Configuratie van systeemlog op RV016, RV042, RV042G en RV082 VPN-routers

Doel

Er wordt een systeemlogboek (Syslog) gebruikt om computergegevens te registreren. U kunt de instanties definiëren die een logbestand genereren. Wanneer een instantie zich voordoet, worden de tijd en de gebeurtenis opgenomen en verzonden naar een syslog server of verzonden in een e-mail. Syslog kan dan worden gebruikt om een netwerk te analyseren en problemen op te lossen, samen met een verhoogde netwerkbeveiliging.

In dit document wordt de procedure uitgelegd voor het configureren van een Syslog-server op RV016, RV042, RV042G en RV082 VPN-routers.

Toepasselijke apparaten

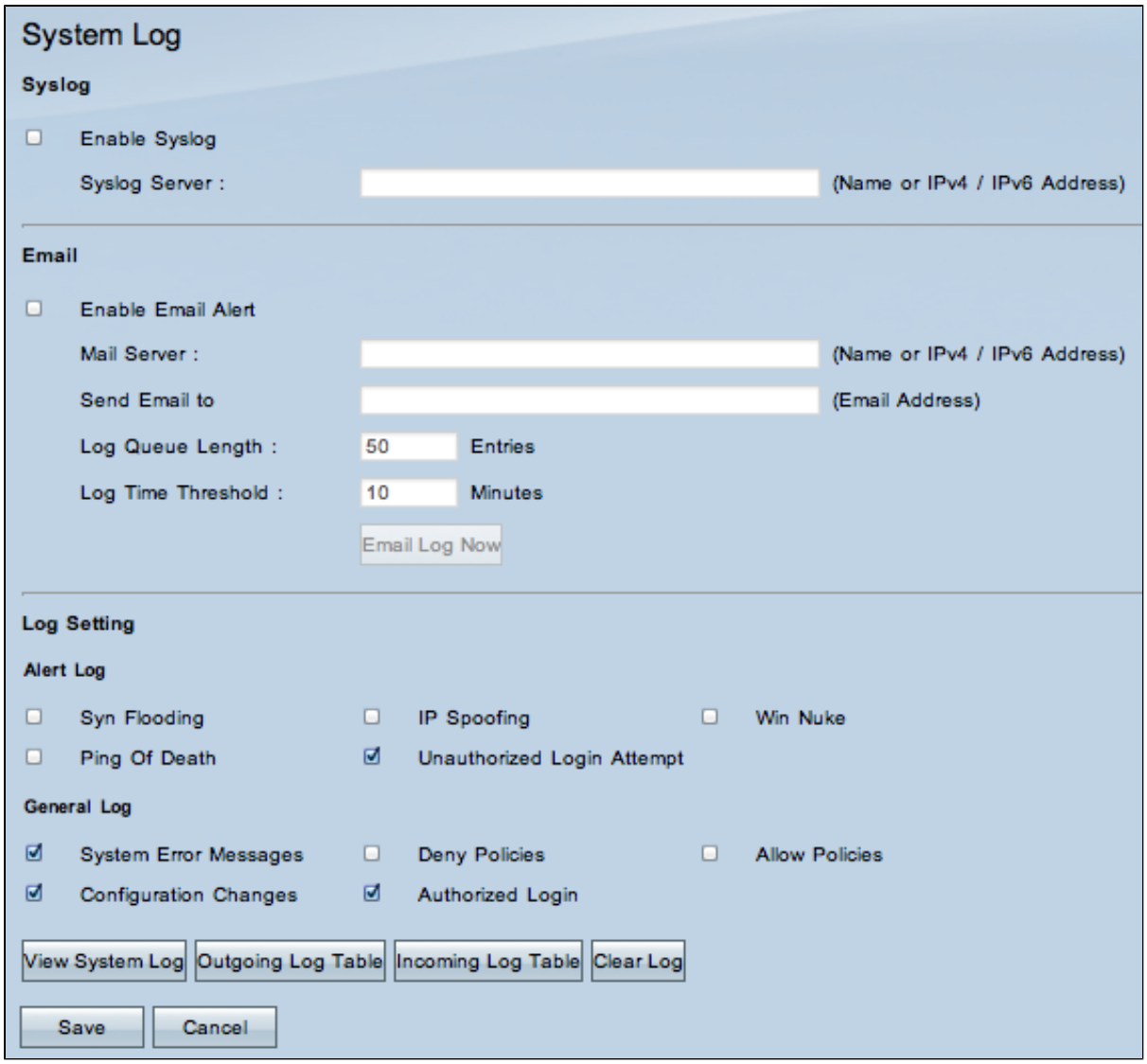
· RV016
â€¢RV042
· RV042G
· RV082

Softwareversie

· v4.2.1.02

Configuratie van syslog en meldingen

Stap 1. Meld u aan bij het hulpprogramma voor webconfiguratie en kies **Log > Systeemlog**. De *systeemlogpagina* wordt geopend:



Syslog

In deze sectie wordt uitgelegd hoe u de router kunt inschakelen om gedetailleerde logbestanden naar uw syslog-server te verzenden wanneer gebeurtenissen worden vastgelegd.

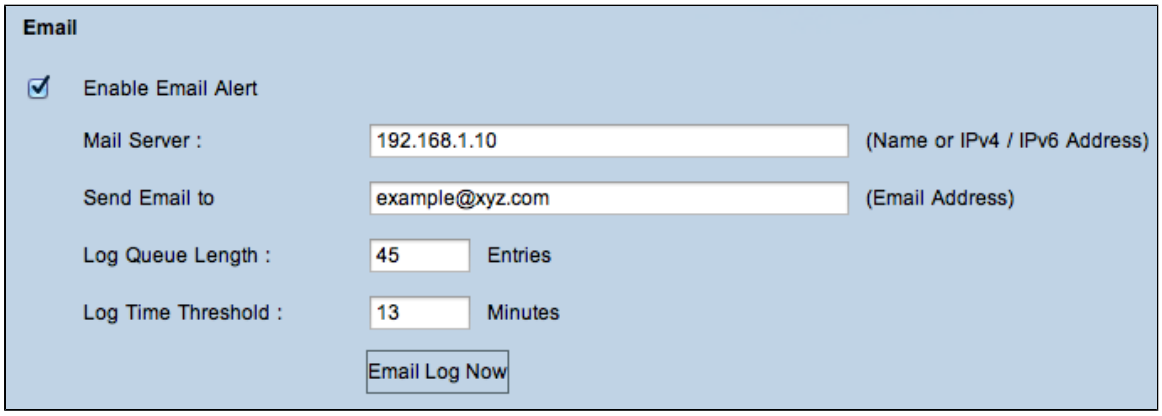
Stap 2. Schakel het aanvinkvakje **Enable Syslog in** om de syslog-service op het apparaat in te schakelen.

Timesaver: Ga naar stap 4 als Syslog moet worden uitgeschakeld.

Stap 3. Voer in het veld Syslog server de domeinnaam of het IP-adres van de syslog server in.

Email

Deze sectie legt uit hoe de router e-mailberichten kan verzenden wanneer gebeurtenissen worden vastgelegd.



Stap 4. Controleer **E-mailwaarschuwing inschakelen** om de functie in te schakelen. Dit laat de router toe om e-mailberichten naar het gebruiker gespecificeerde e-mailadres te verzenden.

Timesaver: Ga naar stap 10 als e-mailwaarschuwing moet worden uitgeschakeld.

Stap 5. Voer in het veld Mail Server het IPv4- of IPv6-adres in van de SMTP-server van uw ISP.

Opmerking: het is mogelijk dat uw ISP vereist dat u uw router identificeert met een hostnaam. Kies **Setup > Netwerk** om uw naam van de routerhost te definiëren.

Stap 6. Voer in het veld E-mail naar het e-mailadres in waar u de waarschuwingen wilt verzenden.

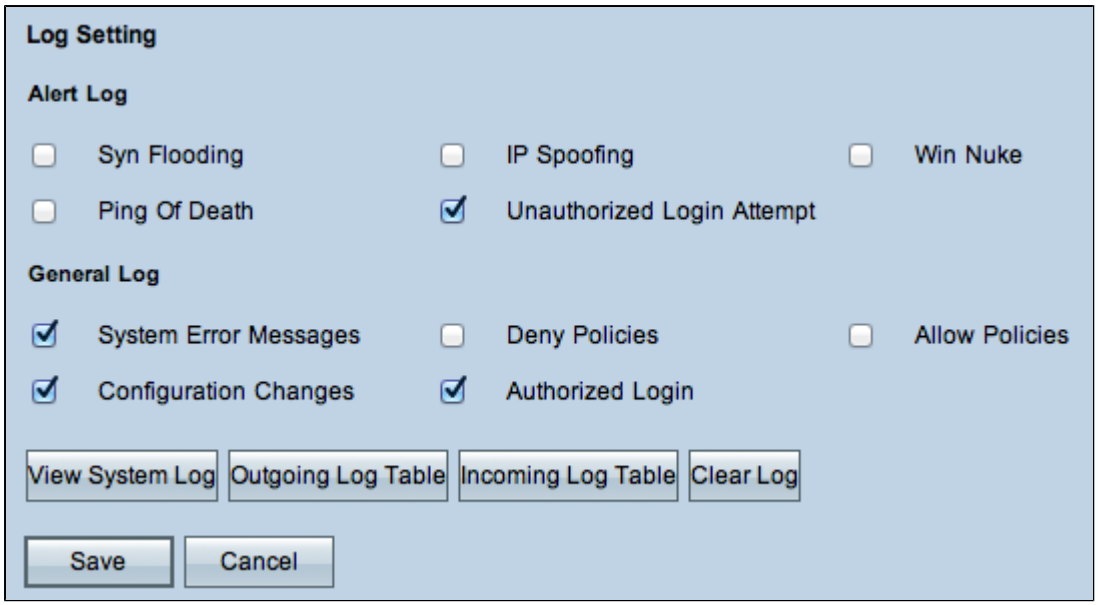
Stap 7. Voer het aantal logitems in dat in de e-mail moet worden opgenomen in het veld Lengte logrij. De standaardwaarde is 50.

Stap 8. Voer het aantal minuten in om gegevens te verzamelen voordat u het logbestand in het veld Logtijd drempelwaarde verzendt. De logtijddrempel is de maximale wachttijd voordat een e-maillogbericht wordt verzonden. Wanneer de logtijddrempel verloopt wordt een e-mail verzonden of de e-maillogbuffer vol is of niet. De standaardinstelling is 10 minuten

Stap 9. (Optioneel) Klik op **Email Log Now** om direct een bericht te verzenden naar het opgegeven e-mailadres om de instellingen te testen.

Loginstelling

In dit gedeelte wordt de verscheidenheid aan gebeurtenissen die in de logboeken kunnen worden gemeld, toegelicht:



Stap 10. Het gebied Waarschuwingslogboek bevat veel voorkomende typen aanvallen en niet-geverifieerde inlogpogingen. Schakel de aankruisvakjes van elk type van gewenste aanvallen in om ze in het gebeurtenissenlogboek op te nemen, of uncheck ze om ze uit het gebeurtenissenlogboek weg te laten.

· SYN overstroming â€" De aanvaller stuurt continu veel SYNC-pakketten, waardoor de router meerdere sessies opent, zodat het verkeer erg overvol wordt en de router legitiem verkeer ontkent.

· IP-spoofing â€" De aanvaller stuurt pakketten vanuit een nep-bron IP-adres om de aanval te laten lijken op legitiem verkeer.

· Win Nuke â€" De aanvaller stuurt een out-of-band bericht naar een Windows-machine om de doelcomputer te laten crashen.

· Ping of Death â€" De aanvaller stuurt een groot IP-pakket om de doelcomputer te laten crashen.

· Onbevoegde Login Poging â€" Iemand probeerde in te loggen op het hulpprogramma van de routerconfiguratie zonder de juiste verificatie.

Stap 11. Het algemene loggebied bevat de acties die worden uitgevoerd om geconfigureerd beleid af te dwingen, evenals routinegebeurtenissen zoals geautoriseerde logins en configuratiewijzigingen. Schakel het aanvinkvakje van een gewenste gebeurtenis in om deze in het algemene logbestand op te nemen. Schakel het aanvinkvakje uit om het te verwijderen uit het algemene logbestand.

· Systeemfoutmeldingen â€" Alle systeemfoutmeldingen.

· Beleidsregels weigeren â€" Gevallen waarin de router toegang geweigerd heeft op basis van uw toegangsregels.

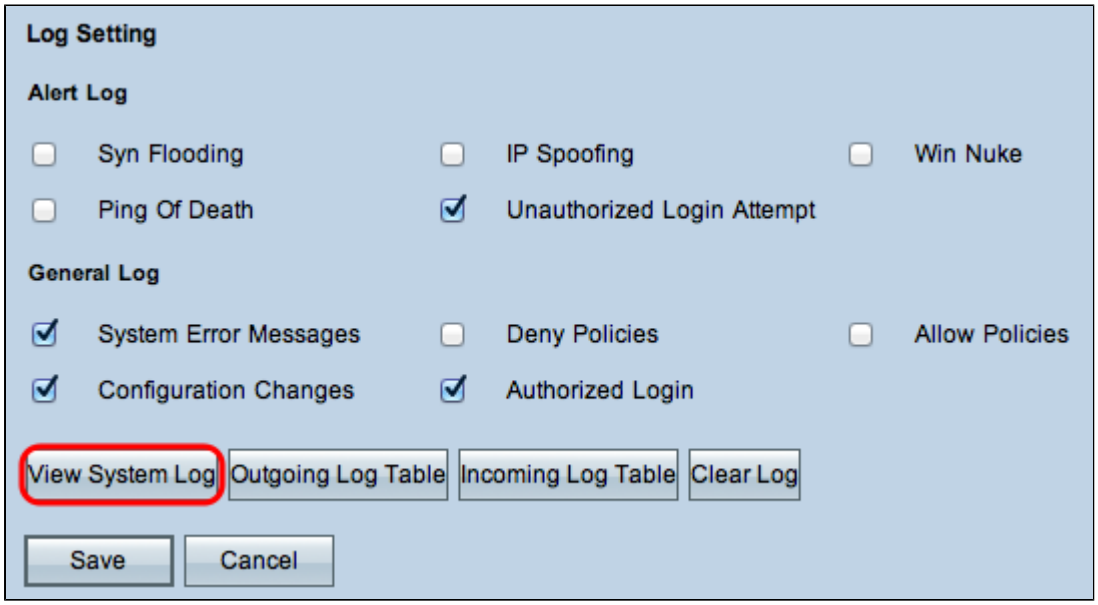
· Sta Beleid toe â€" Instanties wanneer de router toegang verleende die op uw Toegangsregels wordt gebaseerd.

· Configuratie Veranderingen â€" Instanties wanneer iemand veranderingen in de configuratie opslaat.

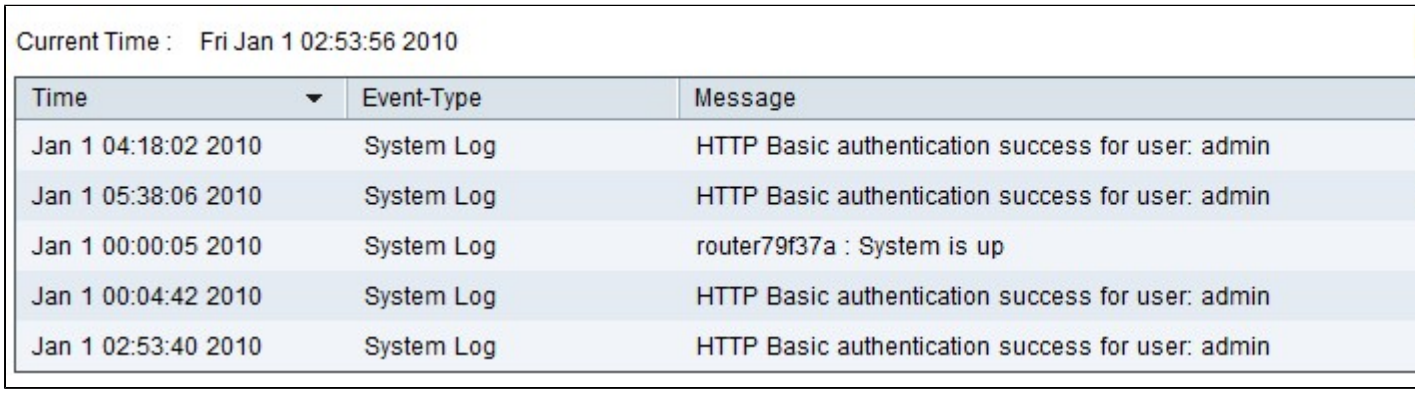
· Geautoriseerde inloggen â€" gevallen waarin iemand met succes is aangemeld bij het hulpprogramma voor routerconfiguratie na het invoeren van de juiste gebruikersnaam en het juiste wachtwoord.

· Output Blocking Event â€" Instanties waar er een gebeurtenis is in de ProtectLink web reputatie, of URL filtering.

Opmerking: Output Blocking Event is alleen beschikbaar op RV082 VPN-routers.



Stap 12. (Optioneel) Klik op **Systeemlogboek weergeven** om het systeemlogboek te bekijken. Het venster *Systeemlogboek* verschijnt:



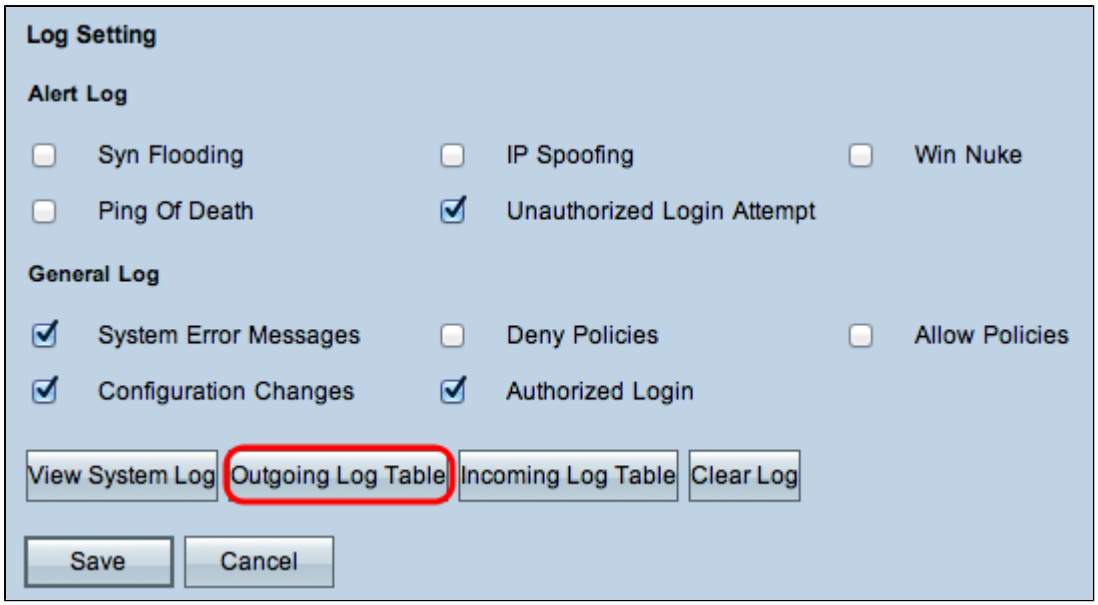
Opmerking: logitems geven de datum en tijd van het gebeurtenistype en een bericht. Dit bericht geeft het type beleid aan, zoals de toegangsregel, het LAN IP-adres van de bron en het MAC-adres.

Stap 13. Kies een bepaald logbestand in de vervolgkeuzelijst.

Stap 14. (Optioneel) Klik op **Vernieuwen** om de gegevens bij te werken.

Stap 15. (Optioneel) Klik op **Wissen** om alle weergegeven informatie te wissen.

Stap 16. Klik op **Sluiten** om het venster te sluiten.

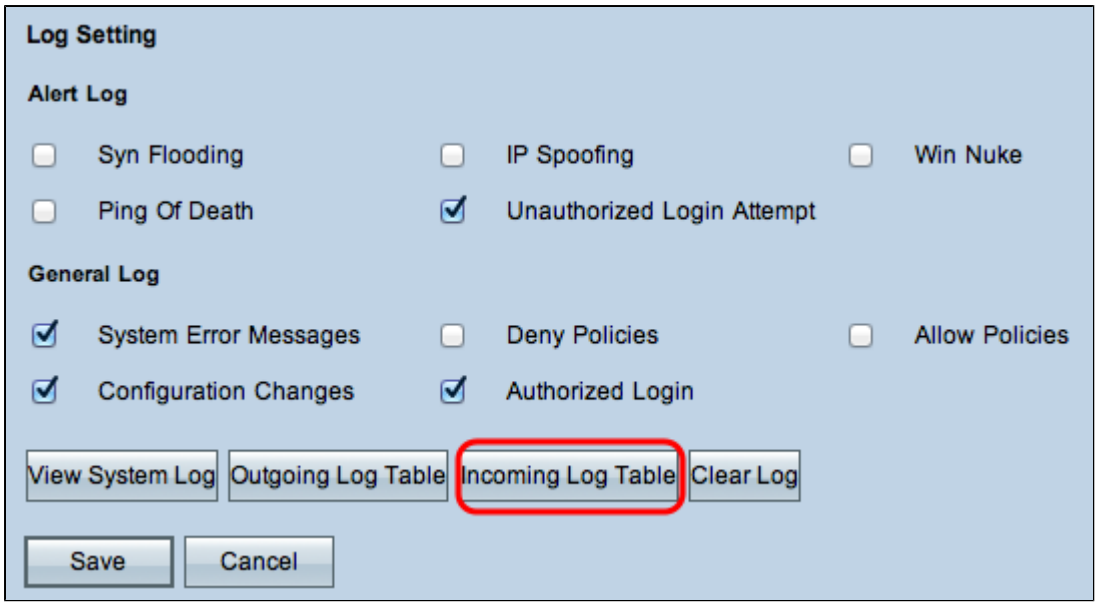


Stap 17. (Optioneel) Klik op **Uitgaande logtabel** om de informatie over de uitgaande pakketten te bekijken. De informatie verschijnt in een nieuw venster.

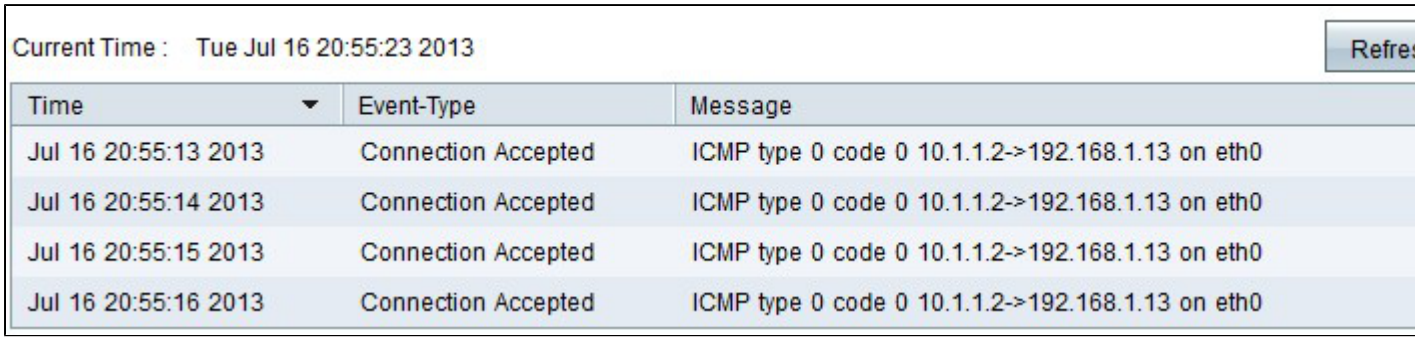
Time	Event-Type	Message
Jul 16 13:24:17 2013	Connection Accepted	TCP 192.168.1.100:52416->74.125.227.113:443 on eth1
Jul 16 13:24:17 2013	Connection Accepted	TCP 192.168.1.100:52416->74.125.227.113:443 on eth1
Jul 16 13:24:17 2013	Connection Accepted	TCP 192.168.1.100:52415->69.171.248.16:443 on eth1
Jul 16 13:24:19 2013	Connection Accepted	TCP 192.168.1.100:52436->157.55.240.222:443 on eth1
Jul 16 13:24:20 2013	Connection Accepted	TCP 192.168.1.100:52437->157.55.240.222:443 on eth1
Jul 16 13:24:29 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1
Jul 16 13:24:29 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1
Jul 16 13:24:30 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1
Jul 16 13:24:31 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1
Jul 16 13:24:31 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1
Jul 16 13:24:33 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1
Jul 16 13:24:33 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1

Stap 18. (Optioneel) Klik op **Vernieuwen** om de gegevens bij te werken.

Stap 19. Klik op **Sluiten** om het venster te sluiten.

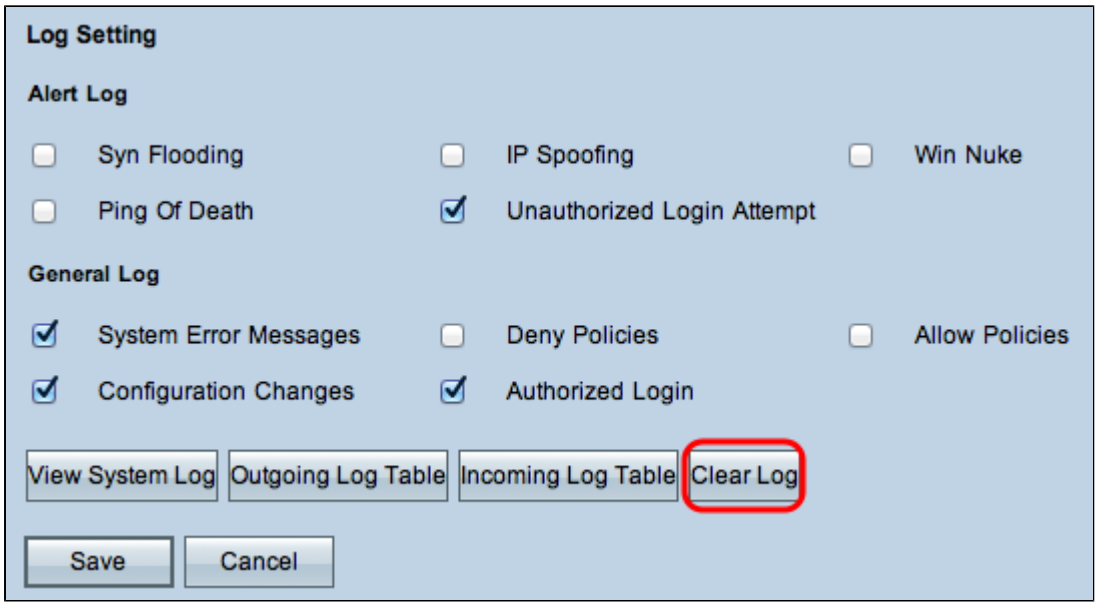


Stap 20. (Optioneel) Klik op **Inkomende logtabel** om de informatie over de inkomende pakketten te bekijken. De informatie wordt in een nieuw venster geopend. Als er een waarschuwing verschijnt over het pop-upvenster, kunt u de geblokkeerde inhoud toestaan.



Stap 21. (optioneel) Klik op **Vernieuwen** om de gegevens bij te werken.

Stap 22. Klik op **Sluiten** om het venster te sluiten.



Stap 23. (optioneel) Klik op **Log nu wissen** om het logbestand te verwijderen. Klik alleen op deze

knop als de informatie in de toekomst niet meer bekeken hoeft te worden.

Stap 24. Klik op **Opslaan** om de configuratie op te slaan.

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.