# PIX/ASA als Remote-VPN-Server mit erweiterter Authentifizierung über CLI und ASDM -Konfigurationsbeispiel

# Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Zugehörige Produkte Konventionen Hintergrundinformationen Konfigurationen Konfigurieren von ASA/PIX als Remote-VPN-Server mithilfe von ASDM Konfigurieren von ASA/PIX als Remote-VPN-Server mithilfe der CLI Cisco VPN Client Password Storage-Konfiguration Deaktivieren der erweiterten Authentifizierung Überprüfen Fehlerbehebung Falsche Verschlüsselungs-ACL Zugehörige Informationen

# **Einführung**

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

Weitere Informationen zum Einrichten der VPN-Verbindung zwischen einem Cisco VPN-Client (4.x für Windows) und der <u>PIX/ASA 7.x-</u>Sicherheitslösung der Serie PIX 500 finden Sie unter <u>Konfigurationsbeispiel für die Authentifizierung von RADIUS (gegen Active Directory) und Cisco VPN Client 4.x mit Windows 2003</u>. Der Remote-VPN-Client-Benutzer authentifiziert sich über Active Directory mithilfe eines RADIUS-Servers des Microsoft Windows 2003 Internet Authentication Service (IAS).

Unter <u>PIX/ASA 7.x und Cisco VPN Client 4.x finden Sie ein Konfigurationsbeispiel für die Cisco</u> <u>Secure ACS-Authentifizierung</u>, um eine VPN-Verbindung für den Remote-Zugriff zwischen einem Cisco VPN-Client (4.x für Windows) und der PIX 500 Security Appliance 7.x mithilfe eines Cisco Secure Access Control Server (ACS Version 3.2) für die erweiterte Authentifizierung (Xauth) einzurichten.

### 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.

**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 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.

### 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 Tunnel-Benutzer 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.

**Hinweis:** In der Beispielkonfiguration in diesem Dokument werden lokale Benutzerkonten für die Authentifizierung verwendet. Wenn Sie einen anderen Dienst verwenden möchten, z. B. LDAP und RADIUS, finden Sie weitere Informationen unter <u>Konfigurieren eines externen RADIUS-Servers für die Autorisierung und Authentifizierung</u>.

Die Internet Security Association und das Key Management Protocol (ISAKMP), auch IKE genannt, ist das Verhandlungsprotokoll, über das Hosts sich auf den Aufbau einer IPSec Security Association einigen. Jede ISAKMP-Aushandlung ist in zwei Abschnitte unterteilt: Phase 1 und Phase 2. Phase 1 erstellt den ersten Tunnel, um spätere ISAKMP-Aushandlungs-Nachrichten zu schützen. Phase 2 erstellt den Tunnel, der Daten schützt, die über die sichere Verbindung übertragen werden. Weitere Informationen zu ISAKMP finden Sie unter <u>ISAKMP-Richtlinienschlüsselwörter für CLI-Befehle</u>.

# **Konfigurationen**

### Konfigurieren von ASA/PIX als Remote-VPN-Server mithilfe von ASDM

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

1. Wählen Sie im Home-Fenster **Wizards > VPN Wizard** aus.

🚰 Cisco ASDM 5.0 for ASA - 172.1	6.1.2				
File Rules Search Options	Tools Wizards Help				
Home Configuration	Monitor VPN Wizard	ch Refresh	🔜 🦓 Save Help		Cisco Systems
-Device Information		Interface Sta	tus —		
General License		Interface	IP Address/Mask	Line Link	Current Kbps
Host Name: ciscoasa.c	cisco.com	inside outside	172.16.1.2/24 10.10.10.2/24	oup Oup oup Oup	1
ASA Version: 7.0(4)	Device Uptime: 0d 0h 12m 35s			• ···	
AGDM Version: 5.0(4)	Device Type: ASA5520				
Firewall Mode: Routed	Context Mode: Single				
Total Flash: 64 MB	Total Memory: 512 MB	Belert an inter	face to view input and	outout Khos	
-VPN Status		-Traffic Status		i ongoti risipis	
IKE Tunnels: 0	IPSec Tunnels: 0	Connections	Per Second Usage		
-System Resources Status -		1			
CPU CPU Usage (pe	roent)	0.5			
901		2		·····	
0% 84 22			700.0	Tataly D	
13.02.40 13:02:20		- 'eutride' Inte	when Testic Is an Albert	10001.0	
Memory Memory Usage	(MB)	adama inte	made manie osage (Hops	y	
5121	(				
304		0.5			
128		13:02:20			
13:02:45 13:02:28		Input Kb	ps: 0 📕	Output Kbps: 0	
-Latest ASDM Syslog Messa	ges			Configure As	DM Syslog Filters
	Syslog Disabled				
Device configuration loaded succe	ssfully.	admin N	A (15)	12/22	905 1:02:46 PM UTC

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

📸 VPN Wizard		×
VPN Wizard	VPN Tunnel Type (Step 1 of)	
Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch	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. VPN Tunnel Type: Site-to-Site VPN	
	Site-to-Site      VPN Remote Access      Remote Access      Remote Access	
	VPN Tunnel Interface: outside 💌	q

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



4. Geben Sie einen Namen für den Tunnelgruppennamen ein. Geben Sie die zu verwendenden Authentifizierungsinformationen an. In diesem Beispiel wird **Pre-shared Key** ausgewählt.

💼 VPN Wizard			
VPN Wizard	VPN Client Tunnel Group Name and Authentication Method (Step 3 of)		
Branch Branch Branch Branch Branch Branch	The ASA allows you to group remote access tunnel users based on common connection parameters and client attributes configured in the following screens. Use the same tunnel group name for the device and the remote client. Select the type of authentication: shared secret or certificate. If certificate, select the certificate name and the certificate signing algorithm.		
Corporate Network	Tunnel Group Name: hillvalleyvpn		
THE HA	Authentication		
	Pre-shared Key		
	Pre-shared Key: cisco123		
JEN LIN	C Certificate		
TR	Certificate Signing Algorithm: rsa-sig		
G RA	Trustpoint Name:		
	< Back Next > Finish Cancel Help		

**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 sollte, die die ASA konfigurieren, oder von Personen, die dem Kunden bei dieser Konfiguration behilflich sind.

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)
Branch Branch ISP Horne Network	To authenticate remote users using local device user database, select the first option below. You can create user accounts in the next screen. 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, use Configuration > Features > Properties > AAA Setup category in the main ASDM window.
<ul> <li>Authenticate using the local user database</li> <li>Authenticate using an AAA server group</li> <li>AAA Server Group</li> <li>New</li> </ul>	
	< Back Next > Finish Cancel Help

6. Fügen Sie bei Bedarf Benutzer zur lokalen Datenbank hinzu. Hinweis: Entfernen Sie keine vorhandenen Benutzer 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)		
Branks	Enter a new username/password int existing entries in the database or to Configuration > Device Administratio ASDM window. User to Be Added	to the user authenti remove them from n > Administration	cation database. To edit the database, go to > User Accounts in the main
Corporate Network	Username: Password (optional): Confirm Password (optional):	Add >> Delete	Usemame admin einstein marty docbrown jennifer biff
		< Back Next >	Finish 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)	
Branch Franklin Frank	Enter a pool of local addresses to be used for assigning dynamic IP addresses to remote VPN clients.	
Corporate Network	Tunnel Group Name: hillvalleyvpn	
THE THE	Pool Name: vpnpool 💌	
	Range Start Address: 172.16.1.100	
TTT	Range End Address: 172.16.1.199	
TA	Subnet Mask (Optional): 255.255.255.0	
	< Back Next > Finish Cancel Help	

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

🔂 VPN Wizard	<u>×</u>
VPN Wizard	Attributes Pushed to Client (Optional) (Step 7 of 11)
Brench Brench Brench Brench	Attributes you configure below are pushed to the VPN client when the client connects to the ASA. If you do not want an attribute pushed to the client, leave the corresponding field blank.
Corporate	Tunnel Group: hillvalleyvpn
Network	Primary DNS Server:
	Secondary DNS Server:
	Primary WINS Server:
TH	Secondary WINS Server:
S.P-	Default Domain Name:

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

薩 VPN Wizard		×
VPN Wizard	IKE Policy (Step 8 of 11)	
Branch Br	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.	
Corporate Network	Encryption:	
	Authentication: SHA	
	DH Group: 2	
	< Back Next > Finish Cancel Help	

10. Geben Sie die Parameter für IPSec an, auch als IKE-Phase 2 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	
VPN Wizard	IPSec Encryption and Authentication (Step 9 of 11)
Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch	Select the encryption and authentication algorithms for this IPSec VPN tunnel. Configurations on both sides of the connection must match exactly.
Network	Encryption: 3DES
	Authentication: SHA
	< Back Next > Finish Cancel Help

11. Geben Sie an, welche internen Hosts oder Netzwerke ggf. Remote-VPN-Benutzern ausgesetzt werden sollen. 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.

🔂 VPN Wizard		X
VPN Wizard	Address Translation Exemption and Split Tunneling (C	Optional) (Step 10 of 11)
Branch Branch I Branch I Branc	Network Address Translation (NAT) is used to hide the users. You can make exceptions to NAT to expose the network to authenticated remote users protected by V To expose the entire network behind the most secure without NAT, leave the selection list blank.	e internal network from outside e entire or part of the internal PN. Interface to remote VPN users
Corporate	Host/Network to Be Added	Selected Hosts/Networks:
C att		
1 Alter	Interface: inside A	.dd >>
THUM	IP address: 0.0.0	Delete
THE P	Mask: 0.0.0.0	
	Enable split tunneling to let remote users have sin resources defined above, and unencrypted acces	multaneous encrypted access to the s to the internet.
	< Back N	ext > Finish Cancel Help

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.



### Konfigurieren von ASA/PIX als Remote-VPN-Server mithilfe der CLI

Führen Sie diese Schritte aus, um einen Remote-VPN-Zugriffsserver über die Befehlszeile zu konfigurieren. Weitere Informationen zu den jeweils verwendeten Befehlen finden Sie unter Konfigurieren von Remote Access VPNs oder Cisco Adaptive Security Appliances der Serie ASA 5500 - Befehlsreferenzen für die Cisco Adaptive Security Appliances der Serie 5500.

 Geben Sie den Befehl ip local pool im globalen Konfigurationsmodus ein, um IP-Adresspools für VPN-Tunnel für Remote-Zugriff zu konfigurieren. Um Adresspools zu löschen, geben Sie die no-Form dieses Befehls ein.Die Sicherheits-Appliance verwendet Adresspools, die auf der Tunnelgruppe für die Verbindung basieren. Wenn Sie mehrere Adresspools für eine Tunnelgruppe konfigurieren, verwendet die Sicherheits-Appliance diese in der Reihenfolge, in der sie konfiguriert sind. Geben Sie diesen Befehl ein, um einen Pool lokaler Adressen zu erstellen, mit dem Remotezugriff-VPN-Clients dynamische Adressen zugewiesen werden können:

ASA-AIP-CLI(config)#ip local pool vpnpool 172.16.1.100-172.16.1.199 mask 255.255.255.0

- 2. Geben Sie den folgenden Befehl ein: ASA-AIP-CLI(config)#username marty password 12345678
- Geben Sie diese Befehlssätze ein, um den jeweiligen Tunnel zu konfigurieren:ASA-AIP-CLI(config)#isakmp Policy 1 Authentifizierung Pre-ShareASA-AIP-CLI(config)#isakmp Policy 1 Verschlüsselung 3 desASA-AIP-CLI(config)#isakmp-Richtlinie 1 Hash-ShaASA-AIP-CLI(config)#isakmp-Richtlinie 1 Gruppe 2ASA-AIP-CLI(config)#isakmp-Richtlinie 1

Lebenszeitgarantie 43200ASA-AIP-CLI(config)#isakmp enable outsideASA-AIP-CLI(config)#crypto ipsec-Transformationssatz ESP-3DES-SHA esp-3des esp-sha-hmacASA-AIP-CLI(config)#crypto dynamic-map outside\_dyn\_map 10 set transformation-set ESP-3DES-SHAASA-AIP-CLI(config)#crypto dynamic-map outside\_dyn\_map 10 set reverserouteASA-AIP-CLI(config)#crypto dynamic-map outside\_dyn\_map 10 set security-associated life seconds 288000ASA-AIP-CLI(config)#crypto map outside\_map 10 ipsec-isakmp dynamic outside\_dyn\_mapASA-AIP-CLI(config)#crypto map outside\_map interface outsideASA-AIP-CLI(config)#crypto isakmp nat-traversal

4. *Optional:* Wenn die Verbindung die Zugriffsliste umgehen soll, die auf die Schnittstelle angewendet wird, führen Sie den folgenden Befehl aus: ASA-AIP-CLI(config)#sysopt connection permit-ipsec

Hinweis: Dieser Befehl funktioniert auf 7.x-Images vor 7.2(2). Wenn Sie Image 7.2(2) verwenden, geben Sie den Befehl ASA-AIP-CLI(config)#sysopt connection permit-vpn ein.

- 5. Geben Sie den folgenden Befehl ein: ASA-AIP-CLI(config)#group-policy hillvalleyvpn internal
- Führen Sie die folgenden Befehle aus, um die Client-Verbindungseinstellungen zu konfigurieren:ASA-AIP-CLI(config)#group-policy hillvalleyvpn-AttributeASA-AIP-CLI(config)#(config-group-policy)#dns-server value 172.16.1.11ASA-AIP-CLI(config)#(configgroup-policy)#vpn-tunnel-protocol IPSecASA-AIP-CLI(config)#(config-group-policy)#defaultdomain value test.com
- 7. Geben Sie den folgenden Befehl ein: ASA-AIP-CLI(config)#tunnel-group hillvalleyvpn ipsec-ra
- 8. Geben Sie den folgenden Befehl ein: ASA-AIP-CLI(config)#tunnel-group hillvalleyvpn ipsec-attributes
- 9. Geben Sie den folgenden Befehl ein: ASA-AIP-CLI(config-tunnel-ipsec)#pre-shared-key cisco123
- 10. Geben Sie den folgenden Befehl ein: ASA-AIP-CLI(config)#tunnel-group hillvalleyvpn general-attributes
- 11. Geben Sie diesen Befehl ein, um die lokale Benutzerdatenbank zur Authentifizierung zu verweisen.

ASA-AIP-CLI(config-tunnel-general)#authentication-server-group LOCAL

- 12. Ordnen Sie die Gruppenrichtlinie der Tunnelgruppe zu. ASA-AIP-CLI(config-tunnel-ipsec)# default-group-policy hillvalleyvpn
- 13. Geben Sie diesen Befehl im allgemeinen Attributmodus der Tunnelgruppe hillvalleyvpn aus, um den in Schritt 1 erstellten vpnpool der Gruppe hillvalleyvpn zuzuweisen. ASA-AIP-CLI(config-tunnel-general)#address-pool vpnpool

#### Ausführen der Konfiguration auf dem ASA-Gerät

ASA-AIP-CLI(config)#**show running-config** ASA Version 7.2(2) !

hostname ASAwAIP-CLI

```
domain-name corp.com
enable password WwXYvtKrnjXqGbul encrypted
names
1
interface Ethernet0/0
nameif outside
security-level 0
ip address 10.10.10.2 255.255.255.0
1
interface Ethernet0/1
nameif inside
security-level 100
ip address 172.16.1.2 255.255.255.0
1
interface Ethernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
1
interface Management0/0
shutdown
no nameif
no security-level
no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
domain-name corp.com
pager lines 24
mtu outside 1500
mtu inside 1500
ip local pool vpnpool 172.16.1.100-172.16.1.199 mask
255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
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
group-policy hillvalleyvpn1 internal
group-policy hillvalleyvpn1 attributes
dns-server value 172.16.1.11
vpn-tunnel-protocol IPSec
default-domain value test.com
username marty password 6XmYwQ009tiYnUDN encrypted
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-
```

```
sha-hmac
crypto dynamic-map outside_dyn_map 10 set transform-set
ESP-3DES-SHA
crypto dynamic-map outside_dyn_map 10 set security-
association lifetime seconds 288000
crypto map outside_map 10 ipsec-isakmp dynamic
outside dyn map
crypto map outside_map interface outside
crypto isakmp enable outside
crypto isakmp policy 10
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
crypto isakmp nat-traversal 20
tunnel-group hillvalleyvpn type ipsec-ra
tunnel-group hillvalleyvpn general-attributes
address-pool vpnpool
default-group-policy hillvalleyvpn
tunnel-group hillvalleyvpn ipsec-attributes
pre-shared-key *
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
match default-inspection-traffic
!
1
policy-map type inspect dns preset_dns_map
parameters
 message-length maximum 512
policy-map global_policy
class inspection_default
 inspect dns preset_dns_map
 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:0f78ee7ef3c196a683ae7a4804ce1192
: end
ASA-AIP-CLI(config)#
```

#### **Cisco VPN Client Password Storage-Konfiguration**

Wenn Sie über zahlreiche Cisco VPN-Clients verfügen, ist es sehr schwer, sich alle Benutzernamen und Passwörter des VPN-Clients zu merken. Um die Kennwörter im VPN Client-System zu speichern, konfigurieren Sie ASA/PIX und den VPN-Client wie in diesem Abschnitt beschrieben.

#### ASA/PIX

Verwenden Sie den Befehl Gruppenrichtlinienattribute im globalen Konfigurationsmodus:

```
group-policy VPNusers attributes
password-storage enable
Cisco VPN-Client
```

Bearbeiten Sie die .pcf-Datei, und ändern Sie diese Parameter:

SaveUserPassword=1 UserPassword=

#### Deaktivieren der erweiterten Authentifizierung

Geben Sie im Tunnelgruppenmodus diesen Befehl ein, um die standardmäßig aktivierte erweiterte Authentifizierung auf PIX/ASA 7.x zu deaktivieren:

```
asa(config)#tunnel-group client ipsec-attributes
asa(config-tunnel-ipsec)#isakmp ikev1-user-authentication none
```

Nachdem Sie die erweiterte Authentifizierung deaktiviert haben, werden von den VPN-Clients keine Benutzernamen/Kennwörter für eine Authentifizierung (Xauth) eingeblendet. Daher ist für ASA/PIX keine Konfiguration von Benutzername und Kennwort erforderlich, um die VPN-Clients zu authentifizieren.

# <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. Wählen Sie Connection Entries > New aus.



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

VPN Client   Create New VPN Connection Entry
Connection Entry: my_remote_vpn
Description:
Host: 10.10.10.2
Authentication Transport Backup Servers Dial-Up
Name: hillvalleyvpn
Password:
C <u>o</u> nfirm Password: ******
Certificate Authentication     Name:     Send CA Certificate Chain
Erase User Password Cancel

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

VPN Client - Version 4.0.5 (Rel)		_ 🗆 ×
Connection Entries Status Certificates Log Options	Help	
Connect New Import Modify	) Delete	CISCO SYSTEMS
Connection Entries Certificates Log		
Connection Entry 🗸	Host	Transport 🔺
my_remote_vpn	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 <u>Schritten 5 und 6</u> angegebenen übereinstimmen.

VPN Client   User Authentication for "my_remote_vpn"					
Enter Username and Password.					
CISCO SYSTEMS Username	marty				
	OK Cancel				

5. Wenn die Verbindung erfolgreich hergestellt wurde, wählen Sie im Menü Status die Option Statistik aus, um die Details des Tunnels zu überprüfen. In diesem Fenster werden der Datenverkehr und die Verschlüsselungsinformationen angezeigt:

VPN Client   Statistics	×
Tunnel Details Route Details	Firewall
Address Information Client: 172.16.1.100	Connection Information Entry: my_remote_vpn
Bytes Received: 240 Sent: 46816	Crypto Encryption: 168-bit 3-DES Authentication: HMAC-SHA1
Packets Encrypted: 332 Decrypted: 4 Discarded: 137 Bupassed: 61	<b>Transport</b> Transparent Tunneling: Inactive Local LAN: Disabled Compression: None
	Reset
	<u>C</u> lose

diesem Fenster werden Split-Tunneling-Informationen angezeigt:

ć	VPN Client   Sta	tistics		×			
Tunnel Details Route Details Firewall							
	Local LAN Routes		Secured Routes				
	Network	Subnet Mask	Network	Subnet Mask			
			0.0.0.0	0.0.0.0			
-	,		,				

### **Fehlerbehebung**

In diesem Abschnitt finden Sie eine Fehlerbehebung für Ihre Konfiguration.

### Falsche Verschlüsselungs-ACL

ASDM 5.0(2) ist bekannt für die Erstellung und Anwendung einer Zugriffskontrollliste (ACL) mit Verschlüsselung, die für VPN-Clients, die Split-Tunneling verwenden, sowie für Hardware-Clients im Netzwerkerweiterungsmodus Probleme verursachen kann. Verwenden Sie ASDM Version 5.0(4.3) oder höher, um dieses Problem zu vermeiden. Weitere Informationen finden Sie unter Cisco Bug ID <u>CSCsc10806</u> (nur <u>registrierte</u> Kunden).

### Zugehörige Informationen

- <u>Cisco Adaptive Security Appliances der Serie ASA 5500</u>
- Häufigste L2L- und IPsec-VPN-Lösungen zur Fehlerbehebung für Remote-Zugriff
- <u>Cisco Adaptive Security Appliances der Serie ASA 5500 Fehlerbehebung und</u>
   <u>Warnmeldungen</u>
- <u>Technischer Support und Dokumentation Cisco Systems</u>