## ASA/PIX: Remote-VPN-Server mit eingehender NAT für VPN-Client-Datenverkehr mit CLI und ASDM - Konfigurationsbeispiel

## Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Zugehörige Produkte Konventionen Hintergrundinformationen Konfigurationen ASA/PIX als Remote-VPN-Server mit ASDM konfigurieren Konfigurieren des ASA/PIX für eingehenden VPN-Client-Datenverkehr von NAT mit ASDM Konfigurieren von ASA/PIX als Remote-VPN-Server und für eingehende NAT mit der CLI Überprüfen ASA/PIX Security Appliance - Befehle anzeigen Fehlerbehebung Zugehörige Informationen

## **Einführung**

Dieses Dokument beschreibt, wie die Cisco Adaptive Security Appliance (ASA) der Serie 5500 so konfiguriert wird, dass sie als Remote-VPN-Server mit dem Adaptive Security Device Manager (ASDM) oder CLI und NAT für den eingehenden VPN-Client-Datenverkehr fungiert. Der ASDM bietet erstklassige Sicherheitsverwaltung und -überwachung über eine intuitive, benutzerfreundliche webbasierte Verwaltungsschnittstelle. Sobald die Cisco ASA-Konfiguration abgeschlossen ist, kann sie über den Cisco VPN-Client verifiziert werden.

## Voraussetzungen

#### Anforderungen

In diesem Dokument wird davon ausgegangen, dass die ASA voll betriebsbereit und konfiguriert ist, damit der Cisco ASDM oder die CLI Konfigurationsänderungen vornehmen können. Es wird auch angenommen, dass die ASA für die ausgehende NAT konfiguriert ist. Weitere Informationen zur Konfiguration der ausgehenden NAT finden Sie unter <u>Zulassen des Zugriffs von internen</u><u>Hosts auf externe Netzwerke mithilfe von PAT</u>.

**Hinweis:** Weitere Informationen finden Sie unter <u>Zulassen von HTTPS-Zugriff für ASDM</u> oder <u>PIX/ASA 7.x: SSH im Konfigurationsbeispiel für die Innen- und Außenschnittstelle</u>, um die Remote-Konfiguration des Geräts durch den ASDM oder Secure Shell (SSH) zu ermöglichen.

#### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Adaptive Security Appliance Software Version 7.x oder höher
- Adaptive Security Device Manager Version 5.x und höher
- Cisco VPN Client Version 4.x oder 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.

#### Zugehörige Produkte

Diese Konfiguration kann auch mit der Cisco PIX Security Appliance Version 7.x oder höher verwendet werden.

#### **Konventionen**

Weitere Informationen zu Dokumentkonventionen finden Sie unter <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

### **Hintergrundinformationen**

Konfigurationen für den Remote-Zugriff bieten sicheren Remote-Zugriff für Cisco VPN-Clients wie mobile Benutzer. Über ein Remote-Access-VPN können Remote-Benutzer sicher auf zentralisierte Netzwerkressourcen zugreifen. Der Cisco VPN Client ist mit dem IPSec-Protokoll kompatibel und wurde speziell für die Verwendung mit der Sicherheits-Appliance entwickelt. Die Sicherheits-Appliance kann jedoch IPSec-Verbindungen mit vielen protokollkonformen Clients herstellen. Weitere Informationen zu IPSec finden Sie in den <u>ASA-Konfigurationsleitfäden</u>.

Gruppen und Benutzer sind zentrale Konzepte für die Verwaltung der VPN-Sicherheit und die Konfiguration der Sicherheits-Appliance. Sie legen Attribute fest, die den Benutzerzugriff auf das VPN und dessen Nutzung bestimmen. Eine Gruppe ist eine Sammlung von Benutzern, die als eine Einheit behandelt werden. Benutzer erhalten ihre Attribute aus Gruppenrichtlinien. Tunnelgruppen identifizieren die Gruppenrichtlinie für bestimmte Verbindungen. Wenn Sie Benutzern keine bestimmte Gruppenrichtlinie zuweisen, gilt die Standardgruppenrichtlinie für die Verbindung.

Eine Tunnelgruppe besteht aus einer Reihe von Datensätzen, die Tunnelverbindungsrichtlinien festlegen. Diese Datensätze enthalten die Server, an die die Tunnelbenutzer authentifiziert werden, sowie ggf. die Accounting-Server, an die die Verbindungsinformationen gesendet werden. Sie identifizieren auch eine Standardgruppenrichtlinie für die Verbindungen und enthalten protokollspezifische Verbindungsparameter. Tunnelgruppen enthalten eine kleine Anzahl von Attributen, die sich auf die Erstellung des Tunnels selbst beziehen. Tunnelgruppen enthalten einen

Zeiger auf eine Gruppenrichtlinie, die benutzerorientierte Attribute definiert.

## **Konfigurationen**

#### ASA/PIX als Remote-VPN-Server mit ASDM konfigurieren

Gehen Sie wie folgt vor, um die Cisco ASA als Remote-VPN-Server mit ASDM zu konfigurieren:

 Öffnen Sie Ihren Browser, und geben Sie https://<IP\_Adresse der ASA-Schnittstelle ein, die für ASDM Access konfiguriert wurde>, um auf das ASDM auf der ASA zuzugreifen.Achten Sie darauf, alle Warnungen zu autorisieren, die Ihr Browser bezüglich der Authentizität von SSL-Zertifikaten ausgibt. Standardmäßig sind Benutzername und Kennwort leer.Die ASA präsentiert dieses Fenster, um den Download der ASDM-Anwendung zu ermöglichen. In diesem Beispiel wird die Anwendung auf den lokalen Computer geladen und nicht in einem Java-Applet

ausgeführt.

Eisco ASDM 6.1	cisco
Cisco ASDM 6.1(3) provides an intuitive graphical user interface that makes it easy configure and manage your Cisco Security Appliances.	to set up,
Cisco ASDM runs as either a local application or Java Web Start.	
Running Cisco ASDM as a local Application	
You can invoke ASDM from desktop shortcuts. No browser is required.     One desktop shortcut allows you to connect to <i>multiple</i> Security Appliance     Install ASDM Launcher and Run ASDM	yes. Is.
Running Cisco ASDM as Java Web Start         You can run Cisco ASDM as Java Web Start that is dynamically downloaded from to which you connect.         • Click Run ASDM to run Cisco ASDM.         • Click Run Startup Wizard to run Startup Wizard.Startup Wizard walks yo step by step, the initial configuration of your security appliance.         Run ASDM       Run Startup Wizard	the device ou through,

- 2. Klicken Sie auf **ASDM Launcher herunterladen und ASDM starten**, um das Installationsprogramm für die ASDM-Anwendung herunterzuladen.
- 3. Wenn der ASDM Launcher heruntergeladen wurde, führen Sie die Schritte aus, die von den Aufforderungen zur Installation der Software und Ausführung des Cisco ASDM Launchers ausgeführt werden.

4. Geben Sie die IP-Adresse für die Schnittstelle ein, die Sie mit dem Befehl http konfiguriert haben, sowie einen Benutzernamen und ein Kennwort, wenn Sie einen Befehl angegeben haben. In diesem Beispiel wird cisco123 als Benutzername und cisco123 als Kennwort

	💕 Cisco ASDM Launch		
	🤏 Cisco AS	SDM Launcher	cisco
	Device IP Address / Name:	10.77.241.111	<b>•</b>
	Username:	cisco123	
	Password:	* * * * * * *	
	📃 Run in Demo Mode		
verwendet.		~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	🗊 👙 🔒

5. Wählen Sie im Home-Fenster Wizards > IPsec VPN Wizard

	Gisco ASDM 6.1 for ASA - 10.77.241.111				
	File View Tools	Wiz	ards	Window Help	
	Home 🖧 Cor		Star	tup Wizard	
			IPsec VPN Wizard		
	Device List		SSL	VPN Wizard	
	🕈 Add 🛅 Delete		High	Availability and Scalability Wizard	
	10.77.241.10		r ligi	r Availability and Scalability wizard	
aus.			Pac	ket Capture Wizard	

6. Wählen Sie den Tunneltyp **Remote Access** VPN aus, stellen Sie sicher, dass die VPN-Tunnel-Schnittstelle wie gewünscht eingestellt ist, und klicken Sie auf **Weiter**, wie hier gezeigt.

🖆 VPN Wizard	2	×
VPN Wizard	PN Tunnel Type (Step 1 of)	
Branch Branch F SSF SSF Home Home	Use this wizard to configure new site-to-site VPN tunnels or new remote access VPN tunnels. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A tunnel established by calls from remote users such as telecommuters is called remote access tunnel. This wizard creates basic tunnel configurations that you can edit later using the ASDM.	
Corporate Network	VPN Tunnel Type: Site-to-Site VPN	
THE REAL	Site-to-Site	
	Remote Access	
	VPN Tunnel Interface: Outside	
	authorization access lists still apply to the traffic.	
	< Back Next > Finish Cancel He	P

 Der VPN-Client-Typ wird wie gezeigt ausgewählt. Hier wird Cisco VPN Client ausgewählt. Klicken Sie auf Weiter.

🖆 VPN Wizard		×
VPN Wizard	Remote Access Client (Step 2 of)	
Brandh	Remote access users of various types can open VPN tunnels to this ASA. Select the type of VPN client for this tunnel.	
	VPN Client Type:	
Home	Clero VPN Clent, Peleace 3 x or binber	
Corporate Notwork	or other Fasy VPN Remote product	
- centra	or other Edgy why Kennete product	
11	Microsoft Windows client using L2TP over IPsec	
	Specify the PPP authentication protocol. If a protocol is not specified on the remote client, do not specify it.	
- I STATUT	PAP V CHAP V MS-CHAP-V1 MS-CHAP-V2 EAP-PROXY	
I I I I	Specify if the client will send tunnel group name as - username@tunnelgroup.	
- A-	Client will send tunnel group name as username@tunnelgroup.	
	If pre-shared authentication is used with this option then DefaultRAGroup's pre-shared key and ppp authentication are also modified.	
	< Back Next > Finish Cancel Help	,

8. Geben Sie einen Namen für den Tunnelgruppennamen ein. Geben Sie die zu verwendenden Authentifizierungsinformationen ein, d. h. den vorinstallierten Schlüssel in diesem Beispiel. Der in diesem Beispiel verwendete vorinstallierte Schlüssel ist cisco123. Der in diesem Beispiel verwendete Tunnel-Gruppenname lautet cisco. Klicken Sie auf Weiter.

🖆 VPN Wizard	
VPN Wizard	VPN Client Authentication Method and Tunnel Group Name (Step 3 of)
Branch Branch Brown Corporato Network	The ASA allows you to group remote access tunnel users based on common connection parameters and clent attributes configured in the subsequent screens. Configure authentication method and tunnel group for this remote connection. Use the same tunnel group name for the device and the remote clent.          Authentication Method <ul> <li>Pre-shared key</li> <li>Pre-Shared Key:</li> <li>Certificate</li> <li>Certificate Signing Algorithm: rsa-sig</li> <li>Certificate Name:</li> <li>Challenge/response authentication (CRACK)</li> </ul>
	< Back Next > Finish Cancel Heb

9. Wählen Sie aus, ob Remote-Benutzer in der lokalen Benutzerdatenbank oder in einer externen AAA-Servergruppe authentifiziert werden sollen. Hinweis: Sie fügen der lokalen Benutzerdatenbank in Schritt 10 Benutzer hinzu. Hinweis: Informationen zur Konfiguration einer externen AAA-Servergruppe mit ASDM finden Sie unter PIX/ASA 7.x Authentication and Authorization Server Groups für VPN-Benutzer unter ASDM Configuration Example (Konfigurationsbeispiel für ASDM).

🖆 VPN Wizard		×
VPN Wizard	Client Authentication (Step 4 of)	
Bandh Hame Corporato Network	To authenticate remote users using local device user database, select the first option below. You can create user accounts in the next step. To use external AAA servers instead, select the second option. You can select an existing AAA server group or create a new one using the New button below. To manage all other AAA settings, go to Configuration > Device Management > Users/AAA in the main ASDM window.	
	< Back Next > Finish Cancel Hel	P

10. Geben Sie einen Benutzernamen und ein optionales Kennwort ein, und klicken Sie auf Hinzufügen, um der Benutzerauthentifizierungsdatenbank neue Benutzer hinzuzufügen. Klicken Sie auf Weiter.Hinweis: Entfernen Sie keine vorhandenen Benutzer aus diesem Fenster. Wählen Sie im ASDM-Hauptfenster Konfiguration > Gerätemanagement > Benutzer/AAA > Benutzerkonten aus, um vorhandene Datenbankeinträge zu bearbeiten oder aus der Datenbank zu entfernen.

🖆 VPN Wizard		×
VPN Wizard	User Accounts (Step 5 of 11)	
Branch Branch	Add new users into the user authentication database. To edit existing entries in the database or to remove them from the database, go to Configuration > Device Management > Users/AAA > User Accounts in the main ASDM window.	
Home	User to Be Added	
Corporate	Username: disco123	
THE THE	cisco  Add >>	
	Password (optional): Delete	
111111	••••••	
THE THE	Confirm Password (optional):	
- C	••••••	
	< Back Next > Finish Cancel Help	•

11. Um einen Pool lokaler Adressen zu definieren, die Remote-VPN-Clients dynamisch zugewiesen werden sollen, klicken Sie auf **Neu**, um einen neuen **IP-Pool** zu erstellen.

🖆 VPN Wizard		$\mathbf{X}$
VPN Wizard	Address Pool (Step 6 of 11)	
Branch Branch ISP ISP Horne Network	Enter a pool of local addresses to be used for assigning dynamic IP addresses to remote VPN clients. Tunnel Group Name : CISCO	
	Pool Name:       New         Pool Settings       Range Start Address:         Range End Address:       Subnet Mask:	
	< Back Next > Finish Cancel Help	

12. Geben Sie im neuen Fenster Add IP Pool (IP-Pool hinzufügen) diese Informationen an, und klicken Sie auf OK.Name des IP-PoolsStart-IP-AdresseEnd-IP-

Name:	vpnpool
Starting IP Address:	192.168.1.1
Ending IP Address:	192.168.1.254
Subnet Mask:	255.255.255.0

#### AdresseSubnetzmaske

13. Nachdem Sie den Pool der lokalen Adressen definiert haben, die Remote-VPN-Clients beim Herstellen einer Verbindung dynamisch zugewiesen werden sollen, klicken Sie auf **Weiter.** 

🖆 VPN Wizard		$\times$
VPN Wizard	Address Pool (Step 6 of 11)	
Branch Branch ISP Home	Enter a pool of local addresses to be used for assigning dynamic IP addresses to remote VPN clients.	
Corporate Network	Tunnel Group Name : Cisco	
THE THE	Pool Name: vpnpool 🖌 New	
	Pool Settings	
THUMM	Range Start Address: 192.168.1.1	
- Ito - Ital	Range End Address: 192.168.1.254	
1 A	Subnet Mask: 255.255.255.0	
		J
	< Back Next > Finish Cancel Help	

14. *Optional:* Geben Sie die DNS- und WINS-Serverinformationen und einen Standard-Domänennamen an, der an Remote-VPN-Clients übertragen werden soll.

🖆 VPN Wizard		
VPN Wizard	Attributes Pushed to Client (Optional) (	Step 7 of 11)
Bronch	Attributes you configure below are pushe ASA. If you do not want an attribute pusi	d to the VPN client when the client connects to the hed to the client, leave the corresponding field blank.
Corporate	Tunnel Group:	cisco
Franks he	Primary DNS Server:	I
	Secondary DNS Server:	
1111	Primary WINS Server:	
	Secondary WINS Server:	
	Default Domain Name:	
		< Back Next > Finish Cancel Help

15. Geben Sie die Parameter für IKE an, auch als IKE-Phase 1 bezeichnet.Konfigurationen auf beiden Seiten des Tunnels müssen genau übereinstimmen. Der Cisco VPN Client wählt jedoch automatisch die richtige Konfiguration für sich aus. Daher ist auf dem Client-PC keine IKE-Konfiguration erforderlich.

🖆 VPN Wizard		X
VPN Wizard	IKE Policy (Step 8 of 11)	
Branch Branch Difference Horne	Select the encryption algorithm, authentication algorithm, and Diffie-Helman group for the devices to use to negotiate an Internet Key Exchange (IKE) security association between them. Configurations on both sides of the connection must match exactly.	
Notwork	Encryption: DES	
	Authentication:	
	Diffie-Helman Group: 2	
	< Back Next Finish Cancel Help	

16. In diesem Fenster wird eine Zusammenfassung der von Ihnen ergriffenen Maßnahmen angezeigt. Klicken Sie auf **Fertig stellen**, wenn Sie mit Ihrer Konfiguration zufrieden sind.



Konfigurieren des ASA/PIX für eingehenden VPN-Client-Datenverkehr von NAT mit ASDM

Gehen Sie wie folgt vor, um den Datenverkehr des Cisco ASA-to-NAT-eingehenden VPN-Clients mit ASDM zu konfigurieren:

1. Wählen Sie Konfiguration > Firewall > NAT Rules aus, und klicken Sie auf Add. Wählen Sie in der Dropdown-Liste die Option Dynamische NAT-Regel hinzufügen



aus.

2. Wählen Sie im Fenster **Dynamische NAT-Regel hinzufügen** die Option **Außerhalb** als Schnittstelle aus, und klicken Sie auf die Schaltfläche Durchsuchen neben dem Feld **Quelle**.

🖆 Add Dynamic NAT Rule		
Original Interface: Outside Source: Translated Select a global pool for dynamic tran	slation.	
Pool ID Interface 0 (outbound) 0 (inbound)	Addresses Pool Same as original address (identity) Same as original address (identity)	Manage
Connection Settings		*

 Wählen Sie im Fenster Quelle durchsuchen die richtigen Netzwerkobjekte aus, wählen Sie im Abschnitt Ausgewählte Quelle auch die Quelle aus, und klicken Sie auf OK. Hier wird das Netzwerkobjekt 192.168.1.0 ausgewählt.

🖆 Browse Source					×
🕈 Add 🍠 Edit î De	lete Q				
Filter:					Filter Clear
Name	1 ID Address		Natroack	Description	i neur cierca
-Network Objects	IF Address	>	Nouridok.	Description	
any	0.0.0.0	0	.0.0.0		
📲 inside-network	172.16.1.0	2	55.255.255.0		1
🚮 Outside-netwo	rk 10.10.10.0	2	55.255.255.0		
i- <b>__</b> 192.168.1.0	192.168.1.	0 2	55.255.255.0		
				_	
Selected Source					
Source -> 192.1	68.1.0/24				
				<u> </u>	Cancel

4. Klicken Sie auf Verwalten.

r.	Add Dyna	amic NAT Rule				X
Or Y	iginal Interface: Source:	Outside 192.168.0.0				
16	Select a glo	bal pool for dynamic t	ranslation.			
	Pool ID	Interface		Addresses Pool		
	0	(outbound)		5ame as original addre	ss (identity)	
	0	(inbound)		5ame as original addre	ss (identity)	Manage
	onnectio	n Settings				8
			ОК	Cancel	Help	

5. Klicken Sie im Fenster Globalen Pool verwalten auf **Hinzufügen**.

	Manage Glo	bal Pool		×
	🔂 🗹	it 💼 Delete		
'	Pool ID	Interface	Addresses Pool	
	-			
	L			
		ОК	Cancel Help	
				_

6. Wählen Sie im Fenster Globalen Adresspool hinzufügen die Option Inside als Schnittstelle und 2 als Pool-ID aus. Stellen Sie außerdem sicher, dass das Optionsfeld neben PAT unter Verwendung der IP-Adresse der Schnittstelle aktiviert ist. Klicken Sie auf Hinzufügen>> und dann auf OK.

🞼 Add Global Address Pool		×
Interface: inside  Pool ID: 2		
IP Addresses to Add		Addresses Pool
Starting IP Address:		inside
Ending IP Address: Netmask (optional):	Add >>	
O Port Address Translation (PAT)	<< Delete	
Netmask (optional):		
<ul> <li>Port Address Translation (PAT) using IP Address of the interface</li> </ul>		
ОК	Cancel	Help

7. Klicken Sie auf **OK**, nachdem Sie den globalen Pool mit der im vorherigen Schritt konfigurierten **Pool-ID 2** ausgewählt haben.

🕵 Add Dyne	amic NAT Rule		
Original			
Interface:	Outside	~	
Source:	192.168.1.0/24		
Translated — Select a glo	ibal pool for dynamic	translation.	
Pool ID	Interface	Addresses Pool	
0	(outbound)	Same as original address (identity)	
	(inbound)	Same as original address (identity)	
2	Inside	inside	Manage
Connectio	n Settings		۲
		Cancel Help	

8. Klicken Sie jetzt auf **Apply**, um die Konfiguration auf die ASA anzuwenden.Damit ist die Konfiguration abgeschlossen.

Add      Edit     Delete     Packet Trace     Original     Source     Destination     Service     Interface     Ad     Outside     I bynamic     Placet     Interface     Ad     Outside     I bynamic     Placet     Interface     Ad     Outside     Interface     Ad     Interface     Interface     Ad     Interface     Interface     Interface     Ad     Interface     Interf	onfigura	ation > Firewall > !	NAT Rules					
Type       Original       Translated         Source       Destination       Service       Interface       Ad         Outside (1 Dynamic rules)       inside       inside       Image: Service       Interface       Ad         I inside (1 Exempt rules, 1 Dynamic rules)       inside       Image: Service       inside       Image: Service       Interface       Ad         I image: Service       Exempt       Image: Service       Interface       Ad         I image: Service       Exempt       Image: Service       Image: Service       Image: Service       Ad         I image: Service       Image: Servi	💠 Add	👻 📝 Edit 🏦 Dela	te 🗲 🗲	አ 🖻	🐘 - 🛛 🔍 Find 🛿	🔁 Diagram 🗐	Packet Trace	
Image: source     Destination     Service     Interface     Addition       Image: source     Outside (1 Dynamic rules)     Image: source     Image: source     Image: source     Addition       Image: source     Image: source     Image: source     Image: source     Image: source     Image: source     Addition       Image: source     Image: source     Image: source     Image: source     Image: source     Image: source     Addition       Image: source		<b>.</b>	Original				Translated	
Outside (1 Dynamic rules)      I Dynamic rules)      I Exempt Q any P 192.168.1.0/24      (outbound)      Q III Dynamic Q any      Outside      III      Enable traffic through the firewall without address translation	#	Туре	Source		Destination	Service	Interface	Addre:
1     Inside     Inside     Inside       1     Exempt rules, 1 Dynamic rules)     Inside     Inside       1     Exempt     Inside     Inside       2     Inside     Inside     Inside	🗏 Outsid	le (1 Dynamic rules)						
Inside (1 Exempt rules, 1 Dynamic rules)   1 Exempt any 192.168.1.0/24 (outbound)   2 III Dynamic any Outside III   ( Image: Contract of the second	1	Dynamic	🛃 192.168.1.	0/24			inside	💷 insi
1       Exempt       any       192.168.1.0/24       (outbound)         2       III Dynamic       any       Outside       III         C       III       III       III       IIII       IIII         Enable traffic through the firewall without address translation       IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	🖻 inside	(1 Exempt rules, 1 D)	namic rules)					
Cutside     Outside     Outside     Enable traffic through the firewall without address translation	1	🔁 Exempt	🌍 any		A 192.168.1.0/24 🎼		(outbound)	
Image: Second Seco	2	Dynamic	🌍 any				Outside	🔤 Out
Enable traffic through the firewall without address translation								
Enable traffic through the firewall without address translation			· · · · ·		1.44			
Apply Decek	Enabl	e traffic through the	tirewall without a	address tr	Posst	1		

# Konfigurieren von ASA/PIX als Remote-VPN-Server und für eingehende NAT mit der CLI

Ausführen der Konfiguration auf dem ASA-Gerät
cigcoaga#show running-config
: Saved
ASA Version 8.0(3)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
nameif Outside
security-level 0
ip address 10.10.10.2 255.255.255.0

interface Ethernet0/1 nameif inside security-level 100 ip address 172.16.1.2 255.255.255.0 1 passwd 2KFQnbNIdI.2KYOU encrypted boot system disk0:/asa803-k8.bin ftp mode passive access-list inside\_nat0\_outbound extended permit ip any 192.168.1.0 255.255.255 0 pager lines 24 logging enable mtu Outside 1500 mtu inside 1500 ip local pool vpnpool 192.168.1.1-192.168.1.254 mask 255.255.255.0 no failover icmp unreachable rate-limit 1 burst-size 1 asdm image disk0:/asdm-615.bin asdm history enable arp timeout 14400 nat-control global (Outside) 1 interface global (inside) 2 interface nat (Outside) 2 192.168.1.0 255.255.255.0 outside nat (inside) 0 access-list inside\_nat0\_outbound nat (inside) 1 0.0.0.0 0.0.0.0 route Outside 0.0.0.0 0.0.0.0 10.10.10.3 1 timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip\_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute dynamic-access-policy-record DfltAccessPolicy http server enable no snmp-server location no snmp-server contact !--- Configuration for IPsec policies. !--- Enables the crypto transform configuration mode, !--- where you can specify the transform sets that are used !--- during an IPsec negotiation. crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5hmac crypto dynamic-map SYSTEM\_DEFAULT\_CRYPTO\_MAP 65535 set pfs group1 crypto dynamic-map SYSTEM\_DEFAULT\_CRYPTO\_MAP 65535 set transform-set ESP-DES-SH ESP-DES-MD5 crypto map Outside\_map 65535 ipsec-isakmp dynamic SYSTEM\_DEFAULT\_CRYPTO\_MAP crypto map Outside\_map interface Outside crypto isakmp enable Outside !--- Configuration for IKE policies. !--- Enables the IKE policy configuration (config-isakmp) !--- command mode, where you can specify the parameters that !--- are

used during an IKE negotiation. Encryption and !-Policy details are hidden as the default values are chosen. crypto isakmp policy 10 authentication pre-share encryption des hash sha group 2 lifetime 86400 crypto isakmp policy 30 authentication pre-share encryption des hash md5 group 2 lifetime 86400 telnet timeout 5 ssh timeout 60 console timeout 0 management-access inside threat-detection basic-threat threat-detection statistics access-list group-policy cisco internal group-policy cisco attributes vpn-tunnel-protocol IPSec !--- Specifies the username and password with their !--respective privilege levels username cisco123 password ffIRPGpDSOJh9YLq encrypted privilege 15 username cisco password ffIRPGpDSOJh9YLq encrypted privilege 0 username cisco attributes vpn-group-policy cisco tunnel-group cisco type remote-access tunnel-group cisco general-attributes address-pool vpnpool default-group-policy cisco !--- Specifies the pre-shared key "cisco123" which must !--- be identical at both peers. This is a global !--configuration mode command. tunnel-group cisco ipsecattributes pre-shared-key \* ! class-map inspection\_default match default-inspection-traffic ! policy-map type inspect dns migrated\_dns\_map\_1 parameters message-length maximum 512 policy-map global\_policy class inspection\_default inspect dns migrated\_dns\_map\_1 inspect ftp inspect h323 h225 inspect h323 ras inspect netbios inspect rsh inspect rtsp inspect skinny inspect esmtp inspect sqlnet inspect sunrpc inspect tftp

```
inspect sip
inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:f2ad6f9d5bf23810a26f5cb464elfdf3
: end
ciscoasa#
```

## <u>Überprüfen</u>

Versuchen Sie, über den Cisco VPN-Client eine Verbindung zur Cisco ASA herzustellen, um zu überprüfen, ob die ASA erfolgreich konfiguriert wurde.

1. Klicken Sie auf

Neu.			
VPN Client - Version 5.0.03.0530			
Connection Entries Status Certificates Log Options	Help		
Connect News Import Modify	) Delete		ahaha cisco
Connection Entries Certificates Log			
Connection Entry	Host	Transport	
Not connected.			

 Füllen Sie die Details Ihrer neuen Verbindung aus.Das Host-Feld muss die IP-Adresse oder den Hostnamen der zuvor konfigurierten Cisco ASA enthalten. Die Informationen zur Gruppenauthentifizierung müssen mit denen in Schritt 4 übereinstimmen. Klicken Sie abschließend auf Speichern.

VPN Client   Create New VPN Connection Entry	
Connection Entry: MyVPNClient	
Description:	
Host: 10.10.10.2	
Authentication Transport Backup Servers Dial-Up	
Group Authentication	Authentication
Name: cisco	
Password:	
Confirm Password: ******	
<ul> <li>Certificate Authentication</li> <li>Name:</li> <li>Send CA Certificate Chain</li> </ul>	
Erase User Password	Cancel

3. Wählen Sie die neu erstellte Verbindung aus, und klicken Sie auf **Verbinden**.

Status: Disconnected   VPN Client - Version 5.	0.03.0530		
Connection Entries Status Certificates Log Options Help	)		
Confect New Import Modify De Connection Entries Certificates Log	iete		cisco
Connection Entry	Host	Transport	
MyVPNClient	10.10.10.2	IPSec/UDP	
Not connected.			

4. Geben Sie einen Benutzernamen und ein Kennwort für die erweiterte Authentifizierung ein. Diese Informationen müssen mit den in den Schritten 5 und 6 angegebenen übereinstimmen.

VPN Client   User Authentication for "MyVPNC	Client" 🛛 🔀
The server has requested the following information to complete t authentication.	he user
Lisco Password:	
ОК	Cancel

5. Wenn die Verbindung erfolgreich hergestellt wurde, wählen Sie im Menü Status die Option **Statistik**, um die Details des Tunnels zu überprüfen.

🥔 status: Connected   VI	PN Client - Version	5.0.03.0530			
Connection Entries Status Ce	ertificates Log Options	Help			
Disconnect N	tics Ctrl+S tations Ctrl+N	) Delete		ciso	ı. :0
Connection Entries Reset	Stats				
Connection Entry	Δ	Host	Transport		
MyVPNClient		10.10.10.2	IPSec/UDP		
Connected to "My¥PNClient".			Connected Time: 0 day(s), 00:0	0.36	•

In diesem Fenster werden der Datenverkehr und die Verschlüsselungsinformationen

Tunnel DetailsRoute DetailsFirewallAddress InformationConnection InformationClient:192.168.1.1Server:10.10.10.2BytesEntry:Received: 5412Encryption:Sent:5416PacketsEncrypted: 39Decrypted: 31Transparent Tunneling:InactiveDiscarded: 8Compression:Bypassed: 22Compression:	VPN Client   Statistics	
VSConnection InformationClient:192.168.1.1Entry:MyVPNClientServer:10.10.10.2Time:0 day(s), 00:01.13BytesCryptoReceived:5412Encryption:56-bit DESSent:5416Authentication:HMAC-MD5PacketsTransportEncrypted:11Local LAN:DisabledDiscarded:8Compression:None	Tunnel Details Route Details	Firewall
BytesCryptoReceived: 5412Encryption:56-bit DESSent:5416Authentication:HMAC-MD5PacketsTransportEncrypted: 39Transparent Tunneling:InactiveDecrypted: 31Local LAN:DisabledDiscarded: 8Compression:NoneBypassed: 2224	لمج Address Information Client: 192.168.1.1 Server: 10.10.10.2	Connection Information Entry: MyVPNClient Time: 0 day(s), 00:01.13
Packets     Transport       Encrypted: 39     Transparent Tunneling:Inactive       Decrypted: 31     Local LAN:       Discarded: 8     Compression:       Bypassed: 22	<b>Bytes</b> Received: 5412 Sent: 5416	Crypto Encryption: 56-bit DES Authentication: HMAC-MD5
	Packets Encrypted: 39 Decrypted: 31 Discarded: 8 Bypassed: 22	Transport Transparent Tunneling:Inactive Local LAN: Disabled Compression: None
		Close

diesem Fenster werden Split-Tunneling-Informationen

e	VPN Client	Statistics		D
	Tunnel Details	Route Details Firev	vall	
	Local LAN Route	\$	Secured Routes	:
	Network	Subnet Mask	Network	Subnet Mask
			0.0.0.0	0.0.0.0
_	1		1	
				Close

#### ASA/PIX Security Appliance - Befehle anzeigen

• show crypto isakmp sa - Zeigt alle aktuellen IKE-SAs in einem Peer an. ASA#show crypto isakmp sa

```
Active SA: 1
     Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
 Total IKE SA: 1
     IKE Peer: 10.10.10.1
 1
                               Role
                                      : responder
     Type : user
     Rekey
             : no
                               State
                                       : AM_ACTIVE
• show crypto ipsec sa - Zeigt alle aktuellen IPsec-SAs in einem Peer an.
 ASA#show crypto ipsec sa
 interface: Outside
     Crypto map tag: SYSTEM_DEFAULT_CRYPTO_MAP, seq num: 65535, local addr: 10.10
 .10.2
       local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
       remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0)
       current_peer: 10.10.10.1, username: cisco123
       dynamic allocated peer ip: 192.168.1.1
       #pkts encaps: 20, #pkts encrypt: 20, #pkts digest: 20
       #pkts decaps: 74, #pkts decrypt: 74, #pkts verify: 74
       #pkts compressed: 0, #pkts decompressed: 0
       #pkts not compressed: 20, #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
       #send errors: 0, #recv errors: 0
       local crypto endpt.: 10.10.10.2, remote crypto endpt.: 10.10.10.1
```

```
path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: F49F954C
    inbound esp sas:
      spi: 0x3C10F9DD (1007745501)
         transform: esp-des esp-md5-hmac none
         in use settings ={RA, Tunnel, }
        slot: 0, conn id: 24576, crypto-map: SYSTEM DEFAULT CRYPTO MAP
         sa timing: remaining key lifetime (sec): 27255
        IV size: 8 bytes
        replay detection support: Y
    outbound esp sas:
      spi: 0xF49F954C (4104099148)
         transform: esp-des esp-md5-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 24576, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP
        sa timing: remaining key lifetime (sec): 27255
        IV size: 8 bytes
        replay detection support: Y
ciscoasa(config)#debug icmp trace
!--- Inbound Nat Translation is shown below for Outside to Inside ICMP echo request
translating Outside:192.168.1.1/768 to inside:172.16.1.2/1
ICMP echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=7936 len=3
2
!--- Inbound Nat Translation is shown below for Inside to Outside ICMP echo reply
untranslating inside:172.16.1.2/1 to Outside:192.168.1.1/768
ICMP echo request from Outside:192.168.1.1 to inside:172.16.1.3 ID=768 seq=8192
len=32
ICMP echo request translating Outside:192.168.1.1/768 to inside:172.16.1.2/1
ICMP echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=8192 len=3
2
ICMP echo reply untranslating inside:172.16.1.2/1 to Outside:192.168.1.1/768
ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8448 len=32
ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8448 len=32
ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8704 len=32
ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8704 len=32
ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8960 len=32
ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8960 len=32
```

#### **Fehlerbehebung**

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Das <u>Output Interpreter Tool</u> (nur <u>registrierte</u> Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Weitere Informationen zur Fehlerbehebung bei Site-Site-VPNs finden Sie unter <u>Häufigste L2L-</u> <u>und Remote Access IPSec VPN-Problemlösung</u>.

## Zugehörige Informationen

- <u>Cisco Adaptive Security Appliances der Serie ASA 5500</u>
- <u>Cisco Adaptive Security Device Manager</u>
- <u>Cisco Adaptive Security Appliances der Serie ASA 5500 Fehlerbehebung und</u>
   <u>Warnmeldungen</u>
- <u>Technischer Support und Dokumentation Cisco Systems</u>