

Basis VPN-instellingen op de CVR100W VPN-router

Doel

Een Virtual Private Network (VPN) wordt gebruikt om endpoints op verschillende netwerken onderling te verbinden via een openbaar netwerk, zoals internet. Deze optie is handig om externe gebruikers die niet op een lokaal netwerk zijn aangesloten, in staat te stellen zich veilig aan te sluiten op het netwerk via het internet.

Dit artikel legt uit hoe u basisVPN op de CVR100W VPN-router kunt configureren. Raadpleeg voor geavanceerde VPN-instellingen het artikel [Advanced VPN-instelling op de CVR100W VPN-router](#).

Opmerking: Zorg ervoor dat de volgende instellingen aan beide zijden van de VPN-tunnel zijn geconfigureerd.

Toepassbaar apparaat

- CVR100W VPN-router

Softwareversie

- 1.0.1.19

Configuratie van basis VPN-instellingen

Stap 1. Meld u aan bij het hulpprogramma voor webconfiguratie en kies **VPN > Basic VPN Setup**. De pagina *Basis VPN Setup* opent:

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](#)

Stap 2. (Optioneel) Klik op **Standaardinstellingen bekijken** om de standaardinstellingen van de VPN-tunnel te bekijken.

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:

Stap 3. Voer in het veld beleidsnaam een naam voor het beleid in. Deze naam wordt gebruikt voor beheerdoeleinden.

Stap 4. Voer in het veld Vooraf gedeelde sleutel een wachtwoord in. De pre-gedeelde sleutel wordt gebruikt door de VPN client of verre gateway om een VPN-verbinding op te zetten. De toets moet minimaal 8 tekens lang zijn.

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:

Stap 5. Kies in de vervolgkeuzelijst Remote Endpoint het juiste adrestype voor het elders geplaatste eindpunt.

- IP-adres - Deze optie gebruikt een IP-adres om het externe eindpunt te identificeren.
- FQDN (Full Qualified Domain Name) - Deze optie gebruikt een domeinnaam om het afstandseindpunt te identificeren.

Stap 6. In het veld Remote WAN (Internet) IP-adres voert u het IP-adres of de domeinnaam van het externe eindpunt in.

Stap 7. (optioneel) Controleer het vakje Redundantie-endpoints in het veld Redundantie om redundantie in te schakelen. De optie redundantie-eindpunt stelt de CVR100W VPN-router in om verbinding te maken met een back-opeindpunt wanneer de primaire VPN-verbinding faalt.

Stap 8. (Optioneel) Kies het type adres voor het redundantie-eindpunt in de vervolgkeuzelijst Redundancy Endpoint en kies het juiste type adres.

- IP-adres - Deze optie gebruikt een IP-adres om het redundantie-eindpunt te identificeren.
- FQDN (Full Qualified Domain Name) - Deze optie gebruikt een domeinnaam om het redundantie-eindpunt te identificeren.

Stap 9. Voer het IP-adres of de domeinnaam van het redundantie-eindpunt in het veld IP-adres van Redundantie WAN (Internet) in.

Opmerking: Het veld Local WAN (Internet) IP-adres wordt gedimd. Wilt u het lokale WAN IP-adres bewerken, dan raadpleegt u het artikel [Internet Setup op de CVR100W VPN-router](#).

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)

Stap 10. Voer in het veld Remote LAN (Local Network) IP-adres in het externe IP-adres van het externe LAN.

Stap 1. Voer in het veld Subnetmasker van Remote LAN (Local Network) het elders geplaatste LAN-masker in.

Stap 12. Voer in het veld Local LAN (Local Network) IP Address in het lokale IP-adres van het lokale LAN.

Stap 13. In het veld Subnetmasker van Local LAN (Local Network) voert u het lokale subnetmasker van het lokale LAN in.

Opmerking: LAN en de afstandsbediening moeten in verschillende subnetwerken zijn om conflicten te voorkomen.

Stap 14. Klik op **Save** om de instellingen toe te passen.