Cisco Router als Remote-VPN-Server mit SDM-Konfigurationsbeispiel

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Konfigurieren Netzwerkdiagramm Konfigurationsverfahren Überprüfen Zugehörige Informationen

Einführung

In diesem Dokument wird beschrieben, wie der <u>Cisco Security Device Manager (SDM)</u> zum Konfigurieren des Cisco Routers als <u>Easy VPN-Server</u> verwendet wird. Mit Cisco SDM können Sie Ihren Router als VPN-Server für den Cisco VPN Client über eine benutzerfreundliche webbasierte Verwaltungsschnittstelle konfigurieren. Sobald die Konfiguration des Cisco Routers abgeschlossen ist, kann sie mit dem Cisco VPN Client verifiziert werden.

Voraussetzungen

<u>Anforderungen</u>

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

Hinweis: Informationen zur Konfiguration des Routers durch das SDM finden Sie unter <u>Zulassen</u> <u>von HTTPS-Zugriff für SDM</u>.

Verwendete Komponenten

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

- Cisco 3640 Router mit Cisco IOS® Software, Version 12.3(14T)
- Security Device Manager Version 2.31
- Cisco VPN Client Version 4.8

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.

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 finden Sie Informationen zum Konfigurieren der Easy VPN Server-Funktion, mit der ein Remote-Endbenutzer über IPsec mit einem beliebigen Cisco IOS® VPN-Gateway kommunizieren kann.

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:



Konfigurationsverfahren

Führen Sie diese Schritte aus, um den Cisco Router mithilfe von SDM als Remote-VPN-Server zu konfigurieren.

 Wählen Sie Configure > VPN > Easy VPN Server im Home-Fenster aus, und klicken Sie auf Easy VPN Server Wizard.



2. AAA muss auf dem Router aktiviert werden, bevor die Konfiguration des Easy VPN-Servers beginnt. Klicken Sie auf Ja, um mit der Konfiguration fortzufahren. Die Meldung "AAA wurde erfolgreich auf dem Router aktiviert" wird im Fenster angezeigt. Klicken Sie auf OK, um die Konfiguration des Easy VPN-Servers zu starten.

Enable AAA	
	AAA is disabled on the router. AAA must be enabled to configure Easy VPN Server.SDM will perform the following precautionary tasks while enabling AAA to prevent loss of access to the router.
	* Configure authentication and authorization for vty lines. The local database will be used for both authentication and authorization. * Configure authentication for the console line. The local database will be used for authentication.
	Do you want to enable AAA?
	Yes No

3. Klicken Sie auf **Weiter**, um den Easy VPN Server-Assistenten zu starten.

Easy VPN Server Wizard		×
VPN Wizard	Welcome to the Easy VPN Server Wizard	
	This wizard will guide you through the configuration of an Easy VPN Server on this router. An Easy VPN Server allows a remote end user to use IP Security (IPSec) when communicating with a Cisco IOS Virtual Private Network (VPN) gateway. Centrally managed IPSec policies are "pushed" 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:	
	* Selecting the interface on which the client connections will terminate. * Configuring IKE policies. * Configuring an IPSec transform set. * Configuring a group policy lookup method. * Configuring user authentication. * Configuring group policies on the local router.	
	< Back Next > Finish Cancel Help	

4. Wählen Sie die Schnittstelle, auf der die Clientverbindungen enden, und den Authentifizierungstyp

aus.

Easy VPN Server Wizard - 10	0% Complete		×
VPN Wizard	Interface and Authentication Interface Please select the interface of Easy VPN clients will connel Interface for this Easy VPN 8 Authentication Select the method used for VPN Server.	on which the Easy VPN Server shou oct to the server through this interfac Server: Server: Serial2/0 authenticating VPN clients connecti C Digital Certificates	Id be configured. e. Details Ing to this Easy C Both
	Interface connected to Internet. This is the interface where the VPN connections from the VPN clients will terminate.	You can select an interface in site to site VPN connect select an interface if it is p IPSec, DMVPN or Easy V For more information plea help button.	e which is participating tion. But you cannot participating in GRE over /PN client connection. ase click the
		< Back Next > F	inish Cancel Help

5. Klicken Sie auf Weiter, um die IKE-Richtlinien (Internet Key Exchange) zu konfigurieren, und verwenden Sie die Schaltfläche Hinzufügen, um die neue Richtlinie zu erstellen.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.

sy VPN Server Wizard - 2	20% Complete			*		
VPN Wizard	IKE Proposals IKE proposals method that is device. Click the Add	specify the er used by this r button to add	ncryption alg outer when I more polici	orithm, authentica negotiating a VPN es and the Edit t	tion algorithm ar connection with outton to edit an o	nd key exchange the remote existing policy.
	Priority	Encryption 3DES	Hash SHA_1	D-H Group group2	Authentication PRE_SHARE	Type User Defined
RA	Add	Edit				
				< Back Nex	t> Finish (Cancel Helj

6. Klicken Sie auf Weiter, um den Standard-Transformationssatz auszuwählen, oder fügen Sie den neuen Transformationssatz hinzu, um den Verschlüsselungs- und Authentifizierungsalgorithmus anzugeben. In diesem Fall wird der Standard-Transformationssatz verwendet.

asy VPN Server Wizard -	35% Complete			
VPN Wizard	Transform Set A transform set specifies the data in the VPN tunnel.	encryption and aut	nentication algorith	ms used to protect the
	Click the Add button to add transform set.	a new transform se	t and the Edit but	ton to edit the specified
A	Select Transform Set			
	Details of the specified tr	ansform set		
	Name	ESP Encryption	ESP Integrity	AH Integrity
RA	ESP-3DES-SHA1	ESP_3DES	ESP_SHA_HMAC	
	Add Edit			
		< [Back Next > Fir	hish Cancel Help

7. Klicken Sie auf **Weiter**, um eine neue Authentifizierungs-, Autorisierungs- und Abrechnungsnetzwerkmethodenliste (Authentication, Authorization, Accounting - AAA) für die Gruppenrichtliniensuche zu erstellen, oder um eine vorhandene Netzwerkmethodenliste für die Gruppenautorisierung auszuwählen.

VPN Wizard	Group Authorization and Group Policy Lookup	
	An ISAKMP client configuration group (or VPN grou same authentication and configuration information on this router, an external server, or both. Easy VPN authenticate VPN clients.	p) is a group of VPN clients that share the . Group policies can be configured locally I Server will use these group policies to
	Method List for Group Policy Lookup	
	Select the servers on which group policies will be policy that defines the servers used for configuring	configured, or select an existing AAA group policies.
a la		
	C RADIUS	
ln 🔪 🚄	C RADIUS and local	
	C Select an existing AAA method list	-Select an entry
A		Add RADIUS Server
	Summary	
	The local database will be used for group authorize you do not have a RADIUS or TACACS+ server in you	ation. This option is recommended if our network.
	< Ba	rk Next > Finish Cancel Hein

8. Konfigurieren Sie die Benutzerauthentifizierung auf dem Easy VPN-Server.Sie können Benutzerauthentifizierungsdetails auf einem externen Server, z. B. einem RADIUS-Server, einer lokalen Datenbank oder auf beiden speichern. Eine Liste mit AAA-Authentifizierungsmethoden wird verwendet, um die Reihenfolge festzulegen, in der die Benutzerauthentifizierungsdetails durchsucht werden sollen.

Easy VPN Server Wizard - I	55% Complete	x
VPN Wizard	User Authentication (XAuth) User authentication (XAuth) provides additional securit after the device has undergone IKE authentication. Use locally on this router, on an external server, or both.	ty by authenticating the user of a device er credentials XAuth can be configured
	Select the servers that will be used for configuring use AAA policy that defines the servers used for configuring C Local Only	er credentials, or select an existing g user credentials.
	C RADIUS and Local Only C Select an existing AAA method list	Add RADIUS Server
Re	SummaryLocal database will be used for user authentication.	Add User Credentials
	< Back	Next > Finish Cancel Help

9. In diesem Fenster können Sie Benutzergruppenrichtlinien in der lokalen Datenbank hinzufügen, bearbeiten, klonen oder löschen.

Easy VPN Server Wizard - 80	% Complete				×
VPN Wizard	Group Authorizati The Easy VPN Ser other Easy VPN Re clients or device th the remote client o Click the Add but Clone button to c	on and User Gr ver allows you t emote client pro at is part of a g r device to ens ton to add more reate a new gro	oup Policies to group remote to oducts. The group iven group. The s ure that appropri- e groups, the Edi oup from an exist	users who are u p attributes will t same group nan ate group attribu t button to edit ting group.	sing Cisco VPN clients or be downloaded through the he should be configured on tes are downloaded. an existing group, or the
	Group Name Group Name Add Configure a time cleared. Idle Timer:	Pool Edit C dle Timer out value after t	DNS	Iete Is from idle clier	Domain Name
	8 		< Ba	ick Next≻ F	inish Cancel Help

10. Geben Sie einen Namen für den Tunnelgruppennamen ein. Geben Sie den für die Authentifizierungsinformationen verwendeten vorinstallierten Schlüssel an. Erstellen Sie einen neuen Pool, oder wählen Sie einen vorhandenen Pool aus, aus dem die IP-Adressen den VPN-Clients zugewiesen werden.

	DNS/WINS S	plit Tunneling 🗍 Clier	nt Settings XAuth Options	
Name (of This Group:		vpn	
Pre	-shared keys —			
Speci	fy the key that wi	II be used to authenti	icate the clients associated with this grou	up.
Curre	int Key:		≺None≻	
Enter	new pre-shared	i key:	******	
Reen	ter new pre-sha	red key:	*****	
	eate a new pool		C Select from an existing pool	
• Cr				
 Cross State 	arting IP address	: 192.168.2.1	-Select an entry 💌 Det	ails
Cri Sta En	arting IP address ding IP address	: 192.168.2.1 : 192.168.2.5	-Select an entry 💌 Det	ails
Cn Sta En Enter	arting IP address ding IP address the subnet mas	s: 192.168.2.1 : 192.168.2.5 k that should be sent	-Select an entry Det	ails
Cr Sta En Enter Su	arting IP address ding IP address the subnet mas bnet Mask:	s: 192.168.2.1 : 192.168.2.5 k that should be sent 255.255.255.0	-Select an entry Det t to the client along with the IP address. (Optional)	ails
Crief Cr	arting IP address ding IP address the subnet mas bnet Mask: Im Connections	s: 192.168.2.1 : 192.168.2.5 k that should be sent 255.255.255.0 Allowed:	-Select an entry Det t to the client along with the IP address. (Optional)	alls

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

VPN Wizard	Summary or the Configuration			
	Click finish to deliver the configuration to the	ne router.		
	IKE Policies:			-
	Hash DH Group	Authentication	Encryption	
	SHA_1 group2	PRE_SHARE	3DES	
	Transform Set Name: ESP-3DES-SHA1 ESP Encryption: ESP_3DES ESP Integrity: ESP_SHA_HMAC Mode: TUNNEL Group Policy Lookup Method List User Authentication Method List	: Local : Local		
	Number of Group Policies	:1		
	Group Policy Name - vonci	iont	 	. ⊁
	Test VPN connectivity after configuring.			

12. Das SDM sendet die Konfiguration an den Router, um die aktuelle Konfiguration zu aktualisieren. Klicken Sie zum Abschließen auf

Commands Delivery Status	
Command Delivery Status:	
Preparing commands for delivery Submitting 27 commands, please wait Configuration delivered to router.	<u>.</u>
	پ ۲
OK	

13. Nach Abschluss können Sie die Änderungen in der Konfiguration bei Bedarf bearbeiten und ändern.



<u>Überprüfen</u>

Versuchen Sie, über den Cisco VPN-Client eine Verbindung zum Cisco Router herzustellen, um zu überprüfen, ob der Cisco Router erfolgreich konfiguriert wurde.

1. Wählen Sie Connection Entries > New aus.

👌 status: Disconnected	VPN Client - Version 4.8.0)1.0300	
Connection Entries Status	Certificates Log Options	Help	
Connect New	Import Modify) Delete	CISCO SYSTEMS
Connection Entries Certific	cates Log		
Connection Entry	∇	Host	Transport
1			
Not connected.			

 Füllen Sie die Details Ihrer neuen Verbindung aus.Das Host-Feld sollte die IP-Adresse oder den Hostnamen des Tunnel-Endpunkts des Easy VPN-Servers (Cisco Router) enthalten. Die Informationen zur Gruppenauthentifizierung müssen mit denen in Schritt 9 übereinstimmen. Klicken Sie abschließend auf

Description:		3	
Host: 1	0.1.1.1		
Authentication	Transport Backup	Servers Dial-Up	
 Group Authenti 	cation	C Mutual Group	Authenticati
Name:	vpn		
Password:	*****		
Confirm Passwo	rd: [******		
C Certificate Auth	entication		
Name:		¥	
🔲 Send CA Ce	rtificate Chain		

Speichern

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

Verbinden.

	👌 status: Disconnected VPN Client - Version 4.8.01.0300					_ 🗆 ×
Connection E	ntries Sta	atus Certific	ates Log Option	s Help		
Connect	ten New) Fa	t Modify) Delete		CISCO SYSTEMS
Connection E	Entries	Certificates	Log			
	Connec	tion Entry /	2	(Host	Transport
	vpn				10.1.1.1	IPSec/UDP
-1						

 Geben Sie einen Benutzernamen und ein Kennwort f
ür die erweiterte Authentifizierung (Xauth) ein. Diese Informationen werden durch die Xauth-Parameter in Schritt 7 bestimmt.

👌 status: Disconnected VPN	Client - Version 4.8.01.0300		
Connection Entries Status Certif	icates Log Options Help		
Cancel Connect New I	mport Modify Dele	f te	CISCO SYSTEMS
Connection Entries Certificates	Log		
Connection Entry	Δ	Host	Transport
vpn		10.1.1.1	IPSec/UDP
1	The server has requested the authentication.	following information to complete th e: Juser d: JERRARERA DK	e user Cancel
Authenticating user			

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:

diesem Fenster werden Split-Tunneling-Informationen angezeigt, falls konfiguriert:

👌 ¥PN Client Statistics 🛛 🔍					×	
Tunnel Details Route Details Firewall						
Local LAN Routes		S	Secured Routes			
[Network	Subnet Mask		Network	Subnet Mask	
			0.	.0.0.0	0.0.0.0	
			L			
			L			
			L			
			L			
			L			
			L			
			L			
_						
					<u>C</u> lose	2

6. Wählen Sie Protokoll > Protokolleinstellungen, um die Protokollstufen im Cisco VPN-Client

window to be cleared.				
KE:	3 - High	•		
Connection Manager:	1 - Low		[LOG.CM]	
Daemon (cvpnd):	1 - Low	_	[LOG.CVPND]	
User Authentication:	1 - Low	-	[LOG.XAUTH]	
Certificates:	1 - Low	•	[LOG.CERT]	
IPSec:	3 - High	-	[LOG.IPSEC]	
Command Line:	1 - Low	-	[LOG.CLI]	
GUI:	1 - Low	-	[LOG.GUI]	
PPP:	1 - Low	•	[LOG.PPP]	
Firewall	1.1.000	-		

7. Wählen Sie Log > Log Windows, um die Protokolleinträge im Cisco VPN Client

	🕹 VPN Client Log Window	1
	Cisco Systems VPN Client Version 4.8.01.0300 Copyright (C) 1998-2005 Cisco Systems, Inc. All Rights Reserved. Client Type(s): Windows, WinNT Running on: 5.0.2195 Service Pack 4	
	227 10:39:32.140 05/31/06 Sev=Info/6 IKE/0x6300003B Attempting to establish a connection with 10.1.1.1.	
	228 10:39:32.156 05/31/06 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID(Xauth), VID(dpd), VID(Frag), VID(Nat-T), VID(Unity)) to 10.1.1.1	
	229 10:39:32.156 05/31/06 Sev=Info/4 IPSEC/0x63700008 IPSec driver successfully started	
	230 10:39:32.156 05/31/06 Sev=Info/4 IPSEC/0x63700014 Deleted all keys	
	231 10:39:32.156 05/31/06 Sev=Info/6 IPSEC/0x6370002C Sent 120 packets, 0 were fragmented.	
	232 10:39:33.921 05/31/06 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 10.1.1.1	
	233 10:39:33.921 05/31/06 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP 0AK AG (SA, VID(Unity), VID(dpd), VID(?), VID(Xauth), VID(Nat-T), KE, ID, NON, HASH, NAT-D, NAT-D) from 10.1.1.1	
	234 10:39:33.921 05/31/06 Sev=Info/5 IKE/0x63000001 Peer is a Cisco-Unity compliant peer	
	235 10:39:33.921 05/31/06 Sev=Info/5 IKE/0x63000001 Peer supports DPD	
	236 10:39:33.921 05/31/06 Sev=Info/5 IKE/0x63000001 Peer supports DWR Code and DWR Text	
	237 10:39:33.921 05/31/06 Sev=Info/5 IKE/0x63000001 Peer supports XAUTH	
	238 10:39:33.921 05/31/06 Sev=Info/5 IKE/0x63000001 Peer supports NAT-T	
	239 10:39:33.937 05/31/06 Sev=Info/6 IKE/0x63000001 IDS Vendor ID Contruction successful	
	Save Log Settings Clear Close	
anzuzeigen.		1

Zugehörige Informationen

- Herunterladen und Installieren von Cisco Router und Security Device Manager
- <u>Support-Seite für Cisco VPN-Clients</u>
- IPsec-Aushandlung/IKE-Protokolle
- Technischer Support und Dokumentation Cisco Systems