Secure Sockets Layer Virtual Private Network (SSL VPN) configureren op de RV340- of RV345-router

Speciale kennisgeving: Licentiestructuur - Firmwareversies 1.0.3.15 en hoger. Als u doorgaat, brengt AnyConnect alleen kosten in rekening voor clientlicenties.

Voor aanvullende informatie over AnyConnect-licenties op routers uit de RV340-reeks, raadpleegt u het artikel AnyConnect-licenties voor routers uit de RV340-reeks.

Doel

De Secure Sockets Layer Virtual Private Network (SSL VPN) gateway stelt externe gebruikers in staat om een beveiligde VPN-tunnel tot stand te brengen met behulp van een webbrowser. Met deze functie kunt u eenvoudig toegang krijgen tot een breed scala aan webbronnen en webtoepassingen met behulp van native Hypertext Transfer Protocol (HTTP) via SSL Hypertext Transfer Protocol Secure (HTTPS)-browserondersteuning.

SSL VPN stelt gebruikers in staat om op afstand toegang te krijgen tot beperkte netwerken, met behulp van een veilige en geverifieerde route door het netwerkverkeer te versleutelen.

De RV340- en RV345-routers ondersteunen de Cisco AnyConnect VPN-client of ook wel Anyconnect Secure Mobility Client genoemd. Deze routers ondersteunen standaard twee SSL VPN-tunnels en de gebruiker kan een licentie registreren om maximaal 50 tunnels te ondersteunen. Zodra het is geïnstalleerd en geactiveerd, zal de SSL VPN een veilige VPN-tunnel voor externe toegang tot stand brengen.

Dit artikel is bedoeld om u te laten zien hoe u SSL VPN configureert op de RV340 of de RV345-router.

Toepasselijke apparaten

- RV340
- RV345
- Cisco Secure Mobility Client

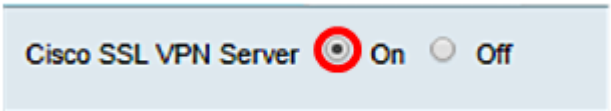
Softwareversie

- 1.0.03.15 — RV340, RV345
- 4.4.01054 — AnyConnect Secure Mobility Client

SSL VPN configureren

Stap 1. Ga naar het webgebaseerde hulpprogramma van de router en kies VPN > SSL VPN.

Stap 2. Klik op de knop Aan om Cisco SSL VPN Server in te schakelen.



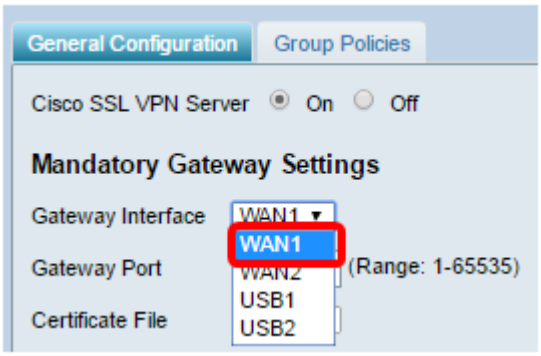
Verplichte gateway-instellingen

De volgende configuratie-instellingen zijn verplicht:

Stap 3. Kies de Gateway Interface in de vervolgkeuzelijst. Dit zal de poort zijn die zal worden gebruikt voor het doorgeven van verkeer door de SSL VPN-tunnels. De opties zijn:

- WAN1
- WAN2

- USB1
- USB2

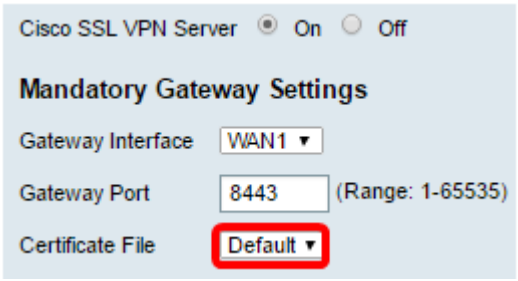


Opmerking: In dit voorbeeld wordt WAN1 gekozen.

Stap 4. Voer het poortnummer in dat wordt gebruikt voor de SSL VPN-gateway in het veld Gateway Port, variërend van 1 tot 65535.

Opmerking: In dit voorbeeld wordt 8443 gebruikt als poortnummer.

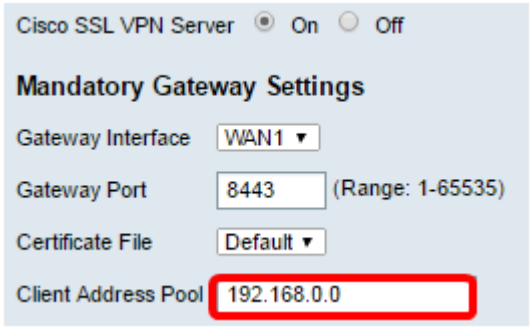
Stap 5. Kies het certificaatbestand in de vervolgkeuzelijst. Dit certificaat verifieert gebruikers die proberen toegang te krijgen tot de netwerkbron via de SSL VPN-tunnels. De vervolgkeuzelijst bevat een standaardcertificaat en de certificaten die worden geïmporteerd.



Opmerking: in dit voorbeeld wordt Standaard gekozen.

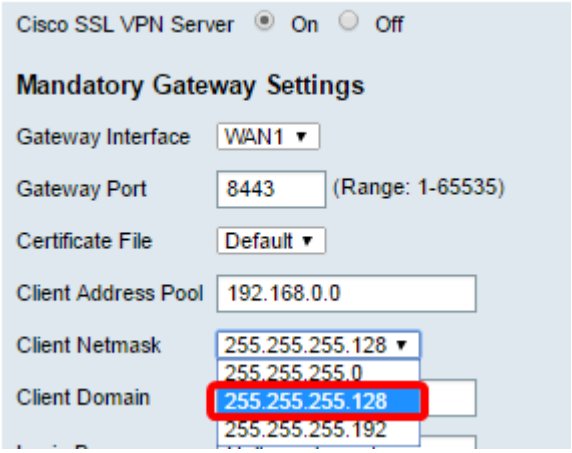
Stap 6. Voer het IP-adres van de adresgroep van de client in het veld Adresgroep client in. Deze pool is het bereik van IP-adressen die worden toegewezen aan externe VPN-clients.

Opmerking: Zorg ervoor dat het IP-adresbereik niet overlapt met een van de IP-adressen in het lokale netwerk.



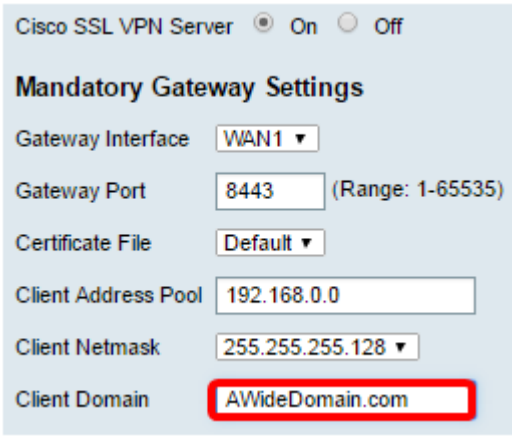
Opmerking: In dit voorbeeld wordt 192.168.0.0 gebruikt.

Stap 7. Kies het Netmasker van de client in de vervolgkeuzelijst.



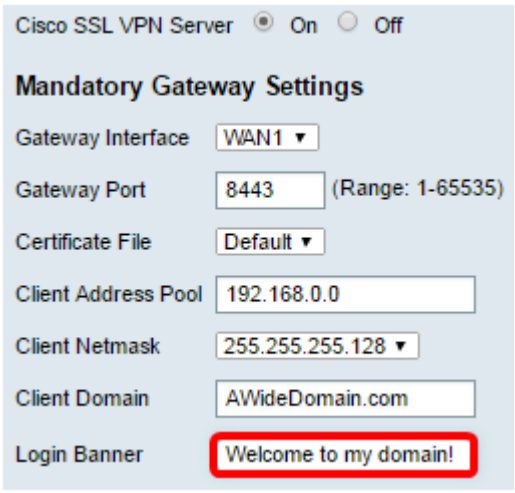
Opmerking: In dit voorbeeld wordt 255.255.255.128 geselecteerd.

Stap 8. Voer de domeinnaam van de client in het veld Client Domain in. Dit zal de domeinnaam zijn die naar SSL VPN-clients moet worden gepusht.



Opmerking: In dit voorbeeld wordt AWideDomain gebruikt als de domeinnaam van de client.

Stap 9. Voer de tekst in die als aanmeldingsbanner wordt weergegeven in het veld Aanmeldingsbanner. Dit is de banner die wordt weergegeven telkens wanneer een klant zich aanmeldt.



Opmerking: In dit voorbeeld wordt Welcome to my domain! gebruikt als de aanmeldingsbanner.

Optionele gateway-instellingen

De volgende configuratie-instellingen zijn optioneel:

Stap 1. Voer in seconden een waarde in voor de time-out voor inactiviteit, variërend van 60 tot 86400. Dit is de tijdsduur dat de SSL VPN-sessie inactief kan blijven.

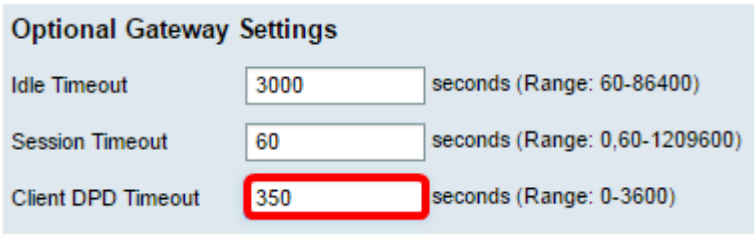
Opmerking: In dit voorbeeld wordt 3000 gebruikt.

Stap 2. Voer een waarde in seconden in het veld Sessietime-out in. Dit is de tijd die nodig is voor de sessie Transmission Control Protocol (TCP) of User Datagram Protocol (UDP) om een time-out te maken na de opgegeven inactieve tijd. Het bereik is van 60 tot 1209600.

Opmerking: In dit voorbeeld wordt 60 gebruikt.

Stap 3. Voer in het veld ClientDPD Timeout een waarde in van 0 tot 3600. Deze waarde specificeert het periodiek verzenden van HELLO/ACK-berichten om de status van de VPN-tunnel te controleren.

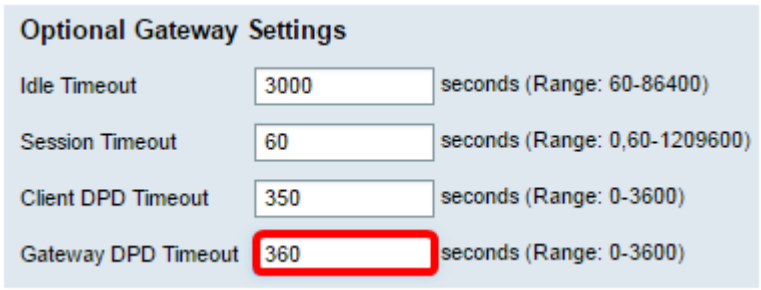
Opmerking: deze functie moet aan beide uiteinden van de VPN-tunnel zijn ingeschakeld.



Opmerking: In dit voorbeeld wordt 350 gebruikt.

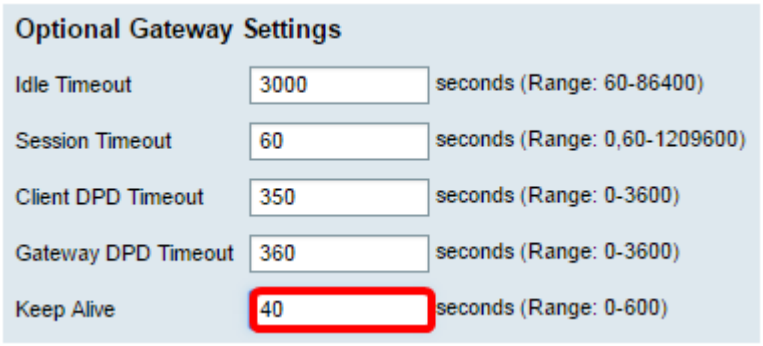
Stap 4. Voer in het veld GatewayDPD Timeout in seconden een waarde in die varieert van 0 tot 3600. Deze waarde specificeert het periodiek verzenden van HELLO/ACK-berichten om de status van de VPN-tunnel te controleren.

Opmerking: deze functie moet aan beide uiteinden van de VPN-tunnel zijn ingeschakeld.



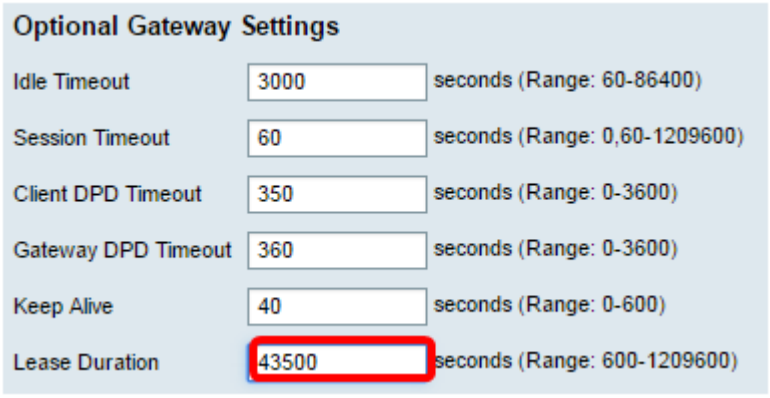
Opmerking: In dit voorbeeld wordt 360 gebruikt.

Stap 5. Voer in seconden een waarde in in het veld Keep Alive van 0 tot 600. Deze functie zorgt ervoor dat uw router altijd verbonden is met internet. Het zal proberen om de VPN-verbinding opnieuw tot stand te brengen als deze wordt verwijderd.



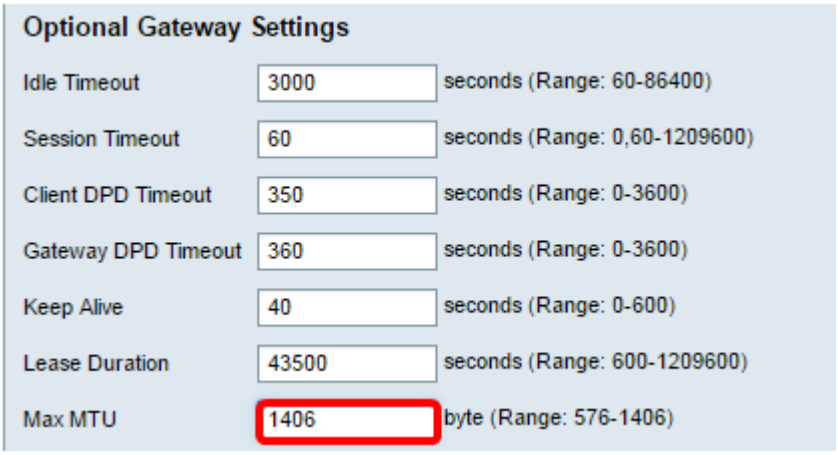
Opmerking: In dit voorbeeld wordt 40 gebruikt.

Stap 6. Voer in het veld Leaseduur een waarde in voor de duur van de tunnel die moet worden aangesloten. Het bereik is van 600 tot 1209600.



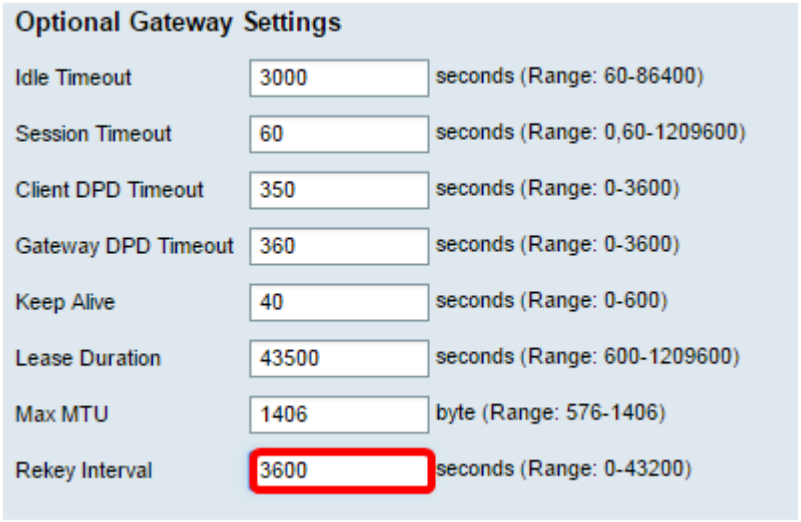
Opmerking: In dit voorbeeld wordt 43500 gebruikt.

Stap 7. Geef de pakketgrootte op in bytes die over het netwerk kunnen worden verzonden. Het bereik ligt van 576 tot 1406.



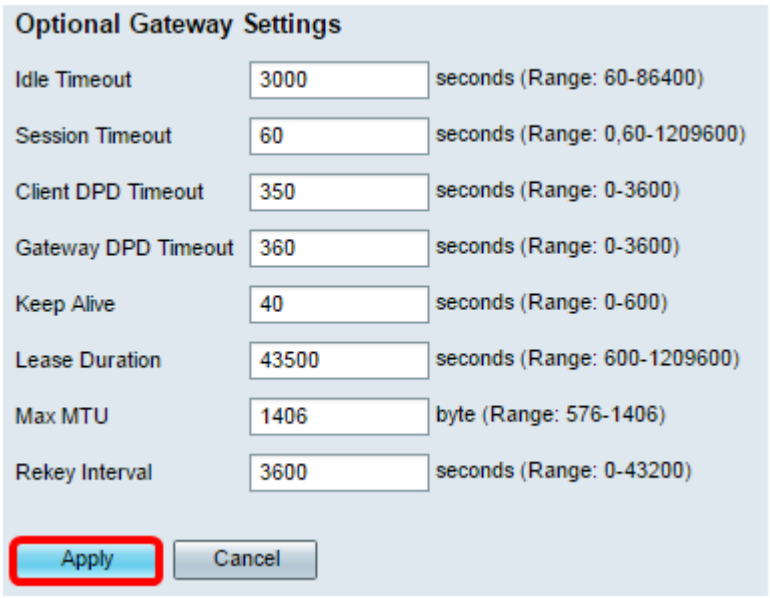
Opmerking: In dit voorbeeld wordt 1406 gebruikt.

Stap 8. Voer de tijd van het relaisinterval in het veld Opnieuw sleutelinterval in. Met de functie Opnieuw sleutelen kunnen de SSL-sleutels opnieuw onderhandelen nadat de sessie is ingesteld. Het bereik ligt tussen 0 en 43200.



Opmerking: In dit voorbeeld wordt 3600 gebruikt.

Stap 9. Klik op Apply (Toepassen).



Stap 10. (Optioneel) Om de configuratie permanent op te slaan, klikt u op het knipperende 

pictogram.

U moet nu SSL VPN met succes hebben geconfigureerd op uw RV34x-router.

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.