Comment bloquer le trafic IPX à l'aide d'un filtre Ethertype sur le point d'accès

Contenu

Introduction

Ce document explique comment utiliser des filtres Ethertype pour bloquer le trafic IPX (Internetwork Packet Exchange) sur le point d'accès Cisco Aironet. Une situation typique dans laquelle cela est utile est lorsque les diffusions de serveur IPX étouffent la liaison sans fil, comme cela arrive parfois sur un réseau d'entreprise de grande taille.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document s'applique aux points d'accès Cisco Aironet qui exécutent VxWorks ou le logiciel Cisco IOS®.

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Connexion au point d'accès

Vous pouvez ouvrir le système de gestion du point d'accès via votre navigateur Web ou via le port série du point d'accès à l'aide d'un émulateur de terminal. Si vous ne savez pas comment vous connecter à un point d'accès, reportez-vous à Utilisation de l'interface du navigateur Web pour obtenir des instructions sur la façon de vous connecter à un point d'accès qui exécute VxWorks ou Utilisation de l'interface du navigateur Web pour vous connecter à un point d'accès qui exécute le logiciel Cisco IOS.

Configuration

Points d'accès qui exécutent VxWorks

Une fois que vous avez établi une connexion de navigateur au point d'accès, procédez comme suit pour configurer et appliquer un filtre pour bloquer le trafic IPX.

Créer un filtre

Procédez comme suit :

1. Dans le menu Setup, sélectionnez **Ethertype Filters**.
2. Dans le champ Set Name, tapez un nom de filtre (par exemple « BlockIPX ») et cliquez sur **Add New**.
3. Sur la page suivante, vous voyez Disposition par défaut. Les deux options sont *avant* et *bloc*. Choisissez **Forward** dans le menu déroulant.
4. Dans le champ Cas spéciaux, saisissez **0x8137** et cliquez sur **Ajouter nouveau**.
5. Une nouvelle fenêtre s'affiche avec les options suivantes :DispositionPriorité Durée de vie de monodiffusionDurée de vie de la multidiffusionAlertePour Disposition, sélectionnez **Block**. Laissez les autres options à leurs paramètres par défaut. Click OK.Vous revenez à l'écran Jeu de filtres Ethertype. Répétez les étapes 4 et 5 et ajoutez les types **0x8138**, **0x00ff** et **0x00e0**.

Appliquer le filtre

Une fois le filtre créé, il doit être appliqué à l'interface afin de prendre effet.

1. Revenir à la page Configuration. Dans la section Ports réseau de la ligne Ethernet, cliquez sur **Filtres**.
2. Vous voyez EtherType avec les paramètres de réception et de transfert. Dans chaque menu déroulant, sélectionnez le filtre que vous avez créé à l'étape 2 de la procédure Créer un filtre et cliquez sur **OK**. Cette étape active le filtre que vous avez créé.

Points d'accès exécutant le logiciel Cisco IOS

Créer un filtre

Procédez comme suit :

1. Cliquez sur **Services** dans la barre de navigation de la page.
2. Dans la liste de la page Services, cliquez sur **Filtres**.
3. Sur la page Apply Filters, cliquez sur l'onglet **Ethertype Filters** en haut de la page.
4. Assurez-vous que **NEW** (la valeur par défaut) est sélectionné dans le menu Create/Edit Filter Index. Si vous souhaitez modifier un filtre existant, sélectionnez le numéro de filtre dans le menu Créer/Modifier un index de filtre.
5. Dans le champ Index de filtre, nommez le filtre par un nombre compris entre 200 et 299. Le numéro que vous attribuez crée une liste de contrôle d'accès (ACL) pour le filtre.
6. Entrez **0x8137** dans le champ Add Ethertype.
7. Laissez le masque de l'Ethernet dans le champ Masque à la valeur par défaut.
8. Choisissez **Bloquer** dans le menu Action.
9. Cliquez sur **Add**. Le type d'Ethernet apparaît dans le champ Classes de filtres.
10. Afin de supprimer l'Ethernet de la liste Classes de filtres, sélectionnez-le et cliquez sur **Supprimer la classe**. Répétez les étapes 6 à 9 et ajoutez les types **0x8138**, **0x00ff** et **0x00e0** au filtre.
11. Choisissez **Transférer tout** dans le menu Action par défaut. Comme vous bloquez tous les paquets IPX avec ce filtre, vous devez avoir une action par défaut qui s'applique à tous les autres paquets.
12. Cliquez sur Apply.

Appliquer le filtre

Àce stade, le filtre a été enregistré sur le point d'accès, mais il n'est activé que lorsque vous l'appliquez sur la page Appliquer les filtres.

1. Cliquez sur l'onglet **Appliquer les filtres** pour revenir à la page Appliquer les filtres.
2. Sélectionnez le numéro de filtre dans l'un des menus déroulants Ethertype. Vous pouvez appliquer le filtre à l'un ou l'autre des ports Ethernet et radio, ainsi qu'à l'un ou l'autre des paquets entrants et sortants.
3. Cliquez sur Apply. Le filtre est activé sur les ports sélectionnés.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Assistance produit LAN sans fil

- Prise en charge de la technologie LAN sans fil
- Logiciel LAN sans fil
- Support et documentation techniques - Cisco Systems