

# ASA-to-ASA Dynamic-to-Static IKEv1/IPsec-Konfigurationsbeispiel

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[ASDM-Konfiguration](#)

[Central-ASA \(Static Peer\)](#)

[Remote-ASA \(Dynamic Peer\)](#)

[CLI-Konfiguration](#)

[Zentrale ASA-Konfiguration \(Static Peer\)](#)

[Remote-ASA \(Dynamic Peer\)](#)

[Überprüfen](#)

[Zentrale ASA](#)

[Remote-ASA](#)

[Fehlerbehebung](#)

[Remote-ASA \(Initiator\)](#)

[Central-ASA \(Responder\)](#)

[Zugehörige Informationen](#)

## Einführung

In diesem Dokument wird beschrieben, wie die Adaptive Security Appliance (ASA) in die Lage versetzt wird, dynamische IPsec-Site-to-Site-VPN-Verbindungen von einem beliebigen dynamischen Peer (in diesem Fall ASA) zu akzeptieren. Wie das Netzwerkdiagramm in diesem Dokument zeigt, wird der IPsec-Tunnel erstellt, wenn der Tunnel nur vom Remote-ASA-Ende aus initiiert wird. Die Central-ASA kann aufgrund der dynamischen IPsec-Konfiguration keinen VPN-Tunnel initiieren. Die IP-Adresse von Remote-ASA ist unbekannt.

Konfigurieren Sie Central-ASA, um Verbindungen von einer Wild-Card-IP-Adresse (0.0.0.0/0) und einem vorinstallierten Wild-Card-Schlüssel dynamisch zu akzeptieren. Die Remote-ASA wird dann so konfiguriert, dass der Datenverkehr von lokalen Subnetzen zu zentralen ASA-Subnetzen verschlüsselt wird, wie in der Crypto Access List angegeben. Beide Seiten führen eine Network Address Translation (NAT)-Ausnahme aus, um NAT für IPsec-Datenverkehr zu umgehen.

## Voraussetzungen

## Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

## Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Firewall-Software Cisco ASA (5510 und 5520), Version 9.x und höher.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Konfigurieren

**Hinweis:** Verwenden Sie das [Command Lookup Tool](#) (nur [registrierte](#) Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

## Netzwerkdiagramm



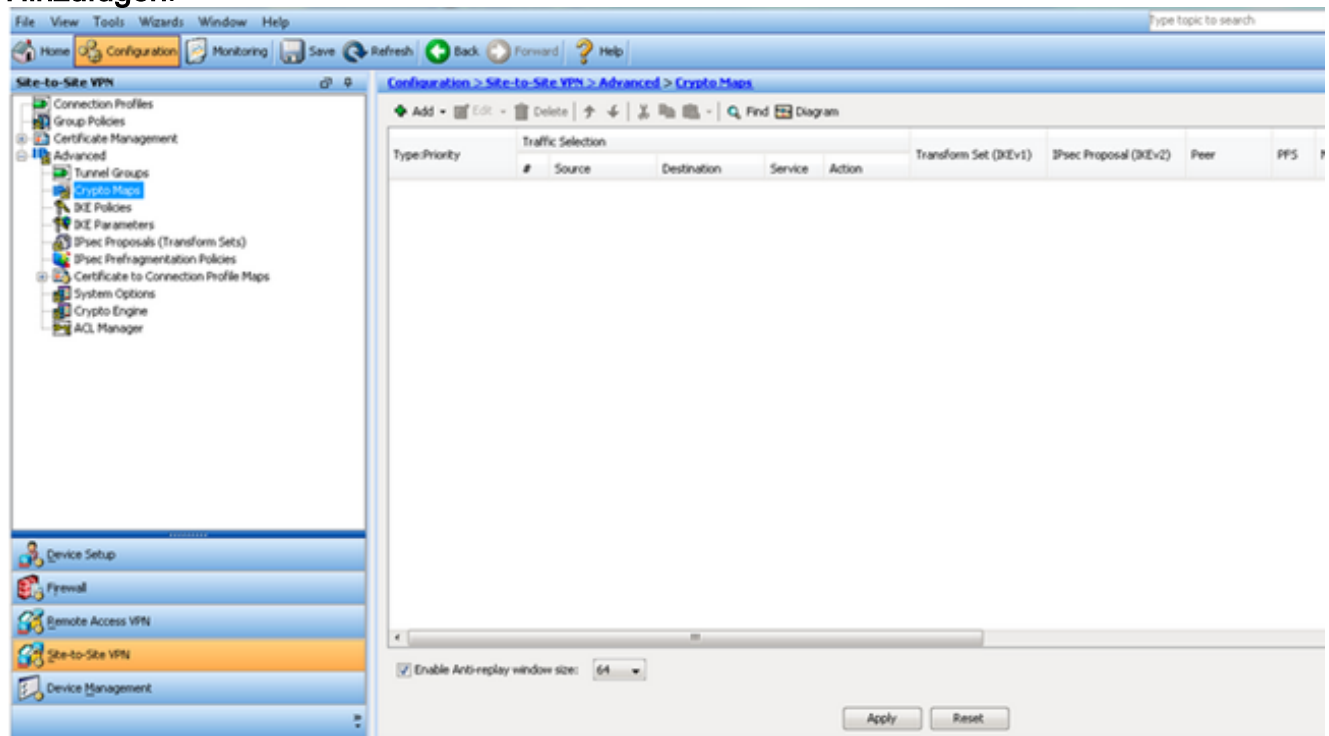
## ASDM-Konfiguration

### Central-ASA (Static Peer)

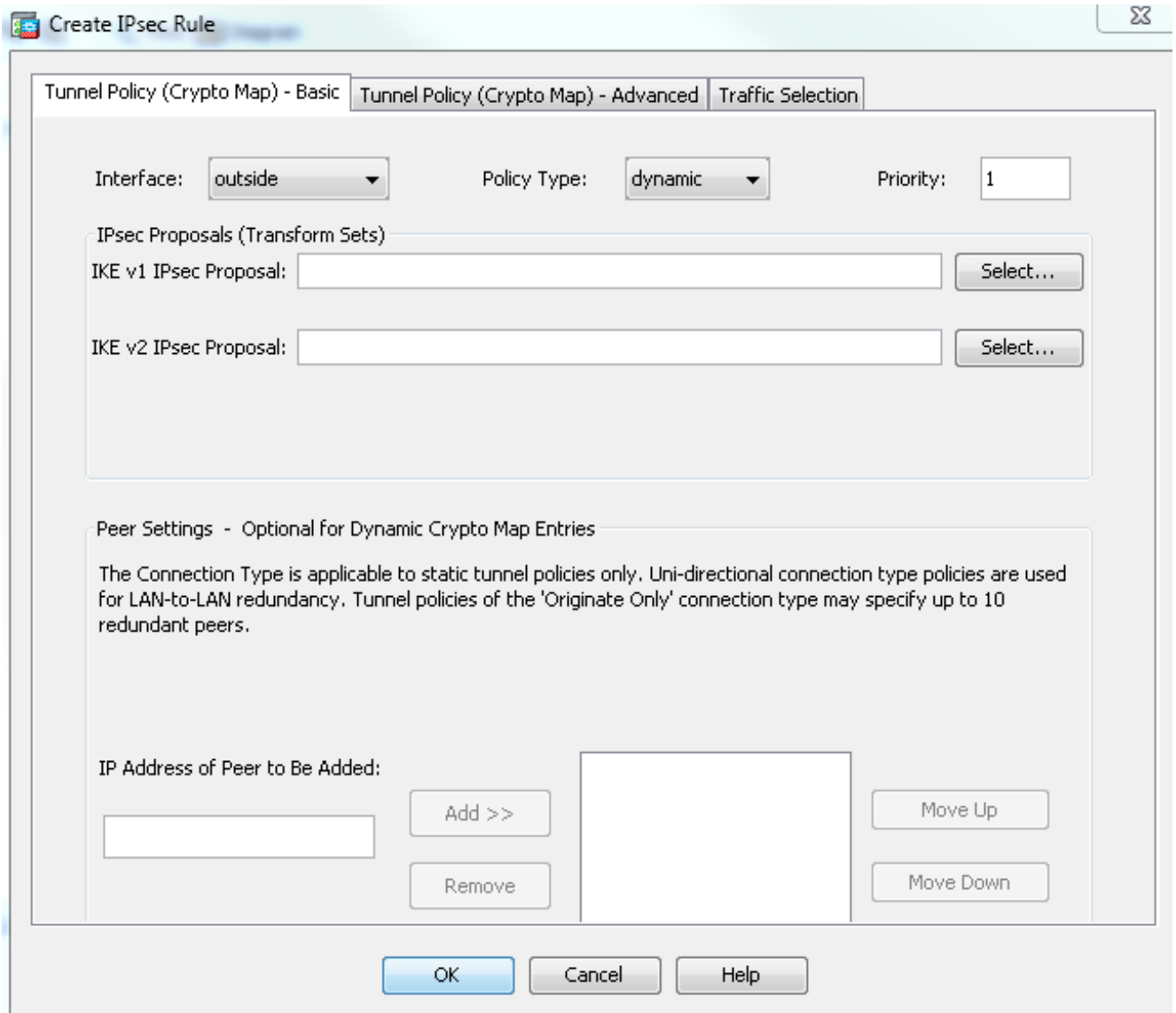
Richten Sie das VPN auf einer ASA mit einer statischen IP-Adresse so ein, dass es dynamische Verbindungen von einem unbekanntem Peer akzeptiert, während es den Peer weiterhin mithilfe eines vorinstallierten IKEv1-Schlüssels authentifiziert:

1. Wählen Sie **Configuration > Site-to-Site VPN > Advanced > Crypto Maps** aus. Das Fenster zeigt eine Liste der bereits vorhandenen Krypto-Map-Einträge an (sofern vorhanden). Da die ASA die Peer-IP-Adresse nicht kennt, muss die **dynamische Zuordnung** der Verbindung mit dem passenden Configurationssatz konfiguriert werden (IPsec-Vorschlag), damit die ASA die Verbindung akzeptiert. Klicken Sie auf

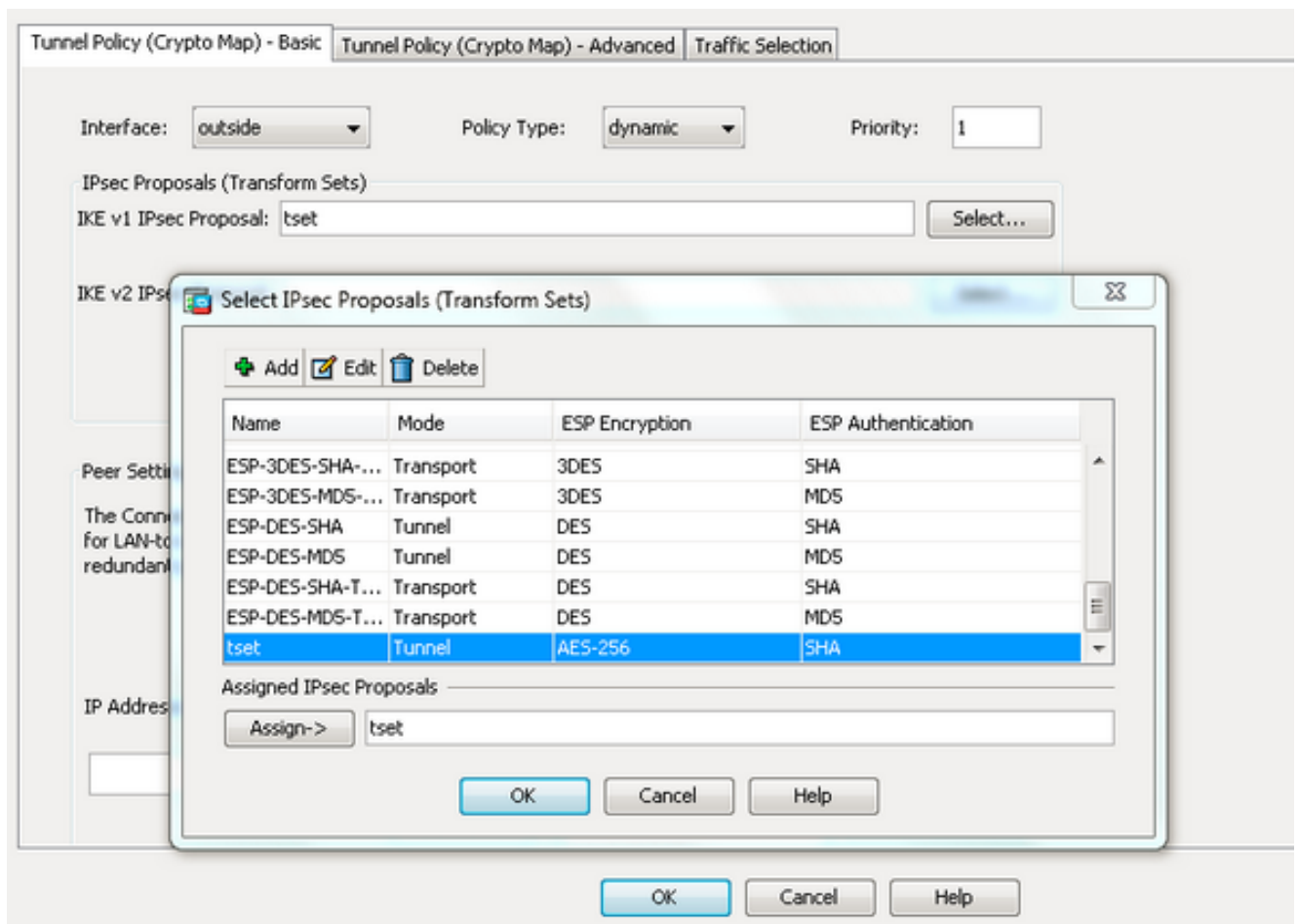
## Hinzufügen.



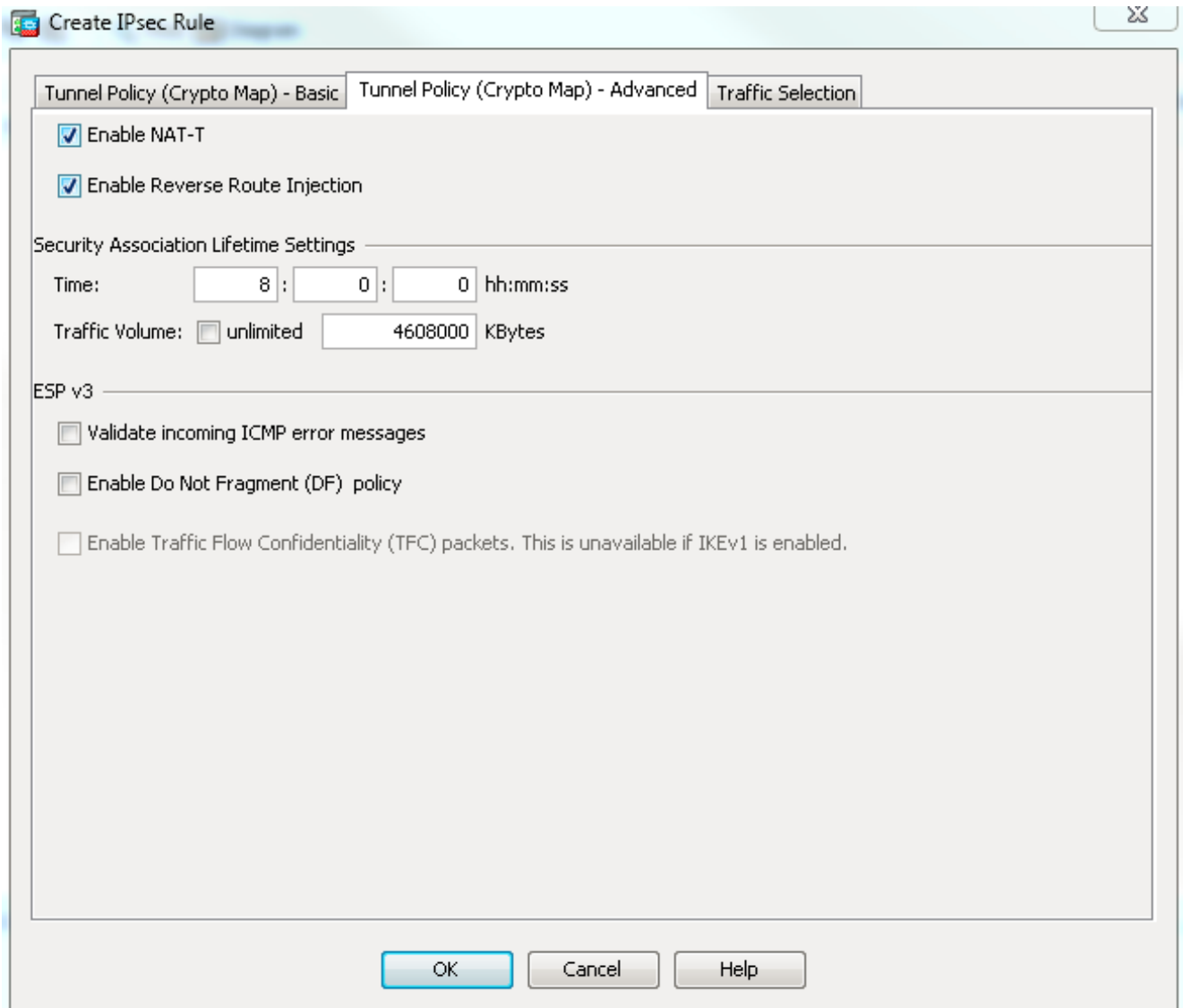
2. Wählen Sie im Fenster Create IPsec Rule (IPsec-Regel erstellen) auf der Registerkarte Tunnel Policy (Crypto Map) - Basic (Tunnelrichtlinie) - Basic (IPsec-Regel erstellen) **außerhalb** der Dropdown-Liste Interface (Schnittstelle) und **dynamic (Dynamisch)** aus der Dropdown-Liste Policy Type (Richtlinientyp) aus. Weisen Sie im Feld Priorität die Priorität für diesen Eintrag zu, falls unter Dynamic Map mehrere Einträge vorhanden sind. Klicken Sie anschließend neben dem Feld "IPsec Proposal" (IPsec-Angebot für IKE v1) auf **Select (Auswählen)**, um das IPsec-Angebot auszuwählen.



3. Wenn das Dialogfeld IPsec-Vorschläge auswählen (Transform Sets) geöffnet wird, wählen Sie unter den aktuellen IPsec-Vorschlägen aus, oder klicken Sie auf **Hinzufügen**, um ein neues Angebot zu erstellen und das gleiche zu verwenden. Klicken Sie abschließend auf **OK**.



4. Aktivieren Sie auf der Registerkarte Tunnel Policy (Crypto Map)-Advanced (Tunnelrichtlinie (Crypto Map)-Advanced (Erweitert) das Kontrollkästchen **Enable NAT-T** (Aktivieren von NAT-T, wenn sich einer der Peers hinter einem NAT-Gerät befindet), und das Kontrollkästchen **Enable Reverse Route Injection**. Wenn der VPN-Tunnel für den dynamischen Peer aktiviert wird, installiert ASA eine dynamische Route für das ausgehandelte Remote-VPN-Netzwerk, die auf die VPN-Schnittstelle zeigt.



Optional können Sie auf der Registerkarte Traffic Selection (Datenverkehrsauswahl) auch den interessanten VPN-Datenverkehr für den dynamischen Peer definieren und auf **OK** klicken.

Tunnel Policy (Crypto Map) - Basic | Tunnel Policy (Crypto Map) - Advanced | **Traffic Selection**

Action:  Protect  Do not Protect

Source Criteria

Source: any4

Destination Criteria

Destination: any4

Service: ip

Description:

**More Options**

Enable Rule

Source Service: (TCP or UDP service only) ⓘ

Time Range:

OK

Cancel

Help

**Configuration > Site-to-Site VPN > Advanced > Crypto Maps**

+ Add | Edit | Delete | ↑ ↓ | Copy | Paste | Find | Diagram

Type:Priority	Traffic Selection					Transform Set (IKEv1)
	#	Source	Destination	Service	Action	
interface: outside						
dynamic: 65535.1	1	any4	any4	IP ip	Protect	tset

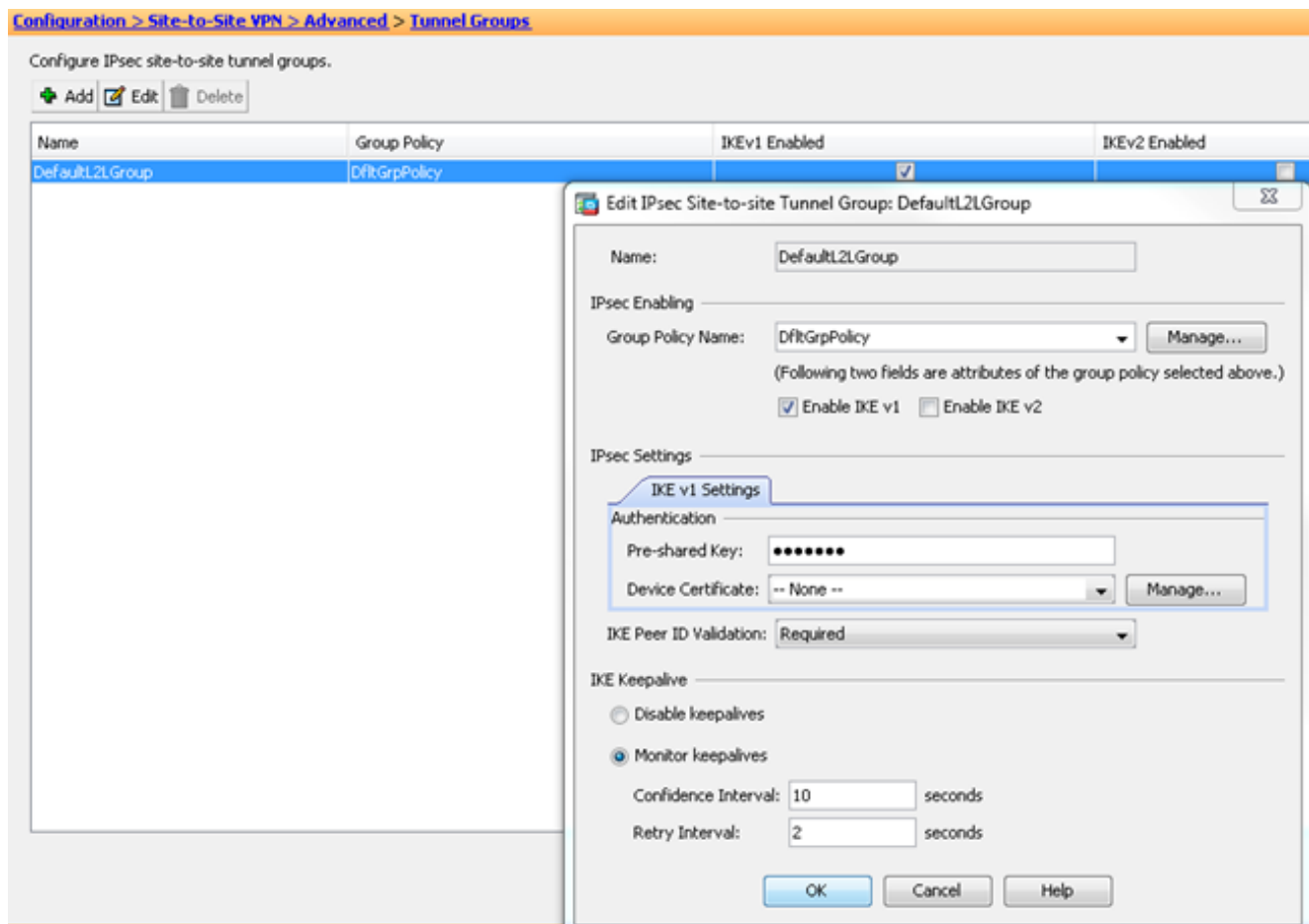
Enable Anti-replay window size: 64

Apply Reset

Da ASA über keine Informationen über die Remote-IP-Adresse des dynamischen Peers verfügt, wird die unbekannte Verbindungsanforderung standardmäßig unter DefaultL2LGroup gespeichert, das auf ASA standardmäßig vorhanden ist. Damit die Authentifizierung den vorinstallierten Schlüssel (in diesem Beispiel cisco123) übernimmt, der auf dem Remote-Peer konfiguriert wurde, muss dieser mit dem vorinstallierten Schlüssel unter DefaultL2LGroup übereinstimmen.

- Wählen Sie **Configuration > Site-to-Site VPN > Advanced > Tunnel Groups**, wählen Sie **DefaultL2LGroup aus**, klicken Sie auf **Edit** und konfigurieren Sie den gewünschten vorinstallierten Schlüssel. Klicken Sie abschließend auf **OK**.





**Hinweis:** Dadurch wird ein vorinstallierter Platzhalterschlüssel auf dem statischen Peer (Central-ASA) erstellt. Alle Geräte/Peers, die diesen vorinstallierten Schlüssel und die entsprechenden Vorschläge kennen, können erfolgreich einen VPN-Tunnel einrichten und auf Ressourcen über VPN zugreifen. Stellen Sie sicher, dass dieser vordefinierte Schlüssel nicht für unbekannte Personen freigegeben ist und nicht leicht zu erraten ist.

6. Wählen Sie **Configuration > Site-to-Site VPN > Group Policies (Konfiguration > Standortübergreifende Gruppenrichtlinien)** und wählen Sie die Gruppenrichtlinie Ihrer Wahl aus (in diesem Fall die Standardgruppenrichtlinie). Klicken Sie auf **Bearbeiten** und bearbeiten Sie die Gruppenrichtlinie im Dialogfeld Richtlinie für interne Gruppen bearbeiten. Klicken Sie abschließend auf **OK**.

**Configuration > Site-to-Site VPN > Group Policies**

Manage VPN group policies. A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. Policy information is referenced by VPN connection profiles and user accounts.

To enforce authorization attributes from an LDAP server you must use an [LDAP attribute map](#).

 Add  Edit  Delete  Assign

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
DfltGrpPolicy (System Default)	Internal	Ikev1;ssl-clientless;l2tp-ipsec	DefaultRAGroup;DefaultWEBVPNGroup;

**Edit Internal Group Policy: DfltGrpPolicy**

Name:

Tunneling Protocols:  Clientless SSL VPN  SSL VPN Client  IPsec IKEv1  IPsec IKEv2  L2TP/IPsec

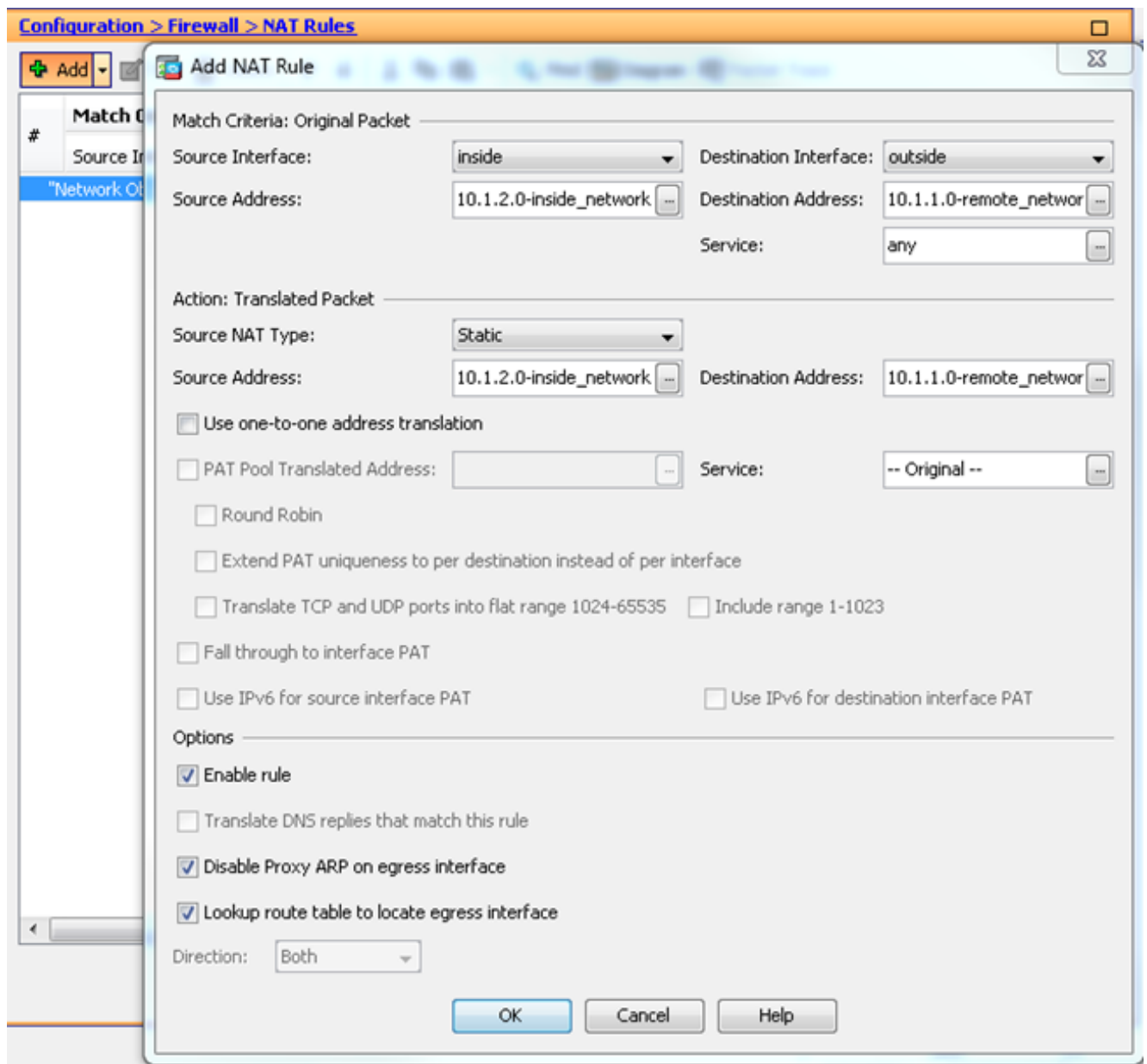
Filter:

Idle Timeout:  Unlimited  minutes

Maximum Connect Time:  Unlimited  minutes

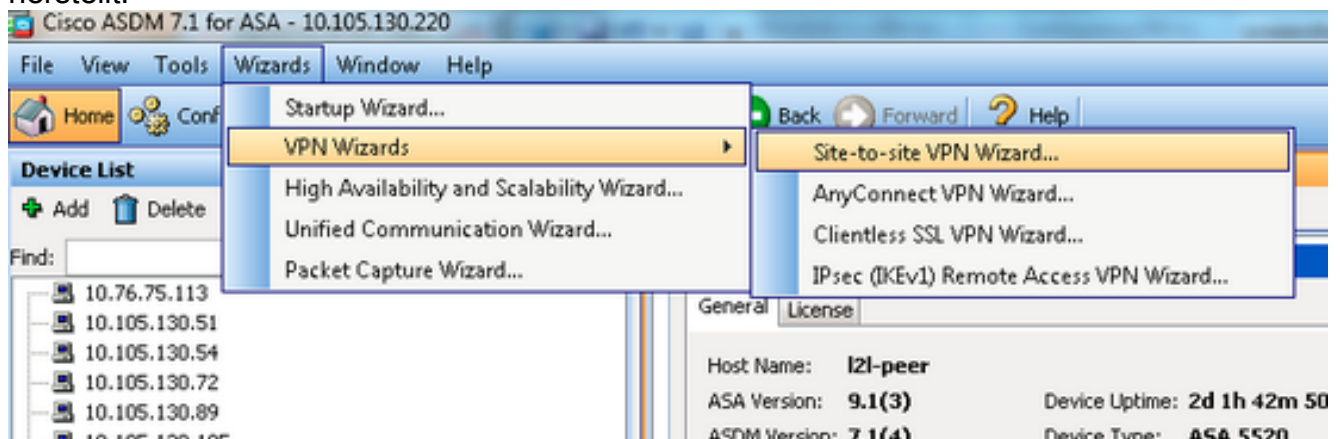
Find:     Match Case

7. Wählen Sie **Configuration > Firewall > NAT Rules** aus, und konfigurieren Sie im Fenster Add Nat Rule (NAT-EXEMPT hinzufügen) eine No nat-Regel für VPN-Datenverkehr. Klicken Sie abschließend auf **OK**.



## Remote-ASA (Dynamic Peer)


1. Wählen Sie **Wizards > VPN Wizards > Site-to-Site VPN Wizard**, sobald die ASDM-Anwendung eine Verbindung mit der ASA herstellt.



2. Klicken Sie auf **Weiter**.


Site-to-site VPN Connection Setup Wizard

### VPN Wizard



**Introduction**

Use this wizard to setup new site-to-site VPN tunnel. A tunnel between two devices is called a site-to-site tunnel and is bidirectional protects the data using the IPsec protocol.



Here is a [video](#) on how to setup a site-to-site VPN connection.

< Back   Next >

3. Wählen Sie **außerhalb** aus der Dropdown-Liste VPN Access Interface (VPN-Zugriffsschnittstelle) aus, um die externe IP-Adresse des Remote-Peers anzugeben. Wählen Sie die Schnittstelle (**WAN**) aus, auf die die Crypto Map angewendet wird. Klicken Sie auf **Weiter**.

Site-to-site VPN Connection Setup Wizard

**Steps**

1. Introduction
2. **Peer Device Identification**
3. Traffic to protect
4. Security
5. NAT Exempt
6. Summary

**Peer Device Identification**

This step lets you identify the peer VPN device by its IP address and the interface used to access the peer.

Peer IP Address:

VPN Access Interface:

< Back   Next >

4. Geben Sie die Hosts/Netzwerke an, die den VPN-Tunnel passieren dürfen. In diesem Schritt müssen Sie die lokalen Netzwerke und Remote-Netzwerke für den VPN-Tunnel bereitstellen. Klicken Sie auf die Schaltflächen neben den Feldern "Lokales Netzwerk" und "Remote Network" (Remote-Netzwerk), und wählen Sie die gewünschte Adresse aus. Klicken Sie

abschließend auf  
**Weiter.**

The screenshot shows the 'Traffic to protect' step of the Site-to-site VPN Connection Setup Wizard. On the left, a 'Steps' sidebar lists: 1. Introduction, 2. Peer Device Identification, 3. Traffic to protect (highlighted), 4. Security, 5. NAT Exempt, and 6. Summary. The main area is titled 'Traffic to protect' and contains the text: 'This step lets you identify the local network and remote network between which the traffic is to be protected using IPsec encryption.' Below this, there are two radio buttons for 'IP Address Type': 'IPv4' (selected) and 'IPv6'. There are two text input fields: 'Local Network' with the value '10.1.1.0/24' and 'Remote Network' with the value '10.1.2.0/24'. At the bottom, there are '< Back' and 'Next >' buttons.

5. Geben Sie die zu verwendenden Authentifizierungsinformationen ein, d. h. den vorinstallierten Schlüssel in diesem Beispiel. Der in diesem Beispiel verwendete Pre-Shared Key ist cisco123. Der Tunnelgruppenname ist standardmäßig die IP-Adresse des Remote-Peers, wenn Sie ein LAN-to-LAN (L2L)-VPN konfigurieren.

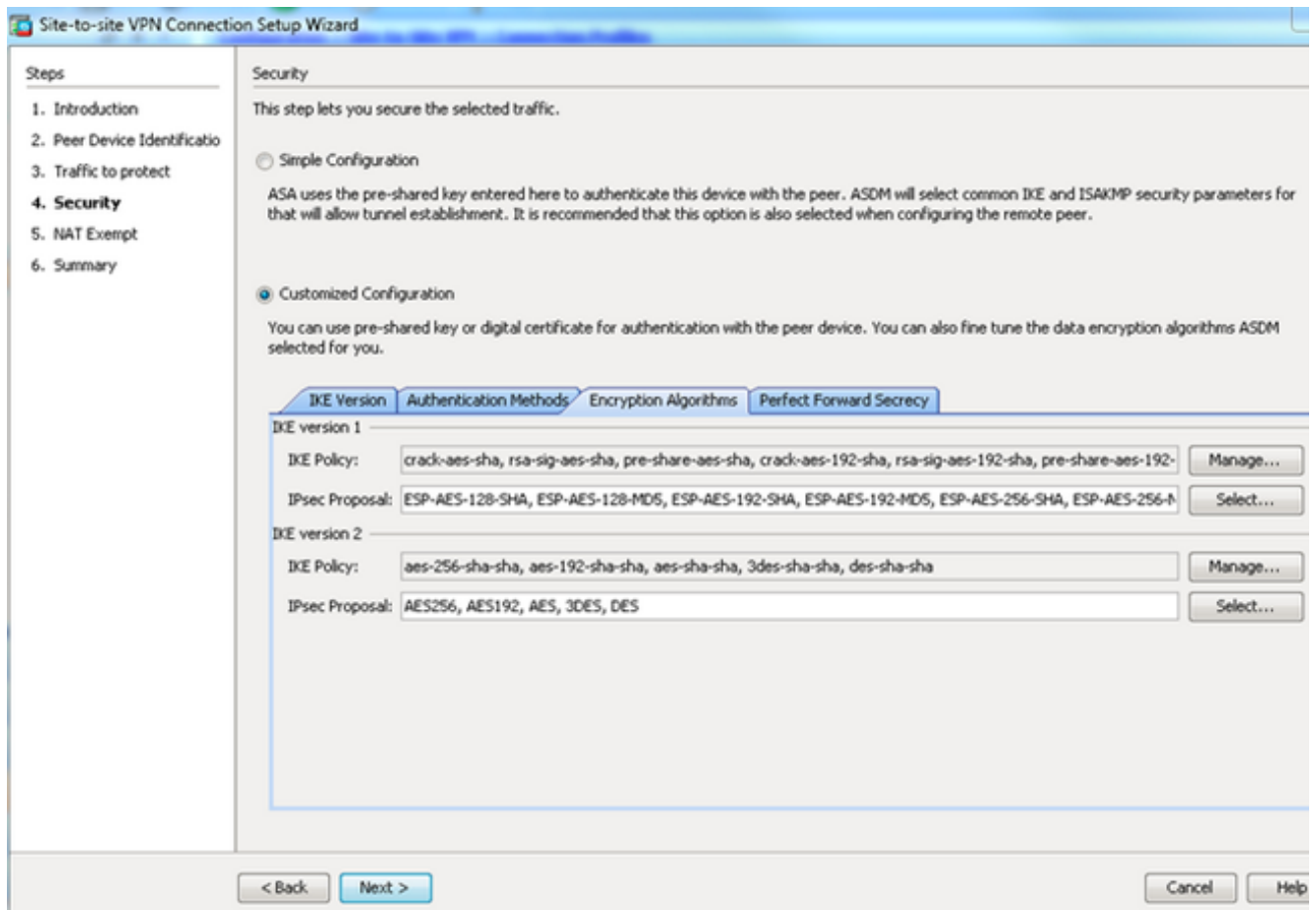
The screenshot shows the 'Security' step of the Site-to-site VPN Connection Setup Wizard. On the left, the 'Steps' sidebar lists: 1. Introduction, 2. Peer Device Identification, 3. Traffic to protect, 4. Security (highlighted), 5. NAT Exempt, and 6. Summary. The main area is titled 'Security' and contains the text: 'This step lets you secure the selected traffic.' There are two radio buttons: 'Simple Configuration' (selected) and 'Customized Configuration'. Below 'Simple Configuration', there is a text input field for 'Pre-shared Key' containing seven dots. Below 'Customized Configuration', there is a paragraph of text: 'You can use pre-shared key or digital certificate for authentication with the peer device. You can also fine tune the data encryption algorithms ASDM selected for you.' At the bottom, there are '< Back', 'Next >', 'Cancel', and 'Help' buttons.

**ODERS** Sie können die Konfiguration so anpassen, dass sie die IKE- und IPsec-Richtlinie Ihrer Wahl enthält. Es muss mindestens eine Übereinstimmungsrichtlinie zwischen den Peers geben: Geben Sie auf der Registerkarte Authentifizierungsmethoden den vorinstallierten IKE-Schlüssel der Version 1 in das Feld Vorinstallierter Schlüssel ein. In diesem Beispiel ist dies

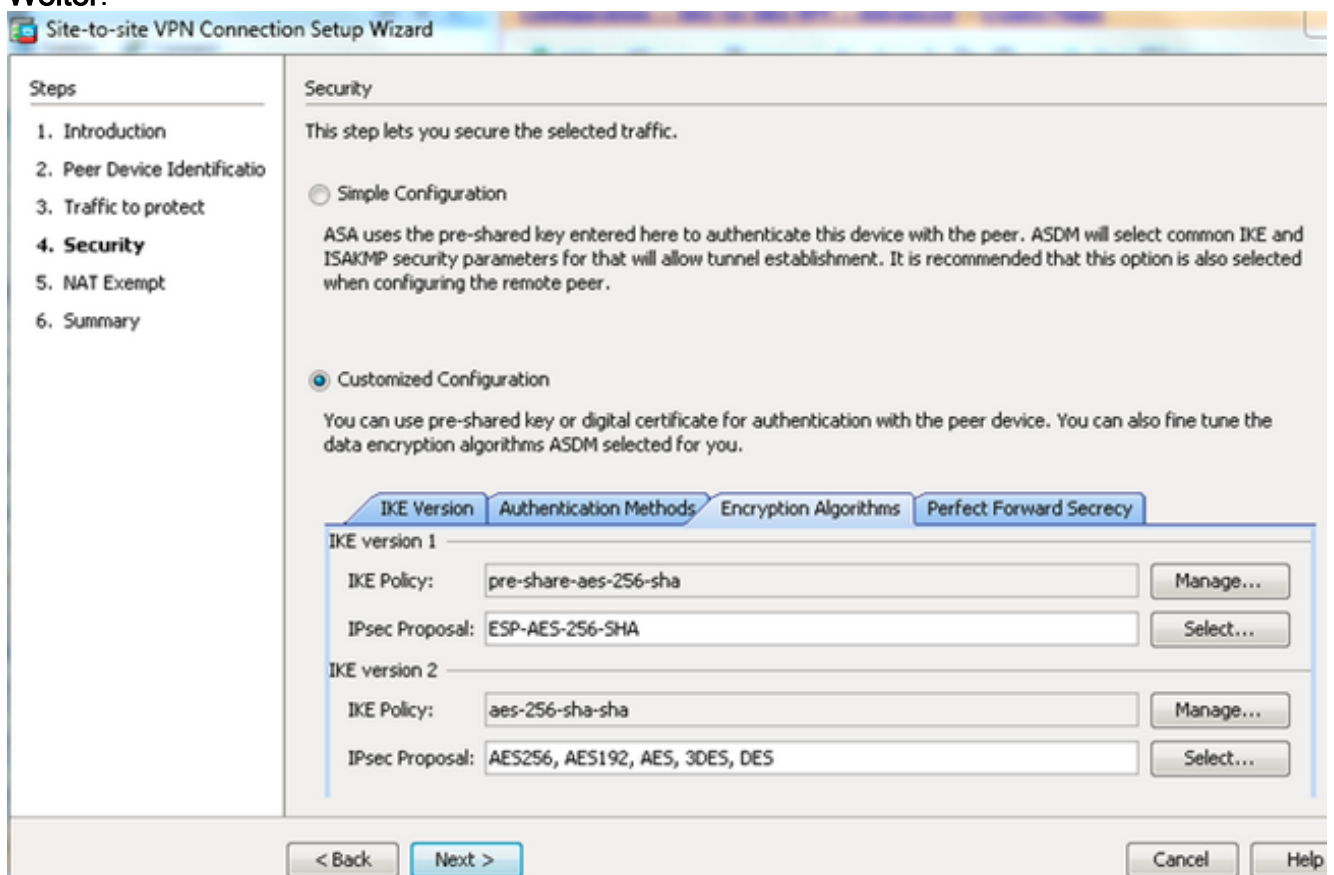
The screenshot shows the 'Security' step of the 'Site-to-site VPN Connection Setup Wizard'. The left sidebar lists the steps: 1. Introduction, 2. Peer Device Identification, 3. Traffic to protect, 4. Security (selected), 5. NAT Exempt, and 6. Summary. The main area is titled 'Security' and contains two radio button options: 'Simple Configuration' and 'Customized Configuration'. The 'Customized Configuration' option is selected. Below this, there are four tabs: 'IKE Version', 'Authentication Methods', 'Encryption Algorithms', and 'Perfect Forward Secrecy'. The 'IKE Version' tab is active, showing configuration for 'IKE version 1' and 'IKE version 2'. For 'IKE version 1', there is a 'Pre-shared Key' field with masked characters, a 'Device Certificate' dropdown menu set to '-- None --', and a 'Manage...' button. For 'IKE version 2', there are four options: 'Local Pre-shared Key' (selected), 'Local Device Certificate' (dropdown set to '-- None --'), 'Remote Peer Pre-shared Key' (text field), and 'Remote Peer Certificate Authentication' (checkbox set to 'Allowed'). Each of these four options has a 'Manage...' button. At the bottom of the wizard, there are '< Back', 'Next >', 'Cancel', and 'Help' buttons.

Klicken Sie auf die Registerkarte **Verschlüsselungsalgorithmen**.

6. Klicken Sie neben dem Feld "IKE-Richtlinie" auf **Verwalten**, klicken Sie auf **Hinzufügen** und konfigurieren Sie eine benutzerdefinierte IKE-Richtlinie (Phase-1). Klicken Sie abschließend auf **OK**.



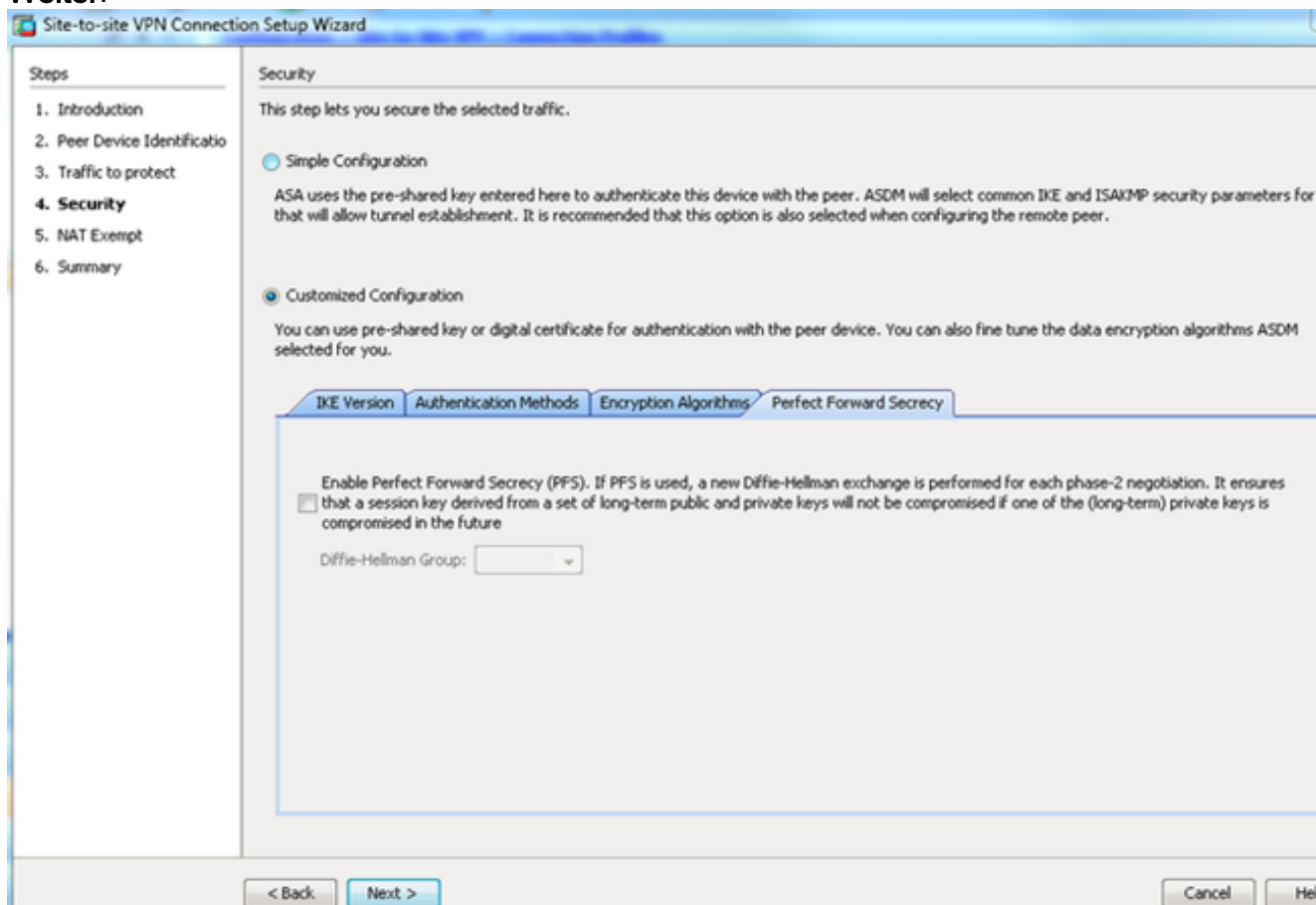
7. Klicken Sie neben dem Feld "IPsec Proposal" (IPsec-Angebot) auf **Select (Auswählen)**, und wählen Sie das gewünschte IPsec-Angebot aus. Klicken Sie abschließend auf **Weiter**.



Optional können Sie auf die Registerkarte Perfect Forward Secrecy (Perfect Forward-Geheimhaltungsgrad) gehen und das Kontrollkästchen **Enable Perfect Forward Secrecy**

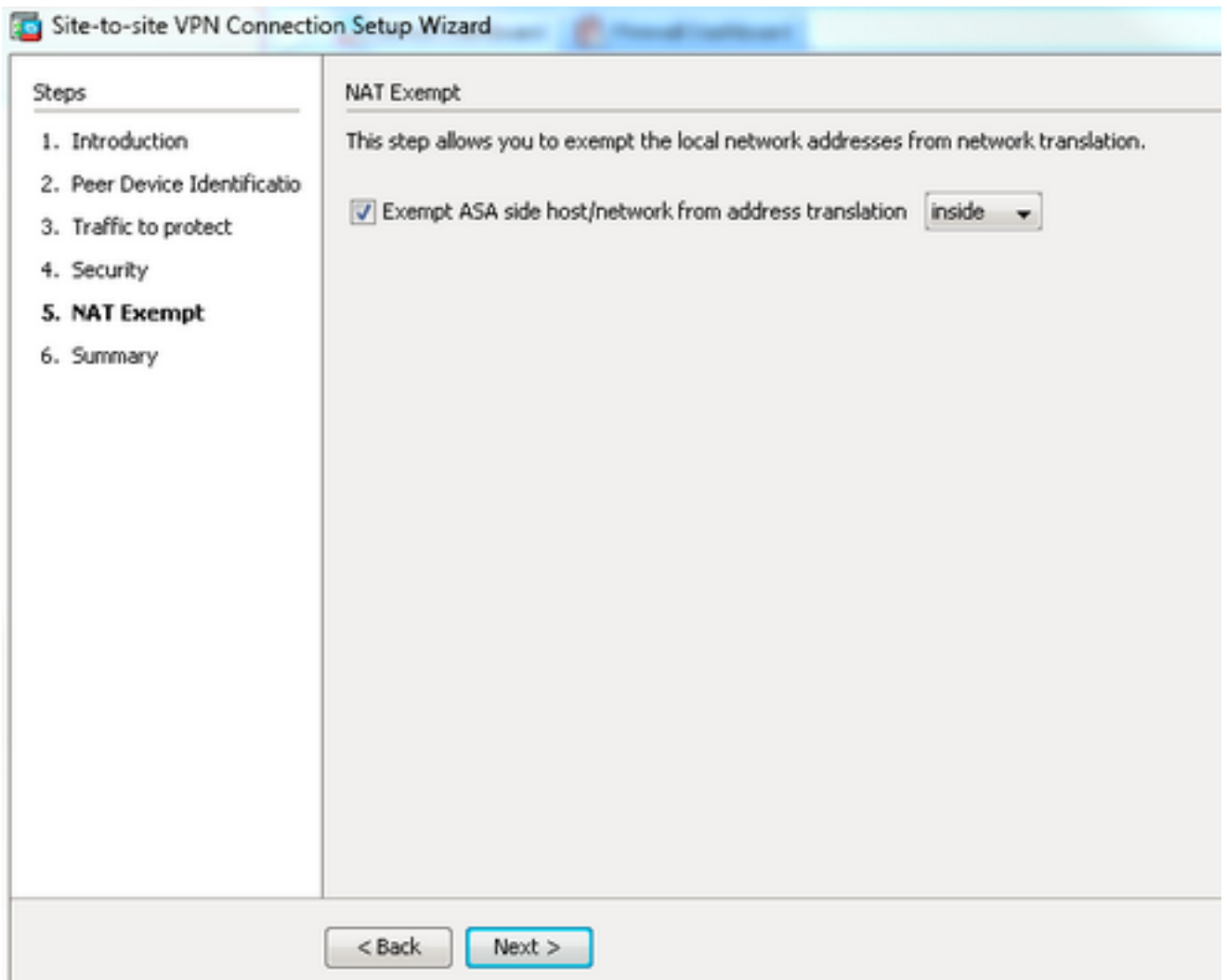


(PFS) aktivieren. Klicken Sie abschließend auf **Weiter**.

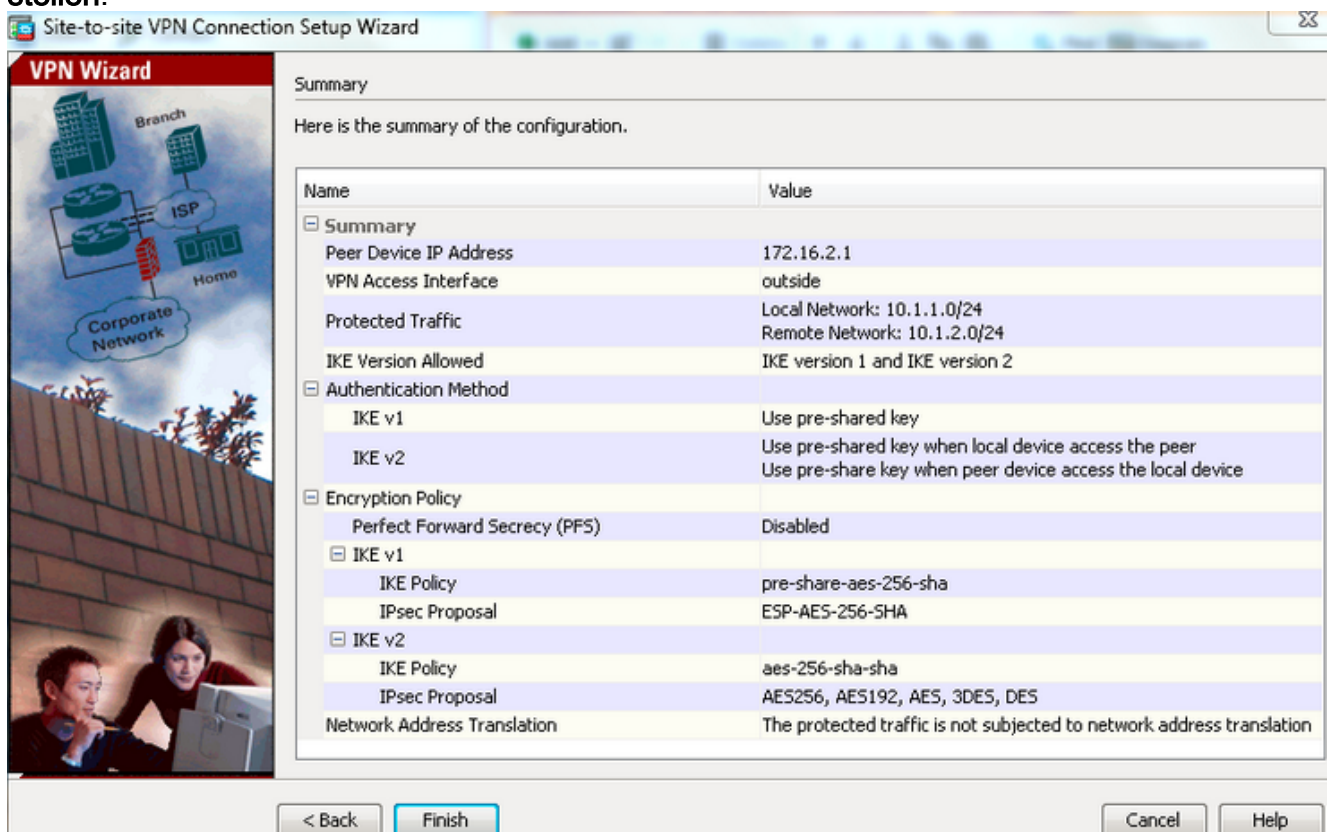


8. Aktivieren Sie das Kontrollkästchen **Exempt ASA side host/network from address translation**, um zu verhindern, dass der Tunnelverkehr zu Beginn der Network Address Translation (Netzwerkadressenumwandlung) beginnt. Wählen Sie entweder **lokal** oder **intern** aus der Dropdown-Liste aus, um die Schnittstelle festzulegen, über die das lokale Netzwerk erreichbar ist. Klicken Sie auf **Weiter**.





9. ASDM zeigt eine Zusammenfassung des gerade konfigurierten VPNs an. Überprüfen und klicken Sie auf **Fertig stellen**.



# CLI-Konfiguration

## Zentrale ASA-Konfiguration (Static Peer)

1. Konfigurieren Sie eine NO-NAT/NAT-EXEMPT-Regel für VPN-Datenverkehr, wie im folgenden Beispiel gezeigt:

```
object network 10.1.1.0-remote_network
 subnet 10.1.1.0 255.255.255.0
```

```
object network 10.1.2.0-inside_network
 subnet 10.1.2.0 255.255.255.0
```

```
nat (inside,outside) source static 10.1.2.0-inside_network 10.1.2.0-inside_network
 destination static 10.1.1.0-remote_network 10.1.1.0-remote_network
 no-proxy-arp route-lookup
```

2. Konfigurieren Sie den vorinstallierten Schlüssel unter DefaultL2LGroup , um einen beliebigen Remote-Dynamic-L2L-Peer zu authentifizieren:

```
tunnel-group DefaultL2LGroup ipsec-attributes
 ikev1 pre-shared-key cisco123
```

3. Definieren der Phase-2-/ISAKMP-Richtlinie:

```
crypto ikev1 policy 10
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
```

4. Definieren der Phase-2-Richtlinie für den Transformationssatz/die IPsec-Richtlinie:

```
crypto ipsec ikev1 transform-set tset esp-aes-256 esp-sha-hmac
```

5. Konfigurieren Sie die dynamische Zuordnung mit folgenden Parametern: Erforderliches TransformationsatzRRI (Reverse Route Injection) aktivieren, sodass die Security Appliance Routing-Informationen für verbundene Clients abrufen kann (optional)

```
crypto dynamic-map outside_dyn_map 1 set ikev1 transform-set tset
 crypto dynamic-map outside_dyn_map 1 set reverse-route
```

6. Binden Sie die dynamische Zuordnung an die Crypto Map, wenden Sie die Crypto Map an, und aktivieren Sie ISAKMP/IKEv1 auf der externen Schnittstelle:

```
crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
```

```
crypto map outside_map interface outside
 crypto ikev1 enable outside
```

## Remote-ASA (Dynamic Peer)

1. Konfigurieren Sie eine NAT-Freistellungsregel für VPN-Datenverkehr:

```
object network 10.1.1.0-inside_network
 subnet 10.1.1.0 255.255.255.0
```

```
object network 10.1.2.0-remote_network
 subnet 10.1.2.0 255.255.255.0
```

```
nat (inside,outside) source static 10.1.1.0-inside_network 10.1.1.0-inside_network
 destination static 10.1.2.0-remote_network 10.1.2.0-remote_network
 no-proxy-arp route-lookup
```

2. Konfigurieren Sie eine Tunnelgruppe für einen statischen VPN-Peer und einen vorinstallierten Schlüssel.

```
tunnel-group 172.16.2.1 type ipsec-l2l
```

```
tunnel-group 172.16.2.1 ipsec-attributes
ikev1 pre-shared-key cisco123
```

### 3. PHASE-1/ISAKMP-Richtlinie definieren:

```
crypto ikev1 policy 10
authentication pre-share
encryption aes-256
hash sha
group 2
lifetime 86400
```

### 4. Definieren einer Phase-2-Transformationssatz-/IPsec-Richtlinie:

```
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
```

### 5. Konfigurieren Sie eine Zugriffsliste, die den interessanten VPN-Datenverkehr bzw. das VPN-Netzwerk definiert:

```
access-list outside_cryptomap extended permit ip object
10.1.1.0-inside_network object 10.1.2.0-remote_network
```

### 6. Konfigurieren Sie die statische Crypto Map mit folgenden Parametern: Verschlüsselungs-/VPN-Zugriffsliste IP-Adresse des Remote-IPsec-Peers Erforderliches Transformationssatz

```
crypto map outside_map 1 match address outside_cryptomap
crypto map outside_map 1 set peer 172.16.2.1
crypto map outside_map 1 set ikev1 transform-set ESP-AES-256-SHA
```

### 7. Wenden Sie die Crypto Map an, und aktivieren Sie ISAKMP/IKEv1 auf der externen Schnittstelle:

```
crypto map outside_map interface outside
crypto ikev1 enable outside
```

## Überprüfen

In diesem Abschnitt überprüfen Sie, ob die Konfiguration ordnungsgemäß funktioniert.

Das [Output Interpreter Tool](#) (nur [registrierte](#) Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter Tool, um eine Analyse der **Ausgabe des Befehls show** anzuzeigen.

- **show crypto isakmp sa** - Zeigt alle aktuellen IKE Security Associations (SAs) in einem Peer an.
- **show crypto ipsec sa** - Zeigt alle aktuellen IPsec-SAs an.

In diesem Abschnitt wird die Beispielüberprüfung für die beiden ASAs veranschaulicht.

## Zentrale ASA

```
Central-ASA#show crypto isakmp sa
```

```
IKEv1 SAs:
```

```
Active SA: 1
```

```
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
```

```
Total IKE SA: 1
```

```
1 IKE Peer: 172.16.1.1
```

```
Type      : L2L           Role      : responder
```

```
Rekey     : no          State     : MM_ACTIVE
```

```
Central-ASA# show crypto ipsec sa
```

```

interface: outside
  Crypto map tag: outside_dyn_map, seq num: 1, local addr: 172.16.2.1

    local ident (addr/mask/prot/port): (10.1.2.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
    current_peer: 172.16.1.1

    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
    #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
    #TFC rcvd: 0, #TFC sent: 0
    #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
    #send errors: 0, #recv errors: 0

    local crypto endpt.: 172.16.2.1/0, remote crypto endpt.: 172.16.1.1/0
    path mtu 1500, ipsec overhead 74(44), media mtu 1500
    PMTU time remaining (sec): 0, DF policy: copy-df
    ICMP error validation: disabled, TFC packets: disabled
    current outbound spi: 30D071C0
    current inbound spi : 38DA6E51

inbound esp sas:
spi: 0x38DA6E51 (953839185)
  transform: esp-aes-256 esp-sha-hmac no compression
  in use settings ={L2L, Tunnel, IKEv1, }
  slot: 0, conn_id: 28672, crypto-map: outside_dyn_map
  sa timing: remaining key lifetime (kB/sec): (3914999/28588)
  IV size: 16 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x0000001F
outbound esp sas:
spi: 0x30D071C0 (818966976)
  transform: esp-aes-256 esp-sha-hmac no compression
  in use settings ={L2L, Tunnel, IKEv1, }
  slot: 0, conn_id: 28672, crypto-map: outside_dyn_map
  sa timing: remaining key lifetime (kB/sec): (3914999/28588)
  IV size: 16 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x00000001

```

## Remote-ASA

```
Remote-ASA#show crypto isakmp sa
```

```
IKEv1 SAs:
```

```

Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

```

```

1  IKE Peer: 172.16.2.1
   Type      : L2L                Role       : initiator
   Rekey     : no                 State      : MM_ACTIVE

```

```
Remote-ASA#show crypto ipsec sa
```

```
interface: outside
```

```
Crypto map tag: outside_map, seq num: 1, local addr: 172.16.1.1

    access-list outside_cryptomap extended permit ip 10.1.1.0
255.255.255.0 10.1.2.0 255.255.255.0
local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.1.2.0/255.255.255.0/0/0)
current_peer: 172.16.2.1

    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

    local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 172.16.2.1/0
path mtu 1500, ipsec overhead 74(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 38DA6E51
current inbound spi : 30D071C0

inbound esp sas:
spi: 0x30D071C0 (818966976)
    transform: esp-aes-256 esp-sha-hmac no compression
    in use settings ={L2L, Tunnel, IKEv1, }
    slot: 0, conn_id: 8192, crypto-map: outside_map
    sa timing: remaining key lifetime (kB/sec): (4373999/28676)
    IV size: 16 bytes
    replay detection support: Y
    Anti replay bitmap:
        0x00000000 0x0000001F
outbound esp sas:
spi: 0x38DA6E51 (953839185)
    transform: esp-aes-256 esp-sha-hmac no compression
    in use settings ={L2L, Tunnel, IKEv1, }
    slot: 0, conn_id: 8192, crypto-map: outside_map
    sa timing: remaining key lifetime (kB/sec): (4373999/28676)
    IV size: 16 bytes
    replay detection support: Y
    Anti replay bitmap:
        0x00000000 0x00000001
```

## Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Das [Output Interpreter Tool](#) (nur [registrierte](#) Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter Tool, um eine Analyse der **Ausgabe des Befehls show** anzuzeigen.

**Hinweis:** Weitere Informationen [zu Debug-Befehlen](#) vor der Verwendung von **Debug**-Befehlen finden Sie unter [Wichtige Informationen](#).

Verwenden Sie die folgenden Befehle:

```
clear crypto ikev1 sa <peer IP address>
Clears the Phase 1 SA for a specific peer.
```

**Vorsicht:** Der Befehl **clear crypto isakmp sa** ist intrusiv, da er alle aktiven VPN-Tunnel löscht.

In der PIX/ASA-Softwareversion 8.0(3) und höher kann eine einzelne IKE SA mithilfe des Befehls **clear crypto isakmp sa <Peer-IP-Adresse>** gelöscht werden. Verwenden Sie in Softwareversionen vor 8.0(3) den Befehl [vpn-sessiondb logoff tunnel-group <tunnel-group-name>](#), um IKE- und IPsec-SAs für einen Tunnel zu löschen.

```
Remote-ASA#vpn-sessiondb logoff tunnel-group 172.16.2.1
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions from TunnelGroup "172.16.2.1" logged off : 1
```

```
clear crypto ipsec sa peer <peer IP address>
!!! Clears the required Phase 2 SA for specific peer.
debug crypto condition peer < Peer address>
!!! Set IPsec/ISAKMP debug filters.
debug crypto isakmp sa <debug level>
!!! Provides debug details of ISAKMP SA negotiation.
debug crypto ipsec sa <debug level>
!!! Provides debug details of IPsec SA negotiations
undebug all
!!! To stop the debugs
```

**Verwendete Debugger:**

```
debug cry condition peer <remote peer public IP>
debug cry ikev1 127
debug cry ipsec 127
```

## Remote-ASA (Initiator)

Geben Sie den Befehl **Packet-Tracer** ein, um den Tunnel zu initiieren:

```
Remote-ASA#packet-tracer input inside icmp 10.1.1.10 8 0 10.1.2.10 detailed

IPSEC(crypto_map_check)-3: Checking crypto map outside_map 1: matched.
Jan 19 22:00:06 [IKEv1 DEBUG]Pitcher: received a key acquire message, spi 0x0
IPSEC(crypto_map_check)-3: Looking for crypto map matching 5-tuple:
Prot=1, saddr=10.1.1.10, sport=0, daddr=10.1.2.10, dport=0
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 1: matched.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE Initiator: New Phase 1, Intf
inside, IKE Peer 172.16.2.1 local Proxy Address 10.1.1.0, remote Proxy Address
10.1.2.0, Crypto map (outside_map)
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NONE (0) total length : 172
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0)
total length : 132
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0)
```

with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) +  
VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304  
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE\_DECODE RECEIVED Message (msgid=0)  
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) +  
VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304  
:  
.  
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, **Connection landed on tunnel\_group 172.16.2.1**  
<skipped>...  
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE\_DECODE SENDING Message (msgid=0) with  
payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) +  
NONE (0) total length : 96  
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,  
**Automatic NAT Detection Status: Remote end is NOT behind a NAT device**  
**This end is NOT behind a NAT device**  
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE\_DECODE RECEIVED Message  
(msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128)  
+ VENDOR (13) + NONE (0) total length : 96  
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, **processing ID payload**  
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,  
**ID\_IPV4\_ADDR ID received 172.16.2.1**  
:  
.  
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, Connection landed on tunnel\_group 172.16.2.1  
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1,  
Oakley begin quick mode  
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1, **PHASE 1 COMPLETED**  
  
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1, **IKE Initiator**  
**starting QM: msg id = c45c7b30**  
:  
.  
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, **Transmitting Proxy Id:**  
**Local subnet: 10.1.1.0 mask 255.255.255.0 Protocol 0 Port 0**  
**Remote subnet: 10.1.2.0 Mask 255.255.255.0 Protocol 0 Port 0**  
:  
.  
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE\_DECODE SENDING Message  
(msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) + NONCE  
(10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200  
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE\_DECODE RECEIVED Message  
(msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) +  
ID (5) + ID (5) + NONE (0) total length : 172  
:  
.  
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, **processing ID payload**  
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,  
**ID\_IPV4\_ADDR\_SUBNET ID received--10.1.1.0--255.255.255.0**  
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, **processing ID payload**  
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,  
**ID\_IPV4\_ADDR\_SUBNET ID received--10.1.2.0--255.255.255.0**  
:  
.  
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,  
Security negotiation complete for LAN-to-LAN Group (172.16.2.1)  
Initiator, **Inbound SPI = 0x30d071c0, Outbound SPI = 0x38da6e51**  
:  
.  
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE\_DECODE SENDING Message  
(msgid=c45c7b30) with payloads : HDR + HASH (8) + NONE (0) total length : 76  
:  
.  
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,

PHASE 2 COMPLETED (msgid=c45c7b30)

## Central-ASA (Responder)

```
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NONE (0) total length : 172
:
.
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length
:
132
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13)
+ VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
:
.
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, Connection landed on tunnel_group
DefaultL2LGroup
Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup, IP = 172.16.1.1,
Generating keys for Responder...
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) +
VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) +
NONE (0) total length : 304
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8)
+ IOS KEEPALIVE (128) + VENDOR (13) + NONE (0) total length : 96
Jan 20 12:42:35 [IKEv1 DECODE]Group = DefaultL2LGroup, IP = 172.16.1.1,
ID_IPV4_ADDR ID received172.16.1.1
:
.
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) +
VENDOR (13) + NONE (0) total length : 96
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, PHASE 1 COMPLETED
:
.
Jan 20 12:42:35 [IKEv1 DECODE]IP = 172.16.1.1, IKE Responder starting QM:
msg id = c45c7b30
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE
RECEIVED Message (msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) +
NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200
:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Received remote
IP Proxy Subnet data in ID Payload: Address 10.1.1.0, Mask 255.255.255.0,
Protocol 0, Port 0:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup,
IP = 172.16.1.1, Received local
IP Proxy Subnet data in ID Payload: Address 10.1.2.0, Mask 255.255.255.0,
Protocol 0, Port 0Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup,
IP = 172.16.1.1, processing notify payload
Jan 20 12:42:35 [IKEv1] Group = DefaultL2LGroup, IP = 172.16.1.1, QM
IsRekeyed old sa not found by addr
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Static Crypto Map
check, map outside_dyn_map, seq = 1 is a successful match
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, IKE
Remote Peer configured for crypto map: outside_dyn_map
```



```
:  
.br/>Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup, IP = 172.16.1.1,  
Transmitting Proxy Id: Remote subnet: 10.1.1.0 Mask 255.255.255.0 Protocol 0 Port 0  
Local subnet: 10.1.2.0 mask 255.255.255.0 Protocol 0 Port 0:  
.br/>Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=c45c7b30)  
with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE  
(0) total length : 172 Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED  
Message (msgid=c45c7b30) with payloads : HDR + HASH (8) + NONE (0) total length : 52:  
.br/>Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Security  
negotiation complete for LAN-to-LAN Group (DefaultL2LGroup) Responder,  
Inbound SPI = 0x38da6e51, Outbound SPI = 0x30d071c0:  
.br/>Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1,  
PHASE 2 COMPLETED (msgid=c45c7b30)  
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Adding static  
route for L2L peer coming in on a dynamic map. address: 10.1.1.0, mask: 255.255.255.0
```

## Zugehörige Informationen

- [Cisco ASA-Serie - Befehlsreferenzen](#)
- [Support-Seite für IPsec-Aushandlung/IKE-Protokolle](#)
- [Anforderungen für Kommentare \(RFCs\)](#)
- [Technischer Support und Dokumentation - Cisco System](#)