

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Onde criar ACL](#)

[Filtros do MAC address](#)

[Filtros IP](#)

[Filtros de Ethertype](#)

Introdução

Este documento descreve como configurar o Access Control List (ACL) - filtros baseados nos Access point do Cisco Aironet (AP) com uso do GUI.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento básico destes assuntos:

- A configuração de uma conexão Wireless com uso de Aironet AP e um adaptador cliente do a/b/g do 802.11 de Aironet
- ACL

Componentes Utilizados

Este documento usa o 1040 Series AP de Aironet que executa o Software Release 15.2(2)JB do [®] do Cisco IOS.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Você pode usar filtros em AP a fim executar estas tarefas:

- Restrinja o acesso à rede do Wireless LAN (WLAN)
- Forneça uma camada adicional de segurança Wireless

Você pode usar tipos diferentes de filtrar tráfego dos filtros baseado sobre:

- Protocolos específicos
- O MAC address do dispositivo do cliente
- O endereço IP de Um ou Mais Servidores Cisco ICM NT do dispositivo do cliente

Você pode igualmente permitir filtros a fim restringir o tráfego dos usuários no LAN ligado com fio. Os filtros do endereço IP de Um ou Mais Servidores Cisco ICM NT e do MAC address permitem ou recusam a transmissão do unicast e dos pacotes de transmissão múltipla que são enviados a ou dos endereços específicos IP ou MAC.

Os filtros com base nos protocolos fornecem uma maneira mais granulada de restringir o acesso aos protocolos específicos através dos Ethernet e das interfaces de rádio do AP. Você pode usar qualquer um destes métodos a fim configurar os filtros nos AP:

- Web GUI
- CLI

Este documento explica como usar ACL a fim configurar filtros com o GUI.

Nota: Para obter mais informações sobre da configuração com o uso do CLI, refira o artigo de Cisco do [exemplo da configuração de filtro do Access point ACL](#).

Configurar

Esta seção descreve como configurar filtros ACL-baseados no Cisco Aironet AP com uso do GUI.

Onde criar ACL

Navegue à **Segurança** > à **Segurança do avanço**. Escolha a aba da lista de acessos da **associação**, e o clique **define o filtro**:

The screenshot shows the Cisco Aironet AP GUI. The top navigation bar includes: HOME, NETWORK, ASSOCIATION, WIRELESS, SECURITY (highlighted), SERVICES, SOFTWARE, EVENT LOG. The left sidebar lists: Admin Access, Encryption Manager, SSID Manager, Server Manager, AP Authentication, Intrusion Detection, Local RADIUS Server, and Advance Security (highlighted). The main content area shows the 'Security Summary' for 'Hostname Autonomous'. It includes a table for 'Administrators' with columns for Username and Read-Only, and a table for 'Service Set Identifiers (SSIDs)' with columns for SSID, VLAN, BandSelect, Radio, and BSSID/Guest Mode.

Administrators	
Username	Read-Only
Cisco	✓

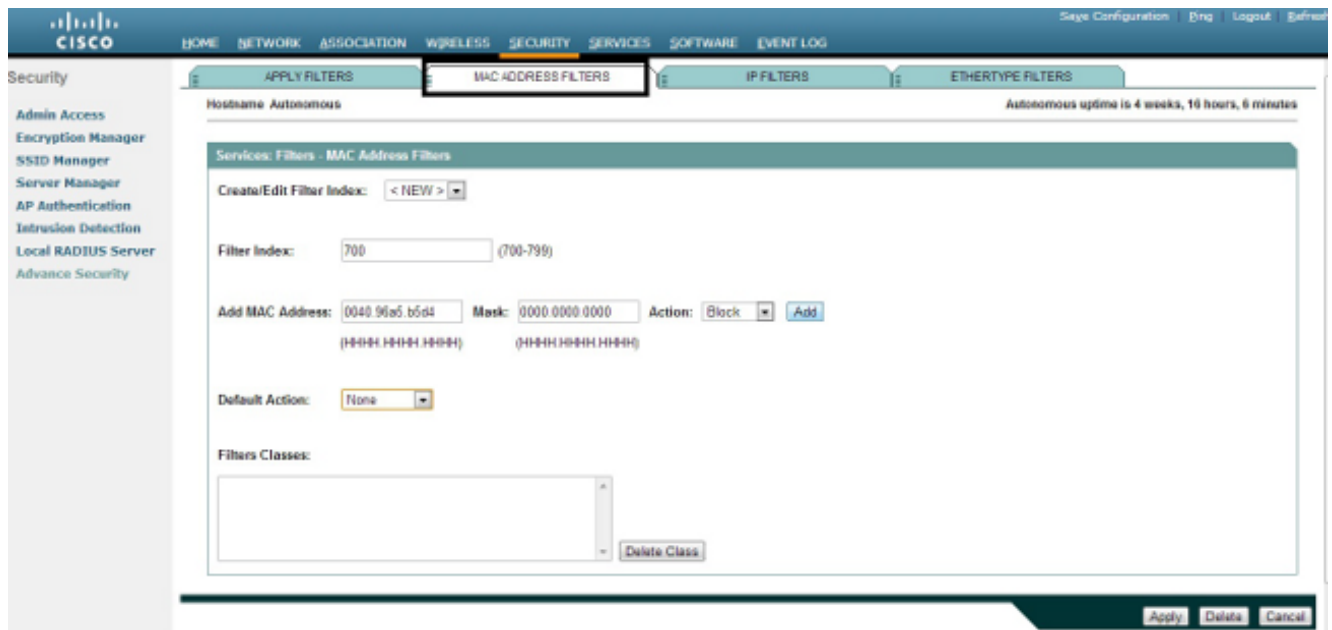
Service Set Identifiers (SSIDs)				
SSID	VLAN	BandSelect	Radio	BSSID/Guest Mode ✓

Filtros do MAC address

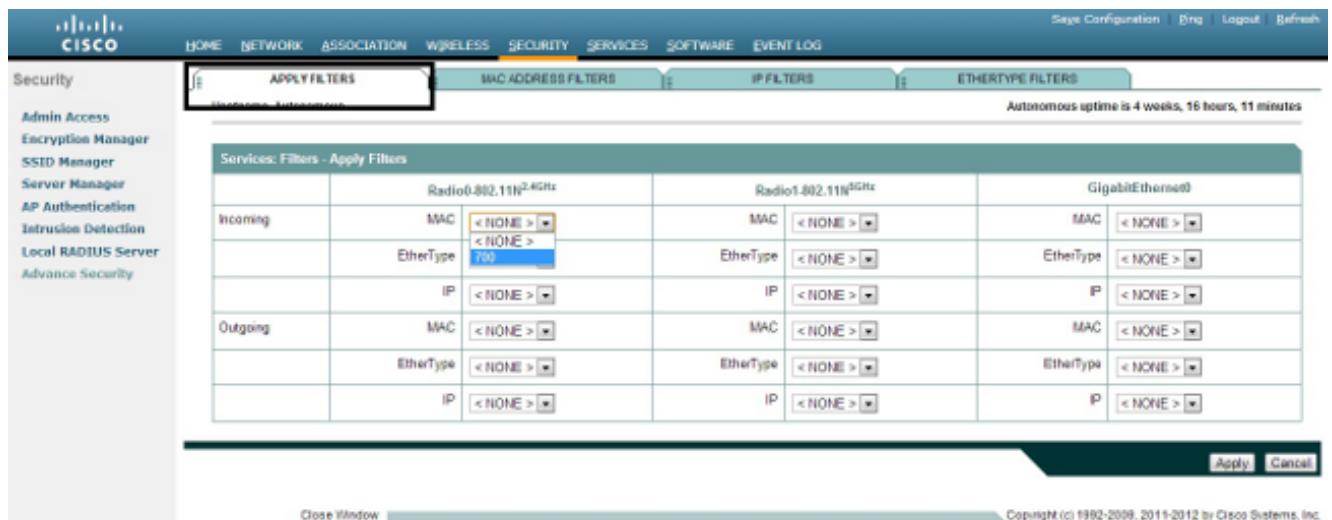
Você pode usar filtros com base em endereço MAC a fim filtrar os dispositivos do cliente baseados no MAC address duro-codificado. Quando um cliente é negado o acesso através de um filtro com base em MAC, o cliente não pode associar com o AP. Os filtros do MAC address permitem ou recusam a transmissão do unicast e dos pacotes de transmissão múltipla enviados, ou endereçados, aos endereços específicos MAC.

Este exemplo ilustra como configurar um filtro com base em MAC com o GUI a fim filtrar o cliente com um MAC address de **0040.96a5.b5d4**:

1. Crie o MAC address **ACL 700**. Este ACL não permite que o cliente **0040.96a5.b5d4** associe com o AP.



2. O clique **adiciona** a fim adicionar este filtro às classes dos filtros. Você pode igualmente definir a ação padrão como **dianteiro todo** ou **negar tudo**.
3. Clique em **Apply**. O **ACL 700** é criado agora.
4. A fim aplicar **ACL 700** a uma interface de rádio, navegue à seção dos **filtros da aplicação**. Você pode agora aplicar este ACL a uma relação entrante ou que parte do rádio ou do gigabitethernet.



O IP filtra

Você pode usar o padrão ou os ACL estendido a fim permitir ou recusar a entrada dos dispositivos do cliente na rede de WLAN baseada no endereço IP de Um ou Mais Servidores Cisco ICM NT do cliente.

Este exemplo de configuração usa ACL estendido. O ACL estendido deve permitir o acesso do telnet aos clientes. Você deve restringir todos protocolos restantes na rede de WLAN. Também, os clientes usam o DHCP a fim obter o endereço IP de Um ou Mais Servidores Cisco ICM NT. Você deve criar um ACL estendido isso:

- Permite o tráfego DHCP e de telnet
- Nega todos tipos de tráfego restantes

Termine estas etapas a fim criá-lo:

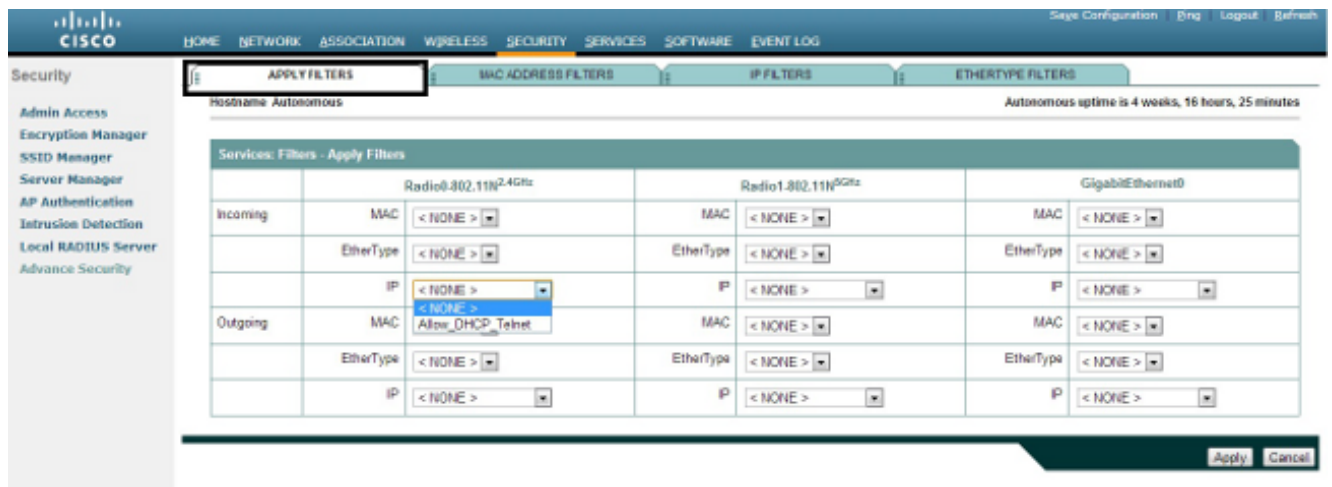
1. Nomeie o filtro, e selecione o **bloco todo da** lista de drop-down da **ação padrão**, desde que o tráfego restante deve ser obstruído:

The screenshot shows the Cisco configuration interface for IP Filters. The 'IP FILTERS' tab is selected. The 'Filter Name' is 'Allow_DHCP_Telnet' and the 'Default Action' is 'Block All'. The 'IP Address' section shows 'Destination Address' and 'Source Address' fields. The 'IP Protocol' section shows 'Authentication Header Protocol (51)' selected.

2. Selecione o **telnet** da lista de drop-down da **porta TCP**, e o **cliente bootp & o servidor de BOOTP** da lista de drop-down da **porta UDP**:

The screenshot shows the Cisco configuration interface for UDP/TCP Port. The 'TCP Port' is 'Telnet (23)' and the 'UDP Port' is 'Bootstrap Protocol (BOOTP) server (67)'. The 'Filters Classes' section shows 'TCP port: Telnet (23) - Forward', 'UDP port: Bootstrap Protocol (BOOTP) client (68) - Forward', and 'UDP port: Bootstrap Protocol (BOOTP) server (67) - Forward'.

3. Clique em Apply. O filtro IP **Allow_DHCP?** o **_Telnet** é criado agora, e você pode aplicar este ACL a uma relação entrante ou que parte do rádio ou do gigabitethernet.

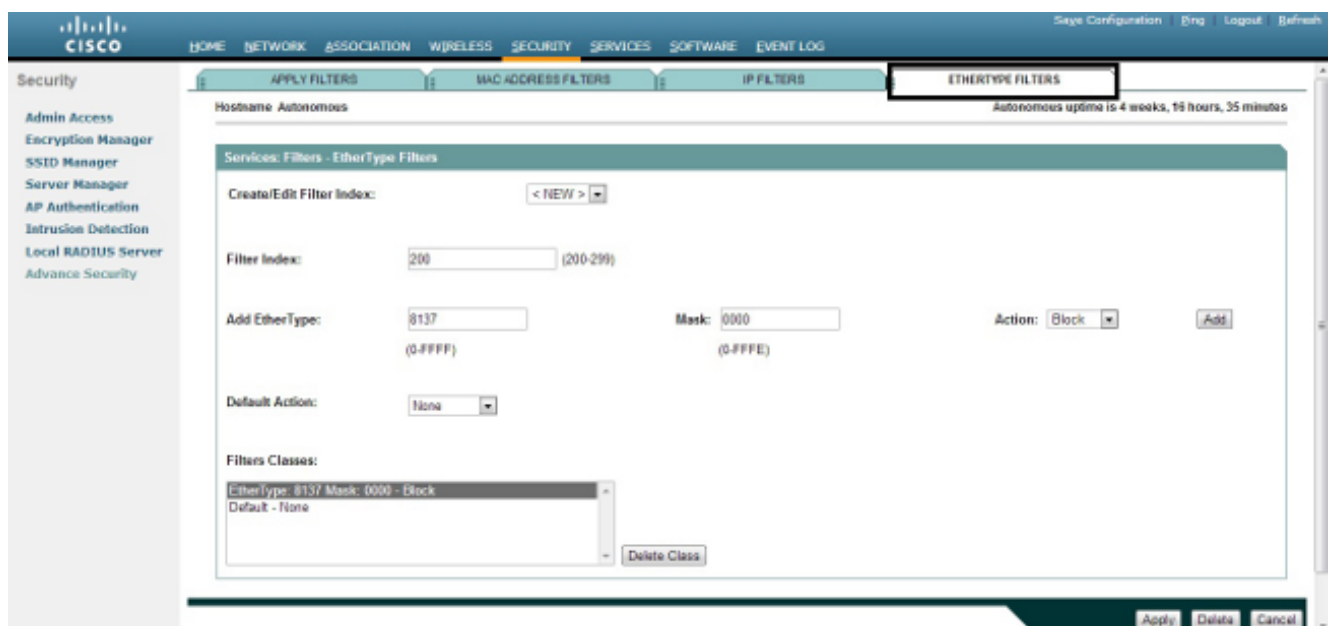


Filtros de Ethertype

Você pode usar filtros de Ethertype a fim obstruir o tráfego das Trocas de Pacote Entre Redes IPX (IPX) no Cisco Aironet AP. Uma situação típica onde esta seja útil está quando as transmissões do servidor de IPX bloqueiam o enlace Wireless, que acontece às vezes em uma grande rede de empreendimento.

Termine estas etapas a fim configurar e aplicar um filtro que obstrua o tráfego IPX:

1. Clique a aba dos **filtros de Ethertype**.
2. **No campo de índice do filtro**, nomeie o filtro com um número de 200 a 299. O número que você atribui cria um ACL para o filtro.
3. Incorpore **8137** ao campo de **Ethertype adicionar**.
4. Deixe a máscara para Ethertype no **campo da máscara** no valor padrão.
5. Selecione o **bloco** do menu de ação, e o clique **adiciona**.



6. A fim remover Ethertype da lista de classes dos filtros, selecioná-lo, e clicar a **classe da**

supressão. Repita as etapas precedentes, e adicionar os tipos **8138**, **00ff**, e **00e0** ao filtro. Você pode agora aplicar este ACL a uma relação entrante ou que parte do rádio ou do gigabitethernet.

The screenshot shows the Cisco configuration interface for the 'Services: Filters - Apply Filters' section. The interface includes a navigation menu on the left with options like 'Admin Access', 'Encryption Manager', 'SSTD Manager', 'Server Manager', 'AP Authentication', 'Intrusion Detection', 'Local RADIUS Server', and 'Advance Security'. The main content area displays a table with three columns: 'Radio0.802.11n2.4GHz', 'Radio1.802.11n5GHz', and 'GigabitEthernet0'. The table is organized into 'Incoming' and 'Outgoing' sections, each with rows for 'MAC', 'EtherType', and 'IP'. The 'APPLY FILTERS' button is highlighted with a red box. The 'IP' field for the 'Radio0.802.11n2.4GHz' Incoming traffic is set to '200'. The 'EtherType' field for the same row is set to '< NONE >'. The 'Radio1.802.11n5GHz' and 'GigabitEthernet0' sections also have rows for 'MAC', 'EtherType', and 'IP', all set to '< NONE >'. The 'Apply' and 'Cancel' buttons are visible at the bottom right of the table.

	Radio0.802.11n2.4GHz	Radio1.802.11n5GHz	GigabitEthernet0
Incoming	MAC	MAC	MAC
	EtherType	EtherType	EtherType
	IP	IP	IP
Outgoing	MAC	MAC	MAC
	EtherType	EtherType	EtherType
	IP	IP	IP