Dépannage des listes d'accès sur un réseau privé virtuel sur des routeurs VPN RV016, RV042, RV042G et RV082

Objectifs

Une liste de contrôle dâ€™accès (ACL) est un ensemble de conditions dâ€™autorisation et de refus. Une liste de contrôle dâ€™accès spécifie les processus utilisateur ou système auxquels lâ€™accès à des ressources spécifiques est accordé. Une liste de contrôle dâ€™accès peut bloquer toute tentative injustifiée dâ€™atteindre les ressources réseau. Le problème dans cette situation peut survenir lorsque vous avez des listes de contrôle dâ€™accès configurées sur les deux routeurs, mais que lâ€™un des routeurs ne peut pas faire la différence entre les listes de trafic autorisé et refusé autorisées par la liste de contrôle dâ€™accès. Zenmap, un outil open source utilisé pour vérifier le type de filtres de paquets/pare-feu actif, est utilisé pour tester la configuration.

Cet article explique comment dépanner les listes de contrôle d'accès autorisées qui ne fonctionnent pas sur un VPN passerelle à passerelle entre deux routeurs VPN.

Périphériques pertinents

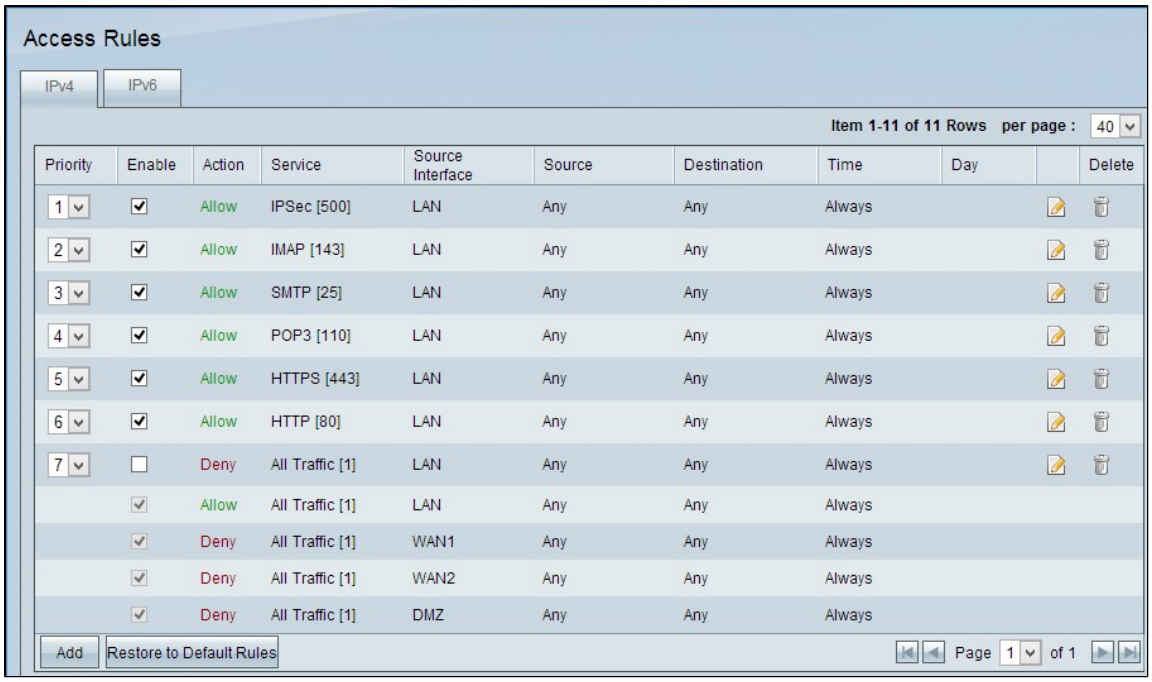
â€¢RV016
â€¢RV042
â€¢RV042G
â€¢RV082

Version du logiciel

â€¢v 4.2.2.08

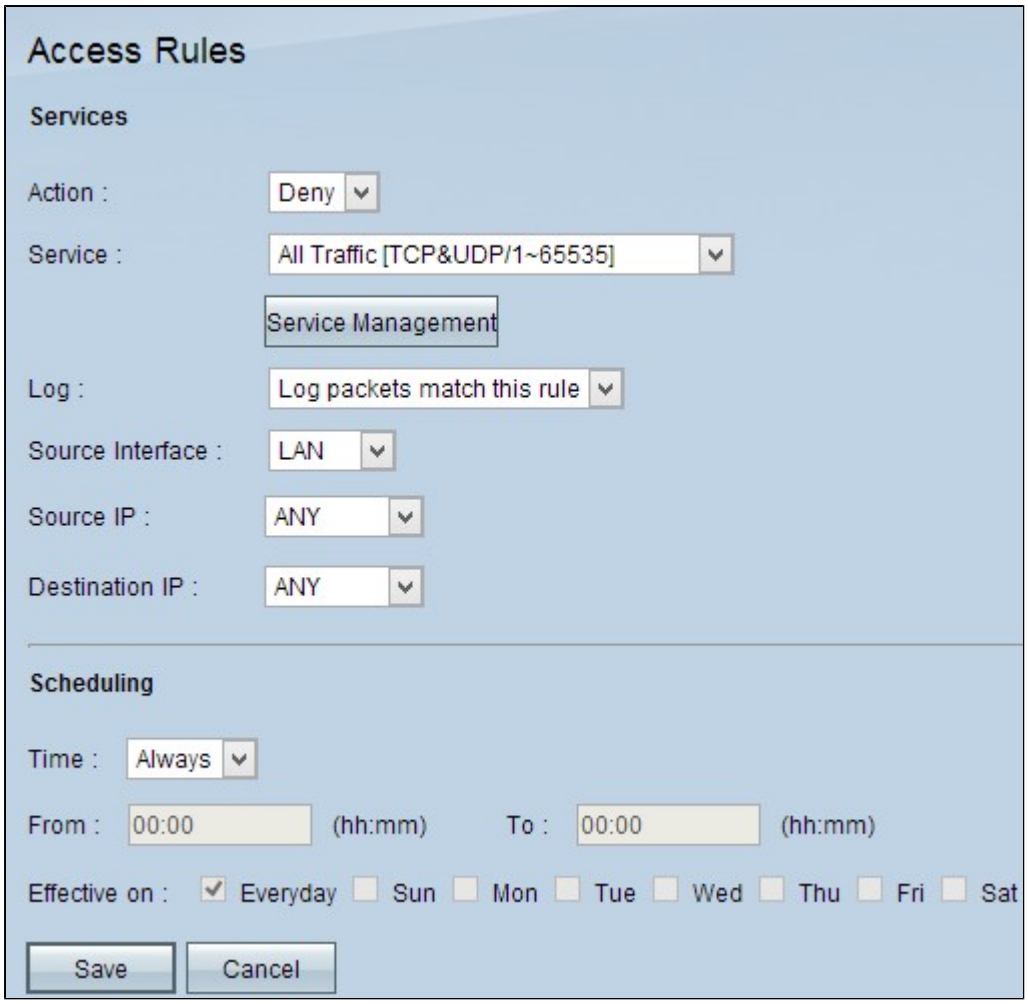
Configuration ACL sur VPN

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez **Firewall > Access Rules**. La page *Règle d'accès* s'ouvre :

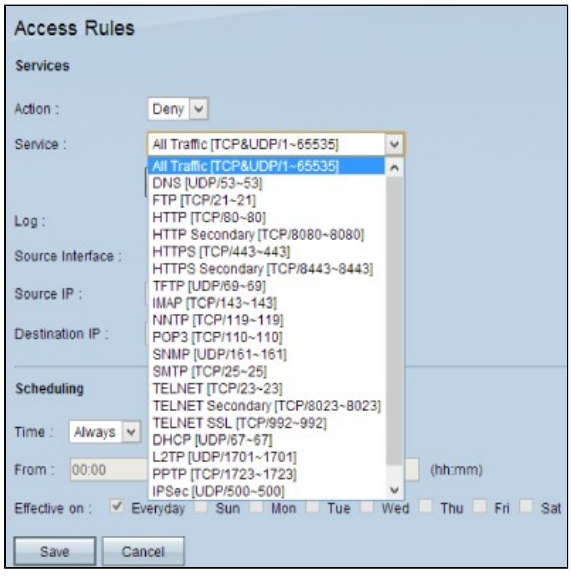


Remarque : les règles d'accès par défaut ne peuvent pas être modifiées. Les règles d'accès mentionnées dans l'image ci-dessus qui sont configurées par l'utilisateur peuvent être modifiées par le processus suivant.

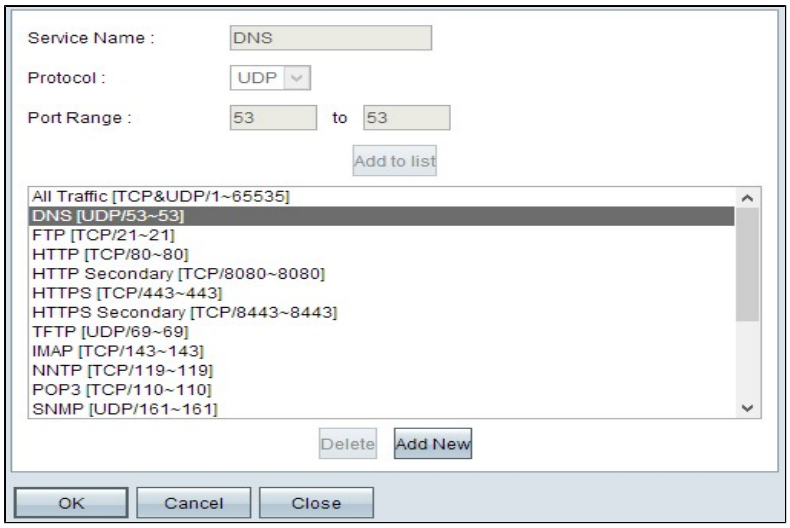
Étape 2. Cliquez sur le bouton **Add** pour ajouter une nouvelle règle d'accès. La page *Access Rules* change pour afficher les zones Services et Scheduling. L'ajout d'une règle d'accès est expliqué dans les étapes suivantes.



Étape 3. Choisissez **Deny** dans la liste déroulante Action pour refuser le service.



Étape 4. Sélectionnez le service requis qui est appliqué à la règle dans la liste déroulante **Service**.



Étape 5. (Facultatif) Pour ajouter un service qui ne figure pas dans la liste déroulante Service, cliquez sur **Gestion des services**. Dans la Gestion des services, un service peut être créé selon les besoins. Après la création d'un service, cliquez sur **OK** pour enregistrer les paramètres.

Étape 6. Choisissez **Log packets that match this rule** dans la liste déroulante Log for only logs that match ou **Not Log** pour les journaux qui ne correspondent pas à la règle d'accès.

Étape 7. Choisissez un type d'interface dans la liste déroulante Interface source qui est la source des règles d'accès. Les options disponibles sont les suivantes :

· LAN : sélectionnez LAN si l'interface source est le réseau local.

· WAN : sélectionnez WAN si l'interface source est le FAI.

· DMZ : sélectionnez DMZ si l'interface source est la zone démilitarisée.

· ANY : sélectionnez ANY pour faire de l'interface source l'une des interfaces mentionnées ci-dessus.

Étape 8. Dans la liste déroulante Source IP, sélectionnez la ou les adresses source qui s'appliquent à la règle d'accès. Les options disponibles sont les suivantes :

· Single : sélectionnez Single s'il s'agit d'une adresse IP unique et entrez l'adresse IP.

· Range : sélectionnez Range s'il s'agit d'une plage d'adresses IP et entrez la première et la dernière adresse IP de la plage.

· ANY : sélectionnez ANY pour appliquer les règles à toutes les adresses IP source.

Étape 9. Dans la liste déroulante Destination IP, sélectionnez la ou les adresses de destination souhaitées qui s'appliquent à la règle d'accès. Les options disponibles sont les suivantes :

· Single : sélectionnez Single s'il s'agit d'une adresse IP unique et entrez l'adresse IP.

· Range : sélectionnez Range s'il s'agit d'une plage d'adresses IP et saisissez la première et la dernière adresse IP de la plage.

· ANY : sélectionnez ANY pour appliquer les règles à toutes les adresses IP de destination.

Étape 10. Choisissez une méthode pour définir le moment où les règles sont actives dans la liste

déroulante Heure. Elles sont :

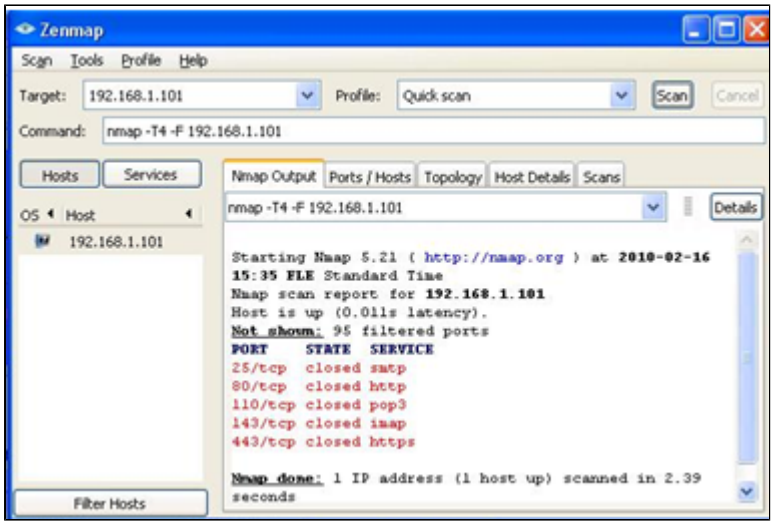
· Always : si vous choisissez Always dans la liste déroulante Time, les règles d'accès seront toujours appliquées au trafic.

· Interval : vous pouvez choisir un intervalle de temps spécifique auquel les règles d'accès sont actives si vous sélectionnez Interval dans la liste déroulante Time. Après avoir spécifié l'intervalle, cochez les cases des jours pendant lesquels vous souhaitez que les règles d'accès soient actives à partir du champ Effectif le.

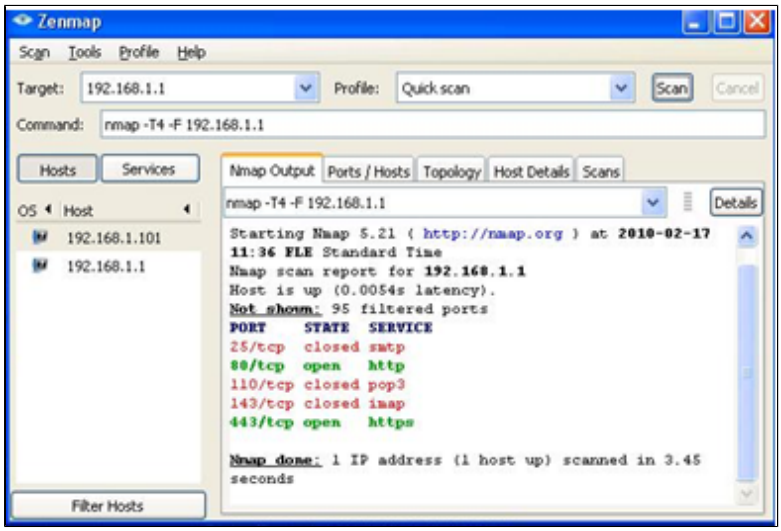
Étape 11. Cliquez sur **Save** pour enregistrer vos paramètres.

Étape 12. Répétez les étapes 2 à 10 avec les champs correspondant respectivement à celui affiché dans l'image. Les règles d'accès selon le client sont appliquées ici. Les 7 premiers autorisent certains services ; le 8 refuse tout autre trafic. Cette configuration est également effectuée sur le deuxième routeur. Le port IPSec 500 est autorisé.

Remarque : effectuez cette opération pour les deux routeurs afin de vérifier que les règles d'accès sont configurées comme vous le souhaitez.



Routeur VPN n° 1

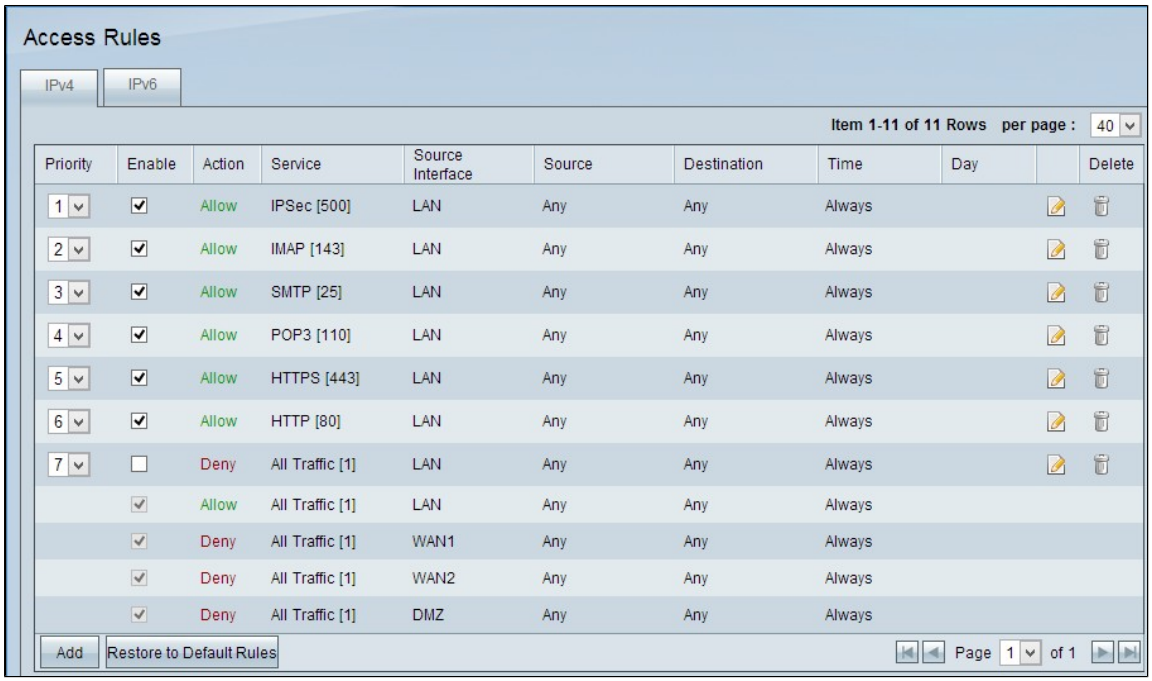


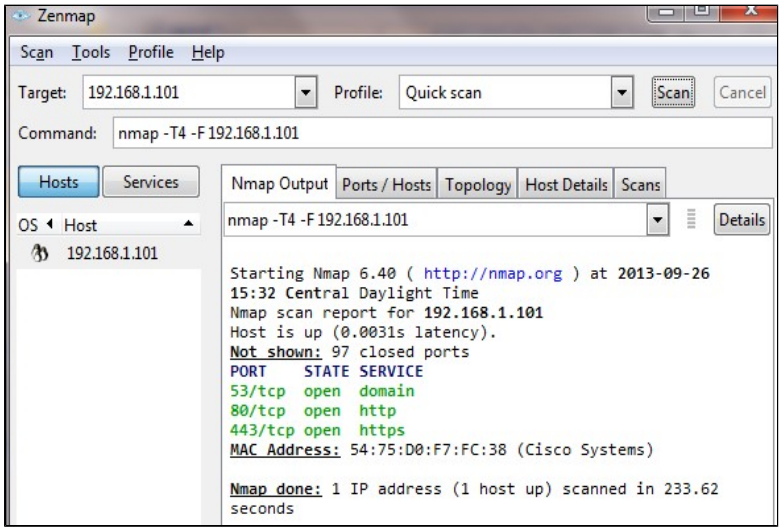
Routeur VPN n° 2

Étape 13. Installez Zenmap(NMAP) à partir de http://nmap.org/download.html et lancez-le sur un PC du réseau local 192.168.2.0.

Remarque : il s'agit du réseau local derrière le routeur avec les sept listes de contrôle d'accès supplémentaires. L'adresse IP cible (192.168.1.101) est un PC sur le réseau local de la passerelle distante.

Étape 14. Sélectionnez **Quick Scan** dans le profil et cliquez sur **Scan**. Grâce à cela, nous pouvons connaître les ports ouverts et filtrés selon les ACL, le résultat affiché est représenté dans l'image ci-dessus. Le résultat montre que ces ports sont fermés, quelles que soient les listes de contrôle d'accès autorisées configurées sur le RV0xx # 1. Si nous essayons de vérifier les ports vers l'IP LAN (192.168.1.1) de la passerelle distante, nous découvrons que les ports 80 et 443 sont ouverts (qui étaient fermés au PC 192.168.1.101).





La liste de contrôle dâ€™accès fonctionne correctement après la suppression de la 7e liste de contrôle dâ€™accès refusée et fonctionne correctement, comme nous pouvons le voir dans le résultat.

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.