Blockieren von IPX-Datenverkehr mithilfe eines Ethertype-Filters auf dem Access Point

Inhalt

Einführung

In diesem Dokument wird erläutert, wie Ethernet-Typfilter verwendet werden, um Internetwork Packet Exchange (IPX)-Datenverkehr auf dem Cisco Aironet Access Point zu blockieren. Eine typische Situation, in der dies nützlich ist, ist, wenn IPX-Server-Broadcasts die Wireless-Verbindung blockieren, wie es manchmal in einem großen Unternehmensnetzwerk der Fall ist.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument gilt für Cisco Aironet Access Points, die entweder VxWorks oder Cisco IOS® Software ausführen.

Die in diesem Dokument enthaltenen Informationen wurden aus Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Sie in einem Live-Netzwerk arbeiten, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen, bevor Sie es verwenden.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Herstellen einer Verbindung zum Access Point

Sie können das Verwaltungssystem des Access Points über Ihren Webbrowser oder über den seriellen Anschluss des Access Points mit einem Terminal-Emulator öffnen. Wenn Sie nicht wissen, wie Sie eine Verbindung zu einem Access Point herstellen, finden Sie unter Verwenden der Webbrowserschnittstelle Anweisungen zum Herstellen einer Verbindung zu einem Access Point, der VxWorks ausführt, oder Verwenden der Webbrowser-Schnittstelle zum Herstellen einer Verbindung mit einem Access Point, auf dem die Cisco IOS-Software ausgeführt wird.

Konfiguration

Access Points, die VxWorks ausführen

Wenn Sie eine Browserverbindung zum Access Point hergestellt haben, führen Sie die folgenden Schritte aus, um einen Filter zu konfigurieren und anzuwenden, um IPX-Datenverkehr zu blockieren.

Filter erstellen

Gehen Sie wie folgt vor:

1. Wählen Sie im Menü Setup (Einrichtung) die Option **Ethertype-Filter aus**.
2. Geben Sie im Feld Name festlegen einen Filternamen ein (z. B. "BlockIPX"), und klicken Sie auf **Neu hinzufügen**.
3. Auf der nächsten Seite sehen Sie die Standardeinstellung. Die beiden Optionen sind *vorwärts* und *blockweise*. Wählen Sie im Dropdown-Menü **nach vorn** aus.
4. Geben Sie im Feld Sonderfälle **0x8137 ein** und klicken Sie auf **Neu hinzufügen**.
5. Ein neues Fenster wird mit den folgenden Optionen angezeigt:DispositionPrioritätUnicast-Zeit bis zum StartMulticast-Zeit bis zur InbetriebnahmeWarnungWählen Sie als Disposition die Option **Block**. Lassen Sie die anderen Optionen in den Standardeinstellungen unverändert. Klicken Sie auf **OK**.Sie kehren zum Bildschirm "Ethertype Filter Set" zurück. Wiederholen Sie Schritt 4 und Schritt 5, und fügen Sie die Typen **0x8138**, **0x00ff** und **0x00e0 hinzu**.

Filter anwenden

Nachdem der Filter erstellt wurde, muss er auf die Schnittstelle angewendet werden, um wirksam zu werden.

1. Kehren Sie zur Seite Setup zurück. Klicken Sie im Abschnitt "Netzwerkports" in der Zeile "Ethernet" auf **Filter**.
2. Sie sehen EtherType mit den Einstellungen für Empfangen und Weiterleiten. Wählen Sie aus jedem Dropdown-Menü den Filter aus, den Sie in Schritt 2 der Prozedur Filter erstellen erstellt haben, und klicken Sie auf **OK**. Dieser Schritt aktiviert den von Ihnen erstellten Filter.

Access Points, die Cisco IOS Software ausführen

Filter erstellen

Gehen Sie wie folgt vor:

1. Klicken Sie in der Navigationsleiste der Seite auf **Services**.
2. Klicken Sie in der Liste Dienste auf **Filter**.
3. Klicken Sie auf der Seite Filter anwenden auf die Registerkarte **Ethertype-Filter** oben auf der Seite.
4. Vergewissern Sie sich, dass **NEU** (Standard) im Menü Filter-Index erstellen/bearbeiten ausgewählt ist. Wenn Sie einen vorhandenen Filter bearbeiten möchten, wählen Sie die Filternummer im Menü Filter erstellen/bearbeiten aus.
5. Geben Sie im Feld Filter Index (Filterindex) dem Filter einen Namen mit einer Zahl zwischen 200 und 299. Durch die zugewiesene Nummer wird eine Zugriffskontrollliste (ACL) für den Filter erstellt.
6. Geben Sie **0x8137** im Feld Add Ethertype ein.
7. Lassen Sie die Maske für den Ethertype im Feld Maske den Standardwert.
8. Wählen Sie **Block** im Menü Aktion aus.
9. Klicken Sie auf **Hinzufügen**. Der Ethertype wird im Feld Filterklassen angezeigt.
10. Um den Ethertype aus der Liste Filterklassen zu entfernen, wählen Sie ihn aus, und klicken Sie auf **Klasse löschen**. Wiederholen Sie die Schritte 6 bis 9, und fügen Sie dem Filter die Typen **0x8138**, **0x00ff** und **0x00e0** hinzu.
11. Wählen Sie im Menü Standardaktion die Option **Alle weiterleiten** aus. Da Sie alle IPX-Pakete mit diesem Filter blockieren, müssen Sie eine Standardaktion haben, die für alle anderen Pakete gilt.
12. Klicken Sie auf **Übernehmen**.

Filter anwenden

Der Filter wurde zu diesem Zeitpunkt auf dem Access Point gespeichert, ist jedoch erst aktiviert, wenn Sie ihn auf der Seite Filter anwenden anwenden anwenden.

1. Klicken Sie auf die Registerkarte **Filter anwenden**, um zur Seite Filter anwenden zurückzukehren.
2. Wählen Sie die Filternummer aus einem der Dropdown-Menüs Ethertype aus. Sie können den Filter entweder auf den Ethernet- und den Funkport oder auf eingehende und ausgehende Pakete anwenden.
3. Klicken Sie auf **Übernehmen**. Der Filter ist auf den ausgewählten Ports aktiviert.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung

verfügbar.

Zugehörige Informationen

- Produktsupport für Wireless LAN
- Unterstützung von Wireless LAN-Technologie
- Wireless LAN-Software
- Technischer Support und Dokumentation - Cisco Systems