Esempio di configurazione SDM per un router Cisco come server VPN remoto

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Configurazione Esempio di rete Procedura di configurazione Verifica Informazioni correlate

Introduzione

In questo documento viene descritto come usare <u>Cisco Security Device Manager (SDM)</u> per configurare il router Cisco in modo che agisca come <u>server Easy VPN</u>. Cisco SDM consente di configurare il router come server VPN per il client VPN Cisco utilizzando un'interfaccia di gestione basata sul Web di facile utilizzo. Una volta completata la configurazione del router Cisco, è possibile verificarla utilizzando il client VPN Cisco.

Prerequisiti

Requisiti

In questo documento si presume che il router Cisco sia completamente operativo e configurato per consentire al Cisco SDM di apportare modifiche alla configurazione.

Nota: per consentire al router di essere configurato dal modulo SDM, consultare il documento sull'<u>autorizzazione</u> dell'<u>accesso HTTPS per</u> SDM.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Router Cisco 3640 con software Cisco IOS® versione 12.3(14T)
- Security Device Manager versione 2.31
- Cisco VPN Client versione 4.8

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a <u>Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni</u> <u>dei documenti.</u>

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare la funzionalità Easy VPN Server che consente a un utente finale remoto di comunicare tramite IPsec con qualsiasi gateway VPN di Cisco IOS®.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo <u>strumento di</u> ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Procedura di configurazione

Completare la procedura seguente per configurare il router Cisco come server VPN remoto con SDM.

 Selezionare Configure > VPN > Easy VPN Server dalla finestra Home e fare clic su Launch Easy VPN Server Wizard.



2. È necessario abilitare AAA sul router prima di avviare la configurazione di Easy VPN Server. Fare clic su Sì per continuare con la configurazione.II messaggio "AAA abilitato sul router" viene visualizzato nella finestra. Fare clic su OK per avviare la configurazione di Easy VPN Server.



3. Fare clic su **Avanti** per avviare la procedura guidata Easy VPN Server.



4. Selezionare l'interfaccia su cui terminano le connessioni client e il tipo di autenticazione.

VPN Wizard	Interface and Authentication
	Interface
A RI	Please select the interface on which the Easy VPN Server should be configured. Easy VPN clients will connect to the server through this interface.
	Interface for this Easy VPN Server:
	Authentication
94 AN	Select the method used for authenticating VPN clients connecting to this Easy VPN Server.
	Pre-shared keys C Digital Certificates C Both
	Interface connected to Internet. This is the interface where the VPN connection. But you cannot select an interface which is participating in GRE over IPSec, DMVPN or Easy VPN client connection. For more information please click the help button.

5. Fare clic su **Avanti** per configurare i criteri IKE (Internet Key Exchange) e utilizzare il pulsante **Aggiungi** per creare il nuovo criterio.Le configurazioni su entrambi i lati del tunnel devono corrispondere esattamente. Tuttavia, il client VPN Cisco seleziona automaticamente la configurazione corretta. Non è pertanto necessaria alcuna configurazione IKE sul PC client.

PN Wizard	IKE Proposals IKE proposals method that is	specify the er	contion alor			
	device. Click the Add	used by this . button to add	router when r	egotiating a VPN	tion algorithm an connection with outton to edit an e	d key exchang the remote xisting policy.
ALL	Priority	Encryption	Hash	D-H Group	Authentication	Туре
Va			1			
	Add	Edit]			

6. Fare clic su **Avanti** per scegliere il set di trasformazioni predefinito o aggiungere il nuovo set di trasformazioni per specificare l'algoritmo di crittografia e autenticazione. In questo caso, viene utilizzato il set di trasformazioni predefinito.

Easy VPN Server Wizard -	35% Complete				1
VPN Wizard	Transform Set A transform set specifies the data in the VPN tunnel.	encryption and aut	hentication 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	ł
	Select Transform Set	m Set			
	Name	EPP Encontion	EQD Integrity	Al-Integrity	Ê.
RE	ESP-3DES-SHA1	ESP_3DES	ESP_SHA_HMAC		
	Add Edit			•	
		<	Back Next > Fir	hish Cancel He	lp

7. Fare clic su **Avanti** per creare un nuovo elenco di metodi di rete di autorizzazione Autenticazione, autorizzazione e accounting (AAA) per la ricerca di Criteri di gruppo o per scegliere un elenco di metodi di rete esistente utilizzato per l'autorizzazione di gruppo.

VPN Wizard	Group Authorization and Group Policy Lookup	
	An ISAKMP client configuration group (or VPN group same authentication and configuration information. on this router, an external server, or both. Easy VPN authenticate VPN clients.	 is a group of VPN clients that share the Group policies can be configured locally Server will use these group policies to
	Method List for Group Policy Lookup	
	Select the servers on which group policies will be o policy that defines the servers used for configuring	configured, or select an existing AAA group policies.
and	@ Local	
	C RADIUS	
	C RADIUS and local	
	C Select an existing AAA method list	-Select an entry
		Add RADIUS Server
	Summary	
	The local database will be used for group authoriza you do not have a RADIUS or TACACS+ server in yo	tion. This option is recommended if ur network.
	< Bac	k Next > Finish Cancel Heln

8. Configurare l'autenticazione utente sul server Easy VPN.Èpossibile memorizzare i dettagli di autenticazione degli utenti su un server esterno, ad esempio un server RADIUS o un database locale oppure su entrambi. L'elenco dei metodi di autenticazione di accesso AAA viene utilizzato per stabilire l'ordine in cui cercare i dettagli di autenticazione dell'utente.

Easy VPN Server Wizard -	65% Complete	×
VPN Wizard	User Authentication (XAuth) User authentication (XAuth) provides additional security by auth after the device has undergone IKE authentication. User creder locally on this router, on an external server, or both.	nenticating the user of a device ntials XAuth can be configured
	 Enable User Authentication Select the servers that will be used for configuring user creder AAA policy that defines the servers used for configuring user creder Local Only 	ntials, or select an existing redentials.
	C RADIUS and Local Only C Select an existing AAA method list	Add RADIUS Server
	Local database will be used for user authentication.	
	< Back Next >	Finish Cancel Help

9. Questa finestra consente di aggiungere, modificare, duplicare o eliminare i criteri di gruppo degli utenti nel database locale.

Easy VPN Server Wizard - 80	% Complete			-	×
VPN Wizard	Group Authorizatio	on and User G	oup Policies		
	The Easy VPN Serv other Easy VPN Re clients or device the the remote client or Click the Add butt Clone button to cr	ver allows you t mote client pro at is part of a g r device to ensi on to add mon reate a new gri	to group remote o oducts. The group iven group. The s ure that appropria e groups, the Edi oup from an exist	users who are u o attributes will b came group nam ate group attribut t button to edit ing group.	sing Cisco VPN clients or te downloaded through the te should be configured on tes are downloaded. an existing group, or the
	Group Name	Pool	DNS	WINS	Domain Name
N	Add	idit	Ione Del	ete	
	Configure a timer cleared. Idle Timer:	out value after	which VPN tunne	ls from idle clier 1:88	its should be
			< Ba	ck Next> Fi	nish Cancel Help

10. Immettere un nome per il nome del gruppo di tunnel. Specificare la chiave già condivisa utilizzata per le informazioni di autenticazione.Creare un nuovo pool o selezionare un pool esistente utilizzato per allocare gli indirizzi IP ai client VPN.

27 A 20 A 20	g Client Settings XAuth Options
Jame of This Group:	vpn
— 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:	******
Specify a local pool containing a ra internal IP address to a client.	ange of addresses that will be used to allocate an
Specify a local pool containing a ra internal IP address to a client.	ange of addresses that will be used to allocate an C Select from an existing pool
Specify a local pool containing a ra internal IP address to a client. Create a new pool Starting IP address: 1921682	ange of addresses that will be used to allocate an C Select from an existing pool -Select an entry C Details
Specify a local pool containing a ra internal IP address to a client. Create a new pool Starting IP address: 192.168.2 Ending IP address: 192.168.2	ange of addresses that will be used to allocate an C Select from an existing pool 2.1
 Specify a local pool containing a rainternal IP address to a client. Create a new pool Starting IP address: 192.168.2 Ending IP address: 192.168.2 Enter the subnet mask that should 	ange of addresses that will be used to allocate an C Select from an existing pool 2.1 -Select an entry Details 1.5 d be sent to the client along with the IP address.
Specify a local pool containing a rainternal IP address to a client. Create a new pool Starting IP address: 192.168.2 Ending IP address: 192.168.2 Enter the subnet mask that should Subnet Mask: 255.255.2	ange of addresses that will be used to allocate an C Select from an existing pool -Select an entry Details C Details C be sent to the client along with the IP address. C (Optional)
Specify a local pool containing a ra internal IP address to a client. Create a new pool Starting IP address: 192.168.2 Ending IP address: 192.168.2 Enter the subnet mask that should Subnet Mask: 255.255.2	ange of addresses that will be used to allocate an C Select from an existing pool -Select an entry Details 1.5 d be sent to the client along with the IP address. 255.0 (Optional)

11. Questa finestra mostra un riepilogo delle azioni intraprese. Se la configurazione è soddisfacente, fare clic su **Fine**.

VPN Wizard	Summary of the Configuration			
	Click finish to deliver the configuration to the	ie 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	local		
	User Authentication Method List	: Local		
	Idle Timer	: «NONE»		
	Number of Group Policies	:1		_
	Group Policy Name - vonel	lont		▼ ≥
	Test VPN connectivity after configuring.			

12. Il modulo SDM invia la configurazione al router per aggiornare la configurazione in esecuzione. Fare clic su **OK** per completare

'operazione.	
Commands Delivery Status	×
Command Delivery Status:	
Preparing commands for delivery Submitting 27 commands, please wait Configuration delivered to router.	<u></u>
•	T T
OK	

13. Al termine, è possibile modificare le modifiche apportate alla configurazione, se necessario.



Verifica

Tentare di connettersi al router Cisco utilizzando il client VPN Cisco per verificare che il router Cisco sia configurato correttamente.

1. Selezionare Voci di connessione > Nuovo.

👶 status: Disconnected	VPN Client - Version 4.8.0	01.0300	
Connection Entries Status	Certificates Log Options	Help	
Connect New	Import Modify) Delete	CISCO SYSTEMS
Connection Entries Certific	cates Log		
Connection Entry	∇	Host	Transport
•			
Not connected.			

2. Specificare i dettagli della nuova connessione.Il campo Host deve contenere l'indirizzo IP o il nome host dell'endpoint del tunnel di Easy VPN Server (router Cisco). Le informazioni di autenticazione del gruppo devono corrispondere a quelle utilizzate nel passaggio 9. Al termine, fare clic su

Connection Entry. J	pn		
Description:			50)
Host: 1	0.1.1.1		
Authentication	Transport Back	up Servers Dial-Up	
Group Authent	ication	C Mutual Grou	p Authentic
Name:	vpn		
Password:	******		
Confirm Passwo	rd: ******		
C Certificate Auth	nentication		
Name;		<u>*</u>	
🔲 Send CA Ce	ertificate Chain		

3. Selezionare la connessione appena creata e fare clic su

Connetti	
----------	--

👌 status: Discon	nected VPN Cl	ient - Version 4.8.	01.0300	_ 🗆 ×
Connection Entries	Status Certifica	tes Log Options	Help	
Connect N	New Impor	Modify	Delete	CISCO SYSTEMS
Connection Entries	Certificates	Log		
Cor	nnection Entry /		Host	Transport
vpr	1		10.1.1.1	IPSec/UDP
4				>
Not connected.				P.

4. Immettere un nome utente e una password per l'autenticazione estesa (Xauth). Queste informazioni sono determinate dai parametri Xauth nel passaggio

Connection Entries	Status Cert	N Client – Ve tificates Log	Options Help		_ III
Cancel Connect	New	Import	Modify [)elete	
Connection Entries	Certificate	s Log			
Con	nection Entry	4		Host	Transport
vpn		-		10.1.1.1	IPSec/UDP
		🥝 YPN Cli	ent User A	uthentication for "vpn"	×
		The serve authentica	ent User A r has requested ation. YSTENS User	uthentication for "vpn" the following information to name: user word: management	complete the user

5. Una volta stabilita la connessione, selezionare **Statistics** dal menu Status per verificare i dettagli del tunnel.In questa finestra vengono visualizzate le informazioni sul traffico e sulla

unnel Details	Route Details	Firewall	
Address In	formation	Connection Informa	tion
Client:	192.168.2.5	Entry:	vpn
Server:	10.1.1.1	Time:	0 day(s), 00:06.43
Bytes		Crypto	
Receive	d: 1800	Encryption:	168-bit 3-DES
Sent:	1800	Authentication:	HMAC-SHA1
Packets		Transport	
Encrypte	d: 30	Transparent Tunne	ling:Inactive
Decrypte	ed:30	Local LAN:	Disabled
Discarde	d: 37	Compression:	None
Bypasse	d: 164		
			Reset
			Close

crittografia: uesta finestra mostra le informazioni sul tunneling suddiviso, se configurato:

8	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			
					_		
				<u>C</u> lose	Ę.		

6. Selezionare Log > Log Settings per abilitare i livelli di log nel client VPN



7. Selezionare Log > Log Windows per visualizzare le voci di log nel client VPN

🕹 VPN Client Log Window	
Cisco Systems VPN Client Version 4.8.01.0300 Copyright (C) 1998-2005 Cisco Systems, Inc. All Rights Client Type(s): Windows, WinNT Running on: 5.0.2195 Service Pack 4	s Reserved.
227 10:39:32.140 05/31/06 Sev=Info/6 K8 Attempting to establish a connection with 10.1.1.1.	E/0x6300003B
228 10:39:32.156 05/31/06 Sev=Info/4 IKE SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, V VID(Nat-T), VID(Unity)) to 10.1.1.1	E/0x63000013 /ID(Xauth), VID(dpd), VID(Frag),
229 10:39:32.156 05/31/06 Sev=Info/4 IPS IPSec driver successfully started	SE C/0x63700008
230 10:39:32.156 05/31/06 Sev=Info/4 IPS Deleted all keys	SEC/0x63700014
231 10:39:32.156 05/31/06 Sev=Info/6 IPS Sent 120 packets, 0 were fragmented.	SEC/0x6370002C
232 10:39:33.921 05/31/06 Sev=Info/5 IKE Received ISAKMP packet peer = 10.1.1.1	E/0x6300002F
233 10:39:33.921 05/31/06 Sev=Info/4 IKE RECEIVING <<< ISAKMP 0AK AG (SA, VID(Unity), VI KE, ID, NON, HASH, NAT-D, NAT-D) from 10.1.1.1	E/0x63000014 ID(dpd), VID(?), VID(Kauth), VID(Nat-T),
234 10:39:33.921 05/31/06 Sev=Info/5 IKE Peer is a Cisco-Unity compliant peer	E/0x63000001
235 10:39:33.921 05/31/06 Sev=Info/5 IKE Peer supports DPD	E/0x63000001
236 10:39:33.921 05/31/06 Sev=Info/5 IKE Peer supports DWR Code and DWR Text	E/0x63000001
237 10:39:33.921 05/31/06 Sev=Info/5 IKE Peer supports XAUTH	E/0x63000001
238 10:39:33.921 05/31/06 Sev=Info/5 IKE Peer supports NAT-T	E/0x63000001
239 10:39:33.937 05/31/06 Sev=Info/6 IKE IOS Vendor ID Contruction successful	E/0x63000001
Save Log Settings Clear	Close

Cisco.

Informazioni correlate

- Download e installazione di Cisco Router and Security Device Manager
- Pagina di supporto per Cisco VPN Client
- Negoziazione IPSec/protocolli IKE
- Documentazione e supporto tecnico Cisco Systems