IOS-Router als Easy VPN-Server mit Konfigurationsbeispiel für Professional

Inhalt

Einführung Voraussetzungen Verwendete Komponenten Installation von Cisco CP Routerkonfiguration zum Ausführen des Cisco CP Anforderungen Konventionen Konfigurieren Netzwerkdiagramm Cisco CP = Easy VPN Server Configuration CLI-Konfiguration Überprüfen Easy VPN-Server - Befehle anzeigen Fehlerbehebung Zugehörige Informationen

Einführung

In diesem Dokument wird beschrieben, wie Sie einen Cisco IOS[®]-Router mithilfe von <u>Cisco</u> <u>Configuration Professional (Cisco CP)</u> und der CLI als Easy VPN (EzVPN)-Server konfigurieren. Mit der Easy VPN Server-Funktion kann ein Remote-Endbenutzer über IP Security (IPsec) mit einem beliebigen Cisco IOS Virtual Private Network (VPN)-Gateway kommunizieren. Zentral verwaltete IPsec-Richtlinien werden vom Server auf das Client-Gerät "übertragen", wodurch die Konfiguration durch den Endbenutzer minimiert wird.

Weitere Informationen zu Easy VPN Server finden Sie im <u>Easy VPN Server-Abschnitt Secure</u> <u>Connectivity Configuration Guide Library, Cisco IOS Release 12.4T</u>.

Voraussetzungen

Verwendete Komponenten

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

- Cisco 1841 Router mit Cisco IOS Software, Version 12.4(15T)
- Cisco CP-Version 2.1

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.

Installation von Cisco CP

Führen Sie die folgenden Schritte aus, um Cisco CP zu installieren:

- 1. Laden Sie Cisco CP V2.1 vom <u>Cisco Software Center</u> (nur <u>registrierte</u> Kunden) herunter, und installieren Sie es auf Ihrem lokalen PC.Die neueste Version des Cisco CP finden Sie auf der <u>Cisco CP-Website</u>.
- Starten Sie Cisco CP von Ihrem lokalen PC aus über Start > Programme > Cisco Configuration Professional (CCP), und wählen Sie die Community aus, für die der Router konfiguriert werden

Application Help		
Home Configure	Monitor 😽	🖄 🥝 Cisco
Select Community Memberi	« Home > Community V	liew
funder and a solution of the solution of the	🚫 Cisco Configuratio	n Professional News
Community View	Date	Title
	24-May-2010	Cisco Configuration Professional v
	24-May-2010	Simplify ISR & ISR 62 deployment
	24-May-2010	Provide CCP Feedback
	Concerns in the Industry ad	The second se
	Calasted Community	New Community Colorts design from
	Selected Community	New Community .Select a desice from
	Selected Community	New Community .Select a device from
	Selected Community: PFilter IP address / Hostn	New Community .Select a device from
	Selected Community PFilter IP address / Hostna	New Community .Select a device from
	Selected Community: PFilter IP address / Hostn	New Community .Select a device from
	Selected Community i Piritur IP address / Hostn	New Community .Select a device from
	Selected Community: PFilter IP address / Hostn	New Community .Select a device from ame Router Hostname
	Selected Community i Piritur IP address / Hostn	New Community .Select a desice from
	Selected Community:	New Community .Select a device from ame Router Hostname
	Selected Community i Piritur IP address / Hostn	New Community .Select a desice from ame Router Hostname
	Selected Community:	New Community .Select a device from ame Router Hostname
	Selected Community	New Community .Select a device from ame Router Hostname
	Selected Community i Pittur IP address / Hostni Hanage Devices	New Community .Select a desice from ame Router Hostname Delete Discover



3. Markieren Sie den Router, um das Gerät zu ermitteln, das Sie konfigurieren möchten, und klicken Sie auf **Discover**

Application Help		
Home 👸 Configure	Monitor 8	e 🙆 🥑 Cisco
Select Community Memberi	Home > Community	y View
and the second sec	Cisco Configura	tion Professional News
Community View	Date	Title
	24-May-2010	Cisco Configuration Professional #2
	24-May-2010	Simplify ISR & ISR 62 deployments
	24-May-2010	Provide CCP Feedback
	Community Inform	ation
	Selected Communit	ty: New Community Select a device from t
	Pitter	1
	IP address / Hos	tname Router Hostname
	Router	
	~	
		>
	Manage Devices	Delete (Discover)
		2

(Erkennung).

Hinweis: Informationen zu den Cisco Router-Modellen und IOS-Versionen, die mit Cisco CP v2.1 kompatibel sind, finden Sie im Abschnitt <u>Kompatible Cisco IOS-Versionen</u>.

Hinweis: Weitere Informationen zu den PC-Anforderungen, auf denen Cisco CP v2.1 ausgeführt wird, finden Sie im Abschnitt <u>Systemanforderungen</u>.

Routerkonfiguration zum Ausführen des Cisco CP

Führen Sie die folgenden Konfigurationsschritte aus, um Cisco CP auf einem Cisco Router auszuführen:

- Stellen Sie über Telnet, SSH oder die Konsole eine Verbindung zum Router her.Wechseln Sie mit dem folgenden Befehl in den globalen Konfigurationsmodus: Router(config)#enable Router(config)#
- 2. Wenn HTTP und HTTPS für die Verwendung von nicht standardmäßigen Portnummern aktiviert und konfiguriert sind, können Sie diesen Schritt überspringen und einfach die bereits konfigurierte Portnummer verwenden. Aktivieren Sie den HTTP- oder HTTPS-Router mithilfe der folgenden Cisco IOS Software-Befehle: Router(config)# ip http server

Router(config)# ip http secure-server
Router(config)# ip http authentication local

3. Erstellen eines Benutzers mit der Berechtigungsstufe 15: Router(config)# username privilege 15 password 0

Hinweis: Ersetzen Sie < *Benutzername>* und < Kennwort> durch den Benutzernamen und das Kennwort, die Sie konfigurieren möchten.

4. Konfigurieren Sie SSH und Telnet für die lokale Anmeldung und die Berechtigungsebene 15. Router(config)# line vty 0 4 Router(config-line)# privilege level 15

Router(config-line)# login local
Router(config-line)# transport input telnet
Router(config-line)# transport input telnet ssh
Router(config-line)# exit

5. (Optional) Aktivieren Sie die lokale Protokollierung, um die Protokollüberwachungsfunktion zu unterstützen:

Router(config)# logging buffered 51200 warning

Anforderungen

In diesem Dokument wird davon ausgegangen, dass der Cisco Router voll betriebsbereit und so konfiguriert ist, dass der Cisco CP Konfigurationsänderungen vornehmen kann.

Vollständige Informationen zum Beginn der Verwendung von Cisco CP finden Sie unter <u>Erste</u> <u>Schritte mit Cisco Configuration Professional</u>.

Konventionen

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

Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der Grundeinstellungen für einen Router in einem Netzwerk.

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:



Easy VPN Client

Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Sie sind <u>RFC 1918</u> -Adressen, die in einer Laborumgebung verwendet werden.

Cisco CP = Easy VPN Server Configuration

Führen Sie die folgenden Schritte aus, um den Cisco IOS-Router als Easy VPN-Server zu konfigurieren:

 Wählen Sie Configure > Security > VPN > Easy VPN Server > Create Easy VPN Server aus, und klicken Sie auf Launch Easy VPN Server Wizard (Easy VPN-Serverassistent starten), um den Cisco IOS-Router als Easy VPN-Server zu konfigurieren:
 Configure > Security > VPN > Easy VPN Server

```
      VPN

      Create Easy VPN Server
      Edit Easy VPN Server

      Cisco CP can guide you through Easy VPN Server configuration tasks.

      Use Case Scenario

      Configure Easy VPN Server

      Configure Easy VPN Server

      Configure Easy VPN Server

      Configure Easy VPN Server

      Use this option to configure this router as an Easy VPN Server. To complete the configuration, you must know the different group policies to which the clients can connect and their attributes.

      Launch Easy VPN Server Wizard
```

2. Klicken Sie auf **Weiter**, um mit der **Easy VPN Server-**Konfiguration fortzufahren.

Easy VPN Server Wizard	
VPN Wizard	Welcome to the Easy VPH Server Wizard
	This wizard will guide you through configuring of an Easy VPN Server on this router. An Easy VPN Server sillows a remote end user to use IP Security (IPSec) when communicating with a Cisco IOS Virtual Private Network (VPN) gateway. Centrally managed IPBec policies are "bushed" to the client by the server, minimizing configuration by the end user. This wizard will guide you in performing the following tasks to successfully configure an Easy VPN Server on this router: * Configuring virtual temp ate interface and authentications. * Configuring IKE policies. * Configuring an IPSec transform set. * Configuring a group policy lookup method. * Configuring user auther traction. * Configuring user auther traction. * Configuring comman RADIUB converted tailo. * Configuring comman RADIUB converted tailo. * Configuring clisto tunne ing control protocol (#TCP) optionally.
	< Back Next > Finish Cancel Help

3. Im Ergebnisfenster wird eine virtuelle Schnittstelle als Teil der Easy VPN Server-Konfiguration konfiguriert. Geben Sie die IP-Adresse der Virtual Tunnel Interface (Schnittstelle für virtuellen Tunnel) an, und wählen Sie die Authentifizierungsmethode für die Authentifizierung der VPN-Clients aus. Hier wird die Authentifizierungsmethode Pre-shared Keys verwendet. Klicken Sie auf Weiter:

Easy VPN Server Wizard -	10% Complete		
VPN Wizard	Interface and Authentication Interface A virtual template interface will b Any Cisco IOS feature that shou the VPIN tunnel can be configure	e proated as part of this Easy v Id be applied before encryption ed on this Interface.	'PN Berver configuration. to the traffic going into
	IP Address of Virtual Tunnel Inte	ərfacə	
	C nnumbered to New L	copback Interface	
	IP Address	10.10.10.10	
\mathbf{i}	Subnet Mask.	255.255 255.0	cr 24
	C Unnumbered to	FastEthernet0/0	Cetails
HA	Aufhentication Select the method used for auth VPN Server.	ienticating VPN clients connect	ing to this Easy
	Pre-shared Keys	C Digital Certificates	C Bull
		< Back Next > P	inish Cancel Help

4. Geben Sie den Verschlüsselungsalgorithmus, den Authentifizierungsalgorithmus und die Schlüsselaustauschmethode an, die dieser Router bei Verhandlungen mit dem Remote-Gerät verwenden soll. Auf dem Router ist eine Standard-IKE-Richtlinie vorhanden, die bei Bedarf verwendet werden kann. Wenn Sie eine neue IKE-Richtlinie hinzufügen möchten, klicken Sie auf Hinzufügen.

Easy VPN Server Wizard -	20% Ci	omplete					
VPN Wizard	IKE Pr IKE pi metho device	oposale roposals od that is e.	specify the en used by this re	eryption algorill cuter when neg	hm, authentica Iotlating a VPN	dion algorithm ar I connection with	nd key exchange the remote
	Clickt	the Add	outton to add	more policies :	and the Edit I	button to ecit an :	evisting policy
		Priority	Encryption	Hash	E-H Group	Authentication	Түре
		1	3DES	SHA 1	group2	PRE SHARE	Cisco CP Defa
	,	dd	Edit				

5. Stellen Sie Verschlüsselungsalgorithmus, Authentifizierungsalgorithmus und die Exchange-Methode wie hier gezeigt bereit, und klicken Sie dann auf

< Back

Next > Finish

Cancel

Help

Add IKE Policy	
Configure IKE Policy	
Priority:	Authentication:
þ	RSA_SIG 💙
Encryption:	D-H Group:
DES 🔽	group1 😽
Hash:	Lifetime:
SHA_1	24 0 0 HH:MM:SS
ок 🛌	Cancel Help

Easy VPN Server Wizard -	20% Complete						
VPN Wizard	IKE Proposale IKE proposals s method that is u device. Click the Add	pepify the end sed by this ro within to add (ryption algorith uter when heq more policies a	nm, authentica otlating a VPN and the Edit II	ation algorithm I connection wi butten to ecitia:	and key exc th the remo n evisting pr	hange te clicy
	Priority E	Encryption DES	Hash SHA 1	<mark>E-H Group</mark> group 2	Authenticatio	in <mark> Type</mark> Cisco CF	° Defau
	Add	Edit					
				< Back Nex	d 🚬 Finish	Cancel	Help

7. Im neuen Fenster sollten die Details zum Konfigurationssatz angegeben werden. Das Transform Set legt die Verschlüsselungs- und Authentifizierungsalgorithmen fest, die zum Schutz von Daten im VPN-Tunnel verwendet werden. Klicken Sie auf Hinzufügen, um diese Details anzugeben. Wenn Sie auf Hinzufügen klicken und die Details angeben, können Sie bei Bedarf beliebig viele Transform Sets hinzufügen.Hinweis: Der standardmäßige Konfigurationssatz des CP ist standardmäßig auf dem Router vorhanden, wenn er mit dem Cisco CP konfiguriert wurde.

Easy VPN Server Wizard	35% Complete				×
VPN Wizard	Traneform Set A transform set specifies the encryption and authentication algor thms used to protect the data in the VPN funnel.				
	Click the Add button to add a transform: set. Select Tranoform Sot	new transtorm se	t and the ±dtl kutto	n to ecit the specified	
	Gisco CP Default Transf	iorm Get 🛛 🔽			
h. 🔪	Name	E3P Encryption	ESP Integrity	A-Integrity	
RA	ESP-3DES-SHA	ESF_3DES	ESP_SHA_HMAC		
	And Enit			>	
		< E	9ack Next≻ Fini	sh Cancel Help	

8. Geben Sie die Details zum **Transform Set** (**Verschlüsselungs- und Authentifizierungsalgorithmus**) an, und klicken Sie auf

Add Transform Set		
Name:		
Data integrity with e	ncryption (ESP)	
Integrity Algorithm:	<none></none>	×
Encryption Algorithm:	<none></none>	*
		Show Advanced >>
ок	Cancel	Help

 In diesem Beispiel wird der Standard-Umwandlungssatz mit dem Namen CP-Standardtransformationssatz verwendet. Wählen Sie als Ergebnis den Standard-Umwandlungssatz aus, und klicken Sie auf Weiter.

Easy VPN Server Wizard -	35% Complete				×
VPN Wizard	Traneform Set A transform set specifies the encryption and authentication algorithms used to protect the data in the VPN tunnel.				
	Click the Add button to add a transform set.	a new transform se	et and the Edil butto	in to ecit the specifie	r
	Cisco CP Default Tran	sform Get 🛛 🛩 – insform set]		
	Name	EBP Encryption	ESP Integrity	AH Integrity	1
RA	ESP-3DES-SHA	ESF 3DES	ESP SHA HMAC	>	
	Ard Ecit				
		< 8	9ack Next≯ <mark>,</mark> Fini	sh Cancel He	elp

10. Wählen Sie im neuen Fenster den Server aus, auf dem die Gruppenrichtlinien konfiguriert werden sollen. Dabei kann es sich um Local oder RADIUS oder Local und RADIUS handeln. In diesem Beispiel verwenden wir den lokalen Server, um Gruppenrichtlinien zu konfigurieren. Wählen Sie Lokal aus, und klicken Sie auf Weiter.

Easy VPN Server Wizard -	50% Complete	×
VPN Wizard	Group Authorization and Group Policy Lookup An ISAKMP dient configuration group (or VPN group) is a group of VPN clients that share the same authentibation and configuration information. Group policies can be configured locally on this router, on an external server, or on both. Easy VPN Gerver will use these group policies to authenticate VPN dients. Mothod Lipt for Group Folicy Lookup Gelect the servers on which group policies will be configured, or select an existing AAA policy that defines the servers used for configuring group policies. Problem Configured Local C RADIUE RADIUE and Local	9 V ies
	Summary The local database will be used for group authorization. This option is recommended if you do not have a RADIUS or TACACE- server in your network.	
	< Back Next > Finish Cancel Help	,

11. Wählen Sie in diesem neuen Fenster den Server für die Benutzerauthentifizierung aus, der entweder nur lokal oder RADIUS oder sowohl Nur lokal als auch RADIUS sein kann. In diesem Beispiel verwenden wir den lokalen Server, um Benutzeranmeldeinformationen für die Authentifizierung zu konfigurieren. Stellen Sie sicher, dass das Kontrollkästchen neben Benutzerauthentifizierung aktivieren aktiviert ist. Wählen Sie Lokal und klicken Sie auf Weiter.

Easy VPN Server Wizard -	65% Complete
VPN Wizard	User Authentication (XAuth) User Authentication (XAuth) provides additional security by authenticating the user of a device offer the device has undergone. KE authentication. User credentials XAuth can be configured locally on this router, on an external server, or on both
	Finable User Authentication Belact the servers that will be used for configuring user credentials, or select an existing AAA policy that defines the servers used for configuring user credentials.
	C RADIUS C RADIUS and Local Only
	Add User Crodentials
	Local database will be used for user authertication.
	< Back Next >> Finish Cancel Help

12. Klicken Sie auf **Hinzufügen**, um eine neue Gruppenrichtlinie zu erstellen und die Remote-Benutzer dieser Gruppe hinzuzufügen.

Easy VPN Server Wizard -	80% Comp	lete					
VPN Wizard	Group Authorization and User Group Policies The Easy VPN Server allows you to group remote users who are using Cisco VPN clients of other Easy VPN Remote of ent products. The group attributes will be downloaded through t						
	clients or device that is part of a given group. The same group name should be the remote client or device to ensure that appropriate group attributes are down Click the Add button to add more groups. The Edit button to edit an existing g Clone button to create a new group from an existing group.						
	Scico:	Grcup Name	Pool	DN3	WN8	Domain Name	>

Ecit.

Configure die Timer

Adc...

١Ē

cleared.

ld e Timer:

Delete

HH:MM:SS

< Back Next > Finish

Configure a timeout value after which VPN tunnels from idle clients should be

Cancel

Help

- Namen dieser Gruppe (in diesem Beispiel cisco) zusammen mit dem vorinstallierten Schlüssel und die Informationen für den IP-Pool (die Start-IP-Adresse und die End-IP-Adresse) wie gezeigt an, und klicken Sie auf OK. Hinweis: Sie können einen neuen IP-Pool erstellen oder, falls vorhanden, einen vorhandenen IP-Pool verwenden.
- 13. Geben Sie im Fenster Gruppenrichtlinie hinzufügen den Gruppennamen im Feld für den

Ad	Group Policy	×					
6	eneral DNS/WINS Split Tunneling Client Settings XAuth Options Client Update						
	Name of This Group: cisco						
	Pre-shared Keys						
	Specify the key that will be used to authenticate the clients associated with this group.						
	Current Key <none></none>						
	Enter new pre-shared key:						
	Reenter new pre-shared key:						
	Pool Information						
	Specify a local pool containing a range of addresses that will be used to allocate an internal IP address to a client.						
	• Create a new pool C Select from an existing pool						
	Starting IP address: 192.168.1.1 -Select an entry 🕑 Details						
	Ending IP address: 192.168.1.254						
	Enter the subnet mask that should be sent to the client along with the IP address.						
	Subnet Mask: (Optional)						
Maximum Connections Allowed:							
	OK Cancel Help						

14. Wählen Sie nun die neue Gruppenrichtlinie aus, die mit dem Namen cisco erstellt wurde, und aktivieren Sie dann das Kontrollkästchen neben Configure Idle Timer (Inaktivitätszeitgeber konfigurieren), um den Leerlaufzeitgeber zu konfigurieren. Klicken Sie auf

Weiter.

Easy VPN Server Wizard -	- 80% Complete	×
VPN Wizard	Group Authorization and User Group Policies The Easy VPN Server allows you to group remote users who are using Cisco VPN clients or other Easy VPN Remote all ent products. The group attributes will be downloaded through the clients or device that is part of a given group. The same group name should be configured of the remote client or device to ensure that appropriate group attributes are downloaded. Click the Add buttor to add more groups the Edit buttor to edit an existing group, or the Clone buttor to create a new group from an existing group.	Ie In
	Scice: Group Name Pool DNB WINS Domain Name Cisco SDM_FO	
	Adc Ecit Clone Lielete	
	Configure de Timer Configure a timeoul value after which VPN tunnels from idle clients should be cleared.	
	ld e Timer: 24 0C 00 HH:MM:SS	
	< Back Next > Finish Cancel Help	

 Aktivieren Sie bei Bedarf Cisco Tunneling Control Protocol (cTCP). Andernfalls klicken Sie auf Weiter.

Easy VPN Server Wizard -	85% Complete 🔀
VPN Wizard	Cisco Tunneling Control Protocol(cTCP) The cTCP allows Easy VPN clients to fur given transparently without modifying firewall
	rules.You must enable cTCF on the server in order to accept connections from remote clients Using cTCP
	from clients.You can add a maximum of 10 port numkers.
	Use comma ' ' to separate entries.
DA	
	< Back Next > Finish Cancel Help

16. Überprüfen Sie die **Konfigurationsübersicht**. Klicken Sie auf **Fertig stellen**.

Easy VPN Server Wizard -	90% Complete			
VPN Wizard	Summary of th e Configuration			
	Click Finish to deliver the configuration to Tunnel Interface Details Interface: Virtual Template1 Type Tunnel	he rouler.		
	Mode: IFSec- Pv4 IP Address: Linnumbered to Loo IKE Folicios:	pbackC		=
	Hash CH Oroup	Authentication	Encryption	
RA	SHA_1 group2 I ransform Set: Name: EOP-CDEO-OLIA ESP Encryption: ESP_3DES ESP Integrity, ESP_SHA_HMAC Mode: TUNNEL	PRE_SHARE	3DES	-
	Test ∨PN connectivity after configuring.			2
		< Back Next>	Finish	Cancel Help

17. Klicken Sie im Fenster **Konfiguration an Router liefern** auf **Bereitstellen**, um die Konfiguration an den Router zu übertragen. Sie können auf **In Datei speichern** klicken, um die Konfiguration als Datei auf dem PC zu speichern.

Deliver Configuration to Router
Deliver delta commands to the router's running config.
Preview commands that will be delivered to the router's running configuration.
aaa authentication login ciscocp_vpn_xauth_ml_1 local aaa authorization network ciscocp_vpn_group_ml_1 local ip local pool SDM_POOL_1 192.168.1.1 192.168.1.254 crypto ipsec transform-set ESP-3DES-SHA esp-sha-hmac esp-3des mode tunnel exit crypto isakmp profile ciscocp-ike-profile-1 isakmp authorization list ciscocp_vpn_group_ml_1 client authentication list ciscocp_vpn_group_ml_1 natch identity group cisco
The differences between the running configuration and the startup configuration are lost whenever the router is turned off.
Save running config. to router's startup config.
This operation can take several minutes.
Deliver Cancel Save to file Help

 Das Fenster Command Delivery Status (Bereitstellungsstatus f
ür Befehle) zeigt den Bereitstellungsstatus der Befehle an den Router an. Sie wird als Konfiguration angezeigt, die an den Router übermittelt wird. Klicken Sie auf

Command Delivery Statu	S:	
Preparing commands fo Submitting 47 commands Configuration delivered f	r delivery s, please wait o router.	
<		>

19. Sie sehen den neu erstellten Easy VPN-Server. Sie können den vorhandenen Server bearbeiten, indem Sie Easy VPN-Server bearbeiten auswählen. Damit ist die Easy VPN-Serverkonfiguration auf dem Cisco IOS-Router abgeschlossen.

			Cloba Cett	ngs., Add., Edit., D	elete
11 H	Interface	Sroup Authorization	User Ault entication	Mode Configuration.	
cCF Profi	or Virtual Temp afer	cipeces ven arous mil 1	e scoop yon yauth milli	REEPOND	
		le .			
		*			

CLI-Konfiguration

Routerkonfiguration
Router# show run
Building configuration
Current configuration : 2069 bytes ! version 12.4 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption hostname Router boot-start-marker boot-end-marker no logging buffered enable password cisco !AAA enabled using aaa newmodel command. Also AAA Authentication and Authorization are enabled! aaa new-model !
!
aaa authentication login ciscocp_vpn_xauth_ml_1 local
aaa authorization network ciscocp_vpn_group_ml_1 local
! !
aaa session-id common ip cef ! ! !
ip domain name cisco.com !

```
multilink bundle-name authenticated
!--- 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 1
encr 3des
authentication pre-share
group 2
crypto isakmp keepalive 10
crypto isakmp client configuration group cisco
key cisco123
pool SDM_POOL_1
crypto isakmp profile ciscocp-ike-profile-1
  match identity group cisco
  client authentication list ciscocp_vpn_xauth_ml_1
  isakmp authorization list ciscocp_vpn_group_ml_1
  client configuration address respond
  virtual-template 1
!--- 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-3DES-
SHA esp-3des esp-sha-hmac
crypto ipsec profile CiscoCP_Profile1
set security-association idle-time 86400
set transform-set ESP-3DES-SHA
set isakmp-profile ciscocp-ike-profile-1
!--- RSA certificate generated after you enable the !---
ip http secure-server command.
crypto pki trustpoint TP-self-signed-1742995674
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-1742995674
revocation-check none
rsakeypair TP-self-signed-1742995674
!--- Create a user account named cisco123 with all
privileges.
username cisco123 privilege 15 password 0 cisco123
archive
log config
 hidekeys
1
1
!--- Interface configurations are done as shown below---
! interface Loopback0 ip address 10.10.10.10
255.255.255.0 ! interface FastEthernet0/0 ip address
10.77.241.111 255.255.255.192 duplex auto speed auto !
interface Virtual-Template1 type tunnel ip unnumbered
Loopback0 tunnel mode ipsec ipv4 tunnel protection ipsec
profile CiscoCP_Profile1 ! !--- VPN pool named
SDM_POOL_1 has been defined in the below command---! ip
```

```
local pool SDM_POOL_1 192.168.1.1 192.168.1.254
```

!--- This is where the commands to enable HTTP and HTTPS are configured. ip http server ip http authentication local ip http secure-server ! ! ! ! control-plane ! line con 0 line aux 0 !--- Telnet enabled with password as cisco. line vty 0 4 password cisco transport input all scheduler allocate 20000 1000 ! ! ! ! end

<u>Überprüfen</u>

Easy VPN-Server - Befehle anzeigen

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

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

IPv4 Crypto ISA	KMP SA			
dst	src	state	conn-id	slot status
10.77.241.111	172.16.1.1	QM_IDLE	1003	0 ACTIVE

• **show crypto ipsec sa** - Zeigt alle aktuellen IPsec-SAs in einem Peer an. Router#**show crypto ipsec sa**

```
interface: Virtual-Access2
   Crypto map tag: Virtual-Access2-head-0, local addr 10.77.241.111
  protected vrf: (none)
  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.1.3/255.255.255.255/0/0)
  current_peer 172.16.1.1 port 1086
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 28, #pkts encrypt: 28, #pkts digest: 28
   #pkts decaps: 36, #pkts decrypt: 36, #pkts verify: 36
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 2
    local crypto endpt.: 10.77.241.111, remote crypto endpt.: 172.16.1.1
    path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
    current outbound spi: 0x186C05EF(409732591)
     inbound esp sas:
     spi: 0x42FC8173(1123844467)
```

transform: esp-3des esp-sha-hmac

Fehlerbehebung

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**.

Hinweis: Bevor Sie Debugbefehle ausgeben, lesen Sie die <u>wichtigen Informationen zu Debug-</u> <u>Befehlen</u>.

Zugehörige Informationen

- IPSec-Aushandlung/IKE-Protokolle
- <u>Schnellstartanleitung für Cisco Configuration Professional</u>
- <u>Cisco Produkt-Support-Seite Router</u>
- Technischer Support und Dokumentation Cisco Systems