Configuration du journal système sur les routeurs VPN RV320 et RV325

Objectif

Les journaux système sont des enregistrements d'événements réseau. Les journaux sont un outil important utilisé pour comprendre le fonctionnement d'un réseau. Ils sont utiles pour la gestion du réseau et le dépannage du réseau.

Cet article explique comment configurer les types de journaux à enregistrer, comment afficher les journaux sur la gamme de routeurs VPN RV32x et comment envoyer les journaux à un destinataire par SMS, à un serveur de journaux système ou à un destinataire par e-mail.

Périphériques pertinents

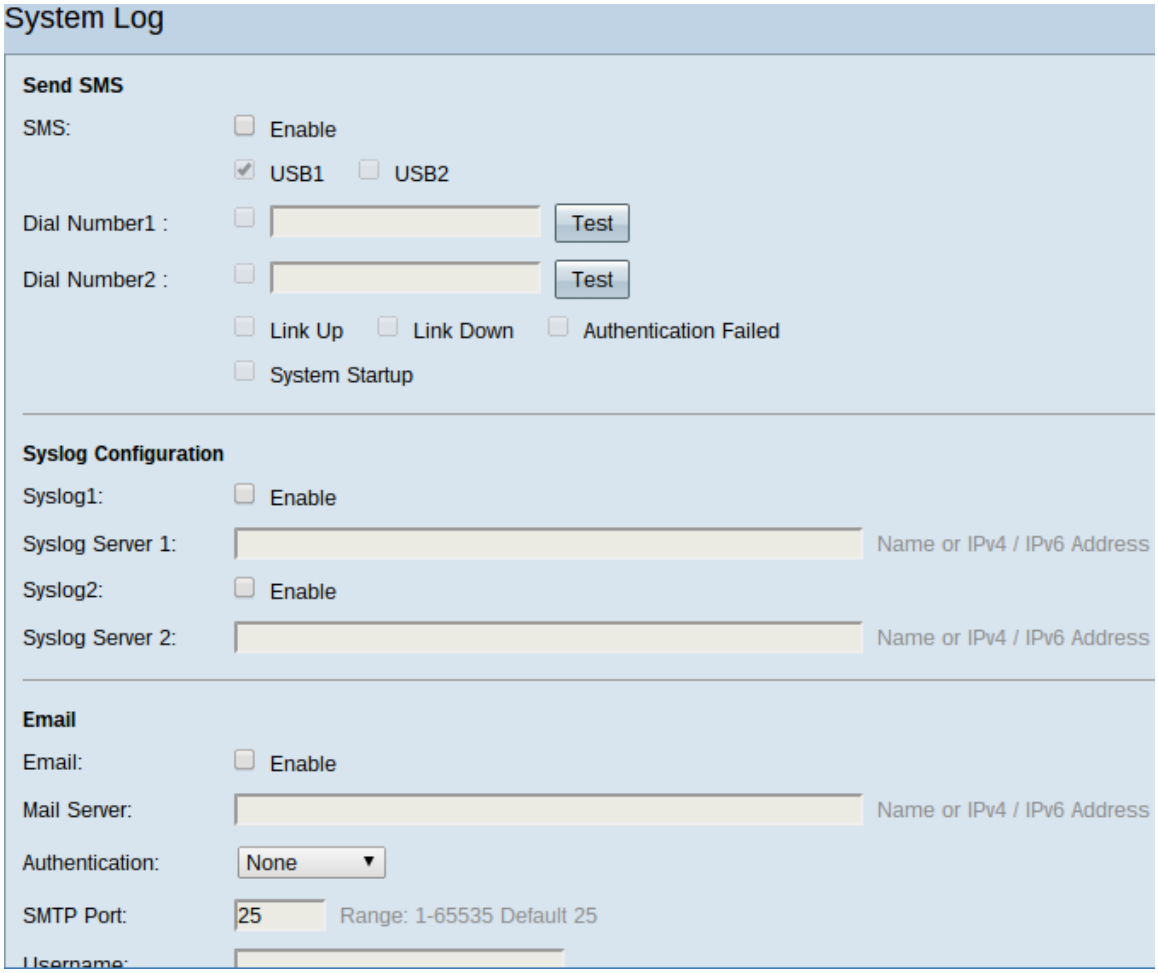
Routeur VPN double WAN · RV320
Routeur VPN double WAN Gigabit · RV325

Version du logiciel

•v 1.1.0.09

Configuration du journal système

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez **Log > System Log**. La page *Journal système* s'ouvre :



Reportez-vous aux sections suivantes pour obtenir des informations sur la page *Journal système*.

·Journaux système par SMS — Comment envoyer les journaux système à un téléphone par SMS.

·System Logs on System Log Servers — Comment envoyer les journaux système à un serveur de journaux système.

·Journaux du système de messagerie — Comment envoyer les journaux du système à une adresse de messagerie.

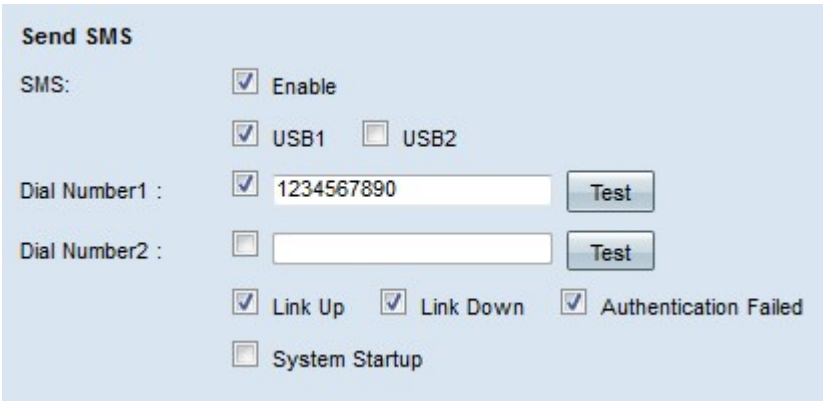
·Log Settings — Comment configurer le type de messages enregistrés dans le journal.

·Afficher le journal système — Comment afficher les journaux système sur le périphérique.

·View Outgoing Log Table — Comment afficher les journaux système qui se rapportent uniquement aux paquets sortants.

·View Incoming Log Table — Comment afficher les journaux système qui se rapportent uniquement aux paquets entrants.

Journaux système par SMS



Étape 1. Cochez **Enable** dans le champ SMS pour envoyer des journaux système à un client via des messages SMS (Short Message Service).

Étape 2. Cochez les cases des ports USB auxquels le modem USB 3G est connecté.

Étape 3. Cochez la case du champ Numéro1 et saisissez le numéro de téléphone vers lequel les messages sont envoyés.

Note: Cliquez sur **Test** pour tester la connexion au numéro 1. Si le numéro configuré ne reçoit pas le message de test, assurez-vous que le numéro de téléphone est entré correctement dans le champ Numéro1.

Étape 4. (Facultatif) Cochez la case du champ Numéro2 et saisissez le numéro de téléphone vers lequel les messages sont envoyés.

Note: Cliquez sur **Test** pour tester la connexion au numéro 2. Si le numéro configuré ne reçoit pas le message de test, assurez-vous que le numéro de téléphone est entré correctement dans le champ Numéro2.

Étape 5. Cochez les cases des événements qui déclencheront l'envoi d'un journal.

Liaison · : une connexion au RV320 a été établie.

Liaison · - Une connexion au RV320 a été désactivée.

Échec de l'authentification · : une authentification a échoué.

·Démarrage du système : le routeur est démarré.

Étape 6. Click **Save**. Les journaux système via SMS sont configurés.

Connexions système sur les serveurs de journal système

Étape 1. Cochez **Enable** dans le champ Syslog1 pour envoyer des journaux système à un serveur de journaux système.

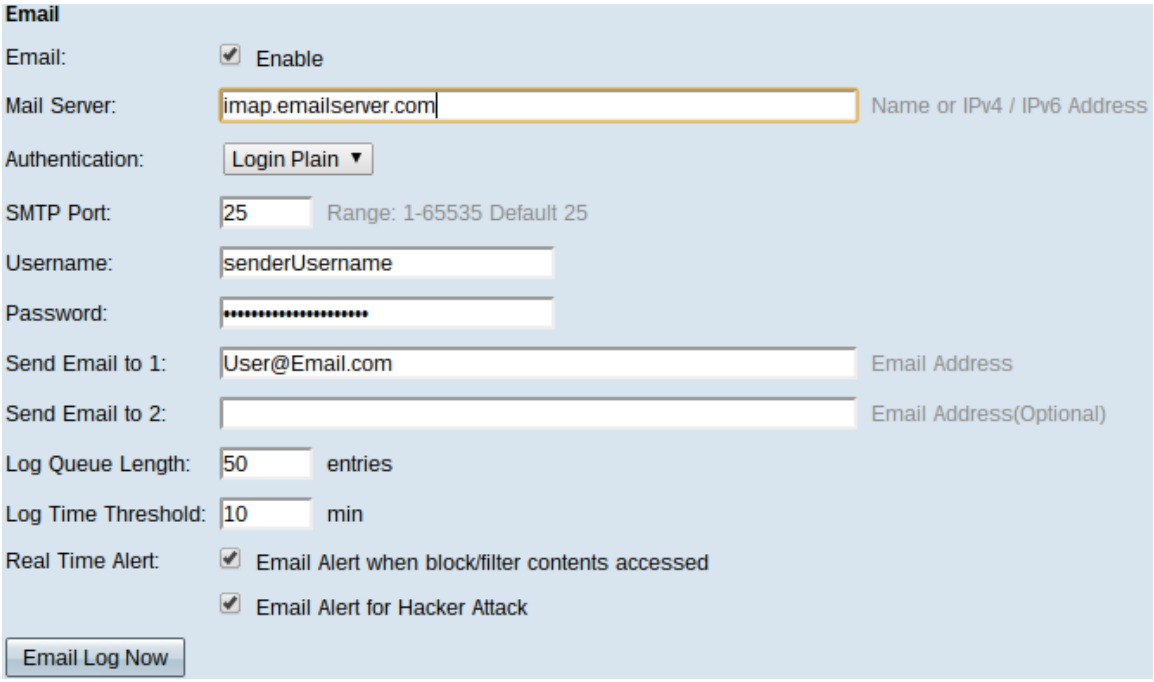
Étape 2. Saisissez le nom d'hôte ou l'adresse IP du serveur de journal système dans le champ Syslog Server 1.

Étape 3. (Facultatif) Pour envoyer des journaux à un autre serveur de journaux système, cochez la case **Activer** dans le champ Syslog2.

Étape 4. Si cette case est cochée dans le champ Syslog2, saisissez le nom d'hôte ou l'adresse IP du serveur de journal système dans le champ Syslog Server 2.

Étape 5. Click **Save**. Les journaux système via les serveurs de journaux système sont configurés.

Journaux du système de messagerie



Étape 1. Cochez **Activer** dans le champ Courrier électronique pour envoyer des journaux système à un destinataire par e-mail.

Étape 2. Saisissez le nom de domaine ou l'adresse IP du serveur de messagerie dans le champ Mail Server.

Étape 3. Sélectionnez le type d'authentification que le serveur de messagerie utilise dans le champ Authentication.

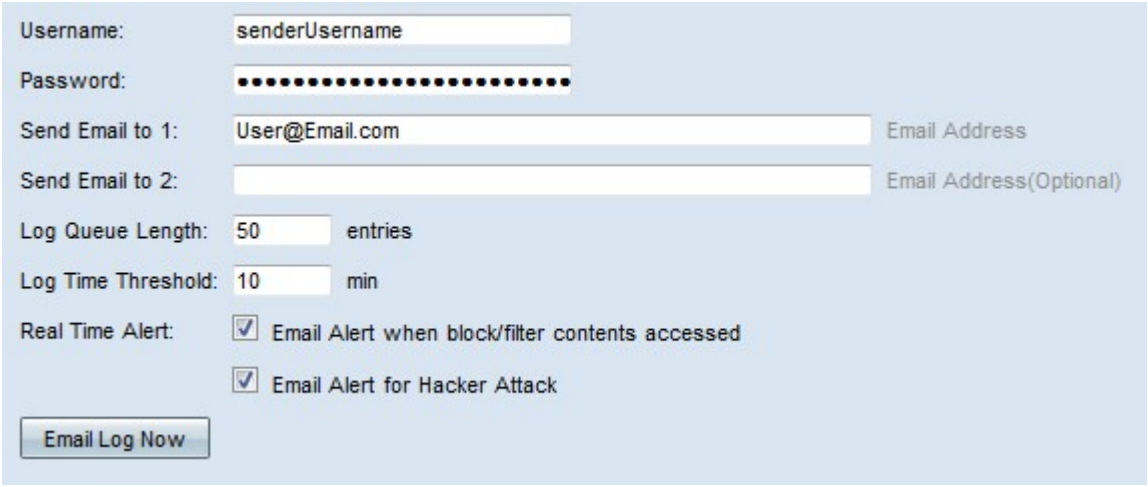
·Aucun : le serveur de messagerie n'utilise aucune authentification.

·Plaque de connexion : le serveur de messagerie utilise une authentification au format texte brut.

·TLS : le serveur de messagerie utilise la sécurité de la couche de transport (TLS) pour permettre au client et au serveur d'échanger des informations d'authentification en toute sécurité.

·SSL : le serveur de messagerie utilise SSL (Secure Sockets Layer) pour permettre au client et au serveur d'échanger des informations d'authentification en toute sécurité.

Étape 4. Saisissez le port SMTP (Simple Mail Transfer Protocol) que le serveur de messagerie utilise dans le champ Port SMTP. SMTP est un protocole qui permet de transmettre des e-mails sur des réseaux IP.



Étape 5. Saisissez le nom d'utilisateur de l'expéditeur de l'e-mail dans le champ Nom d'utilisateur.

Étape 6. Saisissez le mot de passe de l'expéditeur de l'e-mail dans le champ Password (Mot de passe).

Étape 7. Saisissez l'adresse e-mail du destinataire de l'e-mail dans le champ Send Email to 1.

Étape 8. (Facultatif) Saisissez une adresse e-mail supplémentaire à laquelle envoyer les courriels du journal dans le champ Send Email to 2.

Étape 9. Saisissez le nombre d'entrées de journal qui doivent être effectuées avant l'envoi du journal au destinataire de l'e-mail dans le champ Longueur de la file d'attente du journal.

Étape 10. Saisissez l'intervalle auquel le périphérique envoie le journal à l'e-mail dans le champ Log Time Threshold.

Étape 11. Cochez la première case du champ Alerte en temps réel pour envoyer immédiatement un e-mail lorsque quelqu'un, bloqué ou filtré, tente d'accéder au routeur.

Étape 12. Cochez la deuxième case du champ Real Time Alert pour envoyer un e-mail immédiatement lorsqu'un pirate tente d'accéder au routeur par le biais d'une attaque par déni de service (DOS).

Note: Cliquez sur **Journal des courriels maintenant** pour envoyer immédiatement le journal.

Étape 13. Click **Save**. Les journaux système par e-mail sont configurés.

Paramètres du journal

Étape 1. Cochez les cases des événements qui déclencheront une entrée de journal.

Journal d'alertes · : ces journaux sont créés lorsqu'une attaque ou une tentative d'attaque s'est produite.

- Inondation Syn : les requêtes SYN sont reçues plus rapidement que le routeur ne peut les traiter.

- IP Spoofing : le routeur RV320 a reçu des paquets IP avec des adresses IP source falsifiées.

- Tentative de connexion non autorisée - Une tentative de connexion refusée au réseau a échoué.

- Ping of Death : une requête ping d'une taille anormale a été envoyée à une interface pour tenter de bloquer le périphérique cible.

- Win Nuke : l'attaque DDOS (Distributed Denial of Service Attack) distante appelée WinNuke a été envoyée à une interface pour tenter de bloquer le périphérique cible.

·General Log : ces journaux sont créés lorsque des actions réseau générales se produisent.

- Deny Policies : l'accès a été refusé à un utilisateur en fonction des stratégies configurées du routeur.

- Connexion autorisée : un utilisateur a été autorisé à accéder au réseau.

- Messages d'erreur système - Une erreur système s'est produite.

- Autoriser les stratégies : l'accès a été accordé à un utilisateur en fonction des stratégies configurées du routeur.

- Noyau : inclut tous les messages du noyau dans le journal. Le noyau est la première partie du système d'exploitation qui se charge en mémoire au démarrage. Les messages du noyau sont des journaux associés au noyau.

- Modifications de configuration - La configuration du routeur a été modifiée.

- VPN IPSEC et PPTP - Une négociation, une connexion ou une déconnexion IPSEC et PPTP VPN s'est produite.

- VPN SSL : une négociation, une connexion ou une déconnexion VPN SSL s'est produite.

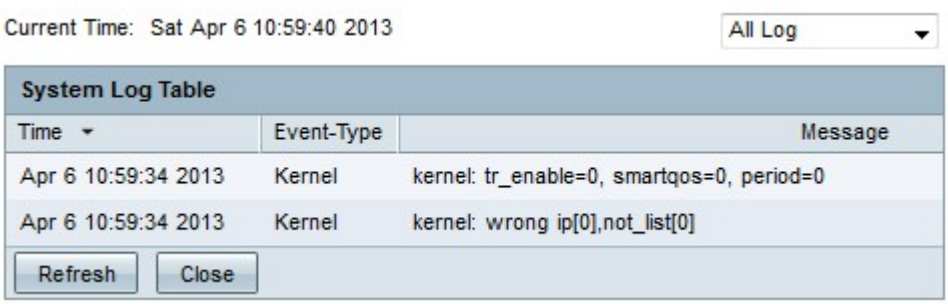
- Réseau : une connexion physique a été établie ou perdue sur les interfaces WAN ou DMZ.

Étape 2. Click **Save**. Les paramètres du journal sont configurés.

Note: Cliquez sur **Effacer le journal** pour effacer le journal en cours.

Afficher le journal système

Étape 1. Cliquez sur **Afficher le journal système** pour afficher la table des journaux système. La fenêtre *System Log Table* apparaît.



Étape 2. (Facultatif) Dans la liste déroulante, sélectionnez le type de journaux à afficher.

·All Log : inclut tous les messages du journal.

·System Log : inclut uniquement les messages d'erreur système.

·Firewall/DoS Log : inclut uniquement les journaux d'alertes.

·VPN Log : inclut uniquement les journaux VPN IPSec et PPTP et VPN SSL.

·Network Log : inclut uniquement les journaux réseau.

·Kernel Log : inclut uniquement les messages du noyau.

Journal des utilisateurs · : inclut uniquement les stratégies de refus, les stratégies d'autorisation, les journaux de modification de configuration et de connexion autorisés.

·SSL Log : inclut uniquement les journaux VPN SSL.

La table des journaux système affiche les informations suivantes.

·Time : heure à laquelle le journal a été créé.

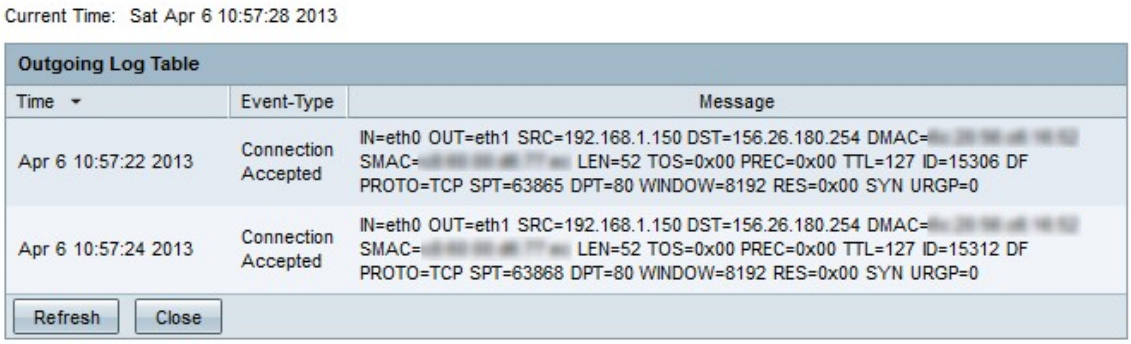
·Event-Type : type de journal.

Message · : informations qui correspondent au journal. Cela inclut le type de stratégie, l'adresse IP source et l'adresse MAC source.

Note: Cliquez sur **Actualiser** pour actualiser la table de journal.

Afficher la table des journaux sortants

Étape 1. Cliquez sur **Table des journaux sortants** pour afficher la table des journaux qui se rapporte uniquement aux paquets sortants. La fenêtre *Table des journaux sortants* apparaît.



La table des journaux sortants affiche les informations suivantes.

·Time : heure à laquelle le journal a été créé.

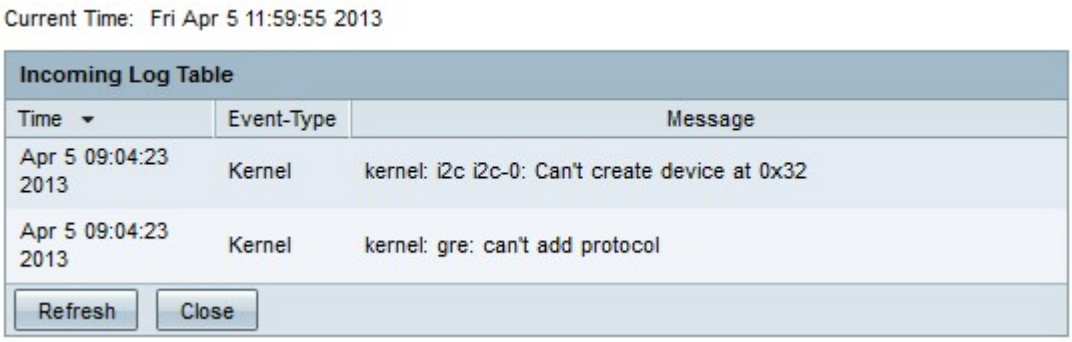
·Event-Type : type de journal.

Message · : informations qui correspondent au journal. Cela inclut le type de stratégie, l'adresse IP source et l'adresse MAC source.

Note: Cliquez sur **Actualiser** pour actualiser la table de journal.

Afficher la table du journal entrant

Étape 1. Cliquez sur **Incoming Log Table** pour afficher la table de journal qui se rapporte uniquement aux paquets entrants. La fenêtre *Table des journaux entrants* apparaît.



La table des journaux entrants affiche les informations suivantes.

·Time : heure à laquelle le journal a été créé.

·Event-Type : type de journal.

Message · : informations qui correspondent au journal. Cela inclut le type de stratégie, l'adresse IP source et l'adresse MAC source.

Note: Cliquez sur **Actualiser** pour actualiser la table de journal.