Probleemoplossing van toegangslijsten via Virtual Private Network op RV016, RV042, RV042G en RV082 VPN-routers

Doelstellingen

Een toegangscontrolelijst (ACL) is een verzameling van vergunningen en weigert voorwaarden. ACL specificeert welke gebruiker of systeemprocessen toegang tot specifieke middelen worden verleend. Een ACL kan alle ongegronde pogingen blokkeren om netwerkbronnen te bereiken. Het probleem in deze situatie kan zich voordoen wanneer u ACL's hebt geconfigureerd op beide routers, maar een van de routers kan niet onderscheiden tussen de toegestane en geweigerde lijsten van verkeer die door ACL zijn toegestaan. Zenmap is een open source tool gebruikt voor het controleren van het type pakketfilters / firewalls actief wordt gebruikt om de configuratie te testen.

Dit artikel legt uit hoe de toegestane ACLâ€™s die niet via gateway-to-gateway VPN tussen twee VPN-routers werken, probleemoplossing kunnen bieden.

Toepasselijke apparaten

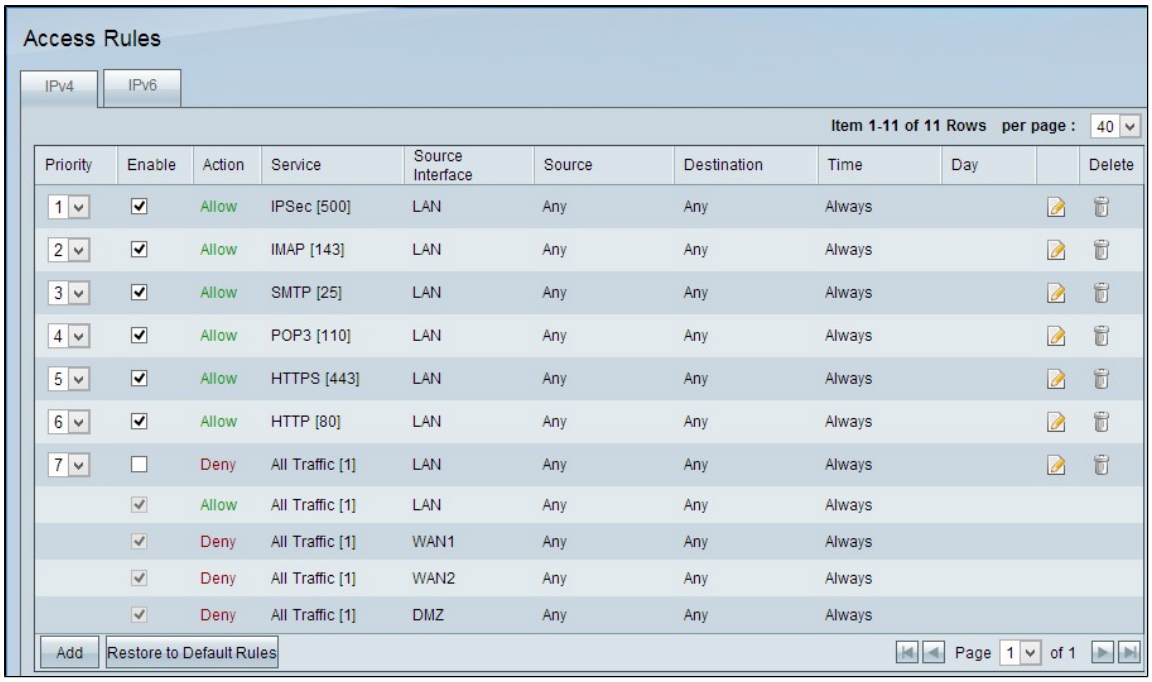
· RV016
â€¢RV042
· RV042G
· RV082

Softwareversie

· v4.2.2.08

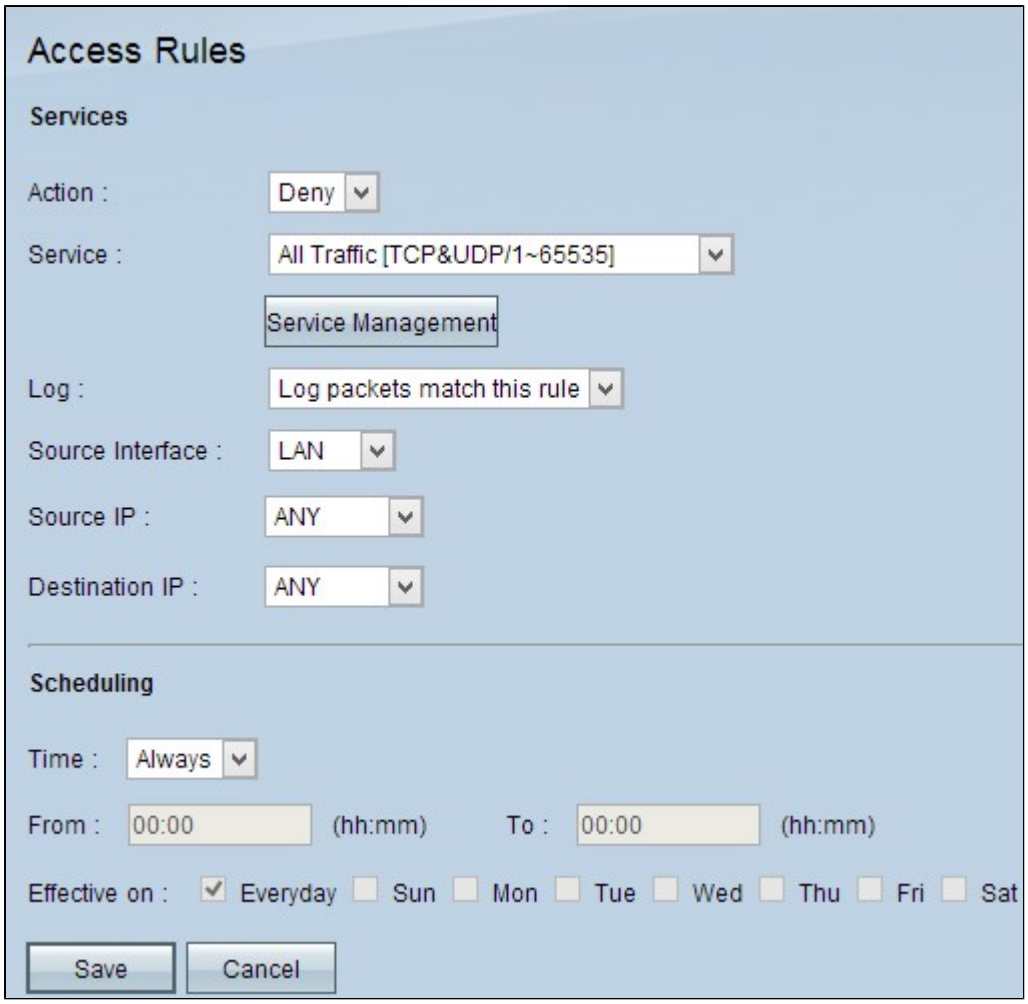
Configuratie van ACL over VPN

Stap 1. Meld u aan bij het hulpprogramma voor webconfiguratie en kies **Firewall > Toegangsregels**. De pagina *Toegangsregels* wordt geopend:

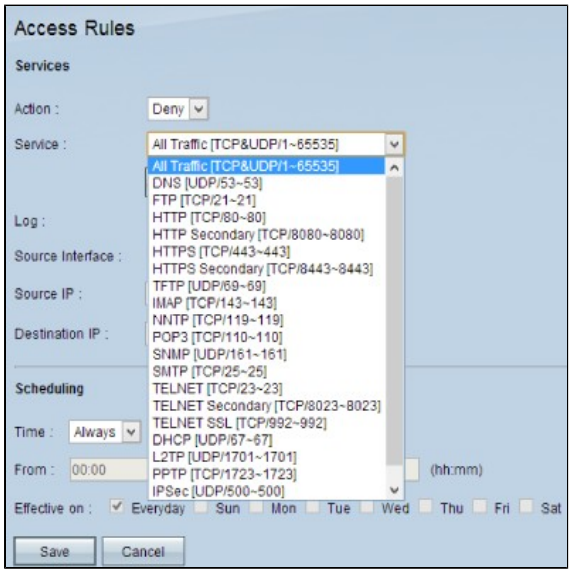


Opmerking: de standaardtoegangsregels kunnen niet worden bewerkt. De toegangsregels die in het bovenstaande beeld worden vermeld en die door de gebruiker zijn geconfigureerd, kunnen via het volgende proces worden bewerkt.

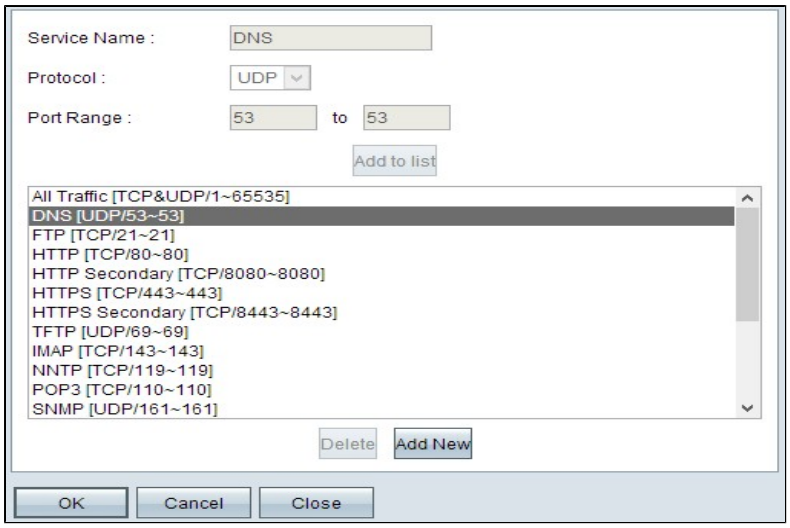
Stap 2. Klik op de knop **Toevoegen** om een nieuwe toegangsregel toe te voegen. De pagina *Toegangsregels* verandert om de services en de planningsgebieden weer te geven. De toevoeging van één toegangsregel wordt in de volgende stappen uitgelegd.



Stap 3. Kies **Ontkennen** in de vervolgkeuzelijst Actie om de service te weigeren.



Stap 4. Kies de gewenste service die op de regel wordt toegepast in de vervolgkeuzelijst **Service**.



Stap 5. (Optioneel) Klik op **Servicebeheer** als u een service wilt toevoegen die niet in de vervolgkeuzelijst voor **de** service voorkomt. Bij Servicebeheer kan een service indien nodig worden gemaakt. Klik nadat een service is gemaakt op **OK** om de instellingen op te slaan.

Stap 6. Kies **Logpakketten die overeenkomen met deze regel** in de vervolgkeuzelijst Log voor alleen logbestanden die overeenkomen met of **niet** inloggen voor logbestanden die niet voldoen aan de toegangsregel.

Stap 7. Kies een interfacetype uit de vervolgkeuzelijst Bron-interface die de bron is voor de toegangsregels. De beschikbare opties zijn:

· LAN â€" Kies LAN als de broninterface het Local Area Network is.

· WAN â€" Kies WAN als de broninterface de ISP is.

· DMZ â€" Kies DMZ als de broninterface de gedemilitariseerde zone is.

· OM HET EVEN WELK â€" Kies OM HET EVEN WELK om de broninterface als om het even welke bovengenoemde interfaces te maken.

Stap 8. Kies in de vervolgkeuzelijst Bron-IP het gewenste bronadres dat van toepassing is op de toegangsregel. De beschikbare opties zijn:

· Enkelvoudig â€" Kies Enkelvoudig als het één IP-adres is en voer het IP-adres in.

· Bereik â€" Kies bereik als het een bereik van IP-adressen is en voer het eerste en laatste IP-adres in het bereik in.

· OM HET EVEN WELK â€" Kies OM HET EVEN WELK om de regels op alle IP-bronadressen toe te passen.

Stap 9. Kies in de vervolgkeuzelijst Bestemming IP het gewenste doeladres dat van toepassing is op de toegangsregel. De beschikbare opties zijn:

· Enkelvoudig â€" Kies Enkelvoudig als het één IP-adres is en voer het IP-adres in.

· Bereik â€" Kies bereik als het een bereik van IP-adres is en voer het eerste en laatste IP-adres in het bereik in.

· OM HET EVEN WELK â€" Kies OM HET EVEN WELK om de regels op alle IP van de

Bestemming adressen toe te passen.

Stap 10. Kies een methode om te definiëren wanneer de regels actief zijn in de vervolgkeuzelijst Tijd. Dit zijn:

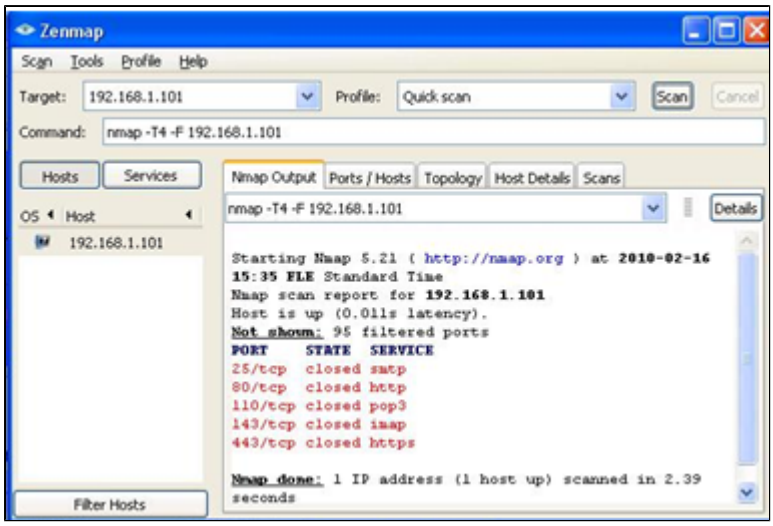
· Altijd â€" Als u altijd kiest uit de vervolgkeuzelijst Tijd, worden de toegangsregels altijd toegepast op het verkeer.

· Interval â€" U kunt een specifiek tijdsinterval kiezen waarbij de toegangsregels actief zijn als u Interval selecteert in de vervolgkeuzelijst Tijd. Nadat u het tijdsinterval hebt opgegeven, schakelt u de selectievakjes in van de dagen waarop u wilt dat de toegangsregels actief zijn in het veld Effectief op.

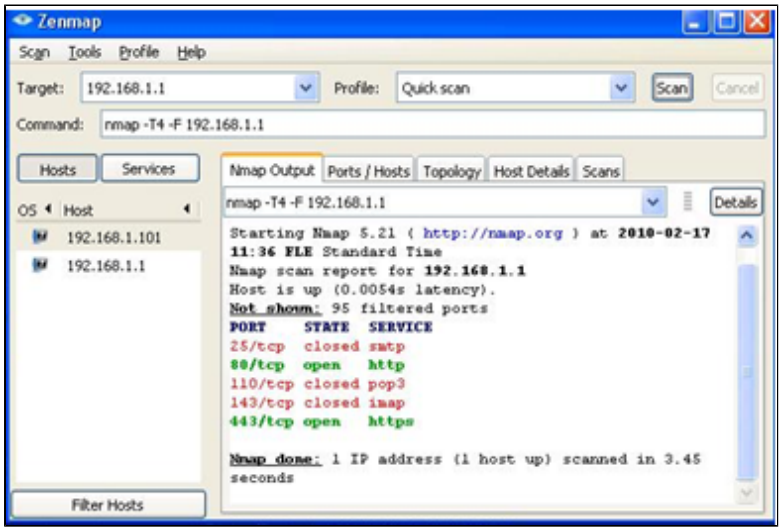
Stap 11. Klik op **Opslaan** om de instellingen op te slaan.

Stap 12. Herhaal stap 2 tot en met 10, waarbij de velden overeenkomen met de velden die in de afbeelding worden weergegeven. De toegangsregels per klant worden hier toegepast. De eerste 7 staan sommige diensten toe; de 8ste ontkent al het andere verkeer. Deze configuratie wordt ook gemaakt op de tweede router. IPsec-poort 500 is toegestaan.

Opmerking: Doe dit voor beide routers om te controleren of toegangsregels naar wens zijn geconfigureerd.



VPN-router # 1

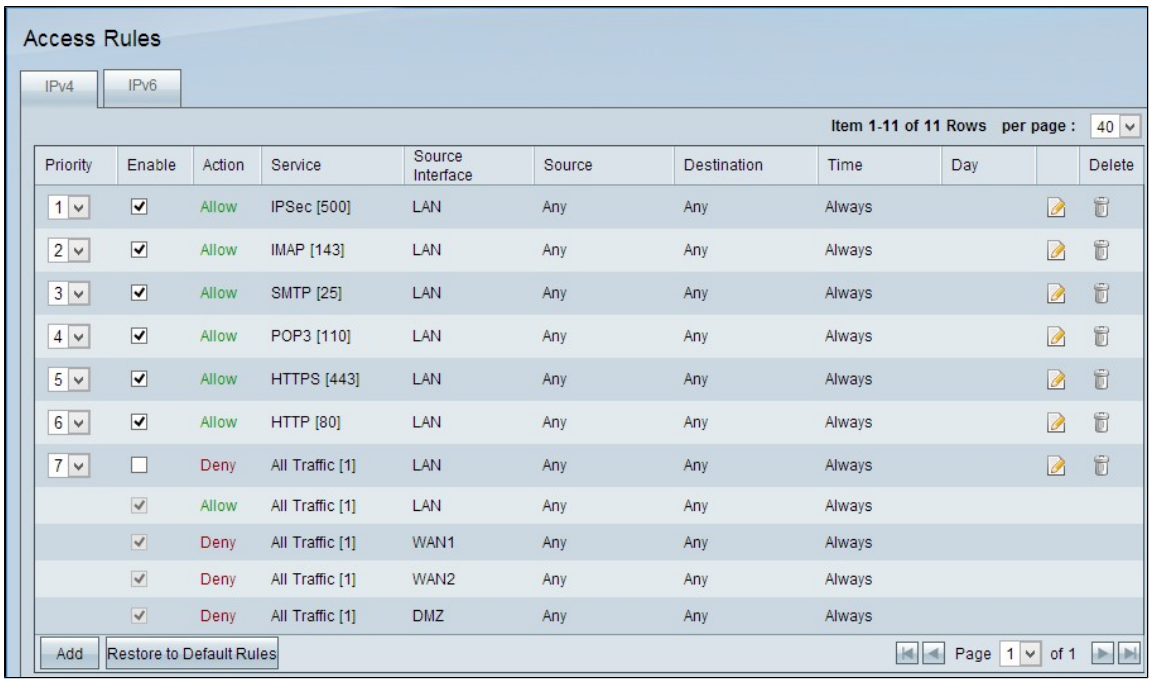


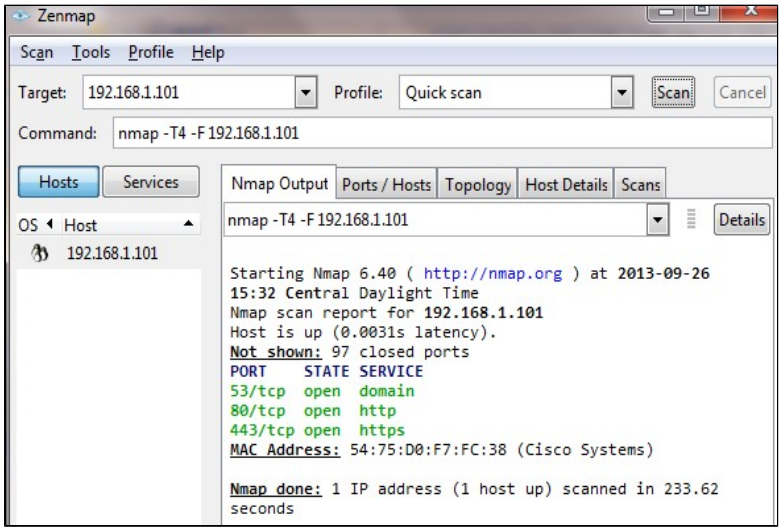
VPN-router # 2

Stap 13. Installeer Zenmap (NMAP) vanaf http://nmap.org/download.html en start het op een PC in het 192.168.2.0 LAN.

Opmerking: dit is het LAN achter de router met de zeven extra ACLâ€™s. Het doel-IP (192.168.1.101) is een pc op het Remote Gateway-LAN.

Stap 14. Selecteer **Snel scannen** in het profiel en klik op **Scannen**. Hierdoor weten we dat de poorten geopend en gefilterd zijn zoals in de ACL's, het getoonde resultaat wordt weergegeven in de afbeelding hierboven. De output toont aan dat deze poorten gesloten zijn, ongeacht of de toegestane ACLâ€™s op de RV0xx # 1 worden geconfigureerd. Als we proberen de poorten naar de LAN IP (192.168.1.1) van de externe gateway te controleren - ontdekken we dat poorten 80 en 443 open zijn (die gesloten waren voor de PC 192.168.1.101).





De ACL functioneert correct na de verwijdering van 7de ontkende ACL en werkt prima zoals we kunnen zien van de uitvoer.

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.