Gebruik Shrew Soft VPN-client om verbinding te maken met IPSec VPN Server op RV130 en RV130W

Doel

Met IPSec VPN (Virtual Private Network) kunt u veilig externe bronnen verkrijgen door een versleutelde tunnel over het internet te maken.

De RV130 en RV130W werken als IPSec VPN servers en ondersteunen de Shrew Soft VPN client.

Zorg ervoor dat u de nieuwste release van de clientsoftware downloadt.

·Shrew Soft (https://www.shrew.net/download/vpn)

Opmerking: Om de Shrew Soft VPN-client met succes te kunnen configureren met een IPSec VPN-server, moet u eerst de IPSec VPN-server configureren. Raadpleeg het artikel *Configuration of a IPSec VPN Server op RV130 en RV130W voor informatie over het* uitvoeren <u>van</u> dit <u>programma</u>.

Het doel van dit document is om u te tonen hoe u de Shrew Soft VPN-client kunt gebruiken om verbinding te maken met een IPSec VPN-server op de RV130 en RV130W.

Toepasselijke apparaten

·RV130W Wireless-N VPN-firewall

·RV130 VPN-firewall

Systeemvereisten

·32- of 64-bits systemen

·Windows 2000, XP, Vista of Windows 7/8

Topologie

Hieronder wordt een topologie op topniveau getoond waarin de apparaten worden geïllustreerd die betrokken zijn bij de configuratie van een Shrewsoft-client naar een locatie.



Een gedetailleerder stroomschema dat de rol van DNS-servers in een netwerkomgeving

voor kleine bedrijven illustreert, wordt hieronder getoond.



Softwareversie

•1.0.1.3

Shrew zachte VPN-client instellen

Configuratie van IPSec VPN en gebruikersconfiguratie

Stap 1. Meld u aan bij het hulpprogramma voor webconfiguratie en kies **VPN > IPSec VPN Server > Setup**. De pagina *Instellen* wordt geopend.

Setup		
Server Enable:		
NAT Traversal:	Disabled Edit	
Phase 1 Configuration		
Pre-Shared Key:	Testkey	1
Exchange Mode:	Main 👻	
Encryption Algorithm:	DES 👻	
Authentication Algorithm:	MD5 👻	
DH Group:	Group1 (768 bit) 👻	
IKE SA Life Time:	3600	Seconds (Range: 30 - 86400, Default: 3600)
Phase 2 Configuration		
Local IP:	Subnet 👻	
IP Address:	192.168.1.0	(Hint: 1.2.3.4)
Subnet Mask:	255.255.255.0	(Hint: 255.255.255.0)
IPSec SA Lifetime:	28800	Seconds (Range: 30 - 86400, Default: 28800)
Encryption Algorithm:	DES 👻	
Authentication Algorithm:	MD5 👻	
PFS Key Group:	Enable	
DH Group:	Group 1(768 bit) 👻	
Save Cancel		

<u>Stap 2.</u> Controleer dat de IPSec VPN Server voor de RV130 correct is geconfigureerd. Als de IPSec VPN Server niet is geconfigureerd of verkeerd is geconfigureerd, raadpleegt u <u>Configuratie van een IPSec VPN-server op RV130 en RV130W</u> en klikt u op **Opslaan**.

Setun		
Setup		
Configuration setti	ings have been saved successfully	
Server Enable:	\checkmark	
NAT Traversal:	Disabled Edit	
Phase 1 Configuration		
Pre-Shared Key:	Testkey	
Exchange Mode:	Main 👻	
Encryption Algorithm:	DES -	
Authentication Algorithm:	MD5 -	
DH Group:	Group1 (768 bit)	
IKE SA Life Time:	3600 Seconds (Range: 30 - 86400, Default: 3600)	
Phase 2 Configuration		
Local IP:	Subnet 👻	
IP Address:	192.168.1.0 (Hint: 1.2.3.4)	
Subnet Mask:	255.255.255.0 (Hint: 255.255.255.0)	
IPSec SA Lifetime:	28800 Seconds (Range: 30 - 86400, Default: 28800)	
Encryption Algorithm:	DES 🔻	
Authentication Algorithm:	MD5 -	
PFS Key Group:	🖉 Enable	
DH Group:	Group 1(768 bit) -	
Sava Canad		
Save Cancel		

Opmerking: De bovenstaande instellingen zijn een voorbeeld van een RV130/RV130W IPSec VPN-serverconfiguratie. De instellingen zijn gebaseerd op het document, <u>Configuration of an IPSec VPN Server op RV130 en RV130W</u> en worden in de volgende stappen vermeld.

Stap 3. Navigeer naar VPN > IPSec VPN Server > Gebruiker. De User-pagina verschijnt.

User		
Heer Assount Table		
UserName	Password	
No data to display		
Add Row Edit Delete Import		
Save Cancel		

<u>Stap 4.</u> Klik op **Rij toevoegen** om gebruikersaccounts toe te voegen, om de VPN-clients te verifiëren (uitgebreide verificatie) en de gewenste gebruikersnaam en wachtwoord in te voeren in de daarvoor bestemde velden.

User		
You must save before you can edit or delete.		
User Account Table		
UserName	Password	
TestUser		
Add Row Edit Delete Import		
Save Cancel		

Stap 5. Klik op **Opslaan** om de instellingen op te slaan.

VPN-clientconfiguratie

Stap 1. Open Shrew VPN Access Manager en klik op Add om een profiel toe te voegen.



Het venster VPN Site Configuration verschijnt.

VPN Site Configuration
General Client Name Resolution Authenticatic
Remote Host
Host Name or IP Address Port
500
Auto Configuration ike config pull 🔻
Local Host
Adapter Mode
Use a virtual adapter and assigned address 🔹
MTU 👽 Obtain Automatically
1380 Address
Netmask
Save Cancel

Stap 2. Voer in het gedeelte *Remote Host* onder het tabblad *General* de openbare hostnaam of het IP-adres in van het netwerk waarmee u verbinding wilt maken.

VPN Site Configuration
General Client Name Resolution Authenticatic
Remote Host Host Name or IP Address Port
(35 4.086 500)
Auto Configuration ike config pull 🔻
Local Host
Adapter Mode
Use a virtual adapter and assigned address 🛛 🔻
MTU 📝 Obtain Automatically
1380 Address
Netmask
Save Cancel

Opmerking: Zorg ervoor dat het poortnummer is ingesteld op de standaardwaarde van 500. Om VPN te kunnen werken, gebruikt de tunnel UDP-poort 500, die moet worden ingesteld om ISAKMP-verkeer door te kunnen sturen naar de firewall.

Stap 3. Kies uitgeschakeld in de vervolgkeuzelijst Auto Configuration.

VPN Site Configuration		
General Client Name Re	solution Authenticatic	
Remote Host		
Host Name or IP Address	Port	
1311455.8	500	
Auto Configuration	ike config pull 🚽	
- Local Host	ike config pull	
Adapter Mode	ike config push dhcp over ipsec	
Use a virtual adapter and assigned address 🔻		
MTU [Obtain Automatically	
1380 Address		
Netmask		
	Save Cancel	

De beschikbare opties zijn als volgt gedefinieerd:

·Uitgeschakeld — schakelt alle automatische clientconfiguraties uit.

·IKE Config Pull — hiermee kunnen aanvragen van een computer door de client worden ingesteld. Met de ondersteuning van de Pull methode door de computer, geeft het verzoek een lijst met instellingen terug die worden ondersteund door de client.

·IKE Config Push — geeft een computer de mogelijkheid om instellingen aan de client aan te bieden tijdens het configuratieproces. Met ondersteuning van de Push methode door de computer, geeft het verzoek een lijst met instellingen terug die worden ondersteund door de client.

·DHCP over IPSec — geeft de client de mogelijkheid om instellingen aan te vragen bij de computer via DHCP via IPSec.

Stap 4. Kies in het gedeelte *Local Host* een bestaande adapter en huidig adres gebruiken in de vervolgkeuzelijst *Adaptermodus*.

VPN Site Configuration		
General Client Name Resolution Authenticatic		
Remote Host		
Host Name or IP Address Port		
1.F !! 4 FF P 500		
Auto Configuration disabled -		
Local Host		
Adapter Mode		
Use a virtual adapter and assigned address		
Use a virtual adapter and assigned address Use a virtual adapter and random address		
Use an existing adapter and current address		
Netmask		
Save Cancel		

De beschikbare opties zijn als volgt gedefinieerd:

·Gebruik een virtuele adapter en toegewezen adres — hiermee kan de client een virtuele adapter met een opgegeven adres gebruiken als bron voor IPsec-communicatie.

·Gebruik een virtuele adapter en een willekeurig adres. Hiermee kan de client een virtuele adapter met een willekeurig adres gebruiken als bron voor IPsec-communicatie.

·Gebruik een bestaande adapter en huidig adres. Hiermee kan de client alleen de bestaande, fysieke adapter met het huidige adres gebruiken als bron voor IPseccommunicatie.

Stap 5. Klik op het tabblad *Cliënt*. Selecteer in de vervolgkeuzelijst *NAT* Traversal de instelling die u in het artikel <u>*Configuration of a IPSec VPN Server op RV130 en RV130W*</u> hebt ingesteld voor de RV130/RV130W voor NAT Traversal.

VPN Site Configuration		
General Client Name Reso	lution Authenticatic	
Firewall Options		
NAT Traversal	disable 🔻	
NAT Traversal Port	disable enable	
Keep-alive packet rate	force-draft	
IKE Fragmentation	force-cisco-udp	
Maximum packet size	540 Bytes	
Other Options		
Enable Dead Peer Detection		
Enable ISAKMP Failure Notifications		
Enable Client Login Banner		
Save Cancel		

De beschikbare menuopties voor Network Address Translation Transversal (NATT) zijn als volgt gedefinieerd:

·Uitschakelen — De NAT-protocolextensies worden niet gebruikt.

·Inschakelen — De NAT-protocoluitbreidingen worden alleen gebruikt als de VPN-gateway aangeeft dat er tijdens de onderhandelingen ondersteuning is en NAT wordt gedetecteerd.

•Force-Draft — De conceptversie van de NAT-protocoluitbreidingen wordt gebruikt ongeacht of de VPN-gateway aangeeft dat er tijdens de onderhandelingen ondersteuning is verleend of dat NAT is gedetecteerd.

•Force-RFC — De RFC-versie van het NATT-protocol wordt gebruikt ongeacht of de VPNgateway aangeeft dat er tijdens de onderhandelingen ondersteuning is of dat NAT is gedetecteerd.

·Force-Cisco-UDP — Force UDP-insluiting voor VPN-clients zonder NAT.

Stap 6. Klik op het tabblad *Naamresolutie* en controleer het vakje **DNS inschakelen** als u DNS wilt inschakelen. Als er geen specifieke DNS-instellingen vereist zijn voor de configuratie van uw site, schakelt u het selectievakje **DNS inschakelen uit**.

VPN Site Configuration		
Client Name Resolution	Authentication Phase	
DNS Split DNS WI	NS	
CEnable DNS	Obtain Automatically	
Server Address #1		
Server Address #2		
Server Address #3		
Server Address #4		
DNS Suffix	Obtain Automatically	
	Save Cancel	

Stap 7. (Optioneel) Als uw externe gateway is geconfigureerd om de Configuration Exchange te ondersteunen, kan de gateway automatisch DNS-instellingen leveren. Als dit niet het geval is, controleert u of het aanvinkvakje **Automatisch verkrijgen** niet is ingeschakeld en voert u handmatig een geldig DNS-serveradres in.

VPN Site Configuration		
Client Name Resolution A	uthentication Phase	
DNS WINS		
🛛 🖾 Enable DNS 🛛 💿	Obtain Automatically	
Server Address #1		
Server Address #2		
Server Address #3		
Server Address #4		
	Obtain Automatically	
DNS Suffix		
	Save Cancel	

Stap 8. (Optioneel) Klik op het tabblad *Naamresolutie* en controleer het aanvinkvakje **Enable WINS** als u de Windows Internet Name Server (WINS) wilt inschakelen. Als uw externe gateway is geconfigureerd om de Configuration Exchange te ondersteunen, kan de gateway automatisch WINT-instellingen leveren. Als dit niet het geval is, controleer dan of het aanvinkvakje **Automatisch verkrijgen** niet is ingeschakeld en voer handmatig een geldig WINS-serveradres in.

VPN Site Configuration	X
Client Name Resolution	Authentication Phase
DNS Split DNS WI	NS
Enable WINS	Obtain Automatically
Server Address #1	
Server Address #2	
(Save Cancel

Opmerking: Door WINT configuratie informatie te verstrekken, zal een client in staat zijn om WINT namen op te lossen met behulp van een server die zich in het externe privé netwerk bevindt. Dit is handig wanneer u probeert externe Windows-netwerkbronnen te benaderen met behulp van een naam van een Uniform Naming Convention path. De WINS-server zou doorgaans behoren tot een Windows Domain Controller of een Samba Server.

Stap 9. Klik op het tabblad *Verificatie* en selecteer **Mutual PSK + XAuth** in de vervolgkeuzelijst *Verificatiemethode*.

VPN Site Configuration	×
Client Name Resolution	Authentication Phase
Authentication Method Local Identity Remote Identification Type IP Address Address String	Mutual PSK + XAuth Hybrid RSA + XAuth Hybrid GRP + XAuth Mutual RSA + XAuth Mutual PSK + XAuth Mutual PSK
	Save Cancel

De beschikbare opties zijn als volgt gedefinieerd:

·Hybrid RSA + XAuth — De klant credential is niet nodig. De client zal de gateway verifiëren. De referenties worden geleverd in de vorm van PEM- of PKCS12-certificaatbestanden of het type sleutelbestanden.

·Hybrid GRP + XAuth — De clientreferenties zijn niet nodig. De client zal de gateway verifiëren. De referenties worden geleverd in de vorm van een PEM- of PKCS12-certificaatbestand en een gedeelde geheime tekenreeks.

·Wederzijdse RSA + XAuth — client en gateway hebben beide referenties nodig om te verifiëren. De referenties worden geleverd in de vorm van PEM- of PKCS12- certificaatbestanden of sleuteltype.

•Wederzijdse PSK + XAuth — client en gateway hebben beide referenties nodig om te verifiëren. De referenties worden in de vorm van een gedeelde geheime string gegeven.

·Wederzijdse RSA — client en gateway hebben beide referenties nodig om te verifiëren. De referenties worden geleverd in de vorm van PEM- of PKCS12-certificaatbestanden of sleuteltype.

·Wederzijdse PSK — client en gateway hebben beide referenties nodig om te verifiëren. De referenties worden in de vorm van een gedeelde geheime string gegeven.

Stap 10. Klik in het gedeelte *Verificatie* op het subtabblad *Credentials* en voer in het veld *Vooraf gedeelde sleutel* in op de pagina *IPsec VPN Server Setup* in.

VPN Site Configuration
Client Name Resolution Authentication Phase
Authentication Method Mutual PSK + XAuth
Local Identity Remote Identity Credentials
Server Certificate Autority File
Client Cestificate File
Client Private Key File
Pre Shared Key
Save Cancel

Stap 1. Klik op het tabblad *Fase 1*. Configureer de volgende parameters zodat ze dezelfde instellingen hebben als die u voor de RV130/RV130W hebt ingesteld in <u>Stap 2 van het</u> gedeelte <u>*Gebruikersconfiguratie van IPSec VPN Server*</u> in dit document.

VPN Site Configuration	×
Name Resolution Authen	tication Phase 1 Pha
Proposal Parameters	
Exchange Type	main 🔻
DH Exchange	group 1 🔹
Cipher Algorithm	des 🔻
Cipher Key Length	→ Bits
Hash Algorithm	md5 🔹
Key Life Time limit	3600 Secs
Key Life Data limit	0 Kbytes
Enable Check Point Compatible Vendor ID	
	ompatible Vendor ID

De parameters in Shrew Soft moeten als volgt overeenkomen met de RV130/RV130Wconfiguraties in fase 1:

·"Type uitwisseling" moet overeenkomen met "Exchange Mode".

·"DH Exchange" moet overeenkomen met "DH Group".

·De "algoritme voor codering" moet overeenkomen met de "algoritme voor codering".

·"Hash Algorithm" moet overeenkomen met "Verificatiealgoritme".

Stap 12. (Optioneel) Als uw gateway een Cisco-compatibele verkoper-ID aanbiedt tijdens fase1-onderhandelingen, vinkt u het aanvinkvakje **Enable Check Point Compatible Vendor ID aan**. Als de gateway niet, of u bent onzeker, laat de controledoos ongecontroleerd.

VPN Site Configuration	X
Name Resolution Authenti	ication Phase 1 Pha:
Proposal Parameters	
Exchange Type	main 💌
DH Exchange	group 1 👻
Cipher Algorithm	des 💌
Cipher Key Length	T Bits
Hash Algorithm	md5 🔻
Key Life Time limit	3600 Secs
Key Life Data limit	0 Kbytes
Enable Check Point Compatible Vendor ID	
	Save Cancel

Stap 13. Klik op het tabblad *Fase 2*. Configureer de volgende parameters zodat ze dezelfde instellingen hebben als die u voor de RV130/RV130W hebt ingesteld in <u>Stap 2 van het</u> gedeelte <u>Gebruikersconfiguratie van IPSec VPN Server</u> in dit document.

VPN Site Configuration	x
Authentication Phase 1	Phase 2 Policy
Proposal Parameters Transform Algorithm	esp-des 🗸
Transform Key Length	Bits
HMAC Algorithm	md5 🔹
PFS Exchange	group 1 🗸
Compress Algorithm	disabled 🔹
Key Life Time limit	28800 Secs
Key Life Data limit	0 Kbytes
(Save Cancel

De parameters in Shrew Soft moeten als volgt overeenkomen met de RV130/RV130Wconfiguraties in fase 2:

"Transformeer algoritme" moet overeenkomen met "Encryptie algoritme".

"HMAC-algoritme" moet overeenkomen met "Verificatiealgoritme".

·PFS Exchange" moet overeenkomen met "DH Group" als PFS Key Group is ingeschakeld op de RV130/RV130W. Anders selecteert u **uitgeschakeled**.

"Key Life Time limit" moet overeenkomen met "IPSec SA Lifetime".

Stap 14. Klik op het tabblad *Beleid* en selecteer **Vereisen** in de vervolgkeuzelijst *Beleidsgeneratieniveau*. De optie *Policy Generation Level* wijzigt het niveau waarop IPsecbeleid wordt gegenereerd. De verschillende niveaus die in de vervolgkeuzelijst worden verstrekt brengen aan IPSec SA onderhandelingsgedrag in kaart dat door verschillende verkopersimplementaties wordt uitgevoerd.

VPN Site Configuration	
Authentication Phase 1 Phase 2 Policy	
IPSEC Policy Configuration	
Maintain Persistent Security auto	
Obtain Topology Automatics unique shared	
Remote Network Resource	
Add Modify Delete	
Save Cancel	

De beschikbare opties zijn als volgt gedefinieerd:

·Auto — De client bepaalt automatisch het juiste IPSec-beleidsniveau.

•Vereist — De klant zal niet onderhandelen over een unieke Security Association (SA) voor elk beleid. Beleid wordt gegenereerd met behulp van het lokale openbare adres als de lokale beleids-ID en de Remote Network Resources als de externe beleids-ID. Voor het voorstel voor fase 2 worden de beleids-ID's tijdens de onderhandelingen gebruikt.

·Uniek — De klant onderhandelt over een unieke SA voor elk beleid.

•Gedeeld - Beleid wordt gegenereerd op het vereiste niveau. In het voorstel voor fase 2 wordt de lokale beleids-ID gebruikt als lokale ID en Any (0.0.0.0/0) als externe ID tijdens de onderhandeling.

Stap 15. Schakel het aankruisvakje **Automatisch topologie verkrijgen of Alles** tunnelen uit. Deze optie wijzigt de manier waarop het beveiligingsbeleid voor de verbinding is geconfigureerd. Als deze optie wordt uitgeschakeld, moet de handmatige configuratie worden uitgevoerd. Als deze optie is ingeschakeld, wordt de automatische configuratie uitgevoerd.

VPN Site Configuration
Authentication Phase 1 Phase 2 Policy
IPSEC Policy Configuration
Policy Generation Level require 🔻
Maintain Persistent Security Associations
ODbtain Topology Automatically or Tunnel All
Bemote Network Besource
Add Modify Delete
Save Cancel

Stap 16. Klik op **Add** om de Remote Network Resource toe te voegen waarmee u verbinding wilt maken. Externe netwerkresources omvatten externe desktoptoegang, afdelingsresources, netwerkdrives en beveiligde elektronische post.

VPN Site Configuration
Authentication Phase 1 Phase 2 Policy
IPSEC Policy Configuration
Policy Generation Level require 👻
Maintain Persistent Security Associations
Obtain Topology Automatically or Tunnel All
Remote Network Resource
Save Cancel

Het venster Topology Entry verschijnt:

VPN Site Configuration
Authentication Phase 1 Phase 2 Policy IPSEC Policy Configuration Policy Generation Level require Policy Generation Level require Image: Configuration Topology Entry X X Address . . Netmask . . Ok Cancel
Add Modify Delete
Save Cancel

Stap 17. Voer in het veld *Adres* de subnetnummer van de RV130/RV130W in. Het adres moet overeenkomen met het veld *IP-adres* in <u>Stap 2 van de</u> sectie <u>IPSec VPN Server Setup</u> <u>en Gebruikersconfiguratie</u> van dit document.

VPN Site Configuration
Authentication Phase 1 Phase 2 Policy IPSEC Policy Configuration Policy Generation Level require Topology Entry X Type Include Address 192.168.1.0 Netmask . Ok Cancel
Add Modify Delete
Save Cancel

Stap 18. Voer in het veld *Netmasker* het subnetmasker in voor het lokale netwerk van de RV130/RV130W. Het netmasker moet overeenkomen met het veld *Subnet Mask* in <u>Stap 2</u> <u>van de</u> sectie <u>Gebruikersconfiguratie IPSec VPN Server</u> van dit document.

VPN Site Configuration
Authentication Phase 1 Phase 2 Policy IPSEC Policy Configuration Policy Generation Level require Policy Generation Level require Image: Configuration Type Include Image: Configuration Address 192.168.1.0 Netmask Ok Cancel
Add Modify Delete
Save Cancel

Stap 19. Klik op **OK** om de externe netwerkbron toe te voegen.

VPN Site Configuration
Authentication Phase 1 Phase 2 Policy IPSEC Policy Configuration Policy Generation Level require Topology Entry Type Include Address 192.168.1.0 Netmask 255.255.255.0
Add Modify Delete
Save Cancel

Stap 20. Klik op **Opslaan** om uw configuraties op te slaan voor verbinding met de VPN-site.

VPN Site Configu	uration			×
Authentication	Phase 1	Phase 2	Policy	4 >
- IPSEC Policy	, Configura	tion		
Policy Generation Level require 🔹				•
Maintain Persistent Security Associations				ns
Obtain Topology Automatically or Tunnel All				
Remote Network Resource				
↔ 192.1	68.1.0 / 25	5.255.255.	0	
Add	N	4odify 🔡	Del	lete
		_		
		Save		Cancel

Stap 21. Ga terug naar het venster *VPN Access Manager* om de VPN-site te selecteren die u hebt geconfigureerd en klik op de knop **Verbinden**.

(B) VPN Acc	ess Mar	nager		- • ×
File Edit	View	Help		
Connect	C) Add	2 Modify	elete	
ELIHARI PLIMARI	н			
				đ

Het venster VPN Connect verschijnt.

VPN Connect - LIIIIIII
Connect Network
config loaded for site 38 4085
Credentials
Password
Connect Exit

Stap 2. Voer in het gedeelte *Credentials* de gebruikersnaam en het wachtwoord in van de account die u in <u>Stap 4 van het</u> gedeelte <u>*Gebruikersconfiguratie* van de *IPSec VPN-server*</u> van dit document hebt ingesteld.

S VPN Connect - 191114 1114
Connect Network
config loaded for site ' 🖽 🛛 🖬 🖬 🖬 🖬
Credentials
Username TestUser
Password
Connect Exit

Stap 23. Klik op Verbinding maken met VPN in de RV130/RV130W.

VPN Connect - 101114 71 H	J
Connect Network	
config loaded for site " 🖽 🖬 🖬 🖬 🖬	
Credentials	
Username TestUser	
Password •••••	
Connect Exit	

De IPSec VPN-tunnel is tot stand gebracht en de VPN-client heeft toegang tot de bron achter de RV130/RV130W LAN.

🕑 VPN C	onnect - 1311141114
Connect	Network
esp pro client co local id remote i pre-shai bringing	posal configured onfigured configured id configured red key configured up tunnel
Creder	ntials
Userr	name TestUser
Pass	word
	Connect Cancel



Bekijk een video met betrekking tot dit artikel...

Klik hier om andere Tech Talks van Cisco te bekijken

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.