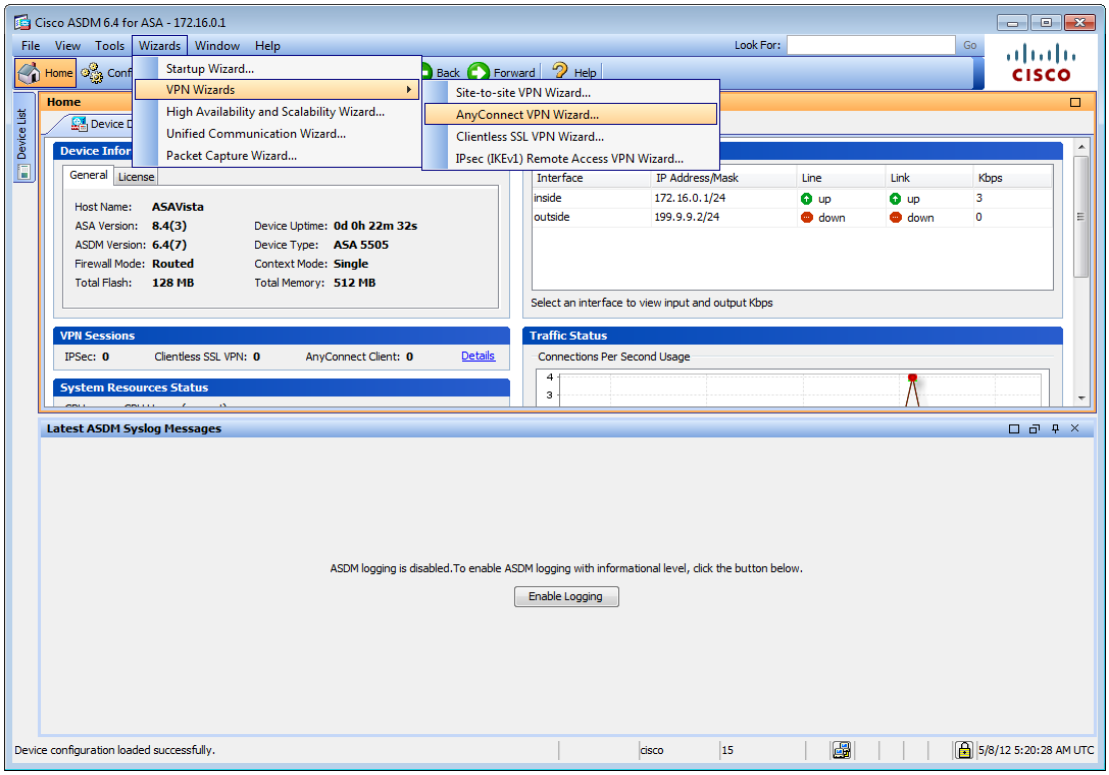

Abb. 21: AnyConnect Wizard aufrufen

Der Setup Wizard führt Sie schrittweise durch die Konfiguration.

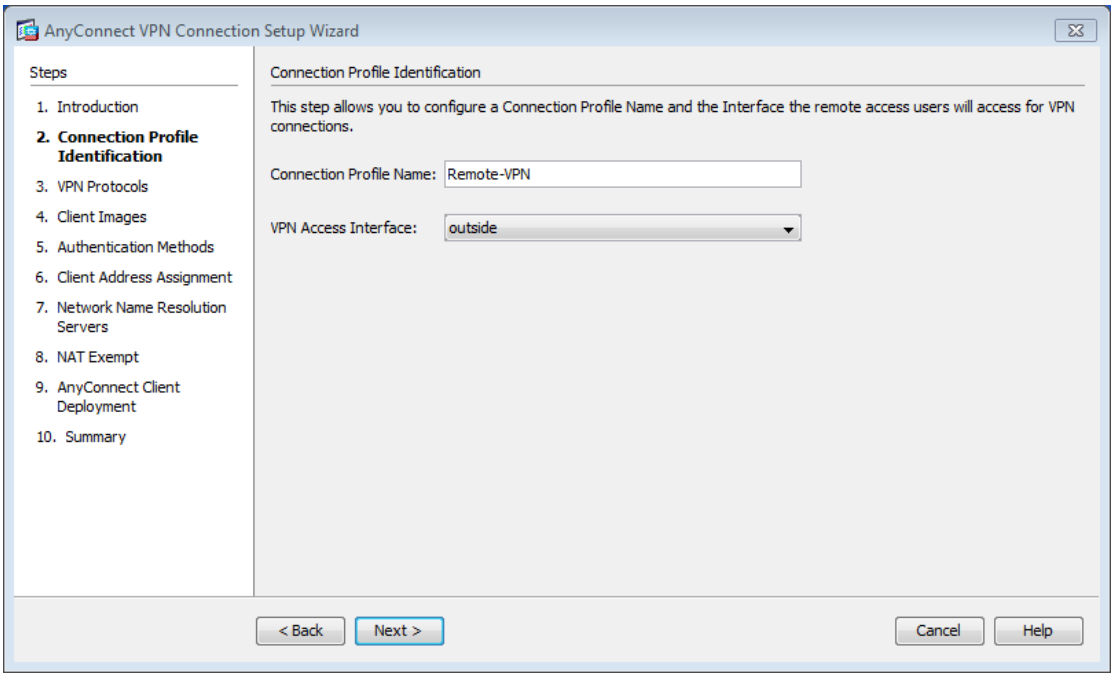

Abb. 22: Connection Profile Identification

Geben Sie Ihrer VPN Verbindung einen passenden Namen.

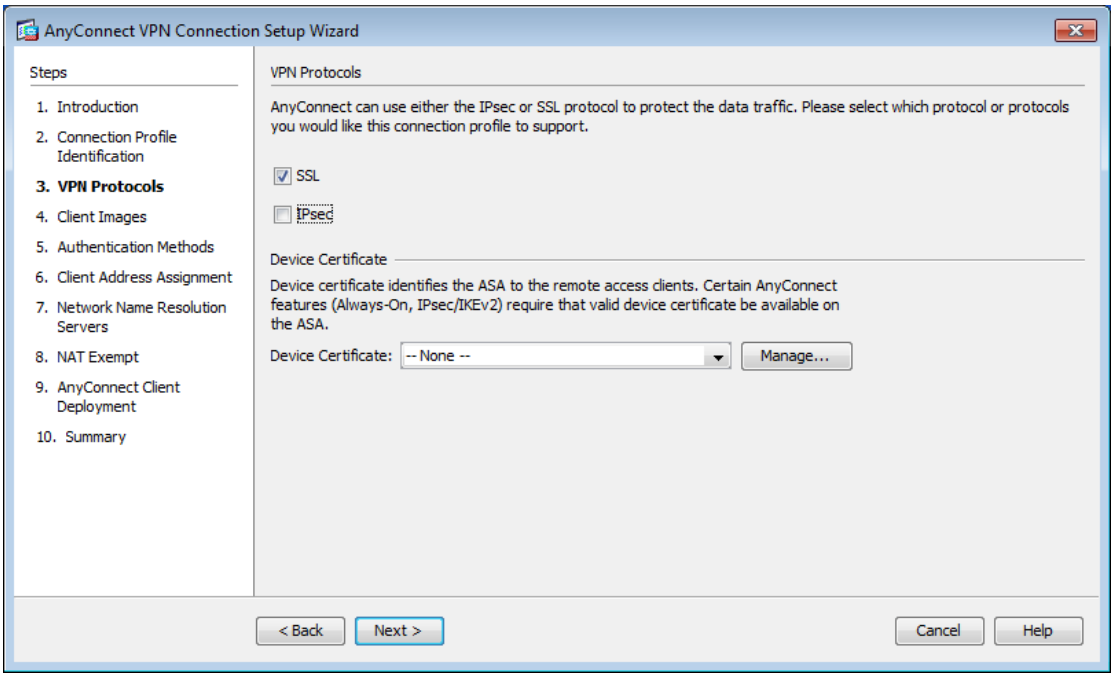

Abb. 23: VPN Protokoll wählen

Da in diesem Versuch keine Zertifikate verwendet werden, wählen Sie als VPN Protokoll SSL aus. Ein Device Certificate wird in diesem Versuch nicht gebraucht.

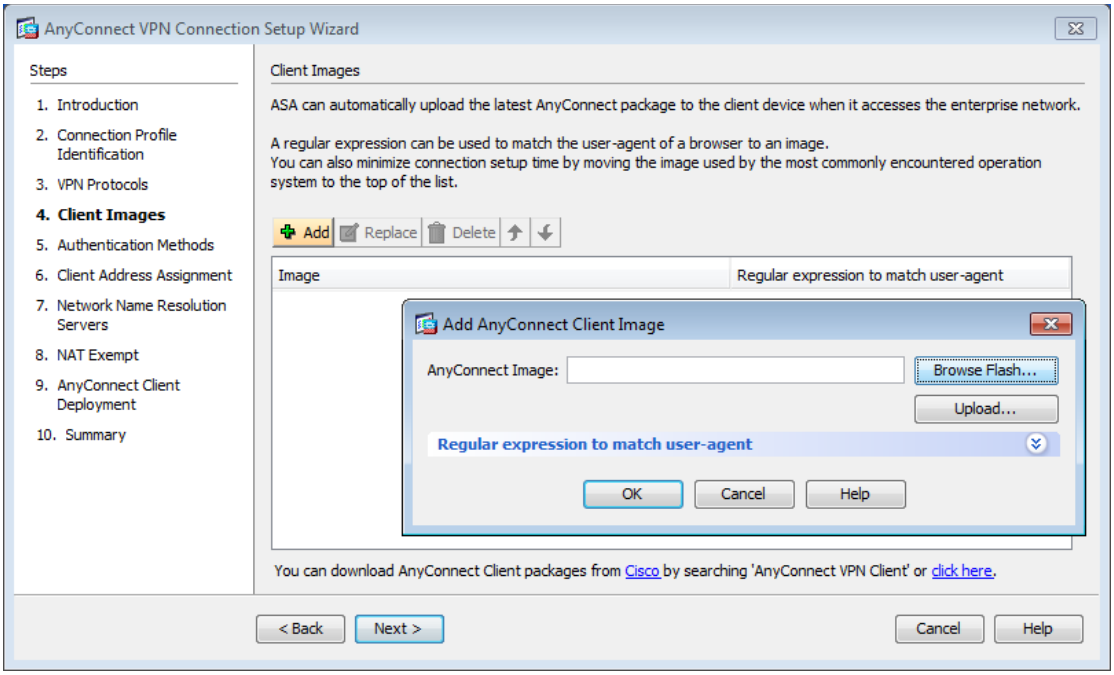

Abb. 24: Client Image hinzufügen

Im nächsten Schritt muss ein oder mehrere Images des AnyConnect Clients in die ASA geladen werden. Cisco stellt auf ihrer Homepage Clients für verschiedene Betriebssysteme zur Verfügung. So profitieren nicht nur Windows User von dieser komfortablen Lösung, sondern auch Mac und Linux User.

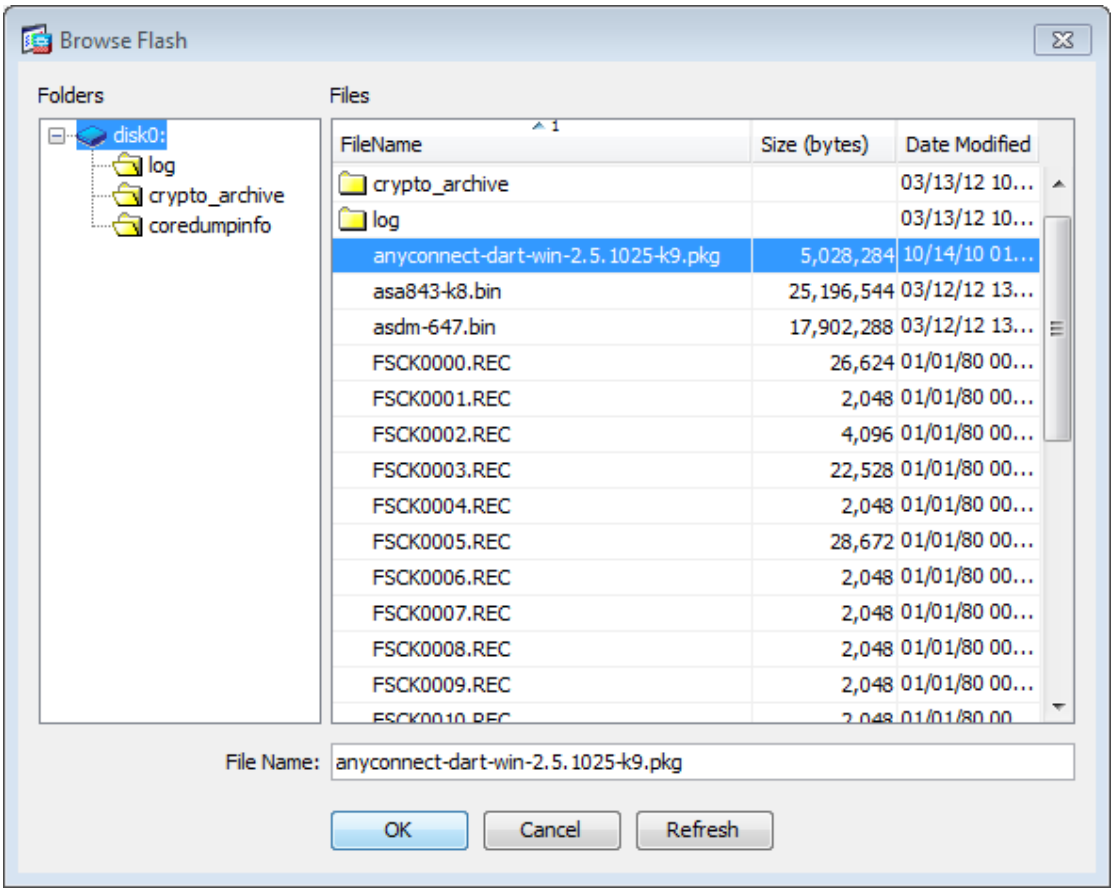

Abb. 25: Gewünschtes AnyCOnnect Image auswählen

Klicken Sie auf „Add“ → „Browse Flash…“ und wählen Sie das AnyConnect Image aus. Sollte die ASA kein AnyConnect Client Image auflisten, dann muss es zuerst mittels „Upload“ Button hochgeladen werden. Wenden Sie sich dafür bitte an das Laborpersonal.

Wie Sie sehen, steht die Software nicht allen zur Verfügung:

Download Cisco AnyConnect Image: http://www.cisco.com/cisco/software/

Log In and Service Contract Required

Pfad: Downloads Home > Products > Security > Virtual Private Networks (VPN) > Cisco VPN > Clients > Cisco AnyConnect VPN Client > Cisco AnyConnect VPN Client v2.x > AnyConnect VPN Client Software-2.5.3055

Linux: anyconnect-linux-2.5.3055-k9.pkg

Mac: anyconnect-macosx-i386-2.5.3055-k9.pkg

Windows: anyconnect-dart-win-2.5.3055-k9.pkg

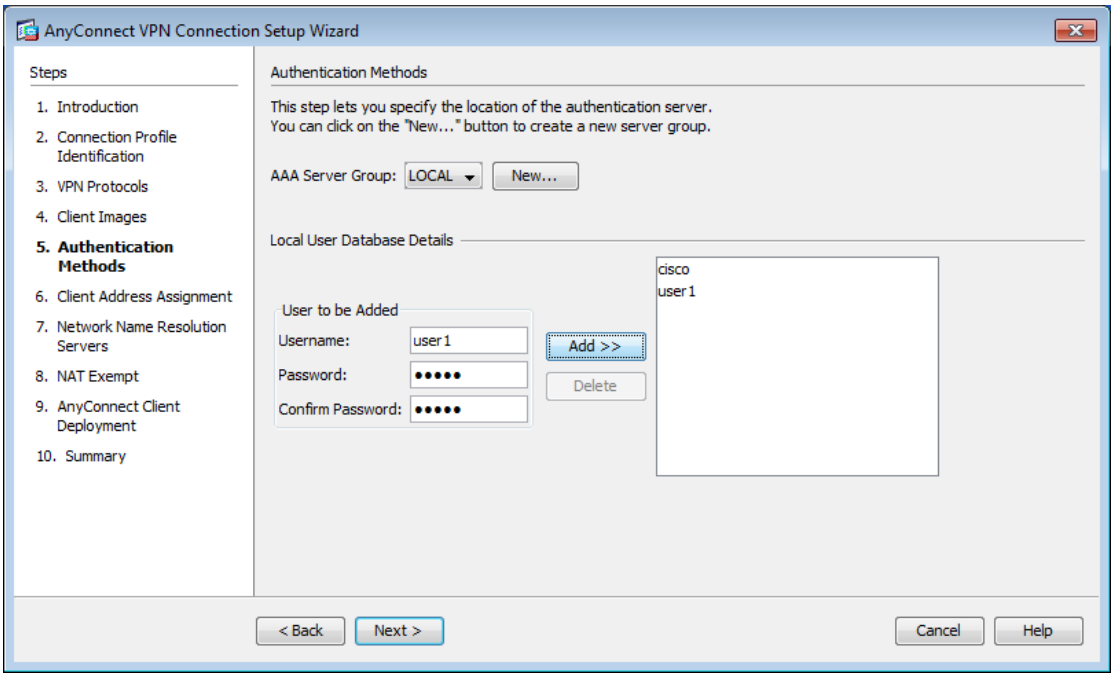

Abb. 26: Authentication Methods

Als nächstes gilt es, den Ort des Authentifizierungs-Servers zu wählen und einen ersten User der Datenbank hinzuzufügen. Die AAA Server Group wird als LOCAL belassen. Erstellen Sie nun einen neuen User. In diesem Beispiel wird er „user1“ genannt. Vergeben Sie ihm das sehr unsichere Passwort „cisco“. Ein Klick auf „Add“ fügt ihn der Datenbank zu.

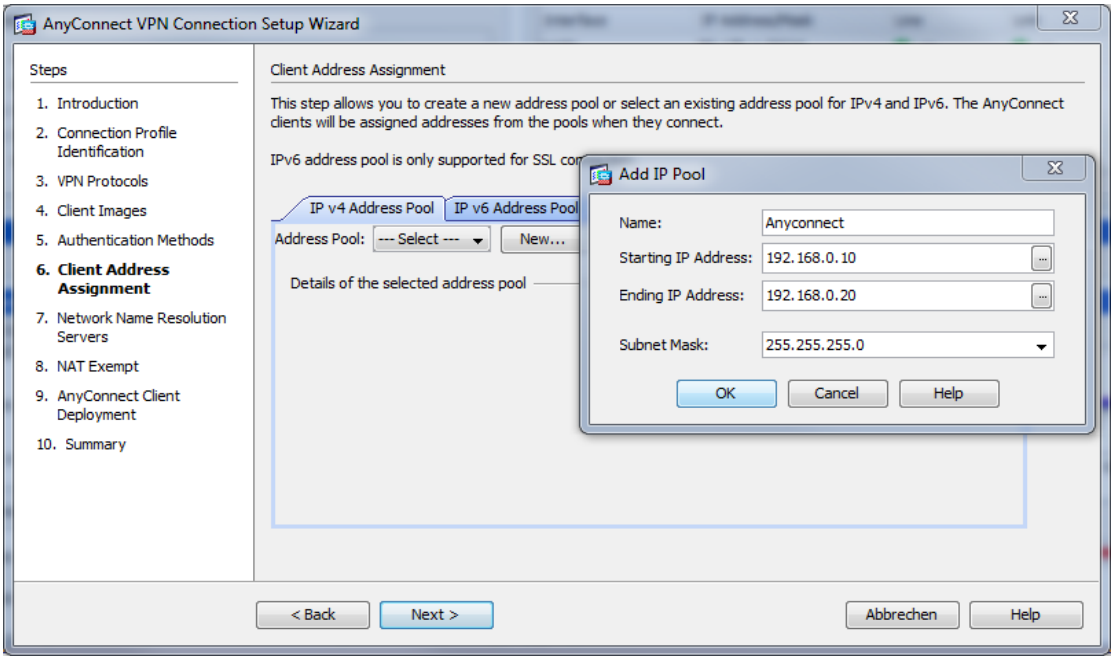

Abb. 27: IP Address Pool hinzufügen

Als nächstes muss ein IP Address Pool festgelegt werden. Jedem Remote-User wird beim Verbinden eine IP Adresse aus diesem Pool zugewiesen. Klicken Sie auf „New…“ und geben Sie die Daten, wie in Abb. 27, ein.

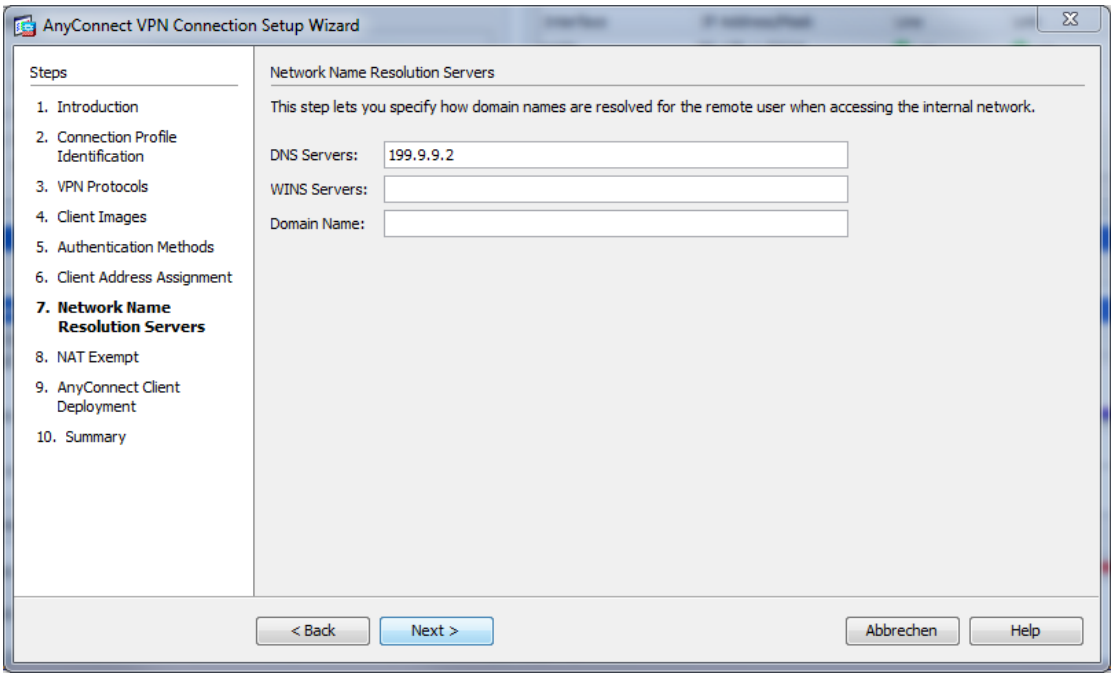

Abb. 28: DNS Server eintragen

Tragen Sie die IP des DNS Servers ein: 199.9.9.2

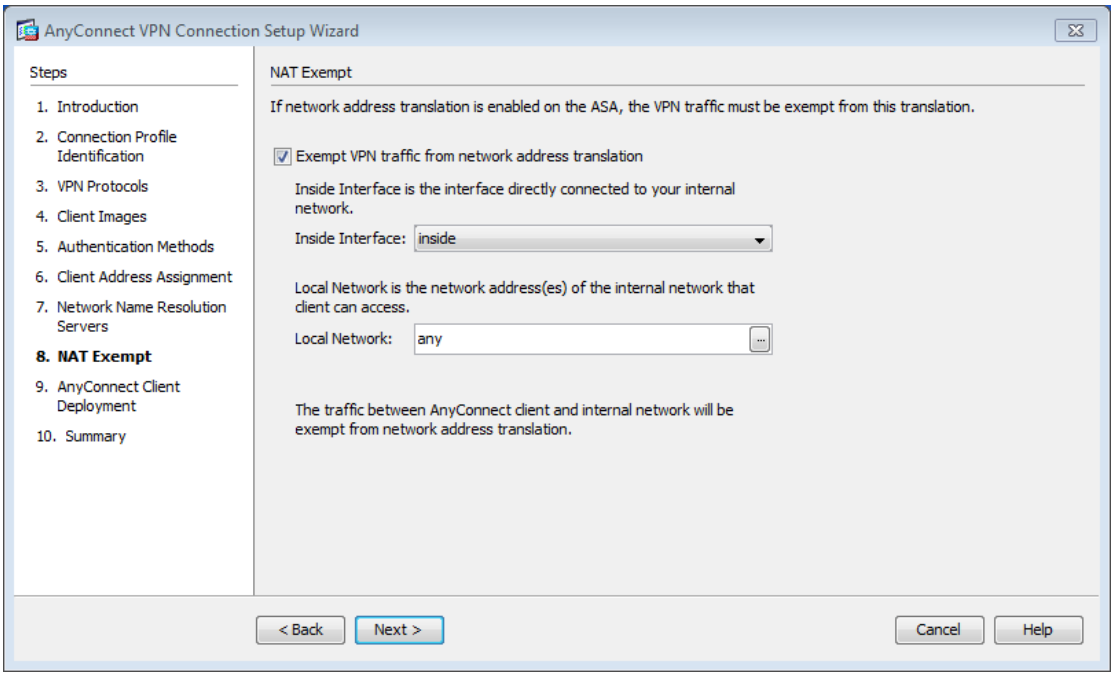

Abb. 29: NAT Ausnahme definieren

Da auf der ASA Luzern NAT eingeschaltet ist, muss dem Gerät noch mitgeteilt werden, dass kein NAT auf den VPN Verkehr angewendet werden soll.

Nehmen Sie die Einstellungen gemäss der obigen Abbildung vor.

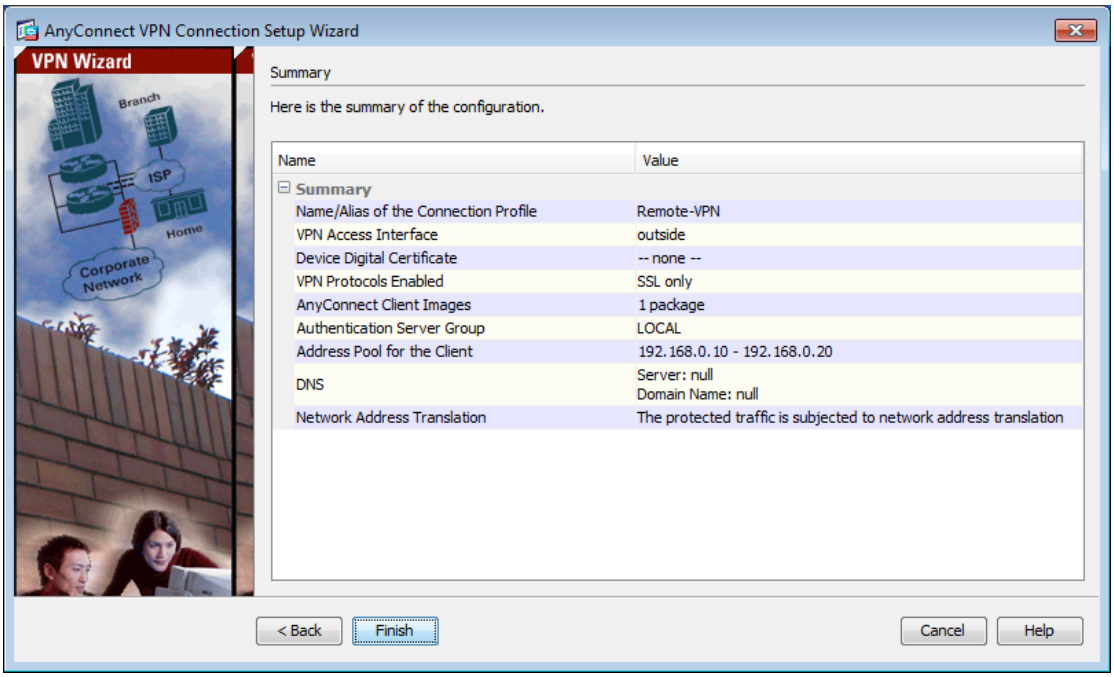

Abb. 30: Zusammenfassung der Konfiguration

Klicken Sie auf „Finish“ und speichern Sie die Konfiguration.

7.3 Testen

Um zu testen, ob alles richtig konfiguriert ist, verbinden Sie Ihren Laptop mit dem ISP. Stellen Sie sicher, dass folgende Einstellungen am Laptop vorgenommen wurden:

IP-Adresse	133.3.3.2
Subnetzmaske	255.255.255.0
Standartgateway	133.3.3.1

Öffnen Sie nun einen Webbrowser und surfen Sie die ASA an:

https://199.9.9.2

Loggen Sie sich im folgenden Screen mit „user1“ und dem Passwort „cisco“ ein.

Es wird nun versucht, den AnyConnect Client zu installieren. Lassen Sie zu, dass der Browser das ActiveX Script ausführt und folgen Sie dem Installationsprozess. Manchmal kann die Installation etwas länger dauern. Glücklicherweise muss sie nur einmal ausgeführt werden.

Nach erfolgreicher Installation sollte sich am rechten Rand der Taskbar ein neues Icon befinden. Ein Klick darauf öffnet das Client Fenster:

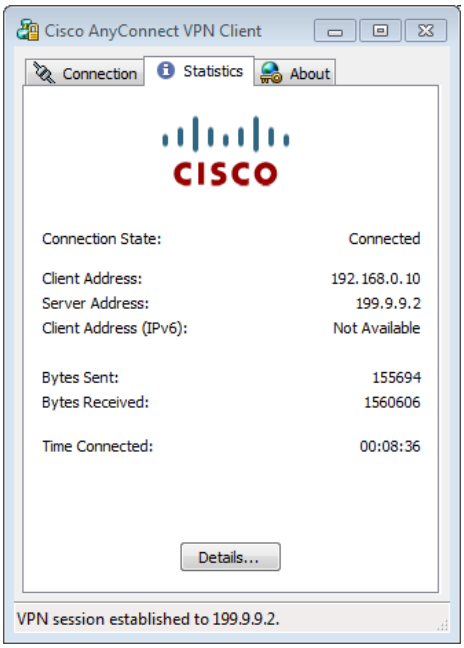

Abb. 31: AnyConnect VPN Client

Der „Connection State:“ sollte nun bereits „Connected“ anzeigen.

Versuchen Sie nun, den Mitarbeiter PC am Hauptsitz Luzern anzupingen. Erhalten Sie Antwort?

Wenn ja, gehen Sie zum nächsten Schritt über: Via Remote Desktop auf den Mitarbeiter PC zugreifen.

Gehen Sie wie folgt vor:

Führen Sie „mstsc.exe“ vom Laptop aus.

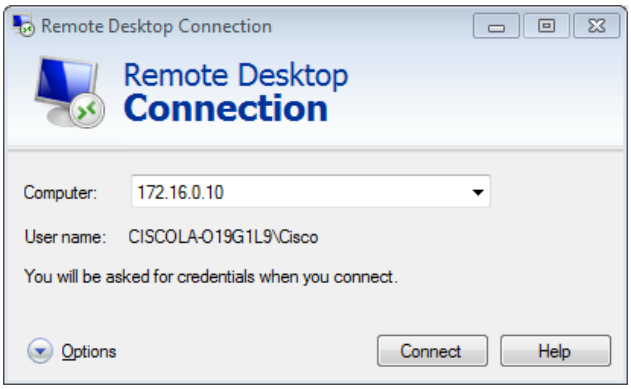

Abb. 32: Remotedesktopverbindung aufbauen

Geben Sie im Dialogfeld die IP des Mitarbeiter PCs ein. Ist die Verbindung erfolgreich, so sollten Sie nun nach dem Login Passwort des Mitarbeiters gefragt werden. Geben Sie „cisco“ ein und klicken Sie auf OK.

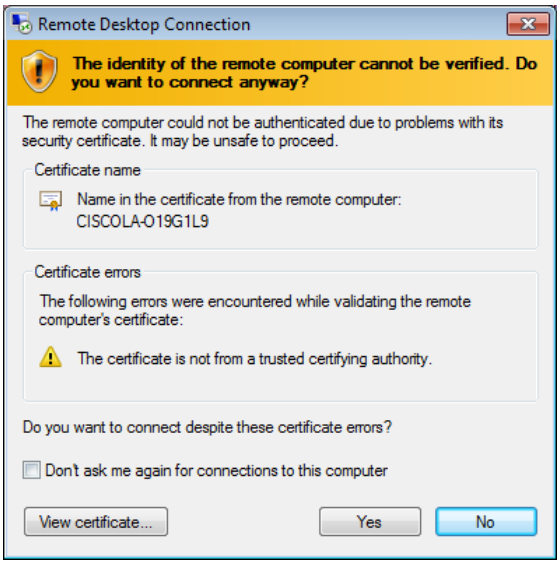

Abb. 33: Warnmeldung ignorieren

Klicken Sie bei der Verifizierungswarnung auf „Yes“.

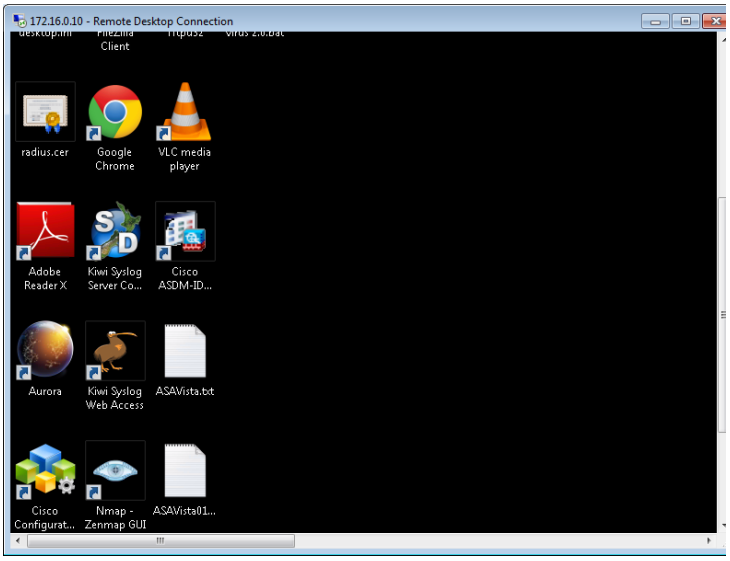

Abb. 34: Erfolgreicher Zugriff auf den PC des Mitarbeiters via Remotedesktopverbindung

Ein Fenster mit dem Desktop des anderen Mitarbeiters öffnet sich und Sie können nun direkt mit dem PC interagieren.

Tipp:

Falls Sie eine Fehlermeldung beim Verbindungsaufbau erhalten sollten, stellen Sie sicher, dass auf dem Mitarbeiter PC Remotedesktopverbindungen zugelassen sind:

Start → Systemsteuerung → System → Remoteeinstellungen

Im Tab „Remote“ müssen die Remoteunterstützung und der Remotedesktop zugelassen sein.

7.4 Kontrollfragen

- Ist es möglich mehrere AnyConnect-Sessions bei einer ASA gleichzeitig zu betreiben? Wenn ja, wie viele?
- Wäre es möglich auch hier den ASA mit einem Router zu ersetzen?

8 Zurücksetzen der Geräte

Sie sind am Ende angekommen. Stellen Sie sicher, dass Sie Ihre Konfigurationen auf allen Geräten, mit den folgenden Befehlen gelöscht haben.

ASA Startup Konfiguration	***write erase***
Router Startup Konfiguration	***write erase***

9 Anhang A - Theorie

[Quelle: CCNP Curriculum VPN 2003]

9.1 Anhang A.1 - Typen

Site-to-Site VPN verbindet die Filialen über eine öffentliche Infrastruktur.

- Intranet – Nur den Mitarbeitern des Unternehmens ist der Zugriff gestattet.
- Extranet – Mitarbeitern, Lieferanten, Geschäftspartnern ist der Zugriff gestattet.

Remote Access VPN ist an mobile Benutzer (Handy, Laptop) und Heimbüros gerichtet.

- Client-Initiated
- Network Access Server-Initiated

9.2 Anhang A.2 - Ziele

Ein privates Netzwerk gewährleistet Confidentiality, Integrity und Authentication (CIA). Ein virtuelles privates Netzwerk (VPN) nimmt sich die gleichen Ziele vor.

- **Geheimhaltung des Inhalts (Encryption)** – Der Sender verschlüsselt die Pakete, bevor er sie durch das Netzwerk übermittelt. Nur ein berechtigter Empfänger kann das Paket entpacken.
- **Datenintegrität (Hash)** – Der Empfänger überprüft, ob die ankommenden Daten während der Reise durch das Internet verändert wurden.
- **Authentifizierung des Senders** – Der Empfänger überprüft den Absender, woher das Paket kommt, und ob der Sender berechtigt war, Informationen mitzuteilen.

9.3 Anhang A.3 - VPN Protokolle

- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)
- IP Security (IPSec – Internet Layer)
- Generic Routing Encapsulation (GRE)
- Secure Sockets Layer (SSL – Transport Layer)
- Secure Shell (SSH – Application Layer)

9.4 Anhang A.4 - Vorteile gegenüber einer Mietleitung

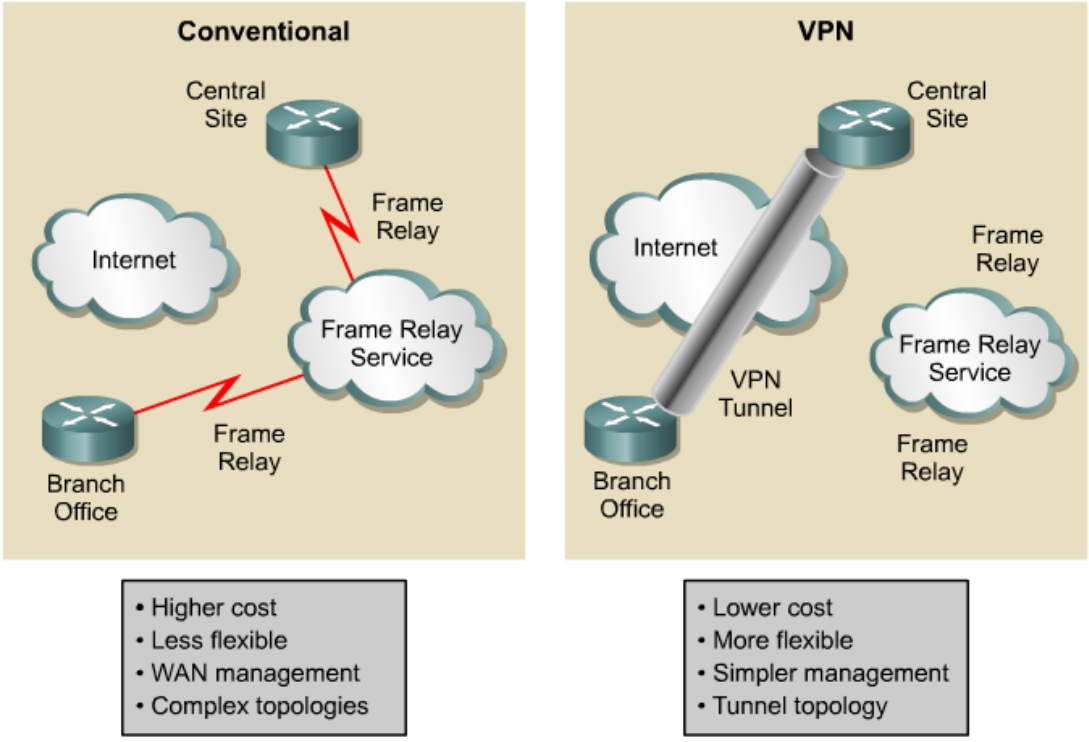

Abb. 35: Vorteile gegenüber einer traditionellen Mietleitung (Quelle: CCNP)

Früher brauchte man Mietleitungen (z.B. Anbieter Swisscom) für eine sichere Verbindung.

9.5 Anhang A.5 - Tunnel- und Transport Modus

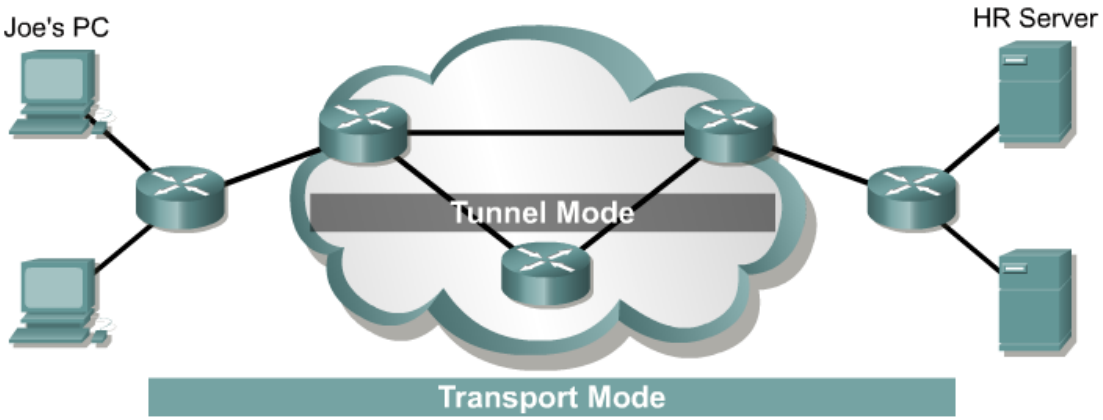

Abb. 36: Tunnel Mode, Transport Mode Unterschied (Quelle: CCNP)

Im **Transport-Modus (host-to-host)** führen die Host eine IPSec Verschlüsselung ihrer eigenen Daten durch. Auf jedem Host muss eine IPSec Konfiguration vorgenommen werden.

Im **Tunnel-Modus (peer-to-peer)** stellen die Gateways eine IPSec Verschlüsselung bereit.

9.6 Anhang A.6 - IPSec

IPSec ist ein Layer 3 Tunneling-Protokoll, bestehend aus drei Sicherheitsprotokollen:

Authentication Header (AH) garantiert die Integrität der Daten. Er kann nicht verhindern, dass die Daten gelesen werden. Der AH erkennt aber, ob die Daten verändert oder manipuliert wurden. Zusätzlich garantiert der AH auch die Authentifizierung des Absenders.
Für die Authentifizierung des Absenders und die Integrität der Daten werden Prüfsummen (Hash mit z.B. 128bit, 2^128 → 10^38) berechnet.

Encapsulation-Security-Payload (ESP) bietet die gleichen Sicherheitsfunktionen wie der AH. Zusätzlich bietet ESP die Vertraulichkeit der Daten, indem es die Daten gegen unbefugtes Lesen verschlüsselt.

Internet Key Exchange (IKE) ist ein Protokoll zur Herstellung einer sicheren Verbindung. Es verwaltet und tauscht authentifiziertes Schlüsselmaterial aus.

IKE baut auf drei Protokollen auf:

- Internet Security Association and Key Management Protocol (ISAKMP)
- Oakley
- SKEME

IKE ist so konzipiert, dass es unabhängig von den Verbindungsprotokollen ist und nicht nur für IPSec verwendet werden kann.

ISAKMP bietet eine Umgebung für Schlüsselaustauschverfahren und ist für die Verhandlung und die Verwaltung der Parameter (z.B. Encryption, Hash) und Mechanismen (Authentifizierungs-Methoden) zuständig. Es gibt diesbezüglich allerdings keine Vorgaben. Solche Vorgaben sind jedoch im Oakley und SKEME implementiert.

9.7 Anhang A.7 - Planungsblatt

Was kann das Gerät alles? Zuerst überprüft man die VPN Kompatibilität der einzelnen Geräte. Nicht alle Geräte unterstützen eine sehr starke Verschlüsselung oder einen bestimmten Algorithmus. Laut Cisco können sogar zwei gleiche Geräte mit unterschiedlicher IOS Version Kompatibilitäts-Mängel aufweisen.

9.8 Anhang A.8 - IKE (ISAKMP Policy)

Message Encryption Algorithm	des, 3des
Schützt die Verwaltungs-Informationen	aes-128, aes-192, aes-256
Message Integrity	md5
Hash-based Message Authentication Code (HMAC) Prüfsumme, Fehler bei Übertragung erkennen	sha
Peer Authentication Method	pre-share, rsa-sig, crack
Key Exchange Algorithm Erstellt eine Verbindung ohne jeweils den richtigen Schlüssel zu übermitteln.	D-H Group 1, 2, 5
Session Lifetime	86400s = 24h, frei wählbar

9.9 Anhang A.9 - Phase 2, IPSec Transform Set

Nach dem Verbindungsaufbau schütz IPSec den Datenaustausch zwischen den zwei Peers.

Mode	Tunnel, Transport
ESP Encryption	des, 3des aes-128, aes-192, aes-256 null
ESP Authentication Ein Hash Algorithmus um die Daten zu authentifizieren.	md5 sha none
Perfect Forward Secrency (PFS) Generiert einen unabhängigen Schlüssel	on / off D-H Group 1, 2, 5

10 Anhang B - Troubleshooting

10.1 Anhang B.1 - Generell

- Der Ping Befehl ermöglicht einen einfachen Test der Verbindung. Dazu gibt man Ping und die Zieladresse ein. Der Befehl funktioniert auf allen Geräten.
- Wireshark ist ein nützliches Tool zur Beobachtung des Netzwerk Verkehrs. Starten Sie das Programm (auf allen Workstations vorinstalliert), wählen Sie die korrekte Netzwerkkarte aus und geben Sie beim Filter „ICMP“ ein. Der Filter sorgt dafür, dass nur der Ping Befehl beobachtet wird.
- Richtiges Kabel ausgewählt? Gerades Kabel oder gekreuztes Kabel?
- Kabel austauschen – Es kann vorkommen, dass ein Kabel defekt ist.

10.2 Anhang B.2 - Packet Tracer

Packet Tracer ist ein im ASDM integriertes Tool. Es kann genutzt werden, um beispielsweise den Weg eines Pings zu simulieren (siehe Abb. 37). Man sieht z.B. ob ein Paket von der ASA überhaupt auf eine NAT Regel (NAT Lookup) zutrifft oder durch den VPN Tunnel (VPN Lookup) geht.

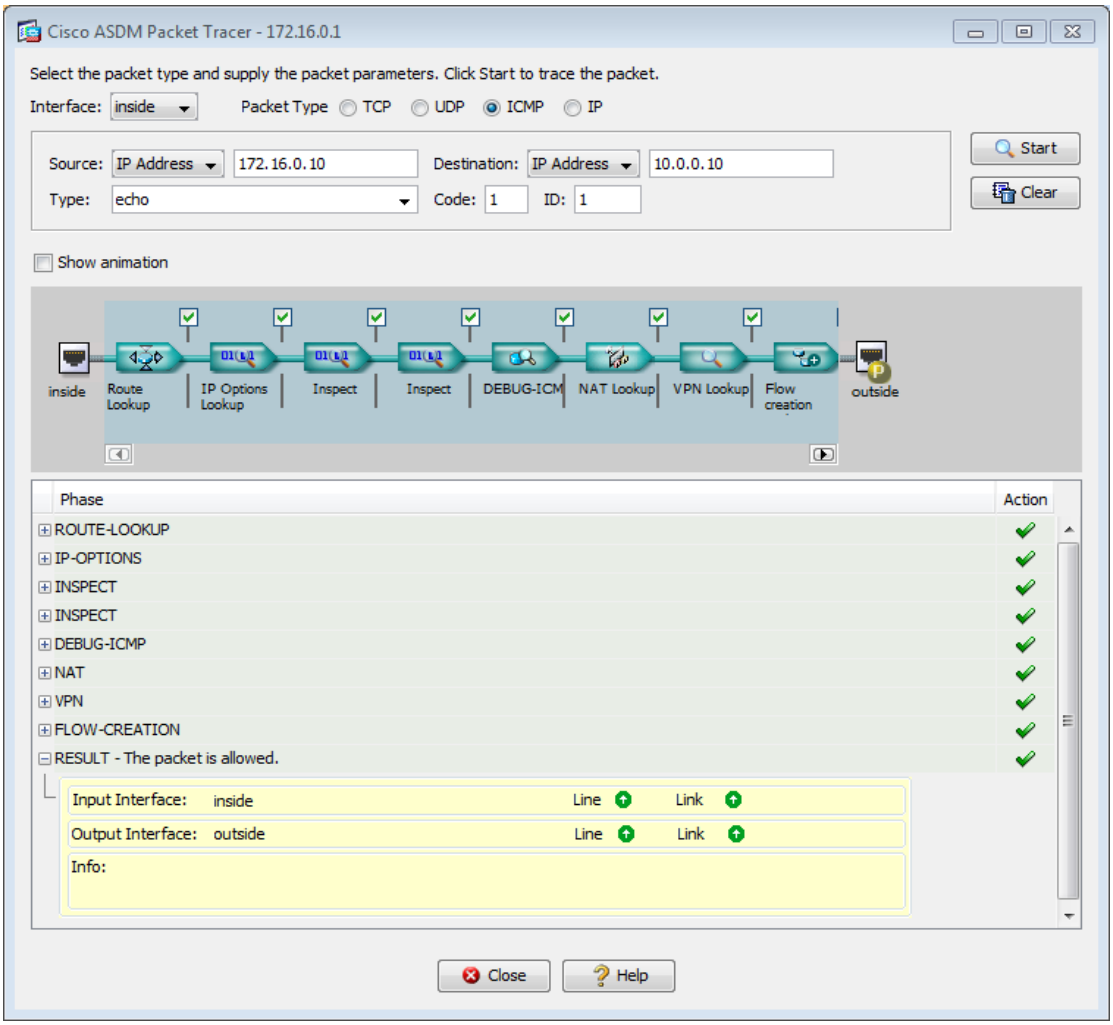

Abb. 37: ASDM Packet Tracer

10.3 Anhang B.3 - AnyConnect Sessions

Beim AnyConnect Versuch können maximal zwei Sessions aktiv sein. Dies ist bereits der Fall, wenn zur Installation des Clients im Webbrowser auf die ASA und danach im Client eingeloggt wurde. Jeder weitere Login Versuch gibt eine Fehlermeldung zurück.

Um die Sessions frei zu geben, geht man im ASDM auf Monitoring, Sessions und klickt unten auf Logout Sessions.

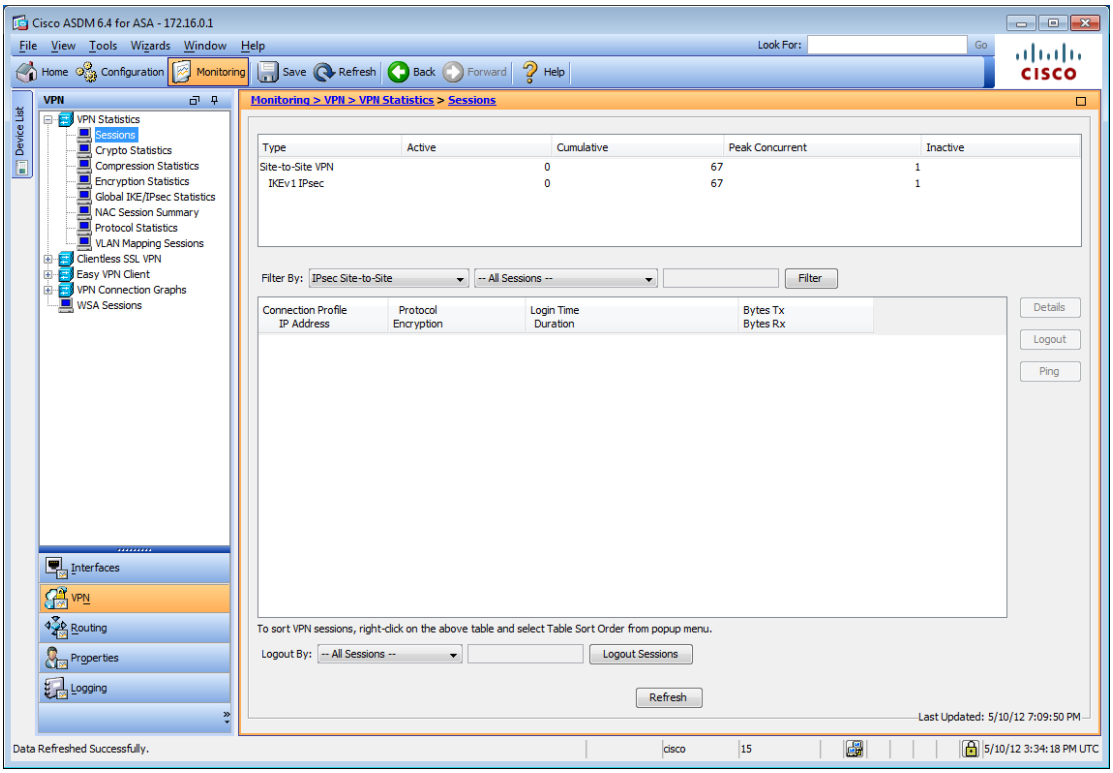

Abb. 38: VPN Sessions

Als Standard sollte der Client ausgeloggt werden. Falls er dies nicht tut, kann die Methode über den ASDM als letzter Ausweg gesehen werden.

10.4 Anhang B.4 - Router

- show ip interface brief
- ping
- show running-config
- show crypto isakmp policy
- show crypto map
- show crypto ipsec transform-set

10.5 Anhang B.5 - ASA

- show interface ip brief
- debug crypto isakmp 4
- clear ipsec sa löscht die laufende VPN Verbindung
- debug icmp trace sorgt dafür, dass im Command-line interface der ASA (Teraterm, Putty) angezeigt wird, wenn ein Ping ankommt. Dadurch erkennt man, ob ein Ping überhaupt bis zur ASA kommt.
- Ob bei der ASA eine VPN Verbindung besteht, kann man leicht an der dafür vorgesehenen Anzeige erkennen.

Abb. 39: Vorderseite ASA

10.6 Anhang B.6 - Host

- Ping von beiden Seiten – Die VPN Verbindung baut sich erst nach einem erstmaligen Austausch auf, z.B. durch einen Ping von einem Host zum anderen. Achtung: Cisco hat einen Bug, bei dem der Aufbau nur von einer Seite aufgebaut werden kann. Ob eine Verbindung besteht, ist leicht am markierten LED der Abb. 1, zu erkennen. → beide Seiten sollten den Ping versuchen.
- Wird ein privater Computer genutzt, müssen die Firewall und andere Netzwerkadapter (z.B. Wireless) deaktiviert werden, da es sonst zu Konflikten kommen kann.
- Tracert zeigt die IP Route eines Pakets bis zum Zielhost. Die erste Zahl steht für die Anzahl Hops.

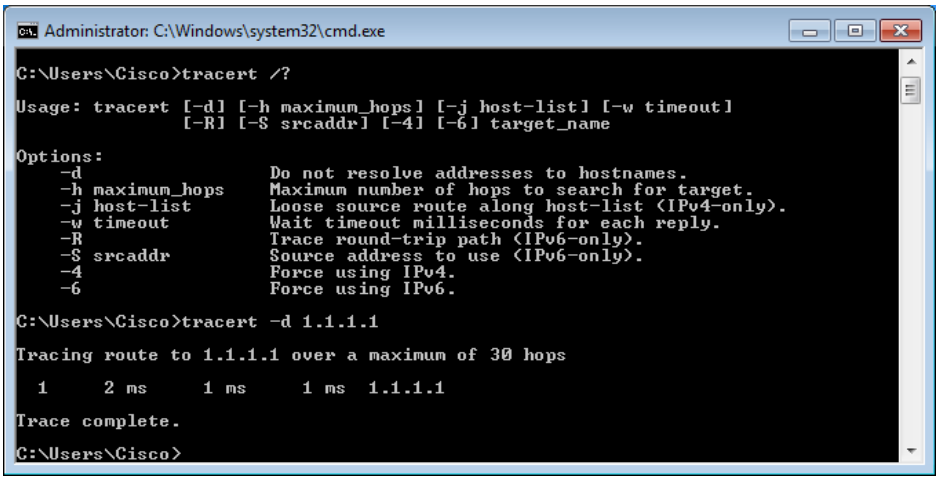

Abb. 40: Tracert Befehl

11 Anhang C - VPN Glossary

[Quelle: CCNP Curriculum VPN 2003]

Die folgenden Ausdrücke sind in VPNs und IPSec Themen geläufig.

- **Authentication** – The process of identifying a user or process attempting to access a computer system or network connection. Authentication ensures that the individual or process is who he, she, or it claims to be. Authentication does not confer associated access rights.
- **Authentication, Authorization, and Accounting (AAA)** – The network security services that provide the primary framework through which access control is set up on routers or access servers. Two major alternatives for AAA are TACACS+ and RADIUS.
- **Authentication Header (AH)** – A security protocol that provides data authentication, data integrity, and optional anti-replay services. AH is embedded in the data to be protected.

- **Authorization** – The process of giving authenticated individuals or processes access to computer system or network connection resources.
- **Certificate of Authority (CA) service** – A third-party service that is trusted to help secure the communications between network entities or users by creating and assigning digital certificates, such as public-key certificates, for encryption purposes. A CA vouches for the binding between the data security items in the certificate. Optionally, a CA creates user's encryption keys.
- **Cryptosystem** – A system to accomplish the encryption/decryption, user authentication, hashing, and key-exchange processes. A cryptosystem may use one of several different methods, depending on the policy intended for various user traffic situations.
- **Data Encryption Standard (DES)** is used to encrypt and decrypt packet data. Both IPSec and IKE use DES. DES uses a 56-bit key to ensure high performance encryption.
- **Diffie-Hellman (DH)** is a public-key cryptography algorithm. It enables two parties to establish a shared secret key over an insecure communications channel. D-H is used within IKE to establish session keys. ASA supports 768-bit, 1024-bit and 1536-bit D-H groups. The 1536-bit group is more secure.
- **Encapsulating Security Payload (ESP)** – A security protocol which provides data confidentiality, data integrity, and protection services, optional data origin authentication, and anti-replay services. ESP encapsulates the data to be protected.
- **Encryption/decryption** – Encryption is the process of transforming information content called clear text, or plain text, into a hidden form called cyphertext so that it will not be readable or usable by unauthorized users. Decryption transforms cyphertext back into clear, or plain, text so that it is accessible for reading or use by authorized users.
- **Hashing** – A data integrity technology that uses a formula or algorithm to convert a variable length message and shared secret key into a single fixed-length string of digits. The message/key and hash travel the network from source to destination. At the destination the recalculated hash is used to verify that the message and key have not changed while traveling the network.
- **Internet Key Exchange (IKE)** – A hybrid protocol that implements Oakley key exchange and Skeme key exchange inside the ISAKMP framework. Oakley and SKEME each define a method to establish an authenticated key exchange. This includes payload construction, the information payloads carried, the order in which keys are processed and how the keys are used.
- **Internet Security Association and Key Management Protocol (ISAKMP)** – A protocol framework that defines payload formats, the mechanics of implementing a key exchange protocol, and the negotiation of an SA.
- **Key management** – A key is information, usually a sequence of random or seemingly random binary digits, used initially to set up and periodically to change the operations performed in a cryptosystem. Key management is the supervision and control of the process whereby keys are generated, stored, protected, transferred, loaded, used, and destroyed.
- **MD5** is an algorithm used to authenticate and provide integrity of packet data by hashing the message digest. A hash is a one-way encryption algorithm that takes an input message of arbitrary length and produces a fixed-length output message. If a message has been altered, an MD5 hash will not be equal on both sides of the tunnel, alerting administrators to a message being corrupted. IKE, AH, and ESP can use MD5 for authentication.
- **Remote Authentication Dial-In User Service (RADIUS)** – A distributed client/server system that secures networks against unauthorized access.

- **RSA** is a public-key cryptographic system used for authentication. Public-key cryptography works by sharing only a public key but retaining a private key that can decipher the encryption of the public key. The public key can decipher information encrypted by the private key to provide for authentication of the sender.
- **Security Association (SA)** – A set of policy and key(s) used to protect information. The ISAKMP SA is the shared policy and key(s) used by the negotiating peers in this protocol to protect their communication.
- **SHA-1** is a secure hash algorithm used to authenticate packet data. ASA uses the SHA-1 Hash-based Message Authentication Code (HMAC) variant, which provides an additional level of hashing. IKE, AH, and ESP can use SHA-1 for authentication.
- **Terminal Access Controller Access Control System Plus (TACACS+)** – A security application that provides centralized validation of users attempting to gain access to a router or network access server.
- **Tunnel** – A virtual point-to-point connection used in a network to carry traffic from one protocol encapsulated inside another protocol. For example, encrypted cyphertext carried in an IP packet.

12 Anhang D - Passwort Recovery Prozedur

Es kann vorkommen, dass die Router mit einem anderen Passwort als cisco versehen sind. Folgen Sie in diesem Fall der unten stehenden Anleitung.

Router

1. Verwenden Sie immer cisco als Passwort.
2. Bevor Sie mit der Recovery-Prozedur anfangen versuchen Sie folgende Passwörter zuerst:
   a. Cisco
   b. cisco (mit Leerschlag am Ende)
   c. class
   d. cisco12345
   e. user01 / user01pass
   f. admin01 / admin01pass
   g. admin / adminpa55
3. Falls keine der oben genannten Passwörter funktioniert, starten Sie mit der Password Recovery Prozedur.
4. Starten Sie den Router neu.
5. In den ersten 10 Sekunden des Boot-Vorganges senden Sie mit dem Terminal-Client einen Break (die Break Sequenz kann von Terminal zu Terminal unterschiedlich sein. (Mit TeraTerm ist sie Ctrl+B)
6. Der Router wird in das rommon: booten
7. Setzen Sie den Configuration Register auf 0x2142 und starten Sie den Router erneut:

```
rommon 1 > confreg 0x2142
rommon 2 > reset
```

8. Nach dem Bootvorgang löschen Sie den startup-config und setzen Sie den Configuration Register auf 0x2102 zurück:

```
Router# delete nvram:startup-config
Router# conf t
Router(config)# config-register 0x2102
Router(config)# end
Router# write
```

9. Starten Sie mit dem Versuch.