Configuration du journal système sur les routeurs VPN RV016, RV042, RV042G et RV082

Objectif

Un journal système (Syslog) est utilisé pour consigner les données de l'ordinateur. Vous pouvez définir les instances qui généreront un journal. Chaque fois qu'une instance se produit, l'heure et l'événement sont enregistrés et envoyés à un serveur syslog ou envoyés dans un e-mail. Syslog peut ensuite être utilisé pour analyser et dépanner un réseau tout en renforçant la sécurité du réseau.

Ce document explique la procédure de configuration d'un serveur Syslog sur les routeurs VPN RV016, RV042, RV042G et RV082.

Périphériques pertinents

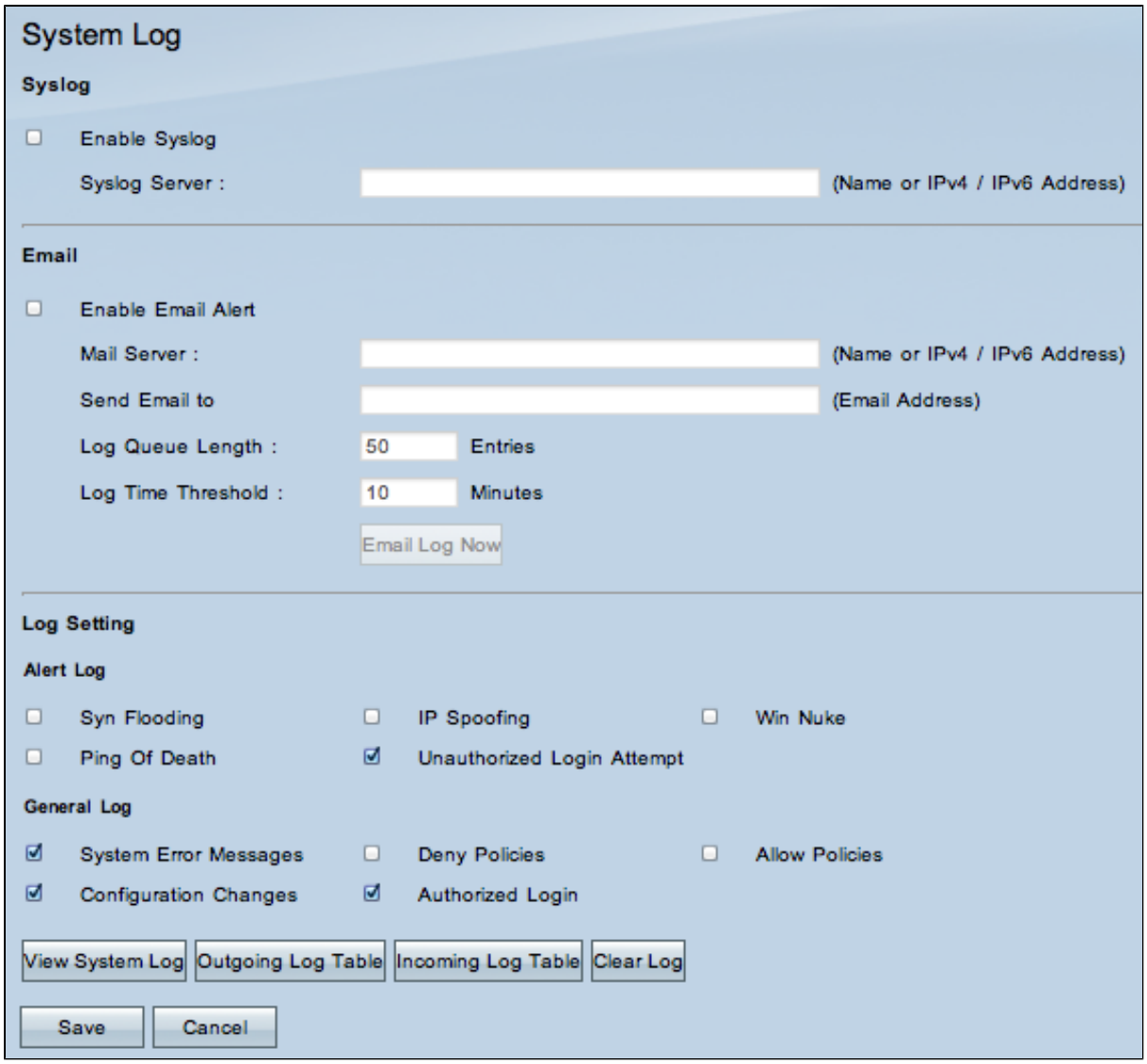
â€¢RV016
â€¢RV042
â€¢RV042G
â€¢RV082

Version du logiciel

â€¢v 4.2.1.02

Configuration de Syslog et des alertes

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



Syslog

Cette section explique comment permettre au routeur d'envoyer des fichiers journaux détaillés à votre serveur Syslog lorsque des événements sont consignés.

Étape 2. Cochez la case **Enable Syslog** pour activer le service Syslog sur le périphérique.

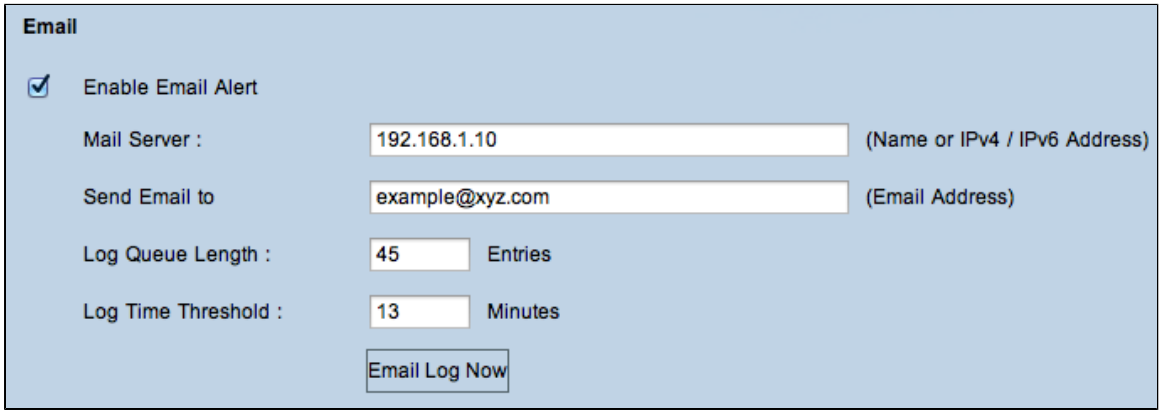
Gain de temps : passez à l'étape 4 si Syslog doit être désactivé.

Étape 3. Saisissez le nom de domaine ou l'adresse IP du serveur Syslog dans le champ Syslog server.

Courriel

Cette section explique comment permettre au routeur d'envoyer des alertes par e-mail lorsque des

événements sont consignés.



Étape 4. Cochez **Enable Email Alert** pour activer la fonctionnalité. Cela permet au routeur d'envoyer des alertes par e-mail à l'adresse électronique spécifiée par l'utilisateur.

Gain de temps : passez à l'étape 10 si l'alerte par e-mail doit être désactivée.

Étape 5. Saisissez l'adresse IPv4 ou IPv6 du serveur SMTP de votre FAI dans le champ Serveur de messagerie.

Remarque : votre FAI peut vous demander d'identifier votre routeur par un nom d'hôte. Choisissez **Setup > Network** pour définir le nom d'hôte de votre routeur.

Étape 6. Saisissez l'adresse e-mail à laquelle vous souhaitez envoyer les alertes dans le champ Envoyer un e-mail à.

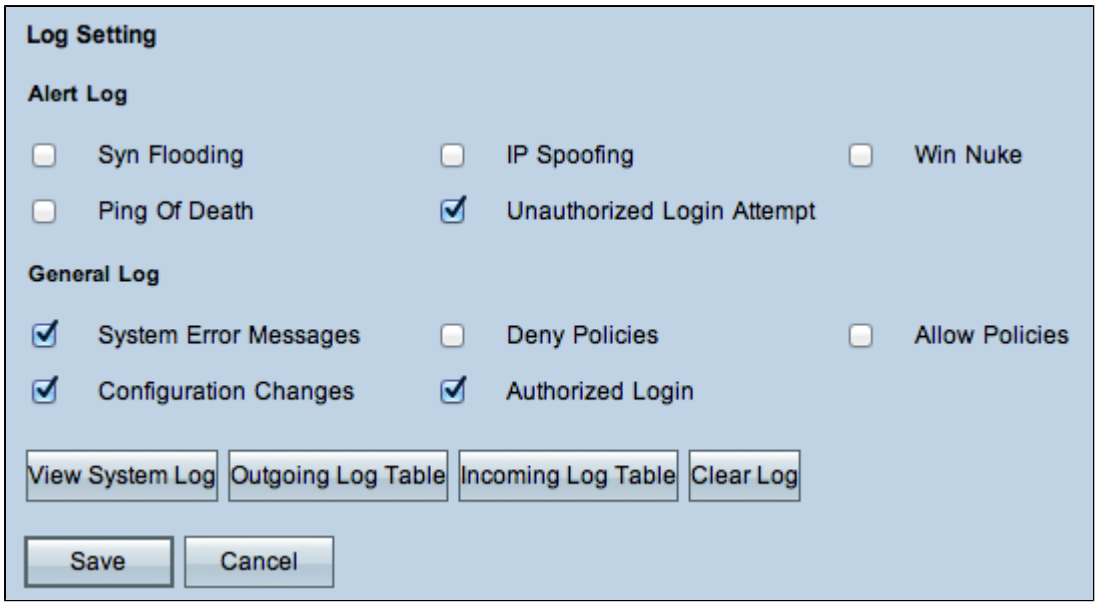
Étape 7. Saisissez le nombre d'entrées de journal à inclure dans l'e-mail dans le champ Longueur de la file d'attente du journal. Il est défini par défaut à 50.

Étape 8. Saisissez le nombre de minutes nécessaires à la collecte des données avant l'envoi du journal dans le champ Seuil de durée du journal. Le seuil de durée de journalisation est la durée d'attente maximale avant l'envoi d'un message dans le journal des e-mails. Lorsque le seuil de durée de connexion expire, un e-mail est envoyé, que le tampon du journal des e-mails soit plein ou non. La valeur par défaut est 10 minutes

Étape 9. (Facultatif) Cliquez sur **Email Log Now** pour envoyer instantanément un message à lâ€™adresse e-mail spécifiée afin de tester les paramètres.

Paramètre du journal

Cette section explique la variété d'événements qui peuvent être signalés dans les journaux :



Étape 10. La zone du journal d'alertes contient les types d'attaques et de tentatives de connexion non authentifiées les plus courants. Cochez les cases de n'importe quel type d'attaque souhaité pour les inclure dans le journal des événements ou décochez-les pour les omettre du journal des événements.

· Inondation SYN : le pirate envoie de nombreux paquets SYNC en continu, ce qui entraîne l'ouverture de plusieurs sessions par le routeur, de sorte que le trafic devient très encombré et le routeur refuse le trafic légitime.

· Usurpation IP : le pirate envoie des paquets à partir d'une adresse IP source falsifiée pour que l'attaque ressemble à du trafic légitime.

· Win Nuke : le pirate envoie un message hors bande à une machine Windows pour faire planter l'ordinateur cible.

· Ping of Death : le pirate envoie un paquet IP volumineux pour faire planter l'ordinateur cible.

· Tentative de connexion non autorisée - Une personne a tenté de se connecter à l'utilitaire de configuration du routeur sans authentification appropriée.

Étape 11. La zone Journal général inclut les actions effectuées pour appliquer les stratégies configurées ainsi que les événements de routine tels que les connexions autorisées et les modifications de configuration. Cochez la case de n'importe quel événement souhaité pour l'inclure dans le journal général. Décochez cette case pour l'omettre du journal général.

· System Error Messages : tous les messages d'erreur système.

· Deny Policies : instances dans lesquelles le routeur a refusé l'accès en fonction de vos règles d'accès.

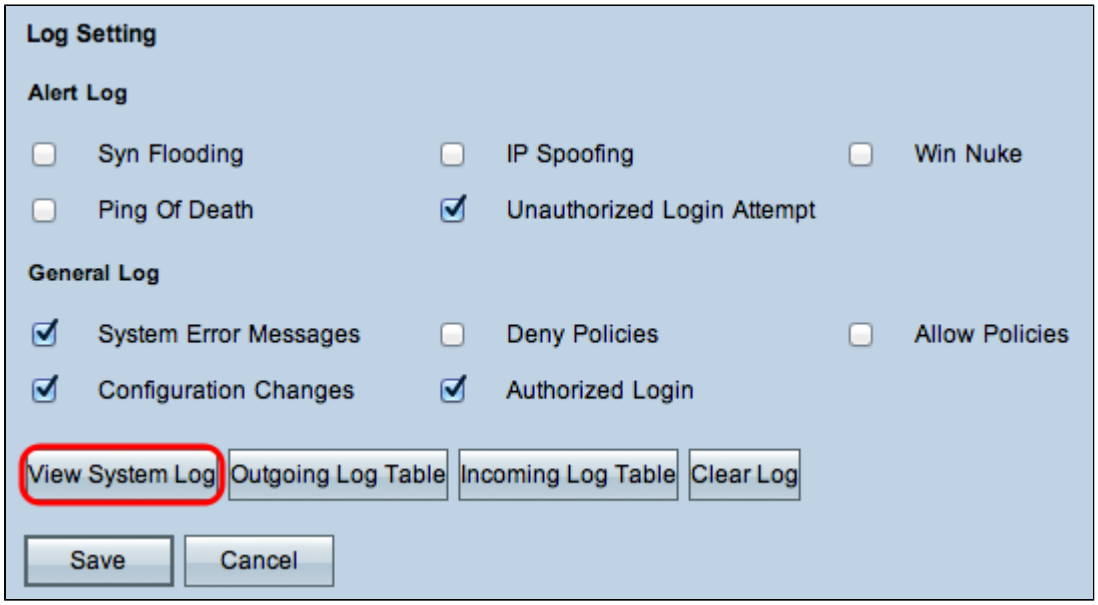
· Autoriser les stratégies â€" Instances où le routeur a autorisé l'accès en fonction de vos règles d'accès.

· Modification de la configuration â€" Instances où quelqu'un a enregistré des modifications dans la configuration.

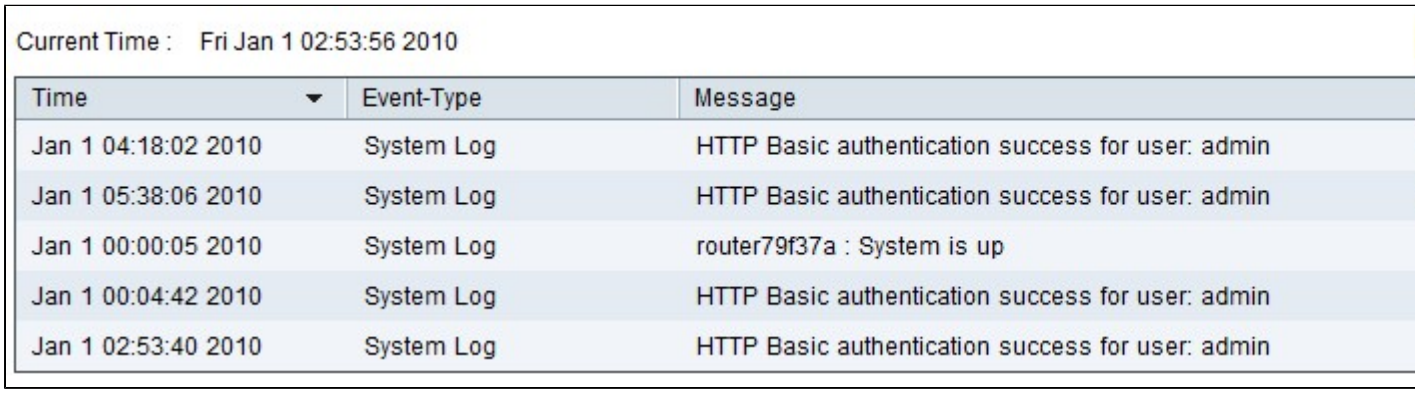
· Authorized Log In : cas où une personne s'est correctement connectée à l'utilitaire de configuration du routeur après avoir saisi le nom d'utilisateur et le mot de passe corrects.

· Événement de blocage de sortie â€" Instances dans lesquelles il y a un événement dans la réputation Web ProtectLink, ou filtrage d'URL.

Remarque : l'événement de blocage de sortie est uniquement disponible sur les routeurs VPN RV082.



Étape 12. (Facultatif) Pour afficher le journal système, cliquez sur **Afficher le journal système**. La fenêtre *System Log* s'affiche :



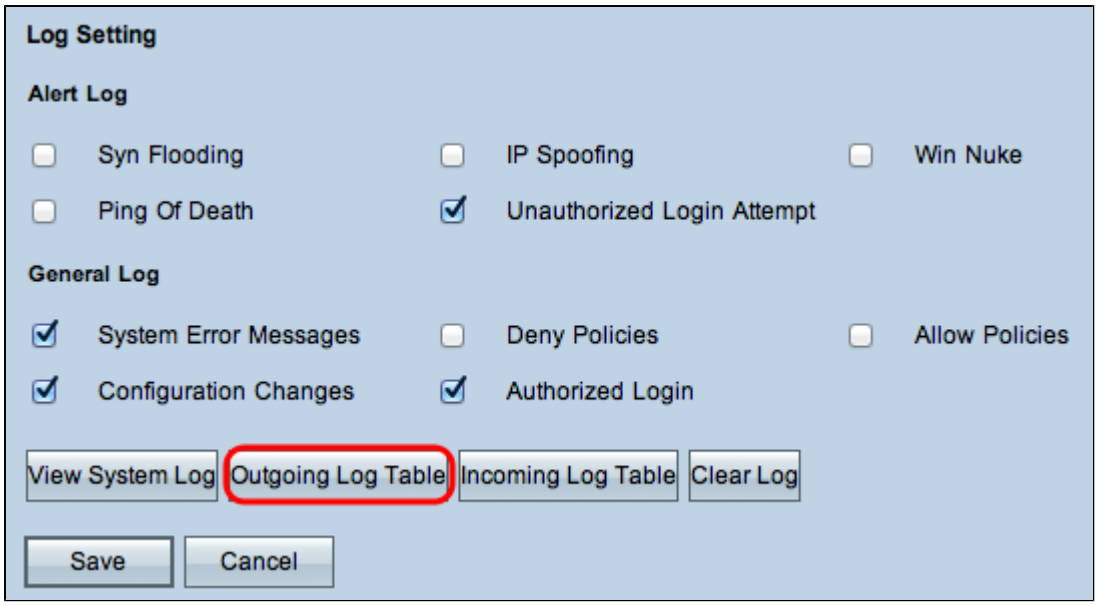
Remarque : les entrées du journal indiquent la date et l'heure du type d'événement et un message. Ce message indique le type de stratégie, comme la règle d'accès, l'adresse IP LAN de la source et l'adresse MAC.

Étape 13. Sélectionnez un journal particulier dans la liste déroulante.

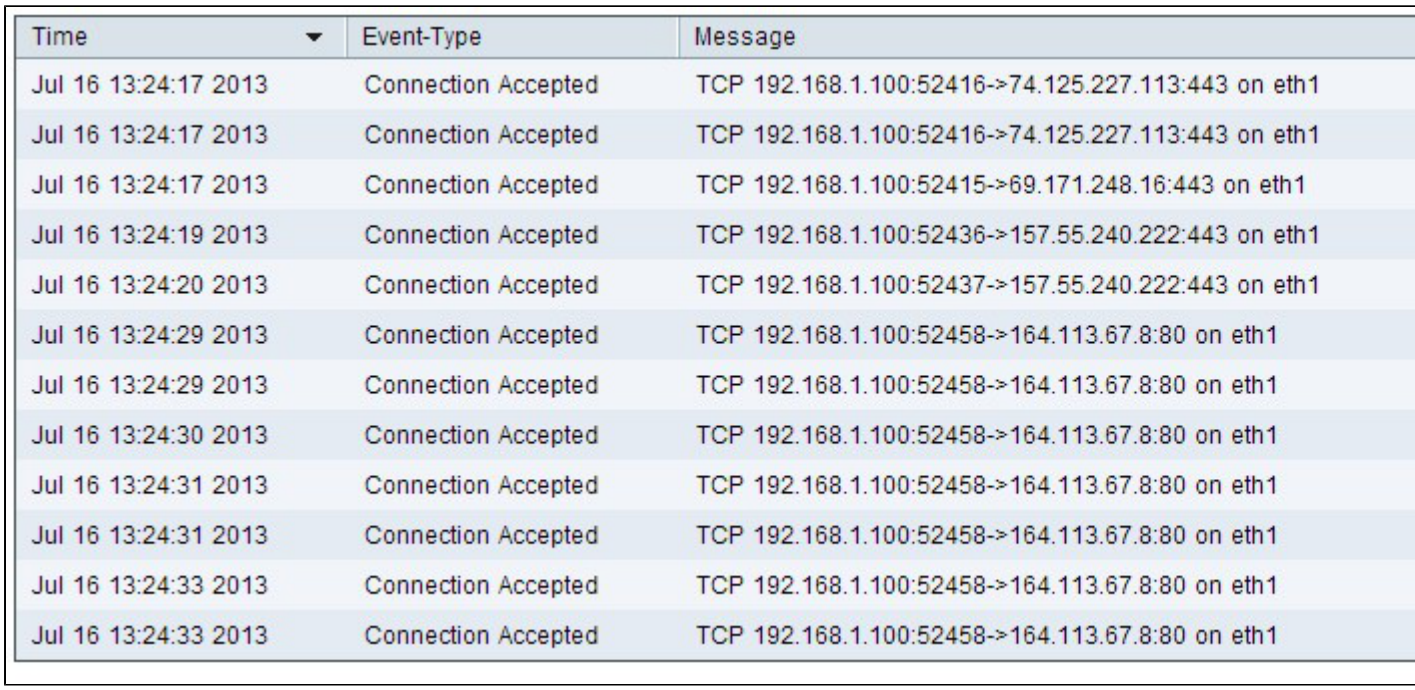
Étape 14. (Facultatif) Pour mettre à jour les données, cliquez sur **Refresh**.

Étape 15. (Facultatif) Pour effacer toutes les informations affichées, cliquez sur **Effacer**.

Étape 16. Cliquez sur **Close** pour fermer la fenêtre.



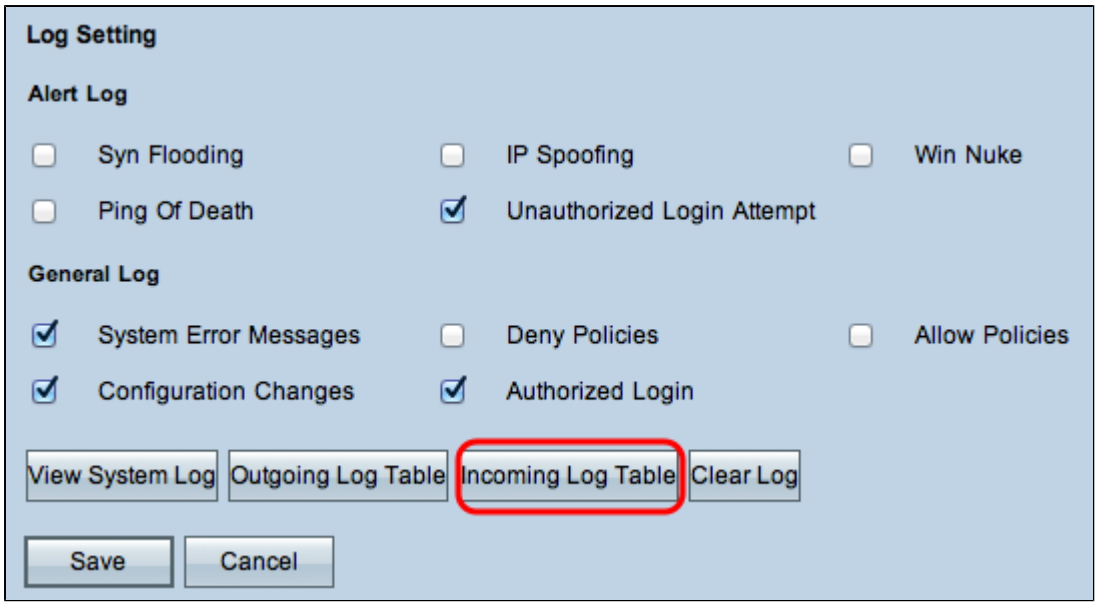
Étape 17. (Facultatif) Pour afficher les informations relatives aux paquets sortants, cliquez sur **Outgoing Log Table**. Les informations apparaissent dans une nouvelle fenêtre.



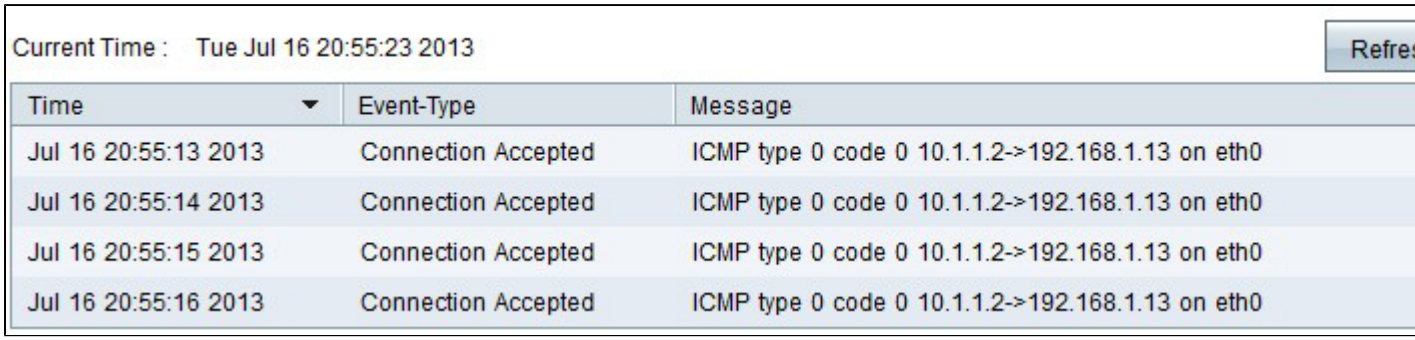
Time	Event-Type	Message
Jul 16 13:24:17 2013	Connection Accepted	TCP 192.168.1.100:52416->74.125.227.113:443 on eth1
Jul 16 13:24:17 2013	Connection Accepted	TCP 192.168.1.100:52416->74.125.227.113:443 on eth1
Jul 16 13:24:17 2013	Connection Accepted	TCP 192.168.1.100:52415->69.171.248.16:443 on eth1
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

Étape 18. (Facultatif) Pour mettre à jour les données, cliquez sur **Refresh**.

Étape 19. Cliquez sur **Fermer** pour fermer la fenêtre.

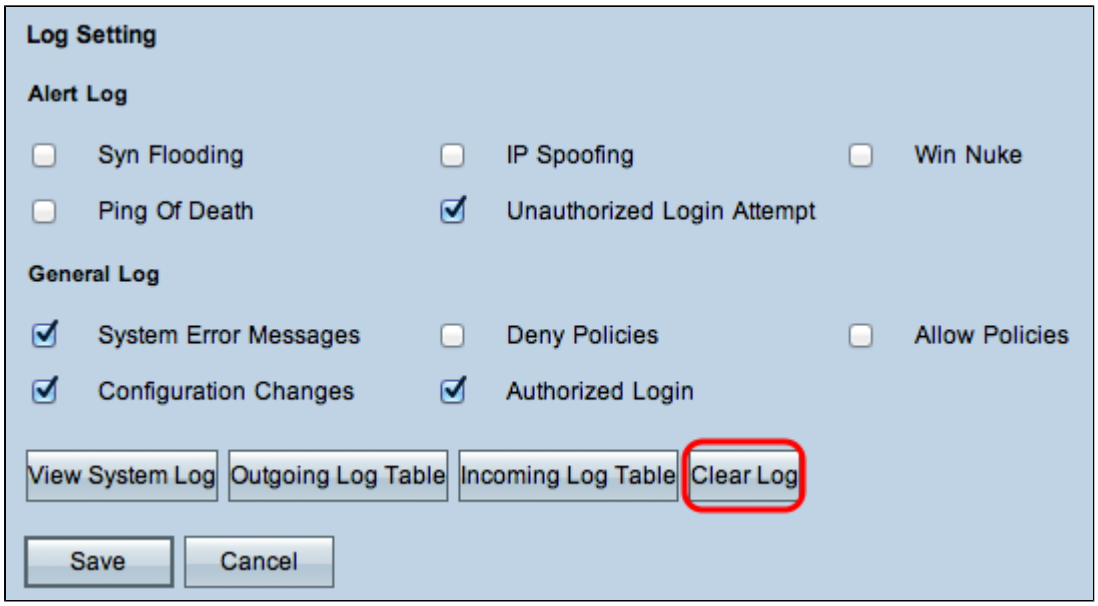


Étape 20. (Facultatif) Cliquez sur **Incoming Log Table** pour afficher les informations relatives aux paquets entrants. Les informations s'ouvrent dans une nouvelle fenêtre. Si un avertissement s'affiche à propos de la fenêtre contextuelle, autorisez le contenu bloqué.



Étape 21. (Facultatif) Pour mettre à jour les données, cliquez sur **Refresh**.

Étape 22. Cliquez sur **Fermer** pour fermer la fenêtre.



Étape 23. (Facultatif) Pour effacer le journal, cliquez sur **Clear Log Now**. Cliquez sur ce bouton

uniquement si vous n'avez pas besoin de les afficher à nouveau ultérieurement.

Étape 24. Cliquez sur **Save** pour enregistrer la configuration.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.