PIX/ASA en VPN-client voor publiek internet VPN op een tick Configuration-voorbeeld

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Verwante producten **Conventies** Achtergrondinformatie Helling of U-bocht Configuraties Netwerkdiagram CLI-configuratie van PIX/ASA ASA/PIX configureren met ASDM **VPN-clientconfiguratie** Verifiëren **VPN-clientverificatie** Problemen oplossen Gerelateerde informatie

Inleiding

Dit document beschrijft hoe u een ASA security applicatie 7.2 kunt instellen en later IPsec op een stick. Deze instelling is van toepassing op een specifiek geval waarin de ASA geen gesplitste tunneling toestaat en gebruikers direct verbinding maken met de ASA voordat ze naar internet mogen.

Opmerking: In PIX/ASA versie 7.2 en later<u>staat</u> het <u>intra-interface</u> sleutelwoord al verkeer toe om dezelfde interface in te gaan en te verlaten en niet alleen IPsec-verkeer.

Raadpleeg <u>Router en VPN-client voor publiekelijk internet op een voorbeeld van de configuratie</u> <u>van de</u> stok om een soortgelijke configuratie op een centrale site router te voltooien.

Raadpleeg <u>PIX/ASA 7.x Enhanced Spoke-to-Client VPN met het Configuratievoorbeeld van</u> <u>TACACS+ Verificatie</u> om meer te weten te komen over het scenario waarin de hub PIX het verkeer van de VPN-client naar de opgenomen PIX omwijst.

Opmerking: om overlapping van IP-adressen in het netwerk te voorkomen, moet u een volledig andere pool van IP-adressen aan de VPN-client toewijzen (bijvoorbeeld 10.x.x, 172.16.x.x en 192.168.x.x). Deze IP-adresseringsregeling is behulpzaam bij het oplossen van uw netwerk.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- De hub PIX/ASA security applicatie moet versie 7.2 of hoger uitvoeren
- Cisco VPN-clientversie 5.x

Gebruikte componenten

De informatie in dit document is gebaseerd op versie 8.0.2 van het PIX- of ASAbeveiligingsapparaat en versie 5.0 van Cisco VPN-client.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Verwante producten

Deze configuratie kan ook worden gebruikt met Cisco PIX security applicatie versie 7.2 en hoger.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrondinformatie

Helling of U-bocht

Deze optie is handig voor VPN-verkeer dat een interface invoert maar vervolgens uit dezelfde interface wordt routeerd. Bijvoorbeeld, als u een netwerk van hub en sprak VPN, waar het veiligheidsapparaat de hub is, en de afgelegen VPN-netwerken zijn spaken, zodat de één sprak met een ander gesproken, moet het verkeer in het security apparaat gaan en dan weer naar de ander uitgezocht.

Gebruik de opdracht **Dezelfde security-traffic** om verkeer in te voeren en dezelfde interface te verlaten.

 $\texttt{securityappliance(config)} \\ \texttt{#same-security-traffic permit intra-interface} \\$

N.B.: Helling of U-bocht is ook van toepassing voor VPN-client voor VPN-communicatie.

Configuraties

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het <u>Opname Gereedschap</u> (<u>alleen geregistreerde</u> klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Public Internet

CLI-configuratie van PIX/ASA

• <u>PIX/ASA</u>

Configuratie uitvoeren op PIX/ASA
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
!
interface Ethernet3
shutdown
no nameif
no security-level
no ip address
1
interface Ethernet4
shutdown
no nameif
no security-level
no ip address
1
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-servergroup 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
!
!
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
```

ASA/PIX configureren met ASDM

Voltooi deze stappen om Cisco ASA als een externe VPN-server met ASDM te configureren:

1. Kies **Wizard > IPsec VPN-wizard** in het startvenster.

🚮 Cisco ASDM 6.0 f	or PIX - 172.16.3.10	1	
File View Tools	Wizards Window	Help	
Home 🖧 Cor	Startup Wizard	•	Back 🕥 Forward
	IPsec VPN Wizan	d,	
Add Delete	High Availability	and Scalability Wizard Wizard Device Information	Firewall Dashboard
172.16.310		General License	t.
		Host Name	
		PIX Version:	Device Uptime:
		ASDM Version:	Device Type:
		Firewall Mode:	Context Mode:
		Total Flash	Total Memory:
		VPN Tunnels	
		IKE: IPsec:	

2. Kies het tunneltype **Remote Access** VPN en controleer of de VPN-tunnelinterface naar wens is



3. Het enige beschikbare VPN-clienttype is al geselecteerd. Klik op

Volgende.

💏 VPN Wizard	×
VPN Wizard	Remote Access Client (Step 2 of)
and and a	Remote access users of various types can open VPN tunnels to this PIX. Select the type of VPN client for this tunnel.
E in	VPN Client Type:
(Curriotate)	 Cisco VPN Client, Release 3.x or higher;
Network	or other Easy VPN Remote product
Trate Ita	Microsoft Windows client using L2TP over IPsec
LINK	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 E 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. Voer een naam in voor de naam van de tunnelgroep. Verstrek de te gebruiken authenticatie informatie. **Vooraf gedeelde sleutel** is in dit voorbeeld geselecteerd.

💏 VPN Wizard	×
VPN Wizard	VPN Client Authentication Method and Tunnel Group Name (Step 3 of)
Brands Br	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:
AULI	C Challenge/response authentication (CRACK)
	Tunnel Group
and the second s	Tunnel Group Name: rtptacypn
	<u>≤Back Next> Einish ⊊ancel Help</u>

N.B.: Er is geen manier om de voorgedeelde toets op de ASDM te verbergen of te versleutelen. De reden is dat ASDM alleen gebruikt mag worden door mensen die de ASA configureren of door mensen die de klant bijstaan met deze configuratie.

5. Kies of u externe gebruikers wilt geauthentiseerd worden naar de lokale gebruikersdatabase of naar een externe AAA server groep. Opmerking: U voegt in stap 6 gebruikers toe aan de lokale gebruikersdatabase. Opmerking: Raadpleeg <u>PIX/ASA 7.x-groepen voor VPN-</u> <u>gebruikers via het ASDM Configuration Voorbeeld</u> voor informatie over de configuratie van een externe AAA-servergroep via ASDM.

💏 VPN Wizard	×
VPN Wizard	Client Authentication (Step 4 of)
	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
	Authenticate using an AAA server group AAA Server Group Name: New
	<u>≤Back Next> Einish Çancel Help</u>

6. Voeg indien nodig gebruikers toe aan de lokale database.N.B.: Verwijder de huidige gebruikers niet uit dit venster. Kies Configuratie > Apparaatbeheer > Administratie > Gebruikersrekeningen in het hoofdvenster van ASDM om bestaande items in de database te bewerken of deze uit de database te verwijderen.

💏 VPN Wizard		×
VPN Wizard	User Accounts (Step 5 of 11)	
erman Barrent Barrent Barrent Barrent	Add new users into the user authent or to remove them from the databas Users/AAA > User Accounts in the m	ication database. To edit existing entries in the database e, go to Configuration > Device Management > ain ASDM window.
Home	User to Be Added	
Corporato	Usernamé:	stick
	Password (optional):	Delete
C C	Confirm Password (optional):	
		Back: Next> Enistri ⊆ancel Help

7. Defineert een pool van lokale adressen die dynamisch aan externe VPN-clients moeten worden toegewezen wanneer ze verbinding maken.

📸 VPN Wizard	\mathbf{x}
VPN Wizard	Address Pool (Step 6 of 11)
	Enter a pool of local addresses to be used for assigning dynamic IP addresses to remote VPN clients.
Corporate Network	Tunnel Group Name : rtptacvpn
FILE IN	Pool Name: vpnpool New
	Pool Settings
	Range Start Address: 192.168.10.1
	Range End Address: 192.168.10.254
	Subnet Mask: 255.255.255.0
S.P.	
	<u>≤Back N</u> ext > <u>Einish</u> <u>Cancel</u> <u>H</u> elp

8. *Optioneel:* Specificeer de DNS- en WINS-serverinformatie en een standaardnaam voor domeinen die naar externe VPN-clients moet worden geduwd.

🖆 VPN Wizard	×
VPN Wizard	Attributes Pushed to Client (Optional) (Step 7 of 11)
	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 Corporate	Tunnel Group: rtptacvpn
Norwork	Primary DN5 Server:
	Secondary DNS Server:
	Primary WINS Server:
	Secondary WINS Server:
S.A.	Default Domain Name:
	<u>≤ Back</u> <u>Next</u> > Enish <u>Cancel</u> <u>Help</u>

9. Specificeer de parameters voor IKE, ook bekend als IKE Fase 1.De configuraties aan beide zijden van de tunnel moeten precies overeenkomen, maar de Cisco VPN-client kiest automatisch de juiste configuratie voor zichzelf. Er is geen IKE-configuratie nodig op de client-

pc.

💏 VPN Wizard		×
VPN Wizard	IKE Policy (Step 8 of 11)	17-18 10000
Brankton Brankton Harrison Harrison Harrison	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.	
Contraction National	Encryption: 3DES Authentication: SHA	
	DH Group:	
		lp

10. Specificeer de parameters voor IPSec, ook bekend als IKE fase 2.De configuraties aan beide zijden van de tunnel moeten precies overeenkomen, maar de Cisco VPN-client kiest automatisch de juiste configuratie voor zichzelf. Er is geen IKE-configuratie nodig op de client-

pc.

🚰 VPN Wizard	×
VPN Wizard	IPsec Encryption and Authentication (Step 9 of 11)
Barners Barners Barners Barners Barners	Select the encryption and authentication algorithms for this IPsec VPN tunnel. Configurations on both sides of the connection must match exactly.
Corporate Network	Encryption: SHA
	≤Back Next > Einişh ⊊ancel Help

11. Specificeer welke, als om het even welke, interne hosts of netwerken kunnen worden blootgesteld aan externe VPN-gebruikers.Als u deze lijst leeg laat, staat het externe VPNgebruikers toe om toegang te krijgen tot het gehele binnennetwerk van de ASA.U kunt ook gesplitste tunneling in dit venster inschakelen. Split-tunneling versleutelt het verkeer naar de bronnen die eerder in deze procedure zijn gedefinieerd en geeft onversleutelde toegang tot internet in het algemeen door dat verkeer niet uit te schakelen. Als gesplitste tunneling *niet* ingeschakeld is, wordt al het verkeer van externe VPN-gebruikers naar de ASA gekanaliseerd. Dit kan zeer bandbreedte en processor intensief worden, gebaseerd op uw configuratie.

VPN Wizard	Address Translation Exemption and Split Tunneling (Op	ptional) (Step 10 of 11)
	Network Address Translation (NAT) is used to hide the interna make exceptions to NAT to expose the entire or part of the in users protected by VPN. To expose the entire network behind the most secure interfa- leave the selection list blank.	al network from outside users. You can nternal network to authenticated remote ce to remote VPN users without NAT,
Corporate Network	Höst/Network	Selected Hosts/Networks: any
<u>UUU</u>	Address: any	Add Delete
<u>s</u>	- Enable split tunneling to let remote users have simultaner	ous encrypted access to the resources
23	defined above, and unencrypted access to the internet.	ous encrypted access to the resources

12. Dit venster geeft een samenvatting van de maatregelen die u hebt genomen. Klik op **Voltooien** als u tevreden bent met de configuratie.

13. Configureer het commando **verkeer met dezelfde beveiliging** om verkeer mogelijk te maken tussen twee of meer hosts die met dezelfde interface zijn verbonden wanneer u op het selectieteken klikt zoals aangegeven in de afbeelding:

le View Iools Wizards Windo	w Help Monitoring 🛄 Save 🔿 Ref	Look For	Enrate	nd 🤊 H	Enis	÷,	ihuhu
Device Setup	Configuration > Device !	Setup > Interfa	ces				
Startup Wizard	Interface	Name	Enabled	Security Level	IP Address	SL	Add 👻
B-+o+ Routing	Ethernet0	outside	Yes	- 0	172.18.124.98	255.2	I
Device Name/Password	Ethernet1	inside	Yes	100	172.16.3.101	255.2	Eat
System Time	Ethernet2	11.	No	-		1.1	Dalasia
	Ethernet3		No				reota.
	Ethernet4		No				
	Ethernet5	1	No			1.1.	
Bevice Setup							
A Device Setup	2 3.4 2.4 2 3.4 2.4 2 3.4 2.4 2 3.4 2.4 2 3.4 2.4 2 3.4 2.4 2 3.4 2.4 2 3.4 2.4 2 3.4 2.4 2 3.4 2.4 2 3.4 2.4 2 3.4 2.4 2 3.4 2.4 3 3.4 3.4 4 3.4 3.4 5 3.4 3.4 5 3.4 3.4 6 3.4 3.4 7 3.4 3.4 8 3.4 3.4 8 3.4 3.4 9 3.4 3.4 9 3.4 3.4 9 3.4 3.4 10 3.4 3.4 10 3.						
Device Setup Firewall						×	
Device Setup Frewall Remote Access VPN	I Enable traffic between I	two or more inter	faces which a	are configur	ed with same secu	rity levels	
Device Setup Frewal Remote Access VPN Ste-to-Site VPN Device Management	Enable traffic between	two or more inter	faces which a s connected t	are configure	ed with same secur interface	rity levels	

14. Kies **Configuratie > Firewall >NAT Regels** en klik op **Dynamische NAT Regel** toevoegen om deze dynamische vertaling met het gebruik van ASDM te maken.

Cisco ASDM 6.0 for PIX - 172.16.3	.101		
File View Tools Wizards Window	Help	k.For:	
Home 🖧 Configuration 📝 Mo	nitoring 🔚 Save 🛞 Refresh 🔇 Back (Forward ? Help	
Device List 📴 🕀 🗙	Configuration > Firewall > NAT Rules		
Add Delete S Connect	🗣 Add 🔸 🎯 Edit 🎯 Delete 🔶 🗲	🗶 🖻 🎆 - 🔍 Rind 🖼 Di	igram 💐 Packet Trace
172.16.3.101	Add Static NAT Rule		- Filter Clear 🔯
	Add Dynamic NAT Rule,	Original	Transla
1	Add NAT Exempt Rule	Destination Service	Interface Ad
	Add Static Policy NAT Rule		
	Add Dynamic Policy NAT Rule		
	1nsert		
FileWalt O V A	🐺 Insert After,		
- MAT Rules			
Q Service Policy Rules			
Filter Rules			
URL Filtering Servers			
Threat Detection Detection			
E- Advanced			
Cevice Setup			
Received			
C C C C C C C C C C C C C C C C C C C			
Remote Access VPN	Baal Addres	Translated address	
Ste-to-Site VPN	Source Address	NAT Type	Destination Address
Device Management	Enable traffic through the firewall without a	ddress translation	

15. Kies **binnen** als de broninterface en voer de adressen in die u wilt NAT. Kies **buiten** voor het **vertaaladres** op de interface en klik op

nterface: In	side	-	
ource: 0	.0.0.0	-	
nslated			
elect a globa	al pool for dynamic translation.		
Pool ID	Interface	Addresses Pool	
0	(outbound)	Same as original address (identity)	
0	(inbound)	Same as original address (identity)	
1	outside	172.18.124.166	Manage
nnection 9	Settings		

16. Kies **buiten** als de broninterface en voer de adressen in die u wilt NAT. Kies **buiten** voor het **vertaaladres** op de interface en klik op

OK.

nterface:	outside	-	
ource:	192.168.10.0		
nslated -			
elect a gli	obal pool for dynamic translation	٦.	
Pool II	D Interface	Addresses Pool	
0	(outbound)	Same as original address (identity)	
0	(inbound)	Same as original address (identity)	
1	outside	172.18.124.166	Manage
nnectio	n Settinos		
nnectio	n Settings		

17. De vertaling verschijnt in de vertaalregels bij **Configuration > Firewall >NAT** Rules

Cisco ASDM 6.0 for PIX - 172.	16.3.101					
File View Tools Wizards Wir	ndow <u>H</u> elp				Look For:	
🚳 Home 🖓 Configuration 👩	Monitoring 🔛 Save	🔇 Refresh 🔇 Back 🤇) Forward 🢡 He	tip		
Device List 🖃 ല 🗡	Configuration > Firew	all > NAT Rules				
Add 📋 Delete 🚿 Connect	🗣 Add 👻 🛃 Edit	î Delete 🛧 🗲 👗	Ba 🖹 - 🔍	Find 🖭 Diag	ram 🥰 Packet Tr	ace
10.77.241.143 172.16.3.101	Filter: Original Source	• 6 •			- Filter	Clear 🔣
	+ Tune		Original			Translated
		Source	Destination	Service	Interface	Address
	🗆 inside		and the second second			
	2 J Dynamic	A 0.0.0.0 192 168 10.0			outside	172.18.124
Device Setup						
Firewall	1			rio kitkinki	and the second second	
Remote Access VPN	0	.0.0.0 0.0.0.0	a outs	ide 18.124.166	+ *	
Ste-to-Site VPN	🗖 Enable traffic throw	en e	Dynamic		Destination Addre	:55
Device Management	j jenave vanic tirou	grane newai victioa, address				
*		A	pply Reset			

Opmerking 1: De **opdracht**<u>voor</u> de <u>systeemverbinding</u> moet worden geconfigureerd. Het <u>tonen in</u> <u>werking stellen-</u>enig systeem bevel verifieert of het wordt gevormd.

Noot 2: Voeg deze output voor het optionele UDP transport toe:

<u>group-policy clientgroup attributes</u> <u>vpn-idle-timeout 20</u> <u>ipsec-udp enable</u> <u>ipsec-udp-port 10000</u> <u>split-tunnel-policy tunnelspecified</u> <u>split-tunnel-network-list value splittunnel</u>

Noot 3: Configureer deze opdracht in de mondiale configuratie van het PIX-apparaat zodat VPNclients via IPsec over TCP kunnen worden aangesloten:

isakmp ipsec-over-tcp port 10000

Opmerking: Raadpleeg het <u>Hair-Pinning op Cisco ASA</u> -video voor meer informatie over verschillende scenario's waar haarspelden kunnen worden gebruikt.

VPN-clientconfiguratie

Volg deze stappen om de VPN-client te configureren:

1. Kies

2. Voer de PIX-externe interface-ip-adres en tunnelgroepnaam in samen met het wachtwoord voor

VPN Client	Create I	New VPN Connec	tion Entry	X
Connection Entry:	pix1			
Description:	pix on stick fo	r internet access		cisco
Host	17.18.124.98			
Authentication	Transport	Backup Servers	Dial-Up	
Group Authen	tication		C Mutual Group	Authentication
Name:	rtptacvp	n		
Password:	******			
Confirm Passw	ord: ******			
C Certificate Aut Name:	t hentication ertificate Cha			
Erase User Passw	rord		Save	Cancel

verificatie.

3. (*Optioneel*) Klik op **Transparent Tunneling** inschakelen onder het tabblad Transport. (Dit is optioneel en vereist de extra PIX/ASA-configuratie die in <u>aantekening 2</u> is

 ASM Crient 	Create I	New VPIN Connec	ction entry	
Connection Entry:	pix1			
Description:	pix on a stick	for internet connecti	ón	CISCO
Host:	172.18.124.9	8		
Authentication	Transport	Backup Servers	Dial-Up	
🔽 Enable Tran	sparent Tunne	ling		
IPSec over	UDP (NAT .	PAT)		
C IPSec ove	ar TCP	TCP Port: 10000		
Allow Local I	LAN Access			
Peer response ti	meout (second	ls): 90		
E U D	used		Cauta	T
Erase User Passi	WOIG		Save	Cance

4. Het profiel opslaan.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het <u>Uitvoer Tolk</u> (<u>uitsluitend geregistreerde</u> klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

- toon crypto isakmp sa-Toont alle huidige IKE security associaties (SAs) bij een peer.
- Laat crypto ipsec sa-displays alle huidige SA's zien. Zoek naar encryptie en decrypteer pakketten op de SA die het verkeer van de VPN client bepalen.

Probeer aan een openbaar IP-adres van de client te pingelen of te bladeren (bijvoorbeeld www.cisco.com).

Opmerking: De interne interface van de PIX kan niet worden ingesloten voor de samenstelling van een tunnel tenzij de <u>opdracht beheertoegang</u> is ingesteld in de wereldwijde bevestigingsmodus.

PIX1(config)#management-access inside
PIX1(config)#show management-access

VPN-clientverificatie

Voltooi deze stappen om de VPN-client te controleren.

- 1. Klik met de rechtermuisknop op het pictogram van het clientslot van VPN dat aanwezig is in het systeemvak na een succesvolle verbinding en kies de optie voor **statistieken** om versleutelingen en decrypts te bekijken.
- 2. Klik op het tabblad Route Details om de niet-gesplitste tunnellijst van het apparaat te controleren.

Problemen oplossen

N.B.: Raadpleeg voor meer informatie over hoe u problemen met VPN-problemen kunt oplossen <u>VPN-oplossingen voor probleemoplossing.</u>

Gerelateerde informatie

- Enhanced Spoke-to-Client VPN-configuratievoorbeeld voor PIX security applicatie versie 7.0
- <u>Cisco VPN-client</u>
- IPsec-onderhandeling/IKE-protocollen
- <u>Cisco PIX-firewallsoftware</u>
- Opdrachtreferenties van Cisco Secure PIX-firewall
- <u>Security meldingen uit het veld (inclusief PIX)</u>
- Hair-draaien op Cisco ASA
- Verzoeken om opmerkingen (RFC's)
- <u>Technische ondersteuning en documentatie Cisco Systems</u>