Systeemconfiguratie op RV320 en RV325 VPN-routerserie

Doel

De logbestanden van het systeem zijn records van netwerkgebeurtenissen. Logs zijn een belangrijk gereedschap dat wordt gebruikt om te begrijpen hoe een netwerk werkt. Ze zijn handig voor netwerkbeheer en netwerkprobleemoplossing.

Dit artikel legt uit hoe u de typen logbestanden die opgenomen moeten worden, kunt configureren, hoe u de logbestanden kunt bekijken in de routerserie van RV32x VPN, en hoe u de logbestanden via sms naar een ontvanger kunt doorsturen, naar een systeemlogserver of naar een ontvanger via e-mail.

Toepasselijke apparaten

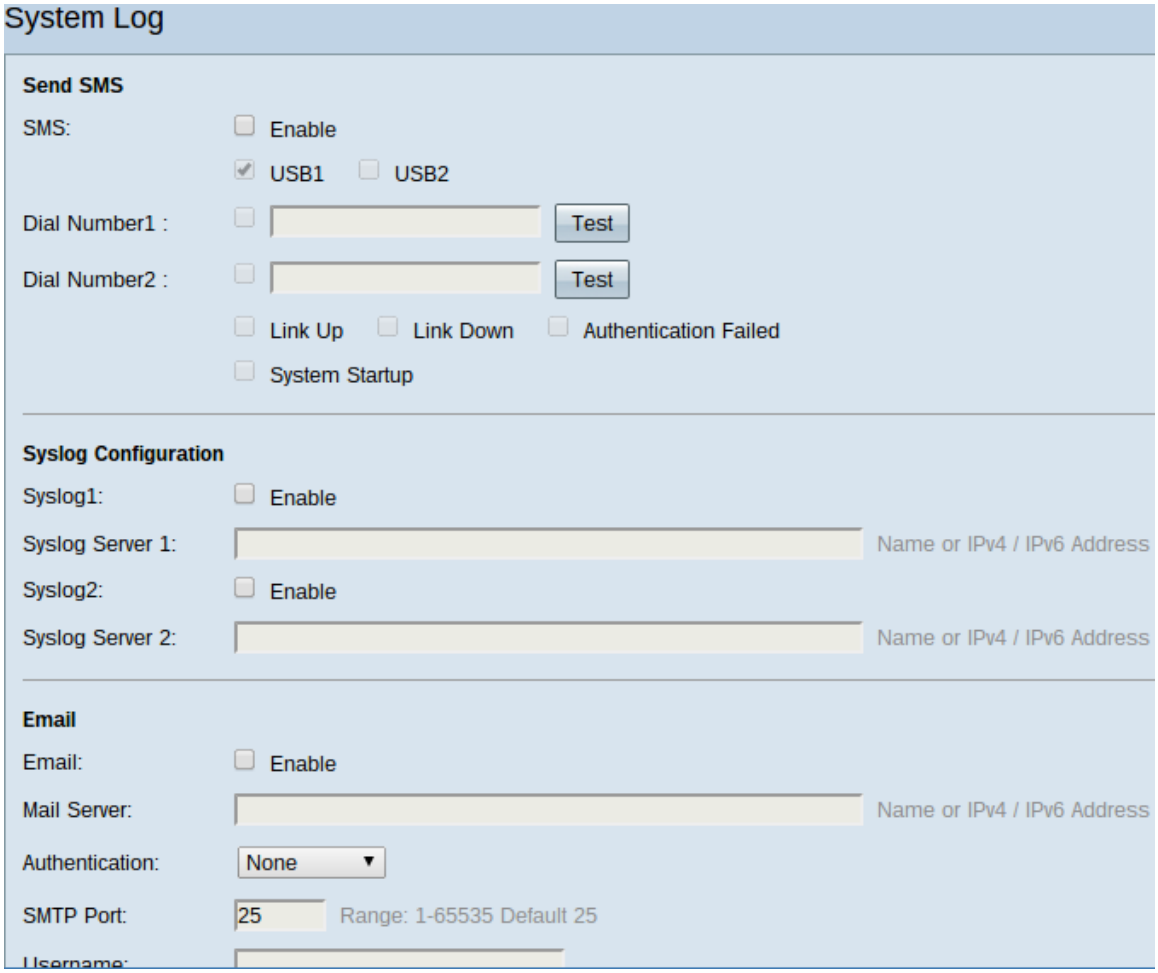
- RV320 VPN-router met dubbel WAN
- RV325 Gigabit VPN-router met dubbel WAN

Softwareversie

- v1.1.0.09

Configuratie van systeemlogboek

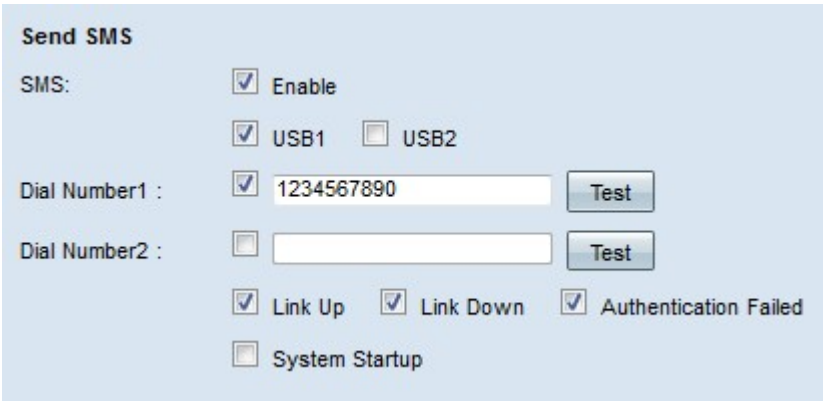
Stap 1. Meld u aan bij het programma voor webconfiguratie en kies **Log > systeemlogboek**. De pagina *Systeemlogboek* wordt geopend:



Raadpleeg de volgende secties voor informatie over de pagina *Systeemlogboek*.

- Systeemmeldingen via sms — Hoe u de systeemmeldingen via sms naar een telefoon kunt sturen.
- System Logs on System Log Server — Hoe de systeemlogbestanden naar een systeemlogserver kunnen worden verzonden.
- E-mailsysteemvastlegging — Hoe de systeemlogs naar een e-mailadres worden verzonden.
- Instellingen logbestand - Hoe moet u het type berichten configureren dat op het logbestand wordt opgeslagen.
- Bekijk het systeemlogboek — Hoe u de systeemmeldingen op het apparaat bekijkt.
- Bekijk uitgaande logatabel - Hoe u de systeemlogbestanden bekijkt die alleen betrekking hebben op uitgaande pakketten.
- Inkomende loglijst bekijken — Hoe u de systeemlogbestanden kunt bekijken die alleen betrekking hebben op inkomende pakketten.

Vastlegging systeem per sms



Stap 1. Controleer in het veld **Sms** de **mogelijkheid** om systeemmeldingen naar een client te verzenden via sms-berichten (Short Message Service).

Stap 2. Controleer de selectievakjes in de USB-poorten waarop de 3G USB-modem is aangesloten.

Stap 3. Controleer het aankruisvakje in het veld Dial Number1 en voer het telefoonnummer in waarop de berichten worden verzonden.

Opmerking: Klik op **Test** om de verbinding te testen om nummer 1 te bellen. Als het geconfigureerde nummer het testbericht niet ontvangt, zorg er dan voor dat het telefoonnummer correct is ingevoerd in het veld Dial Number1.

Stap 4. (Optioneel) Controleer het aankruisvakje in het veld Dial Number2 en voer het telefoonnummer in waarop de berichten worden verzonden.

Opmerking: Klik op **Test** om de verbinding te testen om nummer 2 te bellen. Als het geconfigureerde nummer het testbericht niet ontvangt, zorg er dan voor dat het telefoonnummer correct is ingevoerd in het veld Dial Number2.

Stap 5. Controleer de vinkjes van de gebeurtenissen die het te verzenden logbestand activeren.

- Link Up — Er is een verbinding met de RV320 opgezet.
- Link Down — er is een verbinding met de RV320 gelegd.
- Verificatie is mislukt — Een verificatie is mislukt.
- Systeem starten — De router is opgestart.

Stap 6. Klik op **Opslaan**. Het systeem logt via SMS in.

Systeemlogboek op systeemlogservers

Stap 1. Controleer het veld Scannen1 om systeemlogbestanden naar een systeemlogserver te verzenden.

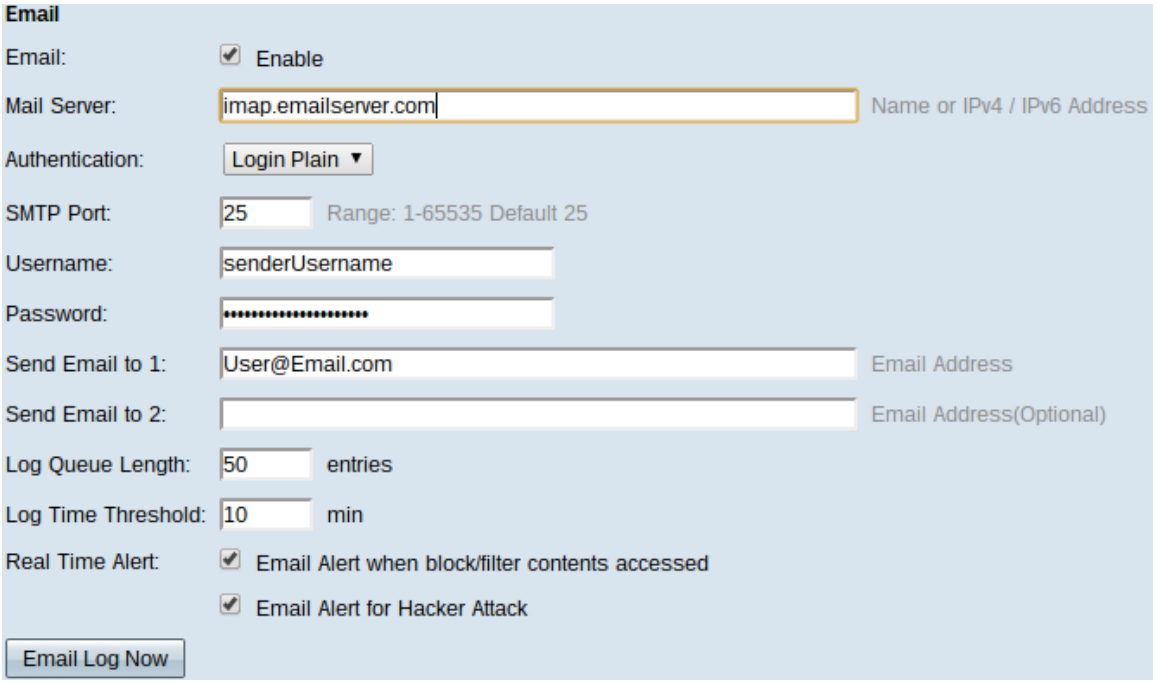
Stap 2. Voer het hostname- of IP-adres van de systeemlogserver in het veld SLB Server 1 in.

Stap 3. (Optioneel) Als u logbestanden naar een andere systeemlogserver wilt doorsturen, controleert u op **Inschakelen** in het veld Sourcg2.

Stap 4. Als het aanvinkvakje in het veld SLOG2 is ingeschakeld, specificeert u de hostnaam of het IP-adres van de systeemlogserver in het veld Slogserver 2.

Stap 5. Klik op **Opslaan**. Het systeem logt via systeemlogservers in.

Vastlegging e-mailsysteem



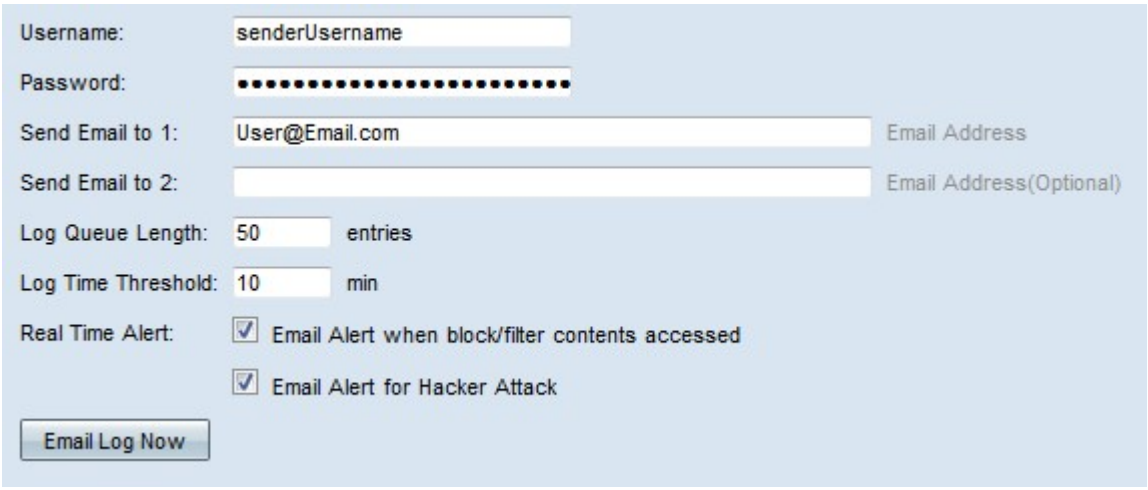
Stap 1. Controleer het veld E-mail in om systeemlogbestanden naar een ontvanger te verzenden via e-mail.

Stap 2. Voer de domeinnaam of IP-adres van de mailserver in het veld Mail Server in.

Stap 3. Kies het type verificatie dat de mailserver gebruikt in het veld Verificatie.

- Geen — De mailserver gebruikt geen authenticatie.
- Aanmelden - De mailserver gebruikt verificatie in een onbewerkte tekstindeling.
- TLS — De mailserver gebruikt Vervoerlaag Beveiliging (TLS) om de client en server in staat te stellen authenticatie informatie veilig uit te wisselen.
- SSL — De mailserver gebruikt Secure Socket Layer (SSL) om de client en server in staat te stellen om authenticatie informatie veilig uit te wisselen.

Stap 4. Voer de Simple Mail Transfer Protocol (MTP) poort in die de mailserver in het veld MTP-poort gebruikt. MTP is een protocol dat het mogelijk maakt om e-mails via IP-netwerken te verzenden.



Stap 5. Voer de gebruikersnaam voor de e-mailzender in het veld Gebruikersnaam.

Stap 6. Voer het wachtwoord in van de e-mailzender in het veld Wachtwoord.

Stap 7. Voer het e-mailadres van de e-mailontvanger in het veld E-mail verzenden naar 1.

Stap 8. (optioneel) Voer een extra e-mailadres in om loge-mails naar in het veld E-mail verzenden naar 2.

Stap 9. Voer het aantal logingangen in dat moet worden gemaakt voordat het logbestand naar de e-mailontvanger wordt verzonden in het veld Lengte logwachtrij.

Stap 10. Voer het interval in waarmee het apparaat het logbestand naar de e-mail stuurt in het veld Timer-tijd.

Stap 1. Controleer het eerste aanvinkvakje in het veld Realtijd om direct een e-mail te verzenden wanneer iemand, die geblokkeerd of gefilterd is, probeert de router te bereiken.

Stap 12. Controleer het tweede aankruisvakje in het veld Realtime signaleren om een e-mail te verzenden wanneer een hacker probeert om de router te bereiken via een DOS-aanval (Denial of Service).

Opmerking: Klik op **E-mail nu** om het logbestand direct te verzenden.

Stap 13. Klik op **Opslaan**. Het systeem logt via e-mail en is ingesteld.

Log instellingen

Stap 1. Controleer de vinkjes van de gebeurtenissen die een logingang veroorzaken.

- Waarschuwingslogboek — Deze stammen worden aangemaakt wanneer een aanval of poging tot aanval heeft plaatsgevonden.

  - Syn Flooding — SYN-verzoek wordt sneller ontvangen dan de router kan verwerken.

  - IP Spoofing - De RV320 heeft IP-pakketten met geforceerde bron-IP-adressen ontvangen.

  - Onbevoegde aanmelding — Een afgewezen poging om zich aan te melden bij het netwerk is mislukt.

  - Ping of Death - Er is een ping van een abnormale omvang naar een interface verstuurd in een poging het doelapparaat te crashen.

  - Win Nuke — The Remote Distributed Denial of Service Attack (DDOS), bekend onder de naam WinNuke, is naar een interface verzonden in een poging het doelapparaat te crashen.

- Algemeen logbestand — Deze logbestanden worden gemaakt wanneer er algemene netwerkacties plaatsvinden.

  - Deny Policy — Toegang is geweigerd aan een gebruiker op basis van het geconfigureerde beleid van de router.

  - Geautoriseerde aanmelding — Een gebruiker is gemachtigd om toegang te krijgen tot het netwerk.

  - Systeemfoutmeldingen - er is een systeemfout opgetreden.

  - Beleid toestaan — Toegang is verleend aan een gebruiker op basis van het geconfigureerde beleid van de router.

  - Kernel — Alle boodschappen op de lijst opnemen. Het kern is het eerste deel van het besturingssysteem dat bij het opstarten in het geheugen is geladen. Kernelberichten zijn blogs die in verband worden gebracht met de kern.

  - Wijzigingen in de configuratie — de routerconfiguratie is aangepast.

  - IPSEC en PPTP VPN — ER is onderhandeling, verbinding of ontbinding van IPSEC en PPTP VPN geweest.

  - SSL VPN — Er is een SSL VPN-onderhandeling, verbinding of ontbinding opgetreden.

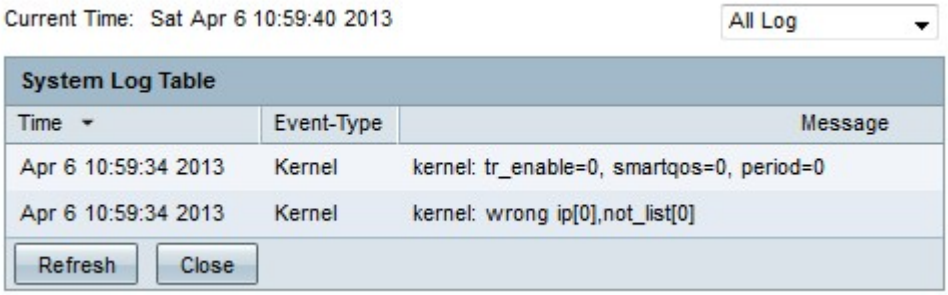
  - Netwerk — Er is een fysieke verbinding gemaakt of verloren op de WAN- of DMZ-interfaces.

Stap 2. Klik op **Opslaan**. De loginstellingen zijn ingesteld.

Opmerking: Klik op **Log wissen** om het huidige logbestand te verwijderen.

Systeemlogboek weergeven

Stap 1. Klik op **Systeemlogbestand weergeven** om de systeemlogtabel te bekijken. Het venster *System Log Table* verschijnt.



Stap 2. (Optioneel) Kies in de vervolgkeuzelijst het type logbestand dat u wilt bekijken.

- Alle logberichten — met inbegrip van alle logberichten.
- systeemlogboek — bevat alleen de systeemfoutmeldingen.
- Firewalllogboek/DoS-logboek — alleen de waarschuwingsblogs.
- VPN-logboek — Alleen de IPSec & PPTP VPN- en SSL VPN-logbestanden.
- Netwerklogboek — Alleen de netwerklogbestanden.
- Kernellogboek — omvat alleen kabelberichten.
- Gebruikerspeld — bevat alleen beleid voor ontkennen, beleid, geautoriseerde inloggen en logwijzigingen in de configuratie
- SSL-logbestand — omvat alleen SSL VPN-documenten.

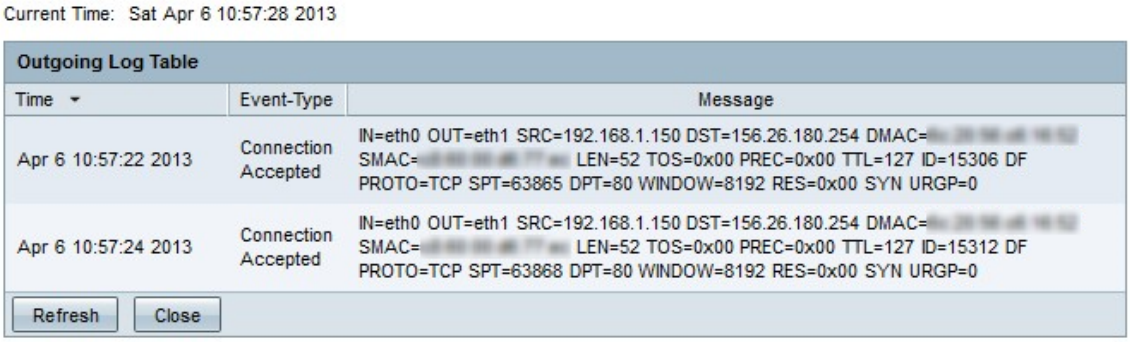
De tabel met systeemlogboek geeft de volgende informatie weer.

- Tijd — Het tijdstip waarop het logbestand is gemaakt.
- Event-type — Het type log.
- Bericht — Informatie die overeenkomt met het logboek. Dit omvat het type beleid, het bron IP adres en het bron MAC adres.

Opmerking: Klik op **Vernieuwen** om de logtabel te verfrissen.

Uitgaande loglijst bekijken

Stap 1. Klik op **Uitgaande loglijst** om de logtabel te bekijken die alleen op uitgaande pakketten betrekking heeft. Het venster *Uitgaande loglijst* verschijnt.



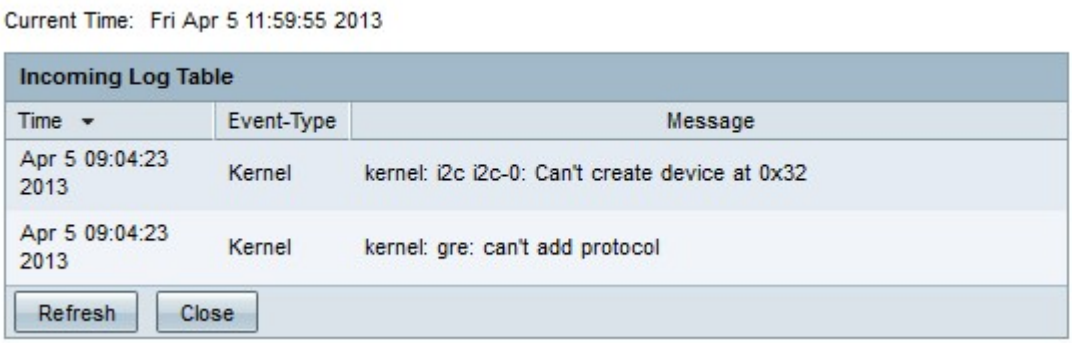
De volgende informatie wordt weergegeven in de aflopende logtabel.

- Tijd — Het tijdstip waarop het logbestand is gemaakt.
- Event-type — Het type log.
- Bericht — Informatie die overeenkomt met het logboek. Dit omvat het type beleid, het bron IP adres en het bron MAC adres.

Opmerking: Klik op **Vernieuwen** om de logtabel te verfrissen.

Inkomende logtabel weergeven

Stap 1. Klik op **Inkomend logbestand** om de logtabel te bekijken die alleen op inkomende pakketten betrekking heeft. Het venster *Inkomend logschema* verschijnt.



De volgende informatie wordt weergegeven in de inkomende logtabel.

- Tijd — Het tijdstip waarop het logbestand is gemaakt.
- Event-type — Het type log.
- Bericht — Informatie die overeenkomt met het logboek. Dit omvat het type beleid, het bron IP adres en het bron MAC adres.

Opmerking: Klik op **Vernieuwen** om de logtabel te verfrissen.