WiNG5 DESIGN GUIDE By Sriram Venkiteswaran

WiNG5 Wireless Association Filters

How To Guide

June, 2011

TABLE OF CONTENTS HEADING STYLE

| ITRODUCTION1 | l |
|------------------------------|---|
| Overview | 1 |
| Applications | 1 |
| Restrictions | 1 |
| ONFIGURATION 1 | Í |
| Deny Wireless Filters | 2 |
| Configuration through Web UI | 2 |
| Configuration through CLI | 3 |
| Allow Wireless Filters | 7 |
| Configuration through Web UI | 3 |
| Configuration through CLI 11 | 1 |
| Points to Remember | 2 |

WiNG5 Wireless Association Filters How To Guide

INTRODUCTION

OVERVIEW

Wireless filters can be applied to specific WLANs to grant or deny access to MUs based on individual or ranges of MAC addresses. Wireless filters may be applied to one or more WLANs and are used to grant or deny access to MUs during association.

APPLICATIONS

Wireless filters can be used for multiple applications including blacklisting malicious devices as well as providing an additional layer of security for less secure WLANs by restricting access to specific devices. Wireless filters may be applied to the WiNG5 Access Points using the CLI and Web UI of RFS Switch or from a Motorola AirDefense Enterprise server using SNMP when a threat is detected

RESTRICTIONS

Wireless filters are only used to allow or deny MUs from associating with a WLAN and are not intended to be used to filter layer 2 traffic passing through the Access Points. To restrict or limit traffic at layer 2, MAC firewall rules can be created which permits or denies traffic based on specific or wildcard source or destination MAC addresses.

CONFIGURATION

The following sections outline the configuration steps required to enable wireless filters on an RF Switch:

- Deny Wireless Association Filters
- Allow Wireless Association Filters

In WiNG5 since the Access Points perform all the WLAN functions, the enforcement happens at the Access Point.

DENY WIRELESS FILTERS

Wireless filters can be used to block devices and a common application for wireless filtering is to block (or blacklist) associations from a suspicious of malicious device. Administrators can create up to 1000 wireless filter entries on the RF Switch which pushes the configuration to all the Access Points. The Access Points can deny access to individual MAC addresses or range of MAC addresses as required. All MAC addresses not matched by the wireless filter list will be able to associate to the WLAN.



As shown in above figure wireless filtering has been deployed on a guest WLAN named MOTO-GUEST to block a device with the MAC address 00-0C-F1-25-18-F2. A wireless filter has been created on the RF Switch with a Start MAC and End MAC set to a specific devices MAC address. If the device attempts to associate with the MOTO-GUEST SSID, the AP will deny the association attempt and a log entry for the association attempt will be made.

| Precedence | Start MAC | End MAC | Allow / Deny |
|------------|-------------------|-------------------|--------------|
| 1 | 00-0C-F1-25-18-F2 | 00-0C-F1-25-18-F2 | Deny |

Configuration through Web UI

1. Create Association ACL

a. Under the context: Configuration->Wireless->Association ACL click 'Add'

| Association Access Control List (ACL) | | (| 0 |
|---------------------------------------|----------------------|-----------------------------|---|
| Association ACL | | ē | à |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Type to search in tables | | Row Count: 0 | |
| | | Add Edit _x Delet | e |
| | Find Functional Area | Type to search | |

b. Enter Association ACL Name 'Deny List' and Click Add Row

c. Enter Precedence as 1, Starting MAC Address as '**00-0C-F1-25-18-F2**', Ending MAC Address '**00-0C-F1-25-18-F2**' and action as 'Deny' and click 'OK'.

| Ass | ociation ACL 🥜 Deny List | | | | 0 |
|------|--------------------------|-----------------------------|-------------------------------|------------|----------|
| Rule | | | | | |
| | Precedence | Starting MAC Address | Ending MAC Address | Allow/Deny | Û |
| | * 1 | 00 - 0C - F1 - 25 - 18 - F2 | / 00 - 0c - f1 - 25 - 18 - f2 | Deny | ▼ |
| | | | | | |
| 1 | | | | | |
| | | | | | |
| | | | | | |

» OK Reset Exit

Add Ro

Note:

- ✓ This will block the client 00-0C-F1-25-18-F2 to connect to the wireless network
- ✓ The default rule is in an association ACL is 'allow all'. So if a client does not match any of the rules, it will be allowed association.
- d. Enter Precedence as 2, Starting MAC Address as '**00-27-10-24-4C-E4**', Ending MAC Address as '**00-27-10-24-4C-E4**', action as 'Allow' and click 'OK'.

| Association ACL Deny | List | | | 0 |
|----------------------|----------------------|--------------------|------------|-----------|
| Rule | | | | |
| Precedence | Starting MAC Address | Ending MAC Address | Allow/Deny | |
| 1 | 00-0C-F1-25-18-F2 | 00-0C-F1-25-18-F2 | × Deny | |
| 2 | 00-27-10-24-4C-E4 | 00-27-10-24-4C-E4 | 🖌 Allow | ŵ. |
| | | | | |
| | | | | |
| | | | | |
| | | | | 🔶 Add Row |

Note:

- ✓ This will ensure that WLAN access is granted to the client with MAC address 00-27-10-24-4C-E4.
- ✓ All other clients will be denied access, as the default rule is deny all.
- 2. Attach Association ACL to WLAN
 - a. Under the context: Configuration->Wireless->Wireless LANS, click on the WLAN that you want to apply the ACL to

| Dashboard Configuration Diagnostics Ope | rations Statistics | | | | | 🔷 RF54000 | M WiNe | G _{v5.1} 🚨 | admin 🌒 |
|---|-----------------------|----------------|-----------------------|-------------|-----------|---------------------|-----------------|---------------------------|-------------------------|
| Devices Wireless Profiles RF Domains Sec | urity Services Ma | nagement | | | | | | 5 Re | vert 🛃 Commit 🛛 🔒 Save |
| and Wireless LANs | Wireless LANs | | | | | | | | 0 |
| WLAN QoS Policy | WLAN | SSID | Description | WLAH Status | VLAN Pool | Authentication Type | Encryption Type | QoS Policy | Association ACL |
| Radio Gos Policy | Motorola-Guest | Motorola-Guest | WLAN for Guest Access | 🧹 Enabled | 10 | None | None | default | |
| Association ACL Sassociation ACL Sassociation ACL | | | | | | | | | |
| V/reless LAN | | | | | | | | | |
| 물일Motorola-Guest | 3 | | | | | | | | |

- b. Under the selected Wireless LAN, go to Firewall settings
- c. Select Association ACL as 'Deny List' from the drop down box. The deny list is the Association ACL that was created above.

| Basic Configuration | and the second state and second states at | | |
|-----------------------|---|---------------------------------------|--|
| Pocurity | IP Firewall Rules | | |
| Security | Inbound IP Firewall Rules | <none></none> | |
| Firewall | Outbound IP Firewall Rules | <none></none> | |
| Client Settings | MAC Firster II Delas | | |
| Accounting | MAC FILEWAII RUIES | | |
| Client Load Balancing | Inbound MAC Firewall Rules | <none></none> | |
| Advanced | Outbound MAC Firewall Rules | <none></none> | |
| | Association ACL | | |
| | Association ACL | 🖉 Deny List 🔹 🐨 | |
| | Trust Parameters | | |
| | ARP Trust | | |
| | Validate ARP Header Mismatch | \checkmark | |
| | DHCP Trust | | |
| | Wireless Client Deny | | |
| | Wireless Client Denied Traffic Threshold | 1 (1 to 1,000,000 packets per second) | |
| | Action | None 💌 | |
| | Blacklist Duration | ✓ 0 (0 to 86,400 seconds) | |
| | Advanced | | |

Configuration through CLI

1. Create Association ACL

rfs4000-22A5DC(config)*#association-acl-policy Deny\ List

rfs4000-22A5DC(config-assoc-acl-Deny List)*#deny 00-0C-F1-25-18-F2 00-0C-F1-25-18-F2

rfs4000-22A5DC(config-assoc-acl-Deny List)*#show context

association-acl-policy Deny\ List

deny 00-0C-F1-25-18-F2 00-0C-F1-25-18-F2 precedence 1

2. Attach Association ACL to WLAN

rfs4000-22A5DC(config)*#wlan Motorola-Guest

rfs4000-22A5DC(config-wlan-Motorola-Guest)*#

 $rfs4000-22A5DC (config-wlan-Motorola-Guest) * \# use association-acl-policy Deny \ List t$

rfs4000-22A5DC(config-wlan-Motorola-Guest)*#show context wlan Motorola-Guest description WLAN for Guest Access ssid Motorola-Guest vlan 10 bridging-mode tunnel encryption-type none authentication-type none use association-acl-policy Deny\ List

ALLOW WIRELESS FILTERS

Wireless filters may also be used to allow access to a specific group of devices such as mobile handhelds or VoIP handsets while blocking associations for all other devices. As most enterprises typically deploy mobile devices from a common vendor, the vendors OUI can be leveraged in a wireless filter to restrict access to a range of the vendor's devices. As no implicit deny is provided an additional wireless filter must be created after the allow filter to block access from all other vendor devices

Note:

A current list of vendor assigned OUIs may be downloaded directly from the IEEE website http://standards.ieee.org/develop/regauth/oui/oui.txt



As shown in above figure, wireless filtering has been deployed on a voice WLAN named MOTO-VOICE to only allow select SpectraLink VoIP handsets to associate with the WLAN. The first wireless filter has been created on the RF Switch / AP allowing a range of MAC addresses (00-40-96-4b-00-00 through 00-40-96-4b-ff-ff) to associate with the WLAN. A second 'catch all' wireless filter has been created denying access to all MAC addresses from 00-00-00-00-00-01 through ff-ff-ff-ff-ff. In this example an device with a MAC address that matches the range in the allow list will be allowed to associated with the WLAN. Devices which do not match the allowed list will be denied association from the Access Point and a log entry for the association attempt will be made

| Precedence | Start MAC | End MAC | Allow / Deny |
|------------|-------------------|-------------------|--------------|
| 1 | 00-40-96-4B-00-00 | 00-40-96-4B-FF-FF | Allow |
| 2 | 00-00-00-00-00-01 | FF-FF-FF-FF-FE | Deny |

Configuration through Web UI

1. Create Association ACL

a. Under the context: Configuration->Wireless->Association ACL click 'Add'

| Association Access Control List (ACL) | | 0 |
|---------------------------------------|----------------------|------------------------------|
| Association ACL | | ۲ |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| Type to search in tables | | Row Count: 0 |
| | | Add Edit _x Delete |
| | Find Functional Area | Type to search |

- b. Enter Association ACL Name 'Allow List' and Click Add Row
- c. Enter Precedence as 1, Starting MAC Address as '**00-40-96-4B-00-00**', Ending MAC Address '**00-40-96-4B-FF-FF**' and action as 'Allow' and click 'OK'.

| Ass | sociation ACL Allow List | | | | | 0 |
|------|--------------------------|----------------------|--------------------|------------|---------|----|
| Rule | e | | | | | |
| | Precedence | Starting MAC Address | Ending MAC Address | Allow/Deny | | ŵ |
| | 1 | 00-40-96-4B-00-00 | 00-40-96-4B-FF-FF | 🖌 Allow | | ŵ |
| | 2 | 00-00-00-00-01 | FF-FF-FF-FF-FE | × Deny | | ŵ |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | 🕂 Add R | ow |
| | | | | | 🕂 Add R | ļ |

This will allow all the clients with MAC address in the range **00-40-96-4B-00-00** and **00-40-96-4B-FF-FF** to associate to the WLAN

Note:

- ✓ The default rule is in an association ACL is 'allow all'. So if a client does not match any of the rules, it will be allowed association.
- d. Click Add Row. Enter Precedence as 2, Starting MAC Address as '**00-00-00-00-00-01**, Ending MAC Address as '**FF-FF-FF-FF-FF-FE**', action as 'Deny' and click 'OK'.

This will ensure that all clients not defined in precedence 1 is denied access to the WLAN

- 2. Attach Association ACL to WLAN
 - a. Under the context: Configuration->Wireless->Wireless LANS, click on the WLAN that you want to apply the ACL to

| Dashboard Configuration Diagnostics Ope | erations Statistics | 8 | | | | 🔷 RFS4000 | M WiNe | G _{v5.1} 🔒 | admin 🌏 |
|--|------------------------|----------------|-----------------------|--------------|-----------|---------------------|-----------------|---------------------------|------------------------|
| Devices Wireless Profiles RF Domains Ser | curity Services Ma | anagement | | | | | | 🌖 Rev | ert 🛃 Commit 🛛 🔚 Save |
| B Wireless LANs | Wireless LANs | | | | | | | | 0 |
| WLAN Gos Policy | WLAN | SSID | Description | WLAII Status | VLAN Pool | Authentication Type | Encryption Type | QoS Policy | Association ACL |
| All AAA Doling | Motorola-Guest | Motorola-Guest | WLAN for Guest Access | Senabled | 10 | None | None | default | |
| GAAFDUICY GASSOLIGUAACL Ç [™] SMART RF Policy | | | | | | | | | |
| Wireless LAN | | | | | | | | | |
| 플ฏMotorola-Guest | 1 | | | | | | | | |
| | | | | | | | | | |

- b. Under the selected Wireless LAN, go to Firewall settings
- c. Select Association ACL as 'Allow List' from the drop down box. The Allow list is the Association ACL that was created above.

| Basic Configuration | IP Firewall Rules | | |
|-----------------------|--|-------------------------------------|----|
| Security | Inbound IP Firewall Rules | <none></none> | |
| Firewall | Outbound IP Firewall Rules | chones V | |
| Client Settings | | | |
| Accounting | MAC Firewall Rules | | |
| Client Load Balancing | Inbound MAC Firewall Rules | <none></none> | |
| Advanced | Outbound MAC Firewall Rules | <none></none> | |
| | Association ACL | | |
| | Association ACL | 🖉 Allow List 🛛 👻 | |
| | Trust Parameters | | 1. |
| | ARP Trust | | |
| | Validate ARP Header Mismatch | V | |
| | DHCP Trust | | |
| | Wireless Client Deny | | |
| | Wireless Client Denied Traffic Threshold | (1 to 1,000,000 packets per second) | |
| | Action | None 🗸 | |
| | Blacklist Duration | (0 to 86,400 seconds) | |
| | Advanced | | |
| | | General Andrewski (1997) | |

Configuration through CLI

1. Create Association ACL

rfs4000-22A5DC(config)*#association-acl-policy Allow\ List

rfs4000-22A5DC(config-assoc-acl-Deny List)*# permit 00-40-96-4B-00-00 00-40-96-4B-FF-FF precedence 1

rfs4000-22A5DC(config-assoc-acl-Deny List)*# deny 00-00-00-00-01 FF-FF-FF-FF-FE precedence 2

2. Attach Association ACL to WLAN

rfs4000-22A5DC(config)*#wlan Motorola-Guest

rfs4000-22A5DC(config-wlan-Motorola-Guest)*#

rfs4000-22A5DC(config-wlan-Motorola-Guest)*#use association-acl-policy Allow\ Lis

Points to Remember

t

- ✓ To configure wireless association filters follow these 2 steps
 - o Create an Association ACL Policy
 - Attach Association ACL policy to WLAN
- The default rule in Association ACL Policy is 'allow all'. So if a wireless client does not match any rule, then it will be allowed access. So to deny access to a wireless clients, explicit deny rules must be created.