OpenVPN su un RV160 e RV260 Router

Obiettivo

L'obiettivo di questo articolo è di guidarvi nella configurazione di OpenVPN sul router RV160 o RV260 e nella configurazione del client VPN di OpenVPN sul computer.

Dispositivi interessati

- RV160
- RV260

Versione del software

• 1.0.00.15

Sommario

Configurazione di una Demo OpenVPN su un router RV160/RV260

Configurazione di OpenVPN su un router RV160/RV260

Accesso con certificato autofirmato dopo la configurazione di Demo OpenVPN

Installazione di OpenVPN Client sul computer

Introduzione

OpenVPN è un'applicazione open source gratuita che può essere configurata e utilizzata per una rete VPN (Virtual Private Network). Utilizza una connessione client-server per garantire comunicazioni protette tra un server e una posizione remota del client tramite Internet.

OpenVPN utilizza OpenSSL per la crittografia di UDP e TCP per la trasmissione del traffico. Una VPN offre un tunnel di protezione sicuro, meno vulnerabile agli hacker poiché crittografa i dati inviati dal computer tramite la connessione VPN. Ad esempio, se si utilizza WiFi in un luogo pubblico, come in un aeroporto, i dati, le transazioni e le query non vengono visualizzati da altri utenti. Analogamente al protocollo HTTPS, crittografa i dati inviati tra due endpoint.

Uno dei passaggi più importanti per la configurazione di OpenVPN è ottenere un certificato da un'Autorità di certificazione (CA). Utilizzato per l'autenticazione. I certificati possono essere acquistati da diversi siti di terze parti. È un modo ufficiale per dimostrare che il tuo sito è sicuro. Essenzialmente, la CA è una fonte attendibile che verifica che l'azienda sia legittima e che possa essere considerata attendibile. Per OpenVPN è sufficiente un certificato di livello inferiore a un costo minimo. L'utente viene estratto dall'autorità di certificazione e, una volta verificate le informazioni, il certificato verrà rilasciato all'utente. Il certificato può essere scaricato come file nel computer. È quindi possibile accedere al router (o al server VPN) e caricarlo in tale posizione. Nota: i client non hanno bisogno di un certificato per usare OpenVPN, è solo per la verifica tramite il router.

Prerequisiti

Installare l'applicazione OpenVPN nel sistema. Fare clic <u>qui</u> per accedere al sito Web OpenVPN.

Per ulteriori informazioni su OpenVPN e le risposte a molte domande che potresti avere, clicca qui

Nota: Questa installazione è specifica di Windows 10.



Una volta installato OpenVPN, l'applicazione dovrebbe apparire sul desktop o come una piccola icona sul lato destro della barra delle applicazioni. Anche i client OpenVPN avranno bisogno di questa installazione.



Assicurarsi di aver impostato l'ora di sistema corretta su tutti i dispositivi. Prima di creare un

certificato, è necessario sincronizzare completamente l'ora di sistema corretta sul router. Questa operazione viene spesso eseguita automaticamente, ma se si verificano problemi, è consigliabile controllare in questa posizione.

Configurazione di una Demo OpenVPN su un router RV160/RV260

Se si desidera provare OpenVPN prima di pagare per una CA, è possibile creare un certificato autofirmato. Questo è un modo a costo zero per vedere se OpenVPN è qualcosa che si desidera installare per la vostra azienda. Se già si è certi di voler acquistare una CA, è possibile saltare questa sezione dell'articolo e andare direttamente a <u>Configurazione di OpenVPN su un router</u> <u>RV160/RV260</u>.

Passaggio 1. Accedere al router utilizzando le credenziali. Il nome utente e la password predefiniti sono *cisco*.

Nota: Si consiglia di modificare tutte le password in modo da renderle più complesse. Altrimenti, è come lasciare la chiave alla porta chiusa a chiave sulla soglia.



Passaggio 2. È necessario ottenere un certificato sul router. Passare a **Amministrazione** > **Certificato** > **Genera CSR/Certificato...** In questo modo viene creata la richiesta di un certificato.

		E¢	cisco	RV260-PnPDemo				Alert cisco(admin)	English	⊻ 🕄	8 0
⊗	Getting Started	Cort	ficato								
Ģ	Status and Statistics	Cert	incate								
*	Administration	Corti	ificato Table								•
	File Management	Cert	incate rabie	,							
	Reboot	_	Index	Certificate	Used by	Туре	Signed By	Duration	Details	Action	
C		0	1	Default	-	Local Certificate	-	From 2018-Sep-17, 00:00:00 To 2048-Sep- 09, 00:00:00	-	1	
	Configuration Management	0	2	CertTi	-	CA Certificate	Self-Signed	From 2018-Apr-04, 00:00:00 To 2023-Apr- 04, 00:00:00		1	
* 0	System Configuration	۲	3	CertImport	NETCONF WebServer RESTCONF	Local Certificate	CiscoTest- DC1-CA	From 2018-Aug-03, 00:00:00 To 2020-Aug- 02, 00:00:00		1	
*	LAN	0	4	AnthonyRouterIm	-	Local Certificate	CiscoTest- DC1-CA	From 2018-Sep-18, 00:00:00 To 2020-Sep- 17, 00:00:00	-	1	
	Firewall			3							
	VPN	Impo	rt Certificate.	Generate CS	R/Certificate	Show bui	lt-in 3rd party C	A Certificates	t as Primary	Certificate	÷

Passaggio 3. Richiedere un certificato CA.

\otimes	Getting Started	Concrete CSP/Cortifica	to	0	Gonorato	Cancol
•	Status and Statistics			U	Generate	Cancer
*	Administration	Type:	CA Certificate			
	File Management	Octificate Name	Cart Taet CA			
	Reboot	Certificate Name:				
	Diagnostic	Subject Alternative Name:	192.168.1.50			
	Certificate		IP Address O FQDN O Email			
	Configuration Management	Country Name (C):	United States ~			
٠	System Configuration	State or Province Name (ST):				
۲	WAN	Locality Name (L):				
	LAN	Organization Name (O):				
Ş	Wireless	Organization Unit Name (OU):	Training			
*	Routing	Common Name (CN):	Cert Test CA			
	Firewall	5	Maissa com			
Ŧ	VPN	Email Address (E):	eciaco.com			
	Security	Key Encryption Length:	2048			

- Selezionare Certificato CA dal menu a discesa
- Immettere il nome di un certificato
- Immettere l'indirizzo IP, il nome di dominio completo (FQDN) o l'indirizzo di posta elettronica. L'immissione dell'indirizzo IP è la scelta più comune.
- Inserire il Paese
- Immettere lo stato
- Inserire il nome della località, in genere la città
- Inserire il nome dell'organizzazione
- Inserire il nome dell'unità organizzativa
- Immetti il tuo indirizzo e-mail
- Immettere la lunghezza di crittografia della chiave, si consiglia 2048

Fare clic sul pulsante Genera in alto a destra.

Passaggio 4. È inoltre necessario un certificato server. Questo *certificato firmato da CA* verrà firmato dal certificato CA appena creato.

		E	cisco					Alert cisco(admin) English	∨ ?	8 C•
\otimes	Getting Started	Corti	ficato								
¢	Status and Statistics	Certi	incate								
*	Administration	Certi	ficate Table	2							~
	File Management	Ceru	noate rabit								
	Reboot		Index	Certificate	Used by	Туре	Signed By	Duration	Details	Action	_
	Diagnostic	0	1	Default	-	Local Certificate	-	From 2018-Sep-17, 00:00:00 To 2048-Sep-		<u>1</u>	
	Certificate	-						09, 00:00:00 From 2018-Apr-04	_	• •	
	Configuration Management	0	2	CertT		CA Certificate	Self-Signed	00:00:00 To 2023-Apr- 04, 00:00:00		⊥ Ш	
٠	System Configuration	٥	3	CertImport	NETCONF WebServer	Local Certificate	CiscoTest- DC1-CA	From 2018-Aug-03, 00:00:00 To 2020-Aug-		1	
۲	WAN				RESTCONF			02, 00:00:00			
#	LAN	0	4	AnthonyRouterIm	-	Local	CiscoTest-	From 2018-Sep-18, 00:00:00 To 2020-Sep-		1	
(\mathfrak{k})	Routing					Gertiliedte	DOT OA	17, 00:00:00			
	Firewall			0							
Ð	VPN	Impor	t Certificate	Generate CS	R/Certificate	Show bu	ilt-in 3rd party C	A Certificates	t as Primar	y Certificate.	

Passaggio 5. Richiedere un certificato firmato da un certificato CA.

\bigotimes	Getting Started	Concrete CSP/Cortifica		
•	Status and Statistics	Generale CSR/Certifica		Generate
*	Administration	Туре:	Certificate Signed by CA Certificate V	
	File Management	Authorize External CSR:		
	Reboot	Certificate Name:	CertTest_CA	
	Diagnostic	Subject Alternative Name	192.168.1.50	
	Certificate	Subject Alternative Name.	IP Address O FODN O Email	
	Configuration Management	Country Name (C):	United States	
٠	System Configuration	State or Province Name (ST):		
۲	WAN	Leeslin Neme (L)		
	LAN	Locality Name (L):		
Ş	Wireless	Organization Name (O):		
*	Routing	Organization Unit Name (OU):		
謹	Firewall	Common Name (CN):	Cert Test CA	
Ð	VPN	Email Address (E):	.com	
	Security	Kee Free stars have the	2048	
T	QoS	Key Encryption Length:	2046	
		Valid Duration:	360	da <i>r</i> s (Range: 1-10950, Default 360)
		Certificate Authority:	~	

- Selezionare Richiesta firma certificato dal menu a discesa
- Immettere il nome di un certificato
- Immettere l'indirizzo IP, il nome di dominio completo (FQDN) o l'indirizzo di posta elettronica. L'immissione dell'indirizzo IP è la scelta più comune.
- Inserire il Paese
- Immettere lo stato
- Inserire il nome della località, in genere la città
- Inserire il nome dell'organizzazione
- Inserire il nome dell'unità organizzativa
- Immetti il tuo indirizzo e-mail
- Immettere la lunghezza di crittografia della chiave, si consiglia 2048
- Scegliere l'autorità di certificazione appropriata dal menu a discesa

Fare clic sul pulsante Genera in alto a destra.

Passaggio 6. Passare a **Configurazione di sistema > Gruppi di utenti**. Selezionare l'icona **più** per aggiungere il nuovo gruppo.

() (Getting Started Status and Statistics	Us	ser	Groups						Ар	ply Ca	incel
 <	Administration 1 System Configuration	3	+	e 1								
	Initial Router Setup			Group	Web Login /NETCONF /RESTCONF	Lobby Ambassa	802.1x	S2S IPSec VPN	C2S IPSec VPN	OpenVPN	PPTP	Captive Portal
	Time			Ambassa	Disable	Enable	Disable	Disable	Disable	Disable	Disable	Enable
	Log			admin	Admin	Enable	Enable	Enable	Enable	Enable	Enable	Enable
	Email			guest	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Disable
ſ	User Accounts User Groups 2											

Passaggio 7. Immettere il nome del gruppo e fare clic su *On* per attivare OpenVPN. Fare clic su **Apply** (Applica).

User Groups	Cancel								
Group Name: Ope	nVPN 1								
Local User Mem	Local User Membership List								
╋ 💼 □ # User									
* Should have at leas	st one account in the 'admin' group.								
Services									
Web Login/NETCON	Web Login/NETCONF/RESTCONF: O Disable O Readonly O Admin								
Site to Site VPN:	 								
Client to Site VPN:	+ 🖮								
	# Group Name .								
OpenVPN: 2									
PPTP VPN:	O On O Off								
802.1x:	O On O Off								
Lobby Ambassador:	O On 🧿 Off								

Passaggio 8. Passare al menu Configurazione di sistema e fare clic su **Account utente**. In Utenti locali, fare clic sull'icona **più**.

\otimes	Getting Started	User Accounts	Apply Cancel
•	Status and Statistics		
**	Administration	Minimal Password Length:	8 (Range: 0-64, Default: 8)
٠	System Configuration	Minimal Number of Character Classes:	3 (Range: 0-4, Default: 3)
	Initial Router Setup	The four classes are: uppercase (A,B,C), lowercase (a,	b,c), numbers (1,2,3) and special characters (!@#\$).
	System	The new password must be different from the current on	e.: D Enabled
	Time		
	Log	Password Aging Time:	180 days (Range: 0-365, 0 means never expires)
(Email User Accounts	Local Users	^
	User Groups	+ 🖉 🖻 📥 土	
	IP Address Groups		Group
	SNMP	Test_Admin	Ambassador
	Discovery-Bonjour	C cisco	admin
	LLDP	auest	quest
	Automatic Updates	* Should have at least one account in the 'admin' grou	ip.
	Schedules	, i i i i i i i i i i i i i i i i i i i	

Passaggio 9. Inserire le informazioni richieste di seguito. Assicurarsi di selezionare OpenVPN dal menu a discesa. Fare clic su **Apply** (Applica).

Add user account

A The current minimun	n requirements are as follo	ows	
 * Minimal Password * Minimal Number of 	Length: 8 f Character Classes: 3		
Username:	VPN		
New Password:	•••••		
Confirm Password:	••••••		
Password Strength meter:			
Group:	OpenVPN ~		
	2	Apply Car	ncel

Tutte le dipendenze sono complete e il router può ora essere configurato per OpenVPN.

Passaggio 10. Passare a VPN > OpenVPN. Viene visualizzata la pagina OpenVPN. Completare ogni casella della pagina, assicurandosi di selezionare i certificati creati in precedenza dal menu a discesa.

\otimes	Getting Started	Open\/DN					alv	Cancel
•	Status and Statistics	Openven					Jiny Contraction	Cancer
**	Administration	Enable: 3						
٠	System Configuration	Interface:	All	~				
۲	WAN	CA Certificate:	A_Trust_	~				
.	LAN	Server Cartificato						
Ş	Wireless	derver Certificate.		-				
R	Routing	Client Authentication:	Password Only	~				
	Firewall	Client Address Pool:	10.1.		Netmask:	255.255.255.0		
E	VPN	Protocol:	UDP	~	Port:	1194		
	VPN Setup Wizard	Encryption:	AES-256	~				
	IPSec VPN	Tunnel Mode:	O Full Tunnel, routing all client traffic throug	h VF	PN			
– (OpenVPN 2		• Split Tunnel, routing client traffic destined	d to f	the following	subnets through VPN		

- Selezionare la casella *Attiva*. Selezionare l'interfaccia che verrà consentita nel traffico. In questo caso, una rete WAN (Wide Area Network) e selezionare un certificato CA (Certification Authority).
- Selezionare il certificato CA dal menu a discesa
- Selezionare il certificato server scaricato dal menu a discesa
- Selezionare Autenticazione client. Se si seleziona Password, è necessario eseguire l'autenticazione con una password. Se si seleziona Password + Certificato, anche il client deve disporre di un certificato. Ciò è più sicuro, ma aumenta il costo della VPN in quanto dovrebbe acquistare una CA separata.
- Immettere il *pool di indirizzi client*. Scegliere un indirizzo IP in una subnet di rete che non venga utilizzato in altre posizioni della società. È possibile selezionare un intervallo tra quelli riservati e scegliere un intervallo non utilizzato altrove.
- Scegliere il tipo di *crittografia*. Assicurarsi che la crittografia sia la stessa del client. DES e 3DES non sono consigliati e devono essere utilizzati solo per compatibilità con le versioni precedenti.
- Scegliere Dividi tunnel se si desidera solo specificare il traffico che attraversa la VPN. Per una VPN, è necessario un tunnel suddiviso. La *modalità tunnel completo* è selezionata in altre situazioni quando si desidera che tutto il traffico client passi attraverso la VPN.

Passaggio 11. Scorrere la pagina verso il basso e compilare i campi Domain Name e DNS1.

Domain Name:	Openvpn.net
DNS1:	192.168.1.1

Nota: l'indirizzo IP DNS1 potrebbe essere un server DNS interno dedicato, lo stesso indirizzo IP del gateway predefinito fornito dal provider di servizi Internet (ISP), in una macchina virtuale o un server DNS trusted in Internet.

Passaggio 12. Fare clic su Apply per salvare la configurazione sul router.

Passaggio 13. Rimanere sulla stessa pagina e scorrere ulteriormente. Generare il modello di configurazione da installare sul client OpenVPN. Questo file ha estensione *.ovpn* e verrà utilizzato dal client OpenVPN. Selezionare la casella per *Esportare* il *modello di configurazione client (ovpn)* e fare clic su **Genera**. Il file verrà scaricato nel computer.

Export setting:	
Include client certificate:	
Please choose the method you want to export:	
1 Export client configuration template (.ovpn)	
Send Email Click here to configure Email settings.	
Email client configuration template (.ovpn) to recipients (multiple email addresses separated by comma):	input email address
Email Subject:	OpenVPN Client Configurat
Generate	

Passaggio 14. Passare a **Stato e statistiche > Stato VPN**. È possibile scorrere verso il basso per ottenere informazioni più dettagliate.

\odot	Getting Started	Suctor Su	man/					
6	Status and Statistics	System Su	ninary					
	System Summary	IPv4 IP	v6					
	TCP/IP Services		WAN (Conner)	LISP				
	Port Traffic	IP Address	210.1.100.20/24	038				
	WAN QoS Statistics	Default Gateway	210.1.100.1					
	Switch QoS Statistics	DNS:	210.1.100.1	h				
	Connected Devices	Dynamic DNS:	Disabled	Disabled				
	Routing Table		Release Renew	(No Attached)			
	DHCP Bindings							
	Mobile Network							
ſ	VPN Status	VPN Status						
	View Logs	Type	Acti	ve	Configured	Max Supported	Connected	
쓭	Administration	IPSec .	Disa	bled	0	20	0	
٥	System Configuration	PPTP	Disa	bied	1	20	0	
0	WAN	OpenVPN	Enab	ied	1	20	0	3
4	LAN							
8	Routing	Eirourall Cott	ng Ctatus		Log Co	ttice Status		
	Firewall	Firewall Sett	ing Status		Log Se	tting Status		
	VPN	SPI (Stateful Packe	t inspection): On		Syslog Ser	ver: Off		
•		on i formation i acom						
	Security	DoS (Denial of Sen	rice): On		Email Log:	Off		

La sezione successiva di questo articolo è importante da rivedere, in quanto spiega come accedere con un certificato autofirmato.

Accesso con certificato autofirmato dopo la configurazione di Demo OpenVPN

Quando si accede con un certificato autofirmato, è possibile che venga visualizzato un messaggio di avviso popup quando si tenta di eseguire l'accesso. Per continuare, è necessario fare clic su Avanzate, Procedi, Considera attendibile o su un'altra opzione a seconda del browser Web utilizzato.

A questo punto è possibile che venga visualizzato un messaggio di avviso per segnalare che non è sicuro. È possibile scegliere di continuare, aggiungere un'eccezione o avanzate. Questo può variare a seconda del browser.

In questo esempio, Chrome è stato utilizzato per un browser Web. Viene visualizzato questo messaggio. Fare clic su **Avanzate**.

Your connection is not private

 Attackers might be trying to steal your information from
 .net (for example, passwords, messages, or credit cards).

 NET::ERR_CERT_AUTHORITY_INVALID

Help improve Safe Browsing by sending some system information and page content to Google. Privacy policy.

ADVANCED

BACK TO SAFETY

Verrà visualizzata una nuova schermata e sarà necessario fare clic su **Procedi a yourwebsite.net** (unsafe)

This server could not prove that it is	. net ; its security certificate is not trusted by your
computer's operating system. This may be	e caused by a misconfiguration or an attacker intercepting your
connection.	

Di seguito è riportato un esempio di accesso all'avviso del dispositivo quando si utilizza Firefox come browser Web. Fare clic su **Advanced** (Avanzate).

Infine, fare clic su Conferma eccezione di protezione.

Add Security Exception	×				
You are about to override how Firefox identifies this site. Legitimate banks, stores, and other public sites will not ask you to do this.					
Server					
Location: https:// /login.html	Get Certificate				
Certificate Status This site attempts to identify itself with invalid information. Wrong Site					
The certificate belongs to a different site, which could mean that someone is trying to impersonate this site.					
Unknown Identity					
The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a	secure signature.				
Permanently store this exception					
<u>C</u> onfirm Security Exception	on Cancel				

Il router è ora configurato con tutti i parametri necessari per supportare una connessione client OpenVPN. Poiché il modello di configurazione client è già stato scaricato nel dispositivo, quello che termina con *.ovpn*, è possibile passare alla sezione <u>Installazione client OpenVPN nel</u> <u>computer</u>. Se si decide di distribuire OpenVPN per la propria azienda, è possibile seguire i passaggi descritti in questa sezione successiva.

Configurazione di OpenVPN su un router RV160/RV260

Si tratta di un processo più complicato in quanto comporta l'ottenimento di un'autorizzazione da parte di terzi, che comporta costi elevati. È inoltre necessario inviare il modello di configurazione del client VPN, che termina con *.ovpn*, a tutti i client in modo che possano eseguire la configurazione nel dispositivo. Affinché i client possano comunicare, hanno bisogno di diverse impostazioni uguali a quelle del router. La parte migliore è che, a un costo minimo, tu e i tuoi dipendenti potete usare Internet e condurre gli affari in modo più sicuro.

Passaggio 1. Accedere al router utilizzando le credenziali. Il nome utente e la password predefiniti sono *cisco*.

Nota: Si consiglia di modificare tutte le password in modo da renderle più complesse. Altrimenti, è come lasciare la chiave alla porta chiusa a chiave sulla soglia.

Passaggio 2. È necessario ottenere un certificato. Passare a **Amministrazione > Certificato > Genera CSR/Certificato...** In questo modo viene creata la richiesta di un certificato.

	<u>^</u>	B	ılı.ılı. cısco	RV260-PnPDemo				 Alert cisco(admin)) English	⊻ 8 €	• •
\otimes	Getting Started	Cort	ficato								
₿	Status and Statistics	Certi	ncate								
*	Administration 1	Certi	ficate Tak								~
	File Management	Oeru	neate rac								
	Reboot		Index	Certificate	Used by	Туре	Signed By	Duration	Details	Action	
\subset		0	1	Default	-	Local Certificate	-	From 2018-Sep-17, 00:00:00 To 2048-Sep- 09, 00:00:00	-	1	_
	Configuration Management	0	2	CertT		CA Certificate	Self-Signed	From 2018-Apr-04, 00:00:00 To 2023-Apr- 04, 00:00:00	-	1 🛍	
* ©	System Configuration WAN	٥	3	CertImport	NETCONF WebServer RESTCONF	Local Certificate	CiscoTest- DC1-CA	From 2018-Aug-03, 00:00:00 To 2020-Aug- 02, 00:00:00	-	1	
- 	LAN	0	4	AnthonyRouterIm	-	Local Certificate	CiscoTest- DC1-CA	From 2018-Sep-18, 00:00:00 To 2020-Sep- 17, 00:00:00		1	
	Firewall			3				· -			
÷	VPN	Impor	t Certificat	Generate CS	R/Certificate	Show bu	ilt-in 3rd party C	A Certificates Selec	t as Primar,	/ Certificate	

Passaggio 3. Richiedere un *certificato firmato da un certificato CA*. Per ulteriori informazioni, selezionare **Amministrazione > Certificato**.

	Getting Started	Generate CSR/Certifica	te
6	Status and Statistics		
1	Administration	Type:	Certificate Signing Request
	File Management	Certificate Name:	Router
	Reboot		
	Diagnostic	Subject Alternative Name:	192.168.
	Certificate 2		IP Address O FQDN O Email
	Configuration	Country Name (C):	United States 🗸
.		State or Province Name (ST):	
	System Configuration	Locality Name (L):	
9	WAN		
	LAN	Organization Name (O):	
	Wireless	Organization Unit Name (OU):	Training
8	Routing	Common Name (CN):	
	Firewall	Empil Address (E)	Driego com
	VPN	Email Address (E).	ecococoli
A	Security	Key Encryption Length:	2048 ~

- Selezionare Richiesta firma certificato dal menu a discesa
- Immettere il nome di un certificato
- Immettere l'indirizzo IP, il nome di dominio completo (FQDN) o l'indirizzo di posta elettronica. L'immissione dell'indirizzo IP è la scelta più comune.
- Inserire il Paese
- Immettere lo stato
- Inserire il nome della località, in genere la città
- Inserire il nome dell'organizzazione
- Inserire il nome dell'unità organizzativa
- Immetti il tuo indirizzo e-mail
- Immettere la lunghezza di crittografia della chiave, si consiglia 2048

Fare clic sul pulsante Genera in alto a destra

Passaggio 4. Selezionare Esporta facendo clic sulla freccia su in Azione.

@ •	Getting Started Status and Statistics	Cert	ificate							
*	Administration	Cert	tificate Table							
	File Management									
	Reboot		Index	Certificate	Used by	Туре	Signed By	Duration	Details	Action
	Diagnostic	0	1	Default	-	Local Certificate	-	From 2018-Sep-17, 00:00:00 To 2048-Sep-09, 00:00:00		<u>1</u>
	Certificate	0	2	CertTest_CA	-	CA Certificate	Self-Signed	From 2018-Apr-04, 00:00:00 To 2023-Apr-04, 00:00:00		1
	Configuration Management		3	CertImport	NETCONF WebServer	Local Certificate	CiscoTest-DC1- CA	From 2018-Aug-03, 00:00:00 To 2020-Aug-02, 00:00:00		1
٠	System Configuration				RESTCONF				2	
Ø	WAN	0	4 🗟	AnthonyRouterImport		Local Certificate	CiscoTest-DC1- CA	From 2018-Sep-18, 00:00:00 To 2020-Sep-17, 00:00:00		(
*	LAN									
8	Routing									
	Firewall	Impo	ort Certificate.	Generate CSR/0	Certificate	Show built-in 3rd part	y CA Certificates	Select as Primary Certificat	te	

Passaggio 5. Viene visualizzata questa schermata. Fare clic su Esporta.

Passaggio 6. Selezionare *Apri con e Blocco note* (impostazione predefinita) dal menu a discesa. Fare clic su **OK**.

Opening AnthonyRo	outer.pem	>
You have chosen to	open:	
AnthonyRout	ter.pem	
which is: PEM	file (1.2 KB)	
from: blob:		
What should Firefo	ax do with this file?	
Open with	Notepad (default)	
Save File		
Do this <u>a</u> uto	matically for files like this from now on.	
	OK Cancel	
Passaggio 7 Verrà a	perto un file XML.	
i ussuggio i . venta a		
AnthonyRouter.pem - Notepad File Edit Format View Help		×

Nota: Assicurarsi che le righe BEGIN CERTIFICATE REQUEST e END CERTIFICATE REQUEST siano separate, come illustrato sopra.

Passaggio 8. Nella parte superiore dello schermo, fare clic su **Modifica** e selezionare **Copia** dal menu a discesa.

<u> </u>	AnthonyRouter.pem - N	lotepad	
File	Edit F1at View	Help	
	Undo	Ctrl+Z	JEST
MIII CwwJ	Cut	Ctrl+X	MDkFu
CgKO	Copy 2	Ctrl+C	₹Xo/6v
az85	Paste	Ctrl+V	AVLOC
+yto +8r4	Delete	Del	1+29JF AsGA1U
MA80	Find	Ctrl+F	/JKoZI
+280	Find Next	F3	PnlGye
1201	Replace	Ctrl+H	5T
	Go To	Ctrl+G	
	Select All	Ctrl+A	
	Time/Date	F5	

Passaggio 9. Scegliere una sede di terze parti attendibile per eseguire la richiesta di certificato. È necessario incollare il file XML copiato come parte della richiesta.

Nota: Se nella rete è presente un server di certificati interno, è possibile utilizzarlo in alternativa, anche se questa condizione non è comune.

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC Saved Request box.

Saved Request:		3
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	TZOTKHXBcMTWpChljPFyALeNH811Y095aBO2WX2e cUNT4jU2YNysV7XkREz7oY1PF5TZW9KzzAIoZW8a 3gO6H2H- END CERTIFICATE REQUEST	• • • •
Certificate Temp	late:	
	Web Server	
Additional Attrib	ites:	
Attributes:		
	Submit >	

Passaggio 10. Dopo la verifica, è possibile scegliere *Scarica certificato*.

Certificate Issued

The certificate you requested was issued to you.

O DER encoded	or	Base 64 encoded
Download certification Download certification	ate ate	chain

Passaggio 11. Fare clic sul pulsante di opzione per salvare il file e fare clic su OK.

Opening openvpn_client_tmpl.ovpn
You have chosen to open:
n openvpn_client_tmpLovpn
which is: ovpn File (5.3 KB)
from: blob:
What should Firefox do with this file?
O Qpen with Browse
💽 ave File
Do this automatically for files like this from now on.

(NK)	Cancel

Passaggio 12. Una volta salvato, selezionare il pulsante di opzione per il certificato e fare clic sull'icona **freccia giù**.

Import Certificate	Generate CSR/Certificate	Show Built-in 3rd-Party CA Certificates

Passaggio 13. Verrà visualizzata questa schermata. Seleziona Sfoglia....

Import Signed-Certificate

Type: Lo	ocal Certificate			
Certificate Name:				
Upload Certific	ate file			
 Import from PC 				
Browse	to file is selected	R		
 Import from USB 	0			
Browse	lo file is selected			
			Upload	Cancel

Passaggio 14. Scegliere il file del certificato e fare clic su Apri.

×

File Upload					2
← → ~ ↑ 💶 > Th	is PC > Desktop	~ č	Search Desktop		P
Organize 🔻 New folde	r .		8	= • 🔳	0
Desktop ^	Name	Date modified	Туре	Size	
Pole Position	export-7e49e72b-80c8-4d2c-9a83-7448f6	8/27/2018 12:09 PM	Microsoft Excel C	16 KB	
	😚 GNS3	10/31/2017 9:01 AM	Shortcut	2 KB	
oneDrive	insurance.txt	8/24/2018 12:28 PM	Text Document	1 KB	
This PC	messages2.txt	9/6/2018 11:51 AM	Text Document	209 KB	
> Desktop	messages3.txt	9/6/2018 11:56 AM	Text Document	225 KB	
Documents	😥 NetSpot	3/30/2017 2:53 PM	Application Refere	1 KB	
Downloads	Router and Wireless Topics-RMHadsx	9/11/2018 3:48 PM	Microsoft Excel W	15 KB	
b Maxia	SolarWinds-TFTP-Server.zip	8/31/2018 3:03 PM	Compressed (zipp	1,416 KB	
> J Music	😰 Switch_Tesla-Tombaugh-Option82-MRv	8/29/2018 1:36 PM	Microsoft PowerP	1,891 KB	
Pictures	Tftpd32	8/31/2018 3:01 PM	Shortcut	2 KB	
> 📓 Videos	Tftpd64	9/10/2018 8:28 AM	Shortcut	2 KB	
> 🏥 OS (C:)	MhatsAnn	8/31/2017 8:48 AM	Shortcut	3 KB	
	AnthonyRouter.cer	9/18/2018 2:01 PM	Security Certificate	3 KB	
File n	ame		 All Files (*.*) 		~
			Com	Cancel	

Passaggio 15. Immettere il nome del certificato da importare e fare clic su Carica.

Import Si	igned-Certificate	ж
Туре:	Local Certificate	
Certificate Na	ime: AnthonyRouterimport	
Upload Ce	ertificate file	
 Import from 	n PC	
Browse	AnthonyRouter.cer	
O Import from	n USB 🔁	
Browse	. No file is selected	
	Upload	Cancel
Passaggio 1	6. L'importazione del certificato verrà notificata. Fare clic	su OK .
Inform	nation	×
🚯 Impo	ort certificate successfully!	
		ок

Passaggio 17. Passare a Amministrazione > Certificato. Il certificato è stato caricato.

Nota: In questo esempio è stato utilizzato un server dei certificati locale.

		0	-1 1-1 1- CISCO	RV260-PnPDemo				cisco(admin)	English	0	0	œ
	Getting Started	Car	ificate									
6	Status and Statistics	Cen	uncate									
	Administration	Cert	sificate Tab	sie								~
	File Management											
	Reboot		Index	Certificate	Used by	Туре	Signed By	Duration	Details	Action		_
	Diagnostic	0	1	Default	-	Local Certificate		From 2018-Sep-17, 00:00:00 To 2048-Sep-09, 00:00:00		*		
(Certificate 2	0	2	CertTest_CA	-	CA Certificate	Self-Signed	From 2018-Apr-04, 00:00:00 To 2023-Apr-04, 00:00:00		21	8	
	Configuration Management	•	3	Certimport	NETCONF WebServer	Local Gertificate	CiscoTest-OC1- CA	From 2018-Aug-03, 00:00:00 To 2020-Aug-02, 00:00:00	•	1	8	
٠	System Configuration	G		Anthony Gradestrand		Local Cartificate	CircoTest-OC1	From 2018-Sep-18, 00:00:00	-			۱.
0	WAN	Č		A set of plan input		total Corricate	¢	To 2020-Sep-17, 00:00:00		_	<u> </u>)
4	LAN											
	Routing	Impo	rt Certifica	Generate CSR/	Certificate	Show built-in 3rd part	y CA Certificates	Select as Primary Certificat				
	Firewall											

Passaggio 18. Passare a VPN > OpenVPN. Viene visualizzata la pagina OpenVPN. Completare le informazioni seguenti.

<u> </u>	Administration		:0W/-RV260		cisco(admin) English v	0	
۵	System Configuration	CISCO (1720			0000(441111	, Linglion	•	
۲	WAN	OpenVPN				5 Apply		Cancel
*	LAN	opontri						
Ş	Wireless	Enable: 3	R					
×	Routing	Interface:	All	~				
	Firewall	CA Certificate:	A_Trust_nQual_03	~				
Ţ	VPN 1	Server Certificate: 4		~				
	VPN Setup Wizard	Olicet Authoritications	Password Only					
►	IPSec VPN	Client Authentication.						
	OpenVPN 2	Client Address Pool:	10.1.4.0	Netmask: 2	255.255.255.0			
	PPTP Server	Protocol:	UDP	✓ Port: 1	1194			
	GRE Tunnel	Encryption:	AES-256	~				
	VPN Passthrough	Tunnel Mode:	O Full Tunnel, routing all client traffic	through VPN				
	Resource Allocation		• Split Tunnel, routing client traffic d	estined to the following su	bnets through VPN			

- Selezionare la casella Attiva. Selezionare l'interfaccia che verrà consentita nel traffico. In questo caso, una rete WAN (Wide Area Network) e selezionare un certificato CA (Certification Authority)
- Selezionare il certificato CA dal menu a discesa
- Selezionare il certificato server scaricato dal menu a discesa
- Selezionare *Autenticazione client*. Se si seleziona Password, è necessario eseguire l'autenticazione con una password. Se si seleziona Password + Certificato, anche il client deve disporre di un certificato. Ciò è più sicuro, ma aumenta il costo della VPN in quanto dovrebbe acquistare una CA separata.
- Immettere il *pool di indirizzi client*. Scegliere un indirizzo IP in una subnet di rete che non venga utilizzato in altre posizioni della società. È possibile selezionare un intervallo tra quelli riservati e scegliere un intervallo non utilizzato altrove.
- Scegliere il tipo di *crittografia*. Assicurarsi che la crittografia sia la stessa del client. DES e 3DES non sono consigliati e devono essere utilizzati solo per compatibilità con le versioni precedenti.
- Scegliere *Modalità tunnel completo* se si desidera che tutto il traffico del client passi attraverso la VPN o il tunnel diviso se si desidera solo specificare il traffico che attraversa la VPN
- L'indirizzo IP *DNS1* potrebbe essere un server DNS interno dedicato, lo stesso indirizzo IP del gateway predefinito fornito dal provider di servizi Internet (ISP), in una macchina virtuale o un server DNS trusted in Internet.

Fare clic su Apply (Applica) per salvare la configurazione.

Passaggio 19 (opzione 1). È possibile inviare questa configurazione per e-mail al client. Selezionare la casella *Send Email*. Immettere un indirizzo di posta elettronica. Aggiungere un titolo Oggetto per l'e-mail. Fare clic su **Genera**.

Export setting:		
Include client certificate:	AnthonyRouterImport	
Please choose the method you w	ant to export:	
1 Export client configuration t	emplate (.ovpn)	
Send Email Click here to c	configure Email settings.	2
Email client configuration temp (multiple email addresses sepa	nick@cisco.com	
Email Subject:		OpenVPN Client Config
Generate 4		

Passaggio 20. (Opzione 2). Selezionare *Esporta modello di configurazione client (.ovpn)* e fare clic su **Genera**.

Export setting:	
Include client certificate:	
Please choose the method you want to export:	
1 Export client configuration template (.ovpn)	
Send Email Click here to configure Email settings.	
Email client configuration template (.ovpn) to recipients (multiple email addresses separated by comma):	input email address
Email Subject: Generate	OpenVPN Client Configurat

Passaggio 21. Si riceverà conferma dell'esito positivo. Fare clic su OK.

Passaggio 23. Nella parte inferiore destra del desktop e fare clic per aprire OpenVPN. Fare clic con il pulsante destro del mouse per aprire il menu a discesa. Fare clic su *Importa file*.

Passaggio 24. Selezionare il file OpenVPN che termina con .ovpn.

📙 🔄 🔜 🗢 260W				
File Home Share V	fiew			
Pin to Quick Copy Paste Cop access Cipboard	t py path ste shortcut to	New folder	tem * Properties	Open - Select all Get History History Select Select
$\leftarrow \rightarrow \circ \uparrow \square \rightarrow$ This PC	> OS (C:) > Users > arenli > Desktop >	config > 260W		
👃 Downloads 🖈 ^ Nat	me	Date modified	Туре	Size
🔤 Pictures 💉 🎧	openvpn_client_trypl.ovpn	9/11/2018 2:44 PM	OpenVPN Config	6 KB
3534	RV260.aml	8/16/2018 8:08 AM	XML Document	117 KB
Desktop 📑	RV260W.xml	8/15/2018 9:36 AM	XML Document	118 KB
marketing	RV260W_syslog_2018-08-21_09-59-23.log	8/21/2018 10:59 AM	Text Document	3 KB
Pole Position	Tftpd32-4.62-setup.exe	8/31/2018 2:50 PM	Application	543 KB
ConeDrive This PC Desktop Cournents Documents Music Divide	Tftpd64-4.62-setup.exe	8/31/2018 2:51 PM	Application	564 KB
Videor				
S OS (C)				

Passaggio 25. Fare clic sul pulsante di opzione Salva file e fare clic su OK.

Opening openvpn_client_tmpl.ovpn	×
You have chosen to open:	
<pre> openvpn_client_tmpLovpn </pre>	
which is: ovpn File (5.3 KB) from: blob:	
What should Firefox do with this file?	
O Open with Browse	
💽 ave File]
Do this automatically for files like this from now on.	
Cance	:

Passaggio 26. Se si sceglie di modificare il nome del file, lasciare *.ovpn* alla fine del nome del file. Fare clic su **Salva**.

Passaggio 27. Passare a **Stato e statistiche > Stato VPN**. È possibile scorrere verso il basso per ottenere informazioni più dettagliate.

\odot	Getting Started										
	Status and Statistics	System Sun	System Summary								
	System Summary	IPv4 IPv	6								
	TCP/IP Services		WAN (Copper)		usa						
	Port Traffic	IP Address:	210.1.100.20/24								
	WAN QoS Statistics	Default Gateway:	210.1.100.1								
	Switch QoS Statistics	DNS:	210.1.100.1								
	Connected Devices	Dynamic DNS:	Disabled		Disabled						
	Routing Table		Release Ren	iew .	(No Attached)						
	DHCP Bindings										
	Mobile Network										
		VPN Status									
	VPN Status										
L	VPN Status 2	Туре		Active	Configured		Max Supported	Connected			
ل چ	VPN Status View Logs Administration	Type IPSec		Active	Configured		Max Supported	Connected			
ل چ	VPN Status View Logs Administration System Configuration	Type IPSec PPTP		Active Disabled Disabled	Configured 0		Max Supported 20 20	Connected 0			
_ ≌ ∘ ∘	VPN Status 2 View Logs Administration System Configuration WAN	Type IPSec PPTP OpenVPN		Active Disabled Disabled Enabled	Configured 0 1		Max Supported 20 20 20	Connected 0 0			
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	VPN Status 2 View Logs Administration System Configuration WAN LAN	Type IPSec PPTP OpenVPN		Active Disabled Disabled Enabled	Configured 0 1 1		Max Supported 20 20	Connected 0 0 0	3		
5 0 0 E	VPN Status 2 View Logs Administration System Configuration WAN LAN Routing	Type PSec PPTP Oper/VPN Eirouvall Sattlin	og Status	Active Disabled Disabled Enabled	Configured 0 1 1	Los Catting	Max Supported 20 20 20	Connected 0 0	3		
	VPN Status 2 View Logs Administration System Configuration WAN LAN Routing Firewall	Type PSec PPTP OpenVPN Firewall Settin	ng Status	Active Disabled Disabled Enabled	Configured 0 1 1	Log Setting	Max Supported 20 20 20 Status	Connected 0 0 0	3		
	VPN Status 2 View Logs Administration System Configuration WAN LAN Routing Firewall VPN	Type IPSec PPTP OpenVPN Firewall Settin SPI (Stateful Packet)	ng Status	Active Disabled Enabled	Configured 0 1 1	Log Setting : Sysiog Server:	Max Supported 20 20 20 Status	Connected 0 0	3		
	VPN Status 2 View Logs Administration System Configuration WAN LAN Routing Firewall VPN Security	Type IPSec PPTP OperVPN Firewall Settin SPI (Stateful Packet DoS (Denial of Servio	ng Status Inspection): On Doe): On	Active Disabled Disabled Enabled	Configured 0 1 1	Log Setting : Sysiog Server: Email Log:	Max Supported 20 20 20 Status off	Connected 0 0	3		

Il router è ora configurato con tutti i parametri necessari per supportare una connessione client OpenVPN per la versione di valutazione personale.

Installazione di OpenVPN Client sul computer

Ogni client OpenVPN deve eseguire le seguenti attività come prerequisito:

- Scaricare l'applicazione OpenVPN sul dispositivo.
- Aprire e salvare il file di configurazione inviato nei passaggi 19-22 della sezione precedente. Il file di configurazione termina in *.ovpn*.

Nota: Questa installazione è specifica per Windows 10.

Passaggio 1. Passare all'icona a forma di freccia nella parte inferiore destra del desktop e fare clic per aprire l'icona OpenVPN. Fare clic con il pulsante destro del mouse e selezionare *Importa file*.

Nota: L'icona è in bianco e nero, a indicare che non è in esecuzione. Una volta eseguita, l'icona viene visualizzata a colori.

Passaggio 2. Fare clic sulla *freccia su*. Fare clic sull'icona OpenVPN. Fare clic con il pulsante destro del mouse e selezionare *Connetti* dal menu a discesa.

Disconnect				
Keconnect				
Show Status	_			
View Log		1	~	
Edit Config			-	
Clear Saved Passwords		WK.	es.	E
Import file				
Settings	2	5	0	C
Exit	C			
2	고르기	8		

Passaggio 3. Inserire il nome utente e la password.

OpenVPN Connection (openvpn_client_tmpl)	- E	a x
Current State: Connecting		
Fit Aug 10 13:31:20 2018 OpenVPN 2.4.6 x86_64-w64-mingw32 [SSL (OpenSSL)] [LZD] Fit Aug 10 13:31:20 2018 Windows version 6.2 (Windows 8 or greater) 64bt Fit Aug 10 13:31:20 2018 Ibrary versions: OpenSSL 1.1.0h 27 Mar 2018, LZO 2, 10	(LZ4) (PKCS	311] (AEAI
openvpn_client_tmpl ×		
Usemame: Cisco		
Password:		
Save password		
OK Cancel		
<		>
OpenVPN G	GUI 11.10.0	.0/2.4.6
Disconnect Reconnect	Hid	-

Passaggio 4. La finestra mostrerà la connessione OpenVPN con alcuni dati di log.

🤠 Ope	nVPN Connection	(openvpn_client_tmp	l)	_		×
Curren	t State: Connecting					
Fri Au Fri Au	g 10 13:31:20 2018 C a 10 13:31:20 2018 V)penVPN 2.4.6 x86_64 Vindowa version 6.2 (Vi	w64-mingw32 (SSL (Open5 Indows 8 or greater) 64bit	SSL)] (LZO) (LZ4	[] [PKCS11] [/	EAI
Fri Au	g 10 13:31:20 2018 li	brary versions: Open SS	L 1.1.0h 27 Mar 2018, LZC	0.2.10		
Fri Au	g 10 13:31:40 2018 v a 10 13:31:40 2018 1	VAHNING: No server o CP/UDP: Preserving re	entricate vertication method cently used remote address	t has been enab s: IAF INETT192	led. See http 2.168.1.118:1	⊜76i 194
Fri Au	g 10 13:31:40 2018 U	IDP link local: (not bour	id)			
Fri Au	g 10 13:31:40 2018 (o 10 13:31:40 2018)	IDP link remote: [AF_IN VARNING: this configu	ET[192.168.1.118.1194 ation may carba passworth	e in mamony	e the arithme	
Fri Au	g 10 13:31:40 2018	AnthonyLab] Peer Conn	ection Initiated with [AF_IN	ET]192.168.1.1	18:1194	-uceu
Fri Au	g 10 13:31:42 2018 d	pen_tun				
Fri Au	g 10 13:31:42 2018 1	AP-WIN32 device [Eth	emet 3] opened: \\\\Global	NCD0193D1-8	586-4568-82/	G-F
Fri Au	g 10 13:31:42 2018 S	et TAP-Windows TUN	subnet mode network/loca	Unetmask = 10.	1.4.0/10.1.4.3	3/25
I'm Au	g 10 13:31:42 2018 f 10 13:31:42 2018 f	lothed TAP-Windows d	river to set a DHLP IP/netr	nask of 10.1.4.2	/ 255.255.255	NU OL
Fit Au	g 10 13(31)42 2018 3 - 10 13(31)42 2018 3	Nuccessful AHIP Hush o	n interface (21) (CD0193D1	-5556-4555-62	A0-544181AC	SET.
HI AU	g 10 15:51:42 2016 c	o_rcoring, tt->aid_rcor	ng_ipv6_setup=0			
<						>
		>				
Bytes	in: 0 8 out: 14 8			OpenVPN GUI	11,10.0.0/2.4	6
	Disconnect	Reconnect			Hide	

Passaggio 5. Un registro eventi di sistema deve segnalare che è presente una connessione.

Passaggio 6. Il client VPN deve essere in grado di eseguire il tunnel delle informazioni in entrata e in uscita tramite OpenVPN. È possibile impostare la connessione automatica nelle impostazioni OpenVPN.

Passaggio 7. L'amministratore può confermare lo stato della VPN passando a **Stato e statistiche > Stato VPN** sul router.

\odot	Getting Started Deptops Suppose										
6	Status and Statistics	System Summary									
	System Summery	IPv4 IP	v6								
	TCP/IP Services		WAN (Copper)		USB						
	Port Traffic	IP Address:	210.1.100.20/24								
	WAN QoS Statistics	Default Gateway	210.1.100.1								
	Switch QoS Statistics	DNS:	210.1.100.1								
	Connected Devices	Dynamic DNS:	Disabled		Disabled						
	Routing Table		Release Re	inew	(No Attached)						
	DHCP Bindings										
	Mobile Network										
ſ	VPN Status	VPN Status									
<u>ر</u>	View Logs	Type		Active	Config	ured	Max Supported	Connected			
쓭	Administration	IPSec		Disabled	0		20	0			
٠	System Configuration	PPTP		Disabled	1		20	0			
0	WAN	Oper/VPN		Enabled	1		20	0	2		
<u>۴</u>	LAN										
8	Routing	Firmul Online Online									
	Firewall	Firewall Setting Status Log Setting Status									
•	LIDNI	SPI (Stateful Packet	Inspection): On			Syslog Server:	Off				
	VPTN										
•	Security	DoS (Denial of Serv	ice): On			Email Log:	Off				

Conclusioni

A questo punto, OpenVPN dovrebbe essere installato correttamente sul router RV160 o RV260 e sul sito del client VPN.

Per le discussioni della community su OpenVPN, fare clic <u>qui</u> ed eseguire una ricerca di OpenVPN.

Qui è disponibile un video relativo a questo articolo...

Fare clic qui per visualizzare altre Tech Talks di Cisco