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

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Conventions
Connectez au Point d'accès
Configuration
Points d'accès qui exécutent VxWorks
Points d'accès qui exécutent le logiciel de Cisco IOS
Vérifier
Dépanner
Informations connexes

Introduction

Ce document explique comment utiliser des filtres d'Ethertype pour bloquer le trafic de l'Internetwork Packet Exchange (IPX) sur le Point d'accès de Cisco Aironet. Une situation typique dans laquelle c'est utile est quand les émissions de serveur IPX obstruent la liaison sans fil, comme se produit parfois sur un grand réseau d'entreprise.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Ce document applique à Cisco Aironet les Points d'accès qui exécutent VxWorks ou logiciel de Cisco IOS®.

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). 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.

Connectez au Point d'accès

Vous pouvez ouvrir le système de gestion du Point d'accès par votre navigateur Web ou par le port série de Point d'accès avec un terminal emulator. Si vous êtes peu familier avec la façon se connecter à un Point d'accès, vous rapportez utilisant l'interface de navigateur Web pour des directions sur la façon dont se connecter à un Point d'accès qui exécute VxWorks, ou employer l'interface de web browser pour se connecter à un Point d'accès qui exécute le logiciel de Cisco IOS.

Configuration

Points d'accès qui exécutent VxWorks

Une fois que vous avez établi une connexion de navigateur au Point d'accès, exécutez ces étapes pour configurer et appliquer un filtre pour bloquer le trafic IPX.

Créez un filtre

Procédez comme suit :

1. Sous le menu Setup, choisissez les **filtres d'Ethertype**.
2. Dans la zone d'identification réglée, introduisez un nom du filtre (par exemple, « BlockIPX ») et cliquez sur Add **nouveau**.
3. Sur la page suivante, vous voyez la disposition par défaut. Les deux options sont *en avant* et *bloc*. Choisissez **en avant du** menu déroulant.
4. Dans les cas particuliers mettez en place, écrivez **0x8137** et cliquez sur Add **nouveau**.
5. Une nouvelle fenêtre est affichée avec ces options :DispositionPrioritéTime to Live d'UnicastTime to Live de MultidiffusionAlertePour la disposition, choisissez le **bloc**. Laissez les autres options à leurs valeurs par défaut. Cliquez sur **OK**.Vous êtes retourné à l'écran réglé de filtre d'Ethertype. Répétez l'étape 4 et l'étape 5, et ajoutez les types **0x8138**, **0x00ff**, et **0x00e0**.

Appliquez le filtre

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

1. Revenez à la page d'installation. Sous la section de ports de réseau sur les Ethernets marqués par ligne, le clic **filtre**.
2. Vous voyez EtherType avec recevoir et expédier des configurations. De chaque menu déroulant, choisissez le filtre que vous avez créé dans l'étape 2 de la création une procédure de filtre et cliquez sur OK. Cette étape lance le filtre que vous avez créé.

Points d'accès qui exécutent le logiciel de Cisco IOS

Créez un filtre

Procédez comme suit :

1. **Services de** clic dans la barre de navigation de page.
2. Dans la liste de page de services, le clic **filtre**.
3. Sur l'application les filtres paginent, cliquent sur l'onglet de **filtres d'Ethertype** en haut de la page.
4. Assurez-vous que **NOUVEAU** (le par défaut) est sélectionné dans le menu d'index de filtre de Create/Edit. Si vous souhaitez éditer un filtre existant, sélectionnez le nombre de filtre du menu d'index de filtre de Create/Edit.
5. Dans le domaine d'index de filtre, nommez le filtre avec un nombre de 200 à 299. Le nombre que vous assignez crée une liste de contrôle d'accès (ACL) pour le filtre.
6. Écrivez **0x8137** dans le domaine d'Ethertype d'ajouter.
7. Laissez le masque pour l'Ethertype dans le masque pour mettre en place à la valeur par défaut.
8. Choisissez le **bloc du** menu Action.
9. Cliquez sur **Add**. L'Ethertype apparaît dans le domaine de classes de filtres.
10. Afin de retirer l'Ethertype de la liste de classes de filtres, le sélectionner et cliquer sur Delete la **classe**. Répétez l'étape 6 à l'étape 9, et ajoutez les types **0x8138**, **0x00ff**, et **0x00e0 au** filtre.
11. Choisissez **en avant tous du** menu d'action par défaut. Puisque vous bloquez tous les paquets IPX avec ce filtre, vous devez avoir une action par défaut qui s'applique à tous autres paquets.
12. Cliquez sur **Apply**.

Appliquez le filtre

Le filtre a été en ce moment enregistré sur le Point d'accès, mais il n'est pas activé jusqu'à ce que vous l'appliquiez à la page de filtres d'application.

1. Cliquez sur l'onglet de **filtres d'application** pour retourner à la page de filtres d'application.
2. Sélectionnez le nombre de filtre d'un des menus déroulants d'Ethertype. Vous pouvez appliquer le filtre au l'un ou l'autre ou les Ethernets et des ports radios, et à l'un ou l'autre ou les paquets entrants et sortants.
3. Cliquez sur **Apply**. Le filtre est activé sur les ports sélectionnés.

Vérifier

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

Dépanner

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

Informations connexes

- Support de produit LAN sans fil
- Support de technologie LAN sans fil
- Logiciel Sans fil de RÉSEAU LOCAL
- Support et documentation techniques - Cisco Systems