Beispiel für eine Stick-Konfiguration: PIX/ASA und VPN-Client für Public Internet VPN

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Zugehörige Produkte Konventionen Hintergrundinformationen Hairpinning oder U-Turn Konfigurationen Netzwerkdiagramm **CLI-Konfiguration von PIX/ASA** Konfigurieren von ASA/PIX mit ASDM **VPN-Client-Konfiguration** Überprüfen **VPN-Client-Verifizierung** Fehlerbehebung Zugehörige Informationen

Einführung

In diesem Dokument wird beschrieben, wie Sie eine ASA Security Appliance 7.2 oder höher einrichten, um IPsec auf einem Stick auszuführen. Diese Konfiguration gilt für einen bestimmten Fall, in dem ASA kein Split-Tunneling zulässt und Benutzer eine direkte Verbindung mit der ASA herstellen, bevor sie das Internet nutzen dürfen.

Hinweis: In PIX/ASA Version 7.2 und höher<u>ermöglicht</u> das <u>Intra-Interface-Schlüsselwort den</u> gesamten Datenverkehr, dieselbe Schnittstelle einzugeben und zu verlassen, und nicht nur den <u>IPsec-Datenverkehr</u>.

Weitere Informationen zum Abschluss einer ähnlichen Konfiguration auf einem Router an einem zentralen Standort finden Sie unter <u>Router und VPN-Client für das öffentliche Internet in einem Stick-Konfigurationsbeispiel</u>.

Unter Konfigurationsbeispiel für PIX/ASA 7.x Enhanced Spoke-to-Client VPN mit TACACS+-Authentifizierung erfahren Sie mehr über das Szenario, in dem der Hub PIX den Datenverkehr vom VPN-Client an den Spoke-PIX umleitet.

Hinweis: Um eine Überschneidung von IP-Adressen im Netzwerk zu vermeiden, weisen Sie dem

VPN-Client einen völlig anderen Pool von IP-Adressen zu (z. B. 10.x.x.x, 172.16.x.x und 192.168.x.x). Dieses IP-Adressierungsschema ist hilfreich bei der Fehlerbehebung in Ihrem Netzwerk.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Die Hub-PIX/ASA Security Appliance muss Version 7.2 oder höher ausführen
- Cisco VPN Client Version 5.x

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der PIX- oder ASA Security Appliance Version 8.0.2 und dem Cisco VPN Client Version 5.0.

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 7.2 oder höher verwendet werden.

Konventionen

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

Hintergrundinformationen

Hairpinning oder U-Turn

Diese Funktion ist nützlich für VPN-Datenverkehr, der in eine Schnittstelle eintritt, aber dann über diese Schnittstelle weitergeleitet wird. Wenn Sie beispielsweise über ein Hub-and-Spoke-VPN-Netzwerk verfügen, in dem die Sicherheits-Appliance der Hub ist und die Remote-VPN-Netzwerke Spokes bilden, muss der Datenverkehr zur Sicherheits-Appliance und dann wieder zum anderen Spoke übertragen werden.

Verwenden Sie den Befehl für den gleichen Sicherheitsdatenverkehr, damit der Datenverkehr dieselbe Schnittstelle betritt und verlässt.

Hinweis: Hairpinning oder U-Turn ist auch für die Kommunikation zwischen VPN-Client und VPN-Client geeignet.

Konfigurationen

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das <u>Command Lookup Tool</u> (nur <u>registrierte</u> Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Public Internet

CLI-Konfiguration von PIX/ASA

• <u>PIX/ASA</u>

Konfiguration auf PIX/ASA ausführen
PIX Version 8.0(2)
names
!

```
interface Ethernet0
nameif outside
security-level 0
ip address 172.18.124.98 255.255.255.0
!
interface Ethernet1
nameif inside
security-level 100
ip address 172.16.3.101 255.255.255.0
!
interface Ethernet2
shutdown
no nameif
no security-level
no ip address
1
interface Ethernet3
shutdown
no nameif
no security-level
no ip address
1
interface Ethernet4
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet5
shutdown
no nameif
no security-level
no ip address
1
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
ftp mode passive
!--- Command that permits IPsec traffic to enter and
exit the same interface. same-security-traffic permit
intra-interface
access-list 100 extended permit icmp any any echo-reply
pager lines 24
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500
ip local pool vpnpool
  192.168.10.1-192.168.10.254 mask 255.255.255.0
no failover
monitor-interface outside
monitor-interface inside
icmp permit any outside
no asdm history enable
arp timeout 14400
nat-control !--- The address pool for the VPN Clients. !-
-- The global address for Internet access used by VPN
Clients. !--- Note: Uses an RFC 1918 range for lab
setup. !--- Apply an address from your public range
provided by your ISP.
global (outside) 1 172.18.124.166
```

--- The NAT statement to define what to encrypt (the addresses from the vpn-pool). nat (outside) 1 192.168.10.0 255.255.255.0 nat (inside) 1 0.0.0.0 0.0.0.0 static (inside,outside) 172.16.3.102 172.16.3.102 netmask 255.255.255.255 access-group 100 in interface outside route outside 0.0.0.0 0.0.0.0 172.18.124.98 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 timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute !--- The configuration of group-policy for VPN Clients. group-policy clientgroup internal group-policy clientgroup attributes vpn-idle-timeout 20 !--- Forces VPN Clients over the tunnel for Internet access. split-tunnel-policy tunnelall no snmp-server location no snmp-server contact snmp-server enable traps snmp !--- Configuration of IPsec Phase 2. crypto ipsec transform-set myset esp-3des esp-sha-hmac !--- Crypto map configuration for VPN Clients that connect to this PIX. crypto dynamic-map rtpdynmap 20 set transform-set myset !--- Binds the dynamic map to the crypto map process. crypto map mymap 20 ipsec-isakmp dynamic rtpdynmap !--- Crypto map applied to the outside interface. crypto map mymap interface outside !--- Enable ISAKMP on the outside interface. isakmp identity address isakmp enable outside !--- Configuration of ISAKMP policy. isakmp policy 10 authentication pre-share isakmp policy 10 encryption 3des isakmp policy 10 hash sha isakmp policy 10 group 2 isakmp policy 10 lifetime 86400 isakmp policy 65535 authentication pre-share isakmp policy 65535 encryption 3des isakmp policy 65535 hash sha isakmp policy 65535 group 2 isakmp policy 65535 lifetime 86400 telnet timeout 5 ssh timeout 5 console timeout 0 !--- Configuration of tunnel-group with group

```
information for VPN Clients. tunnel-group rtptacvpn type
ipsec-ra
!--- Configuration of group parameters for the VPN
Clients. tunnel-group rtptacvpn general-attributes
address-pool vpnpool
!--- Disable user authentication. authentication-server-
group none
!--- Bind group-policy parameters to the tunnel-group
for VPN Clients. default-group-policy clientgroup
tunnel-group rtptacvpn ipsec-attributes
pre-shared-key *
class-map inspection_default
match default-inspection-traffic
!
1
policy-map global_policy
class inspection_default
inspect dns maximum-length 512
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
Cryptochecksum: 1a1ad58226e700404e1053159f0c5fb0
: end
```

Konfigurieren von ASA/PIX mit ASDM

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

1. Wählen Sie im Hauptfenster **Wizards > IPsec VPN Wizard** aus.

🚰 Cisco ASDM 6.0 fe	or PIX - 172.16.3.101				
<u>File View T</u> ods	Wizards <u>W</u> indow <u>H</u> el	P			
Home 🖧 Cor	Startup Wizard			Back 🕜 Forward 🤌	
Device List	IPsec VPN Wizard				
Add Delete	High Availability and Packet Capture Wiz	l Scalability Wizar ard	d	Firewall Dashboard	
172.16.3.101		General License	e]	1	
		Host Name		Device Linking:	
		ASDM Version:		Device Type:	
		Firewall Mode:		Context Mode:	
		Total Flash		Total Memory:	
		PN Tunnels			
		IKE:	IPsec:		

2. Wählen Sie den Tunneltyp **Remote Access** VPN aus, und stellen Sie sicher, dass die VPN-Tunnel-Schnittstelle wie gewünscht eingestellt



3. Der einzige verfügbare VPN-Client-Typ ist bereits ausgewählt. Klicken Sie auf

Weiter.

👬 VPN Wizard	×
VPN Wizard	Remote Access Client (Step 2 of)
erandi	Remote access users of various types can open VPN tunnels to this PIX. Select the type of VPN client for this tunnel.
	VPN Client Type:
(arroptate)	 Cisco VPN Client, Release 3.x or higher;
Network	or other Easy VPN Remote product
THE IN	C 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.
	E PAP F CHAP MS-CHAP-VI E MS-CHAP-VZ EAP-PROXY
	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 > Einish ⊆ancel Help

4. Geben Sie einen Namen für den Tunnelgruppennamen ein. Geben Sie die zu verwendenden Authentifizierungsinformationen an. Vorinstallierter Schlüssel wird in diesem Beispiel ausgewählt.

💏 VPN Wizard	X
VPN Wizard	VPN Client Authentication Method and Tunnel Group Name (Step 3 of)
Branch Branch ISP ISP ISP ISP ISP ISP ISP ISP ISP ISP	The PIX allows you to group remote access tunnel users based on common connection parameters and client 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 client. Authentication Method Pre-shared key Pre-Shared Key: cisco123 Certificate
	Certificate Signing Algorithm: rsa-sig Certificate Name:
	Tunnel Group Tunnel Group Name: htptacvpn
	<u>≤Back N</u> ext> Einish <u>C</u> ancel <u>H</u> elp

Hinweis: Es gibt keine Möglichkeit, den Pre-Shared Key auf dem ASDM auszublenden/zu verschlüsseln. Der Grund hierfür ist, dass das ASDM nur von Personen verwendet werden darf, die die ASA konfigurieren, oder von Personen, die den Kunden bei dieser Konfiguration unterstützen.

5. 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 6 Benutzer hinzu. Hinweis: Informationen zur Konfiguration einer externen AAA-Servergruppe über ASDM finden Sie unter <u>PIX/ASA 7.x Authentication</u> and Authorization Server Groups für VPN-Benutzer unter <u>ASDM Configuration Example</u> (Beispiel für die ASDM-Konfiguration).

🙀 VPN Wizard	×
VPN Wizard	Client Authentication (Step 4 of)
arman arman	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.
Network	Authenticate using the local user database
THE SEA	C Authenticate using an AAA server group
	AAA Server Group Name:
	<u>≤Back Next> Einish Çancel Help</u>

6. Fügen Sie bei Bedarf Benutzer zur lokalen Datenbank hinzu. Hinweis: Entfernen Sie aktuelle Benutzer nicht aus diesem Fenster. Wählen Sie im ASDM-Hauptfenster die Optionen Konfiguration > Geräteverwaltung > Verwaltung > Benutzerkonten aus, um vorhandene Datenbankeinträge zu bearbeiten oder aus der Datenbank zu entfernen.

🚰 VPN Wizard		×		
VPN Wizard	User Accounts (Step 5 of 11)			
	Add new users into the user authenti or to remove them from the database Users/AAA > User Accounts in the m	cation database. To edit existing entries in the database e, go to Configuration > Device Management > ain ASDM window.		
Home	User to Be Added			
Corporate Network	Username:	stick		
	Password (optional):	Delete		
	Confirm Password (optional):			
		≤Back Next > Enish Cancel Help		

7. Definieren Sie einen Pool lokaler Adressen, der Remote-VPN-Clients bei der Verbindung dynamisch zugewiesen wird.

📸 VPN Wizard		×
VPN Wizard	Address Pool (Step 6 of 11)	
	Enter a pool of local addresses to be us clients.	ed for assigning dynamic IP addresses to remote VPN
Colporate Network	Tunnel Group Name :	rtptacvpn
The said	Pool Name:	vpnpool
A A A A A A A A A A A A A A A A A A A	-Pool Settings	
	Range Start Address:	192.168.10.1
	Range End Address:	192,168,10,254
	Subnet Mask:	255.255.255.0
		<u>≤Back N</u> ext > Einish, <u>Cancel</u> <u>H</u> elp

8. *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)			
Brandh Brandh Brandh Brandh	Attributes you configure below are pushed to the VPN client when the client connects to the PIX. If you do not want an attribute pushed to the client, leave the corresponding field blank.			
Corporate)	Tunnel Group: rtptacvpn			
Notwork	Primary DNS Server:			
	Secondary DNS Server:			
	Primary WINS Server:			
	Secondary WINS Server:			
S.P.	Default Domain Name:			
	<u>≤ Back</u> <u>N</u> ext > Enish <u>ancel</u> <u></u> Help			

 Geben Sie die Parameter f
ür IKE an, auch als IKE-Phase 1 bezeichnet.Konfigurationen auf beiden Seiten des Tunnels m
üssen genau
übereinstimmen, aber der Cisco VPN Client w
ählt automatisch die richtige Konfiguration f
ür sich aus. Auf dem Client-PC ist keine IKE-Konfiguration erforderlich.

🔂 VPN Wizard		×
VPN Wizard	IKE Policy (Step 8 of 11)	a 200 Printi
Barrison Barrison Barrison Hearrison Hearrison	Select the encryption algorithm, authentication algorithm, and Diffie-Hellman 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.	
Corporato	Encryption: 3DES Authentication: SHA	
	DH Group:	
	BackNext > ⊟nishGancelHe	elp

10. Geben Sie die Parameter für IPSec an, auch als IKE-Phase 2 bezeichnet.Konfigurationen auf beiden Seiten des Tunnels müssen genau übereinstimmen, aber der Cisco VPN Client wählt automatisch die richtige Konfiguration für sich aus. Auf dem Client-PC ist keine IKE-Konfiguration erforderlich.

💏 VPN Wizard	×			
VPN Wizard	IPsec Encryption and Authentication (Step 9 of 11)			
	Select the encryption and authentication algorithms for this IPsec VPN tunnel. Configurations on both sides of the connection must match exactly.			
Carbonnin (Encryption: SDES Authentication: SHA:			

11. Geben Sie an, welche internen Hosts oder Netzwerke Remote-VPN-Benutzern ausgesetzt werden können, falls vorhanden. Wenn Sie diese Liste leer lassen, können Remote-VPN-Benutzer auf das gesamte interne Netzwerk der ASA zugreifen. In diesem Fenster können Sie auch Split-Tunneling aktivieren. Split-Tunneling verschlüsselt den Datenverkehr mit den zuvor in diesem Verfahren definierten Ressourcen und bietet im Allgemeinen unverschlüsselten Zugriff auf das Internet, indem dieser Datenverkehr nicht getunnelt wird. Wenn Split-Tunneling *nicht* aktiviert ist, wird der gesamte Datenverkehr von Remote-VPN-Benutzern an die ASA getunnelt. Je nach Konfiguration kann dies zu einer sehr hohen Bandbreite und einem hohen Prozessor führen.

I'W WIZalu	Address Translation Exemption and Split Tur	ineling (Optional) (Step 10 of 11)
	Network Address Translation (NAT) is used to hid make exceptions to NAT to expose the entire or p users protected by VPN. To expose the entire network behind the most se leave the selection list blank.	e the internal network from outside users. You can art of the internal network to authenticated remote cure interface to remote VPN users without NAT,
Corporate		Selected Hosts/Networks:
THE THE	Host/Network	any
	Interface: inside	Add
A A A	Address: any	Delete
S.S-	Enable split tunneling to let remote users hav defined above, and unencrypted access to the	e simultaneous encrypted access to the resources re internet.

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



13. Konfigurieren Sie den Befehl **same** Sicherheit-**Verkehr**, um den Datenverkehr zwischen zwei oder mehr Hosts zu aktivieren, die mit derselben Schnittstelle verbunden sind, wenn Sie auf das Kontrollkästchen wie gezeigt klicken:

File Yiew Tools Wizards Wind	dow Help	Look For	1		Find		diada.
home 🖧 Configuration	Monitoring Save 🐼 Ref	resh 🔇 Back	Forwe	rd ? H	lelp		cisco
Device Setup 급 무 ×	Configuration > Device !	Setup > Interfa	ces			11111	C
Startup Wizard	Interface	Name	Enabled	Security Level	IP Address	SI	Add 👻
Provide March Decoursed	Ethernet0	outside	Yes	- 0	172.18.124.98	255.2	Can
Custom Time	Ethernet1	inside	Yes	100	172.16.3.101	255,2	Eat
e O System Time	Ethernet2		No				maria
	Ethernet3		No				rania
	Ethernet4		No				
	Ethernet5		No		E.E.		
A Device Setup							
A Device Setup					****	1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.	
Device Setup Errewal Remote Access VPN						×	
Evice Setup Frewal Remote Access VPN		two or more interf	faces which a	are configure	ed with same secu	rity levels	
Device Setup Firewal Remote Access VPN Ste-to-Site VPN Device Management	I Enable traffic between I Enable traffic between I I I I I I I I I I I I I I I I I I	two or more inter	faces which a	are configure	ed with same secur interface	rity levels :	
Device Setup Eirewal Eirewal Eemote Access VPN Site-to-Site VPN Device Management	Enable traffic between Enable traffic between	two or more inter two or more hosts	faces which a s connected (are configure to the same Reset	ed with same secur interface	₽ rity levels	

14. Wählen Sie **Configuration > Firewall >NAT Rules**, und klicken Sie auf **Add Dynamic NAT Rule (Dynamische NAT-Regel hinzufügen)**, um diese dynamische Übersetzung mit ASDM zu

erstellen.

Cisco ASDM 6.0 for PIX - 172.16.3.1	101		
<u>File View T</u> ools Wizards <u>W</u> indow	Help	Lo	sk.For:
Home 🔥 Configuration 🐼 Mon	itoring 🔚 Save 🛞 Refresh 🔇 Back 🔇	Forward 💡 Help	
Device List 📑 🔍 🗙	Configuration > Firewall > NAT Bules		
Add Delete S Connect	🗣 Add 🔹 🧭 Edik 🏦 Delete 🔶 🗲	🗶 🖻 🏙 - 🔍 Find 🖽 Di	agram 🦉 Pathet Trace
172.16.3.101	Add Static NAT Rule		- Filter Clear 🔯
	Add Dynamic NAT Rule	Original	Transla
	😅 Add NAT Exempt Rule	Destination Service	Interface Ad
1 1	Add Static Policy NAT Rule		
1 1	Add Dynamic Policy NAT Rule		
	Insert		
Firewall 🗇 🗘 🗡	Tinsert After		
AAA Rules			
Hiter Rules			
E-Cobjects			
E B Advanced			
1			
Device Setup			
Ricewall	4		nenenenenenenen i
Different line life			F 🖷 🔟
Remote Access VPN	Real Address	Translated Address	
Ste-to-Site VPN	Source Address	🔶 📢 NAT Type ┥ 🚥 🖬 🌺	Destination Address
Device Management	Enable traffic through the firewall without ad	dress translation	

15. Wählen Sie **innen** als Quellschnittstelle aus, und geben Sie die Adressen ein, die Sie NAT hinzufügen möchten. Wählen Sie als Übersetzen der Adresse auf der Schnittstelle die Option **Außen** aus, und klicken Sie auf

ource: 0.	0.0.0		
nslated			
Pool ID	l pool for dynamic translation. Interface	Addresses Pool	
0	(outbound)	Same as original address (identity)	
0 1	(inbound) outside	Same as original address (identity)	Manage
unnection S	offinac		

16. Wählen Sie außen als Quellschnittstelle aus, und geben Sie die Adressen ein, die Sie NAT

hinzufügen möchten. Wählen Sie als Übersetzen der Adresse auf der Schnittstelle die Option **Außen** aus, und klicken Sie auf

urce: 1	32.168.10.0	-	
slated	l pool for dynamic translation.		
Pool ID	Interface	Addresses Pool	
0	(outbound)	Same as original address (identity)	
0 (inbound)		Same as original address (identity)	
1	putside	■ 172.18.124.166	Manage

17. Die Übersetzung wird unter Übersetzungsregeln unter Konfiguration > Firewall >NAT Rules angezeigt.

Cisco ASDM 6.0 for PIX - 172.	16.3.101						
le <u>V</u> iew <u>T</u> ools Wi <u>z</u> ards <u>W</u> ir	ndow <u>H</u> elp				Loo	k For:	
home 🖧 Configuration	Monitoring	🔜 Save 🔇	Refresh 🔇 Back 💮) Forward 🧖 Help			
Device List ⊡ ≏ ×	Configura	tion > Firewall >	NAT Rules				
🖡 Add 📋 Delete 🚿 Connect	Add	• 🕑 Edit 🔒	Delete 🛉 💰 👗		ind 💽 Diagram	🔄 Packet Tra	ce
- 10.77.241.143	Ethou Cont	ninal Counce		11		Eller	Chear I
17210-5-101	Filter: Jon	jinai source				- Inca	Ciedi 🖬
	#	Туре		Original	Envire	Interferen I	Iranslated
	(=) inside		Source	Desthation	Service	Interface	HOOLESS
	1	Dynamic	B , 0.0.0.0		outs	ide	172.18.124
	2	Dynamic	192.168.10.0		outsi	de	172.18.124
Threat Detection Objects Advanced							
Device Setup							
Firewall	•						
Remote Access VPN		0.0.0	.0 0.0.0.0	172.18	.124.166	- 🐠	×
Site-to-Site VPN			•••••	Dynamic = = = =	• 🔶 D	estination Addres	15
Device Management	T Enable	traffic through th	e firewall without address b	anslation			
*			Ap	ply Reset			

Anmerkung 1: Der Befehl <u>sysopt connection permit-vpn</u> muss konfiguriert werden. Der Befehl <u>show running-config sysopt</u> überprüft, ob die Konfiguration vorgenommen wurde.

Anmerkung 2: Fügen Sie diese Ausgabe für den optionalen UDP-Transport hinzu:

group-policy clientgroup attributes vpn-idle-timeout 20 ipsec-udp enable ipsec-udp-port 10000

split-tunnel-policy tunnelspecified split-tunnel-network-list value splittunnel

Anmerkung 3: Konfigurieren Sie diesen Befehl in der globalen Konfiguration der PIX-Appliance, damit VPN-Clients über IPsec über TCP eine Verbindung herstellen können:

isakmp ipsec-over-tcp port 10000

Hinweis: Weitere Informationen zu den verschiedenen Szenarien, in denen Haarpinning verwendet werden kann, <u>finden Sie im</u> Video <u>Hair Pinning auf Cisco ASA</u>.

VPN-Client-Konfiguration

Gehen Sie wie folgt vor, um den VPN-Client zu konfigurieren:

1. Wählen Sie

onnection Entries	Status Certifica	tes Lon Ontions	Help	
Connect N	ew Import	Modily	Delete	cisco
Conr	nection Entry /		Host	Transport
Lonr	iection Entry /		Host	Transport

2. Geben Sie die IP-Adresse der externen PIX-Schnittstelle und den Namen der Tunnelgruppe zusammen mit dem Kennwort für die Authentifizierung

VPN Client	Create New VPN Connect	ion Entry	×		
Connection Entry: pix					
Description: pix		cisco			
Host: 17					
Authentication 1	ransport Backup Servers	Dial-Up			
Group Authentication G Mutual Group Authentication					
Name:	rtptacvpn				
Password:	*****				
Confirm Password					
C Certificate Author Name:	ificate Chain				
Erase User Passwor	d	Save	Cancel		

 (Optional) Klicken Sie auf der Registerkarte Transport auf Transparentes Tunneling aktivieren. (Dies ist optional und erfordert die in <u>Hinweis 2</u> erwähnte zusätzliche PIX/ASA-Konfiguration.)

VPN Client Create New VPN Connect	ion Entry	X
Connection Entry: pix1		
Description: pix on a stick for internet connection	1 I	CISCO
Host: 172,18,124,98		
Authentication Transport Backup Servers	Dial-Up	
Enable Transparent Tunneling		
IPSec over UDP (NAT / PAT)		
C IPSec over TCP TCP Port 10000		
Allow Local LAN Access		
Peer response timeout (seconds): 90		
Erase User Password	Save	Cancel

4. Profil speichern

<u>Überprüfen</u>

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

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**.

- <u>show crypto isakmp sa</u>: Zeigt alle aktuellen IKE-Sicherheitszuordnungen (SAs) in einem Peer an.
- <u>show crypto ipsec sa</u>: Zeigt alle aktuellen SAs an. Suchen Sie nach verschlüsselten und entschlüsselten Paketen auf dem SA, die den VPN-Client-Datenverkehr definieren.

Versuchen Sie, vom Client aus einen Ping zu senden oder eine öffentliche IP-Adresse anzuzeigen (z. B. www.cisco.com).

Hinweis: Die interne Schnittstelle des PIX kann nur dann für die Erstellung eines Tunnels gepingt werden, wenn der <u>Befehl Management-Access im globalen Bestätigungsmodus konfiguriert ist.</u>

management-access inside

VPN-Client-Verifizierung

Führen Sie diese Schritte aus, um den VPN-Client zu überprüfen.

- 1. Klicken Sie mit der rechten Maustaste auf das im Systembereich angezeigte VPN Client-Sperrsymbol nach erfolgreicher Verbindung, und wählen Sie die Option für **Statistiken** zum Anzeigen von Verschlüsselungen und Entschlüsseln aus.
- 2. Klicken Sie auf die Registerkarte Route Details (Routendetails), um die Liste "Kein Split-Tunnel" zu überprüfen, die von der Appliance weitergeleitet wurde.

Fehlerbehebung

Hinweis: Weitere Informationen zur Fehlerbehebung bei VPN-Problemen finden Sie unter <u>VPN-</u> <u>Fehlerbehebungslösungen</u>.

Zugehörige Informationen

- Erweiterte Spoke-to-Client-VPN-Konfiguration Beispiel für PIX Security Appliance Version 7.0
- <u>Cisco VPN-Client</u>
- IPsec-Aushandlung/IKE-Protokolle
- <u>Cisco PIX Firewall-Software</u>
- <u>Cisco Secure PIX Firewall Befehlsreferenzen</u>
- Problemhinweise zu Sicherheitsprodukten (einschließlich PIX)
- Hair Pinning auf Cisco ASA
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation Cisco Systems