

Configurazione VPN di base sul router VPN CVR100W

Obiettivo

Una rete privata virtuale (VPN) viene utilizzata per connettere gli endpoint di diverse reti tramite una rete pubblica, ad esempio Internet. Questa funzionalità è utile per consentire agli utenti remoti che non sono connessi a una rete locale di connettersi in modo sicuro alla rete tramite Internet.

Questo articolo spiega come configurare la VPN di base sul router VPN CVR100W. Per la configurazione VPN avanzata, fare riferimento all'articolo [Advanced VPN Setup sul CVR100W VPN Router](#).

Nota: Verificare che le impostazioni seguenti siano configurate su entrambi i lati del tunnel VPN.

Dispositivo applicabile

- CVR100W VPN Router

Versione del software

- 1.0.1.19

Configurazione VPN di base

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **VPN > Configurazione VPN di base**. Viene visualizzata la pagina *Configurazione VPN di base*:

Basic VPN Setup

About Basic VPN Setup

The basic VPN setup sets most parameters to defaults as proposed by the VPN Consortium (VPNC), and assumes a Pre-shared Key, which greatly simplifies setup. After creating the policies through the Basic VPN Setup, you can always update the parameters through the Policies menu

[View Default Settings](#)

Policy Name and Remote IP Type

Policy Name:

Pre-Shared Key:

Endpoint Information

Remote Endpoint:

Remote WAN (Internet) IP Address: (Hint: 1.2.3.4 or abc.com)

Redundancy Endpoint: Enable

Redundancy WAN (Internet) IP Address: (Hint: 1.2.3.4 or abc.com)

Local WAN (Internet) IP Address:

Secure Connection Remote Accessibility

Remote LAN (Local Network) IP Address: (Hint: 1.2.3.4)

Remote LAN (Local Network) Subnet Mask: (Hint: 255.255.255.0)

Local LAN (Local Network) IP Address: (Hint: 1.2.3.4)

Local LAN (Local Network) Subnet Mask: (Hint: 255.255.255.0)

[Save](#)

[Cancel](#)

[Back](#)

Basic VPN Setup

Basic VPN Setup Default Values for IKE

Exchange Mode: Main
Local WAN (Internet) ID: Local WAN (Internet) IP Address
Remote WAN (Internet) ID: Remote WAN (Internet) IP Address
Encryption Algorithm: AES-128
Authentication Algorithm: SHA-1
Authentication Method: Pre-Shared Key
Diffie-Hellman (DH) Group: Group2 (1024 bit)
SA-Lifetime: 8 Hours

Basic VPN Setup Default Values for VPN

Encryption Algorithm: AES-128
Integrity Algorithm: SHA-1
SA-Lifetime: 1 Hours
PFS Key Group: DH-Group 2(1024 bit)

[Back](#)

Passaggio 2. (Facoltativo) Per visualizzare le impostazioni di base predefinite del tunnel VPN, fare clic su **Visualizza impostazioni predefinite**.

About Basic VPN Setup

The basic VPN setup sets most parameters to defaults as proposed by the VPN Consortium (VPNC), and assumes a Pre-shared Key, which greatly simplifies setup. After creating the policies through the Basic VPN Setup, you can always update the parameters through the Policies menu

[View Default Settings](#)

Policy Name and Remote IP Type

Policy Name:

Pre-Shared Key:

Passaggio 3. Nel campo Nome criterio, inserire un nome per il criterio. Questo nome viene utilizzato a scopo di gestione.

Passaggio 4. Nel campo Chiave già condivisa, immettere una password. La chiave precondivisa viene utilizzata dal client VPN o dal gateway remoto per stabilire una connessione VPN. La chiave deve avere una lunghezza di almeno 8 caratteri.

Endpoint Information

Remote Endpoint: (dropdown)

Remote WAN (Internet) IP Address: (Hint: 1.2.3.4 or abc.com)

Redundancy Endpoint: (dropdown) Enable

Redundancy WAN (Internet) IP Address: (Hint: 1.2.3.4 or abc.com)

Local WAN (Internet) IP Address:

Passaggio 5. Dall'elenco a discesa Remote Endpoint, scegliere il tipo di indirizzo appropriato per l'endpoint remoto.

- Indirizzo IP: questa opzione utilizza un indirizzo IP per identificare l'endpoint remoto.
- FQDN (Fully Qualified Domain Name) - Questa opzione utilizza un nome di dominio per identificare l'endpoint remoto.

Passaggio 6. Nel campo Indirizzo IP WAN remota (Internet), immettere l'indirizzo IP o il nome di dominio dell'endpoint remoto.

Passaggio 7. (Facoltativo) Per abilitare l'endpoint di ridondanza, selezionare la casella di controllo **Abilita** nel campo Endpoint ridondanza. L'opzione Endpoint di ridondanza consente al router VPN CVR100W di connettersi a un endpoint VPN di backup quando la connessione VPN primaria non riesce.

Passaggio 8. (Facoltativo) Per scegliere il tipo di indirizzo per l'endpoint di ridondanza, dall'elenco a discesa Endpoint di ridondanza, scegliere il tipo di indirizzo appropriato.

- Indirizzo IP: questa opzione utilizza un indirizzo IP per identificare l'endpoint di ridondanza.
- FQDN (Fully Qualified Domain Name) - Questa opzione utilizza un nome di dominio per identificare l'endpoint di ridondanza.

Passaggio 9. Immettere l'indirizzo IP o il nome di dominio dell'endpoint di ridondanza nel campo Indirizzo IP WAN (Internet) di ridondanza.

Nota: Il campo Indirizzo IP WAN locale (Internet) è inattivo. Per modificare l'indirizzo IP della WAN locale, consultare l'articolo [Internet Setup sul router VPN CVR100W](#).

Secure Connection Remote Accessibility		
Remote LAN (Local Network) IP Address:	<input type="text" value="10.1.1.5"/>	(Hint: 1.2.3.4)
Remote LAN (Local Network) Subnet Mask:	<input type="text" value="255.0.0.0"/>	(Hint: 255.255.255.0)
Local LAN (Local Network) IP Address:	<input type="text" value="192.168.1.55"/>	(Hint: 1.2.3.4)
Local LAN (Local Network) Subnet Mask:	<input type="text" value="255.255.255.0"/>	(Hint: 255.255.255.0)

Passaggio 10. Nel campo Indirizzo IP LAN remota (rete locale), immettere l'indirizzo IP remoto della LAN remota.

Passaggio 11. Nel campo Subnet mask LAN remota (rete locale), immettere la subnet mask remota della LAN remota.

Passaggio 12. Nel campo Indirizzo IP LAN locale (rete locale), immettere l'indirizzo IP locale della LAN locale.

Passaggio 13. Nel campo Subnet mask LAN locale (rete locale), immettere la subnet mask locale della LAN locale.

Nota: Per evitare conflitti, la LAN locale e la LAN remota devono trovarsi in subnet diverse.

Passaggio 14. Fare clic su **Save** per applicare le impostazioni.