WiNG 5 Feature Guide

Firewall How To

Published: April 2017

Extreme Networks, Inc.
Phone / +1 408.579.2800
Toll-free / +1 888.257.3000

www.extremenetworks.com

P/N XXXXX-XX

Contents

Introduction

WiNG 5 firewall steps away from the centralized, controller-based solution that most vendors are using and distributes that service to all devices, access-points and controllers alike. The granular, distributed approach allows policy to be carried out at the edge, without reliance on or the potential bottleneck of a centralized device.

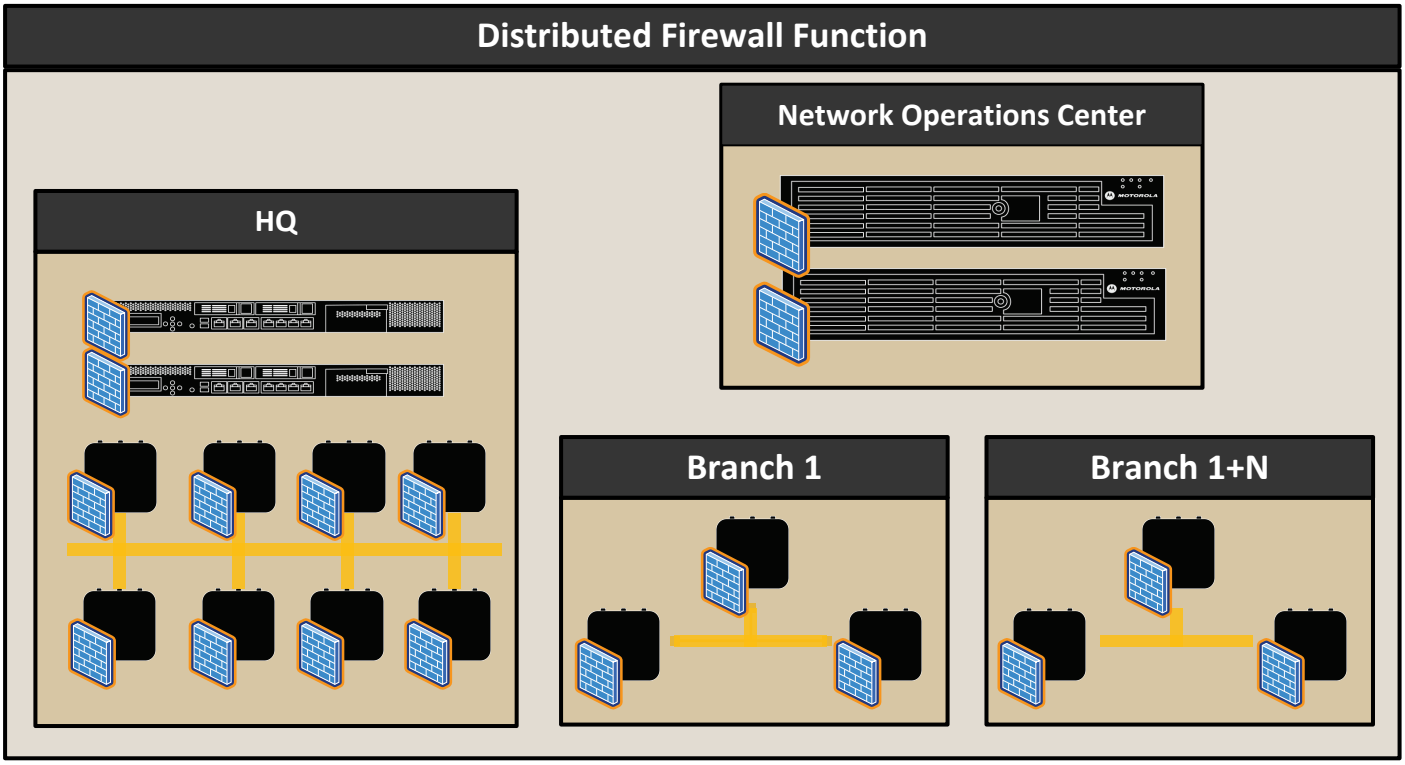
This how-to guide provides a detailed overview of the L2/L3 stateful inspection process and provides examples of configuration for various scenarios, including role-based firewall. It will also cover firewall policies, although details of services such as DoS attack/detection, Storm Control and DHCP conversion are beyond the scope of this writing.

Overview

WiNG 5 firewall services can be categorized as two main functions: policies, which are applied to controllers and access points as a whole and enable services such as Storm Control, DoS mitigation, DHCP Offer conversion and various Application Layer Gateways (ALG's). Next are firewall rules in the form of IP (L3) and Mac (L2) ACL's, which are applied to WLAN's, ports, virtual IP interfaces or wireless clients. Rules are stateful at L2 and L3 for IPv4 and IPv6 flows and stateless for non-IP flows, such as IPX or Appletalk.

Distributed Stateful Inspection

The major feature in WiNG 5 is distribution of services or services at the edge. Since controllers and access points alike run the same OS and thus feature set, processing of traffic for various services is pushed to the edge where it can be performed in real-time and done so dynamically with firewall state migration upon wireless client roam. Figure 1. Distributed Stateful Inspection



The distributed nature of the firewall allows stateful flows to migrate with clients as they roam between access points. Rules are made up of one or more traffic matching conditions, for which an action is then performed (permit, deny, mark, log). As is the case with firewalls, at least one permit action must be met in order for traffic to be forwarded and at the end of a rule set, there is an implied deny for all traffic not meeting a match condition.

Role Based Firewall

Roles based firewall is an enhancement to the existing firewall features and was designed to meet the security needs of the mobile enterprise. The role based firewall allows administrators to dynamically apply firewall rules to client WLAN sessions based on various match criteria, such as:

- Location: the access point or group of access points the wireless clients connects to Group
- Membership: The local group the user is assigned to as passed down by AAA policies
- Hotspot: Authentication State
- Encryption Type: The encryption method used Authentication Type: The authentication method used SSID: The SSID to which the client has associated.
- MAC Address: The specific or a range of mac-addresses of the client(s)
- Device Identity: Device Type and OS based on DHCP fingerprinting.

Role-based firewall is covered more extensively in the document "*WiNG 5 Role-Based Firewall How-To*".

Components

The hierarchical configuration model of WiNG 5 breaks up the overall firewall feature set into various components.

- Firewall Policies
- Firewall Rules (Access Control Lists)
    - IPv4 Firewall Rules
    - IPv6 Firewall Rules
    - MAC Firewall Rules
- Wireless Client Roles

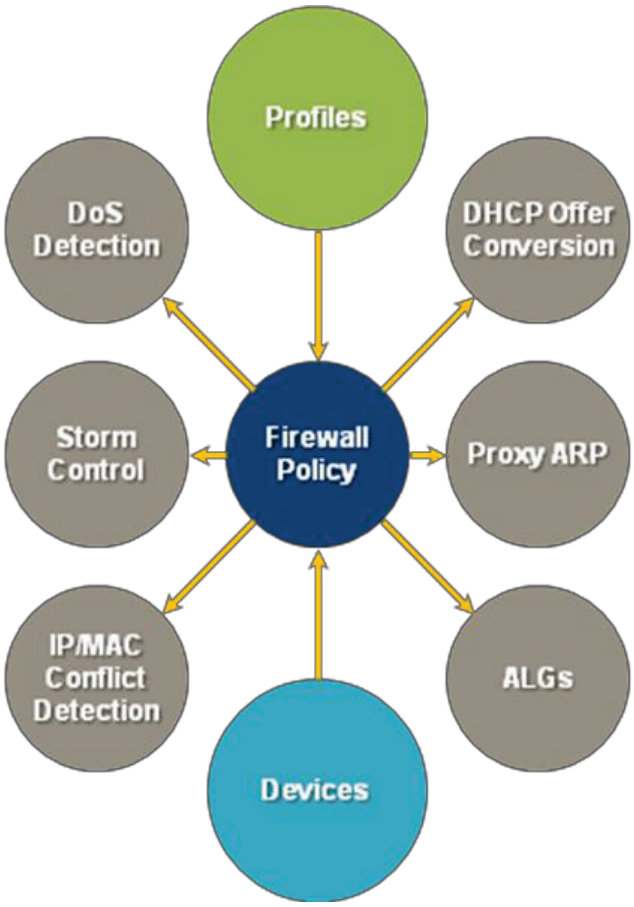
Firewall Policies

Policies apply to WiNG 5 devices; controllers and / or access points. They are used to enable or disable various services at the device level and only one policy can be applied to a device at a time, either through hardware profiles or as device overrides. There is a default firewall policy in a WiNG 5 master configuration that is applied to all devices unless otherwise configured by an administrator.

The services controlled by firewall policies are:

- Layer-2/Layer-3 firewall state
- Application Layer Gateways
- DoS Detection
- DHCP Offer Conversion
- Firewall flow timeouts
- IP/MAC conflict detection

- Proxy ARP
- Storm Controls



Application Layer Gateways (ALGs)

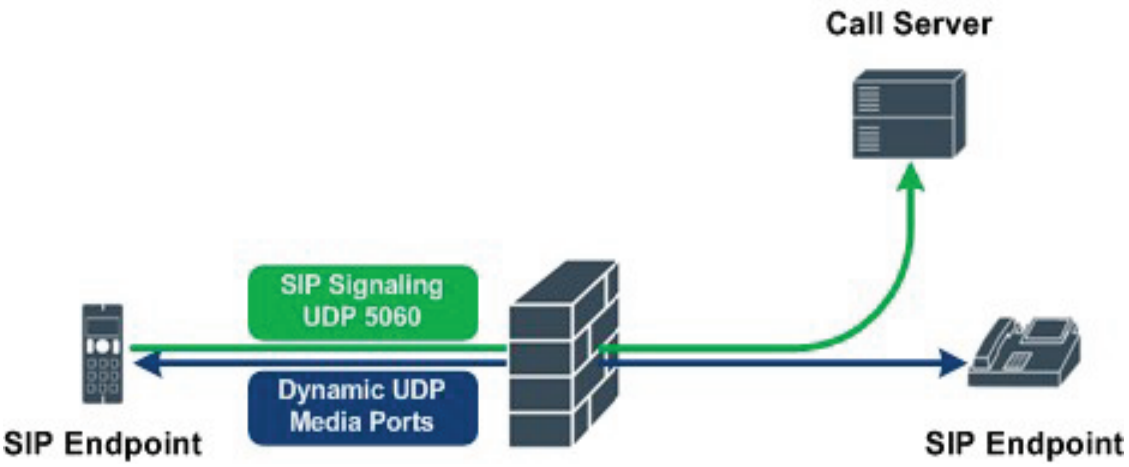
An application layer gateway (ALG) is a feature integrated into the stateful firewall that allows the WiNG 5 device to inspect and verify application payloads and dynamically open additional ports for protocols to function. ALGs typically support applications that use Transmission Control Protocol (TCP) or User Datagram Protocol (UDP), but sometimes applications that use different IP protocols (like PPTP).

- File Transfer Protocol (FTP)
- Session Initiation Protocol (SIP)
- Domain Name Service (DNS)
- Trivial File Transfer Protocol (TFTP)
- Apple Facetime
- Skinny Call Control Protocol (SCCP)
- Point-to-Point Tunneling Protocol (PPTP)

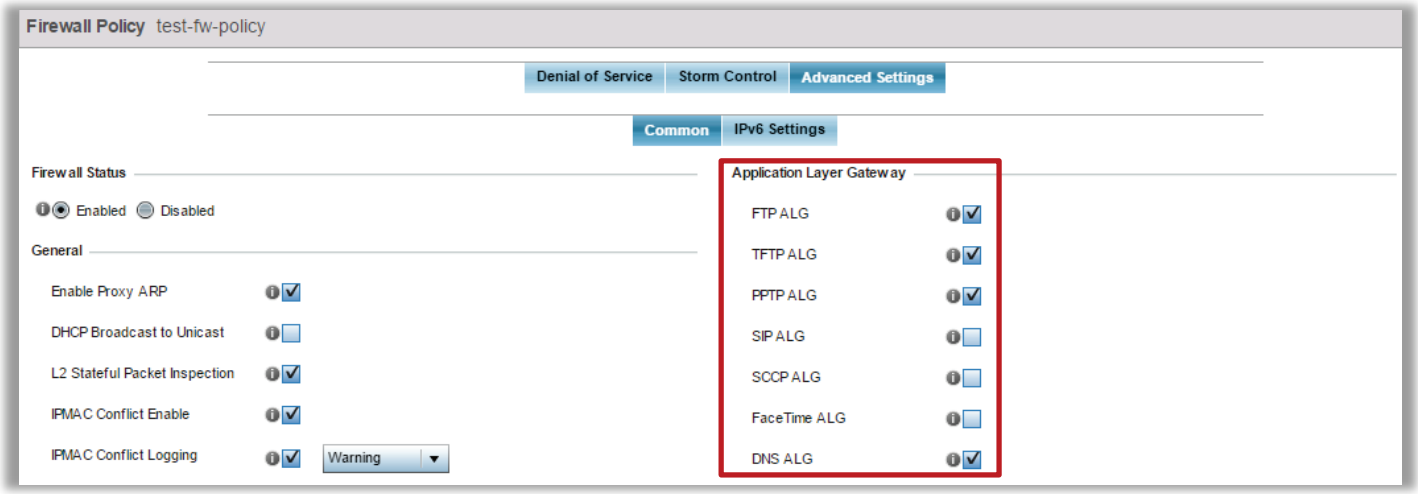
An ALG implementation requires the WiNG 5 device to inspect the application layer payload of a packet and understand the application control messages. When a firewall rule is enabled permitting traffic for a supported protocol, the Access Point will automatically perform application layer inspection and the dynamic opening/closing of any associated TCP/UDP ports. For example, if SIP signaling port 5060 is permitted in a firewall rule, the SIP ALG will dynamically open the required RTP media ports based on the call setup

information contained in the SIP signaling payload. This approach allows RTP (voice media path) to be permitted through the firewall without having to permit a wide range of ports.

SIP ALG



ALG Configuration (Defaults)



Another advantage of using an ALG is that additional information can be extracted from the protocol payload. For example, the SIP payload additional information beyond protocol ids and port numbers such as bandwidth requirements which can be leveraged for voice Call Admission Control (CAC) to ensure radio capacity is not exceeded. In addition, the SIP ALG can also be used to inspect RTP packets and provide information about call quality including R-Values and Mean Opinion Scores (MOS).

DoS Detection

Each firewall policy supports 30 different DoS violations for IPv4 and IPv6 traffic. These can be enabled or disabled at will by the administrator and each supports drop and/or log actions against the traffic. By default detection for all violations is enabled.

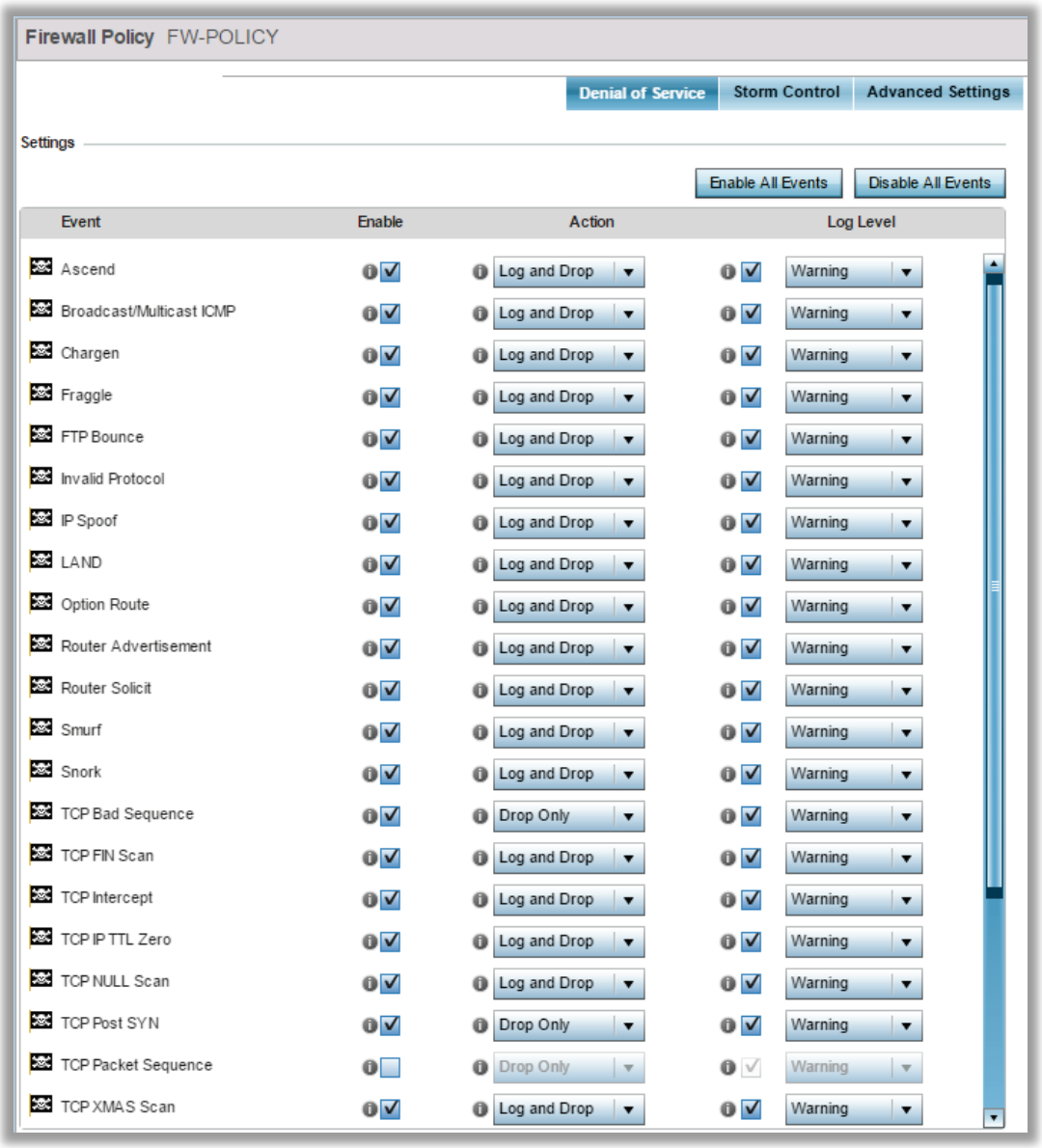
The following table provides current list of DoS violation that can be discovered and mitigated by WiNG5 firewall:

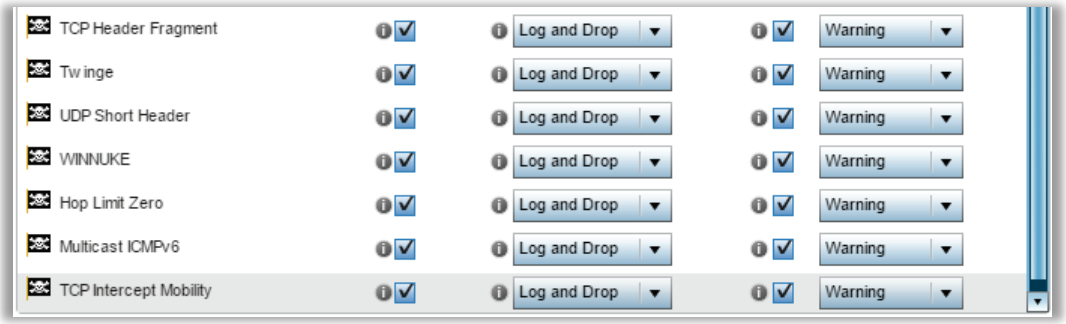
DoS Attack	Description
Ascend	The Ascend DoS attacks are a series of attacks that target known vulnerabilities in various versions of Ascend routers. Malformed UDP probe packets are sent to the UDP discard port (port 9). Applicable to IPv4 and IPv6 traffic.
Broadcast / Multicast ICMP	Broadcast or Multicast ICMP DoS attacks are a series of attacks that take advantage of ICMP behavior in response to echo replies. These usually involve spoofing the source address of the target and sending ICMP broadcast or multicast echo requests to the rest of the network and in the process flooding the target machine with replies.
Chargen	The Chargen attack establishes a Telnet connection with a spoofed IP address to port 19 and attempts to use the character generator service to create a string of characters which is then directed to the DNS service on port 53 to disrupt DNS services. Applicable to IPv4 and IPv6 traffic.
Fraggle	The Fraggle DoS attack uses a list of broadcast addresses to send spoofed UDP packets to each broadcast address' echo port (port 7). Each of those addresses that have port 7 open will respond to the request generating a lot of traffic on the network. For those that do not have port 7 open they will send an unreachable message back to the originator, further clogging the network with more traffic. Source IP spoofing and UDP echo to an IP broadcast address. This traffic is aimed at UDP port 7 (echo) and UDP port 19 (chargen). Applicable to IPv4 and IPv6 traffic.
FTP Bounce	The FTP Bounce DoS attack uses a vulnerability in the FTP "PORT" command as a way to scan ports on a target machine by using another machine in the middle. IP address in the FTP PORT command is not the same as the IP address of the client (in case of active FTP) and server (passive FTP). Applicable to IPv4 and IPv6 traffic.
Invalid Protocol	Attackers may use vulnerability in the endpoint implementation by sending invalid protocol fields, or may misuse the misinterpretation of endpoint software. This can lead to inadvertent leakage of sensitive network topology information, call hijacking, or a DoS attack. Applicable to IPv4 and IPv6 traffic
IP Spoof	IP Spoof is a category of DoS attack that sends IP packets with forged source addresses that may belong to another host. This can hide the identity of the attacker. Applicable to IPv4 and IPv6 traffic.
LAND	The LAND DoS attack sends spoofed packets containing the SYN flag to the target destination using the target port and IP address as both the source and destination. This will either crash the target system or result in high resource utilization slowing down all other processes. Applicable to IPv4 and IPv6 traffic.
Option Route	IPv4 packet with source route IPv4 options (Lose Source Routing Options - LSSR and Strict Source Routing Options - SSR)
Router Advertisement	In this attack, the attacker uses ICMP (packet type 9) to redirect the network router function to some other host. If that host cannot provide router services, a DoS of network communications occurs as routing stops. This can also be modified to single out a specific system, so that only that system is subject to attack (because only that system sees the 'false' router). By providing router services from a compromised host, the attacker can also place themselves in a man-in-the-middle situation and

	take control of any open channel at will (as mentioned earlier, this is often used with TCP packet forgery and spoofing to intercept and change open TELNET sessions).
Router Solicit	The ICMP Router Solicitation scan is used to actively find routers on a network. Of course, a hacker could set up a protocol analyzer to detect routers as they broadcast routing information on the network. In some instances, however, routers may not send updates. For example, if the local network does not have other routers, the router may be configured to not send routing information packets onto the local network. ICMP offers a method for router discovery. Clients send ICMP router solicitation multicasts onto the network, and routers must respond (as defined in RFC 1122). (For more information about the process of ICMP router solicitation, see "Routing Sequences for ICMP.") By sending ICMP router solicitation packets (ICMP type 9) on the network and listening for ICMP router discovery replies (ICMP type 10), hackers can build a list of all of the routers that exist on a network segment. Hackers often use this scan to locate routers that do not reply to ICMP echo requests.
Smurf	The Smurf DoS Attack sends ICMP echo requests to a list of broadcast addresses in a row, and then repeats the requests, thus flooding the network. Source IP is spoofed and ICMP echo to an IP broadcast address. Applicable to IPv4 and IPv6 traffic.
Snork	The Snork DoS attack uses UDP packet broadcasts (src port 7 or 19 or 135; dst port 135) to consume network and system resources. Applicable to IPv4 and IPv6 traffic.
TCP Bad Sequence	TCP packet with a bad sequence number. Applicable to IPv4 and IPv6 traffic.
TCP FIN Scan	Hackers use the TCP FIN scan to identify listening TCP port numbers based on how the target device reacts to a transaction close request for a TCP port (even though no connection may exist before these close requests are made). This type of scan can get through basic firewalls and boundary routers that filter on incoming TCP packets with the Finish (FIN) and ACK flag combination. The TCP packets used in this scan include only the TCP FIN flag setting. If the target device's TCP port is closed, the target device sends a TCP RST packet in reply. If the target device's TCP port is open, the target device discards the FIN and sends no reply. Applicable to IPv4 and IPv6 traffic.
TCP Intercept	A SYN-flooding attack occurs when a hacker floods a server with a barrage of requests for connection. Because these messages have unreachable return addresses, the connections cannot be established. The resulting volume of unresolved open connections eventually overwhelms the server and can cause it to deny service to valid requests, thereby preventing legitimate users from connecting to a Web site, accessing email, using FTP service, and so on. The TCP intercept feature helps prevent SYN-flooding attacks by intercepting and validating TCP connection requests. In intercept mode, the TCP intercept software intercepts TCP synchronization (SYN) packets from clients to servers that match an extended access list. The software establishes a connection with the client on behalf of the destination server, and if successful, establishes the connection with the server on behalf of the client and knits the two half-connections together transparently. Thus, connection attempts from unreachable hosts will never reach the server. The software continues to intercept and forward packets throughout the duration of the connection. The number of SYNs per second and the number of concurrent connections proxied depends on the platform, memory, processor, and other factors. In the case of illegitimate requests, the software's aggressive timeouts on half-open connections and its thresholds on TCP connection requests protect destination servers while still allowing valid requests.

	When establishing a security policy using TCP intercept, you can choose to intercept all requests or only those coming from specific networks or destined for specific servers. You can also configure the connection rate and threshold of outstanding connections. Optionally operate TCP intercept in watch mode, as opposed to intercept mode. In watch mode, the software passively watches the connection requests flowing through the router. If a connection fails to get established in a configurable interval, the software intervenes and terminates the connection attempt. Applicable to IPv4 and IPv6 traffic. This feature has additional thresholds to define SYN Flood rate: ip dos tcp-max-incomplete high 500 ip dos tcp-max-incomplete low 200
TCP IP TTL Zero	The TCP IP TTL Zero DoS attack sends spoofed multicast packets onto the network which have a Time To Live (TTL) of 0. This causes packets to loop back to the spoofed originating machine, and can cause the network to overload: TTL in the IPv4 packet is less than the minimum value (1).
TCP NULL Scan	Attackers use the TCP NULL scan to identify listening TCP ports. This scan also uses a series of strangely configured TCP packets, which contain a sequence number of 0 and no flags. This type of scan can get through some firewalls and boundary routers that filter incoming TCP packets with standard flag settings. If the target device's TCP port is closed, the target device sends a TCP RST packet in reply. If the target device's TCP port is open, the target discards the TCP NULL scan, sending no reply: TCP Sequence Number zero and all control bits are set to zero. Applicable to IPv4 and IPv6 traffic.
TCP Post SYN	A remote attacker may be attempting to avoid detection by sending a SYN frame with a different sequence number than the original SYN. This can cause an Intrusion Detection System (IDS) to become unsynchronized with the data in a connection. Subsequent frames sent during the connection are ignored by the IDS: TCP packet with SYN flag set after the connection is established. Applicable to IPv4 and IPv6 traffic.
TCP Packet Sequence	An attempt to predict the sequence number used to identify packets in a TCP connection, which can be used to counterfeit packets. The attacker hopes to correctly guess the sequence number used by the sending host. If successful, they can send counterfeit packets to the receiving host which will seem to originate from the sending host, even though the counterfeit packets may originate from some third host controlled by the attacker: TCP packet with a sequence number past the receiver's window, but past 2* the window. Applicable to IPv4 and IPv6 traffic.
TCP XMAS Scan	The TCP XMAS Scan floods the target system with TCP packets including the FIN, URG, and PUSH flags. This is used to determine details about the target system and can crash a system: TCP Sequence Number zero and FIN, URG and PUSH bits are set. Applicable to IPv4 and IPv6 traffic.
TCP Header Fragment	IP Fragments containing in-complete TCP header. Applicable to IPv4 and IPv6 traffic.
Twinge	The Twinge DoS attack sends ICMP packets and cycles through using all ICMP types and codes. This can crash some Windows systems: Flood of non-echo ICMP packets sent to the target. Applicable to IPv4 and IPv6 traffic.
UDP Short Header	IP datagram with total packet length < 28. Applicable to IPv4 and IPv6 traffic.

WINNUKE	The WINNUKE DoS attack sends a large amount of data to UDP port 137 to crash the NETBIOS service on windows and results in high CPU utilization on the target machine: TCP URG bit in header and sets URG pointer to point beyond the end of the frame. It uses port 139. Applicable to IPv4 traffic only.
Hop Limit Zero	Hop limits within IPv6 packets is set to 0 preventing hops as needed. Applicable to IPv6 traffic only.
Multicast ICMPv6	ICMPv6 packets contain multicast L2 DMACs. Applicable to IPv6 traffic only.
TCP Intercept Mobility	Detect IPv6 TCP packet with mobility option home address option (HAO) or route header (RH) type one set and do not generate SYN cookies for such packets. Applicable to IPv6 traffic only.



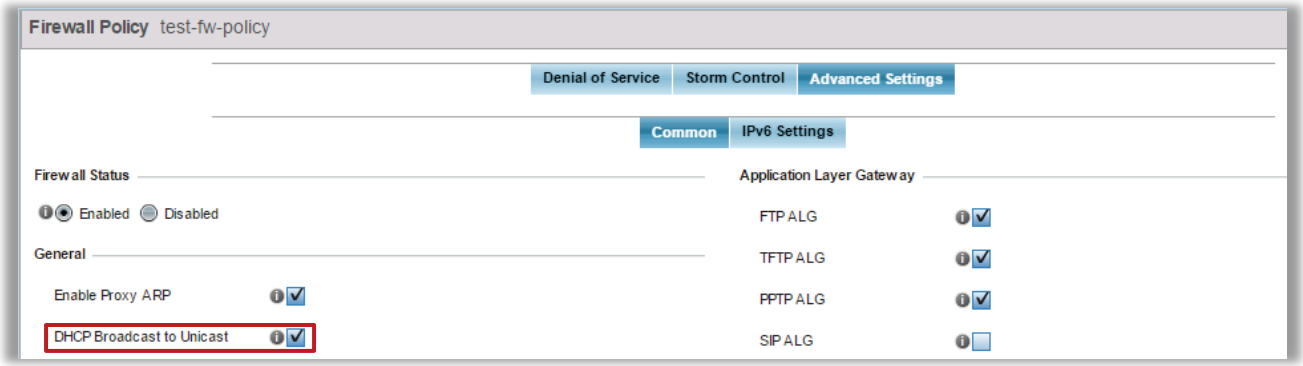


DHCP Offer Conversion

This feature removes some overhead from the network, allowing an access point to convert DHCP offer and ACK broadcasts to unicast packets, directly to the intended client. This results in less traffic over the air and fewer devices having to process traffic that is not intended for them.

DHCP Packet Type	Discover	Offer	Request	ACK
Without DHCP Offer Conversion	Broadcast	Broadcast	Broadcast	Broadcast
With DHCP Offer Conversion	Broadcast	Unicast	Broadcast	Unicast

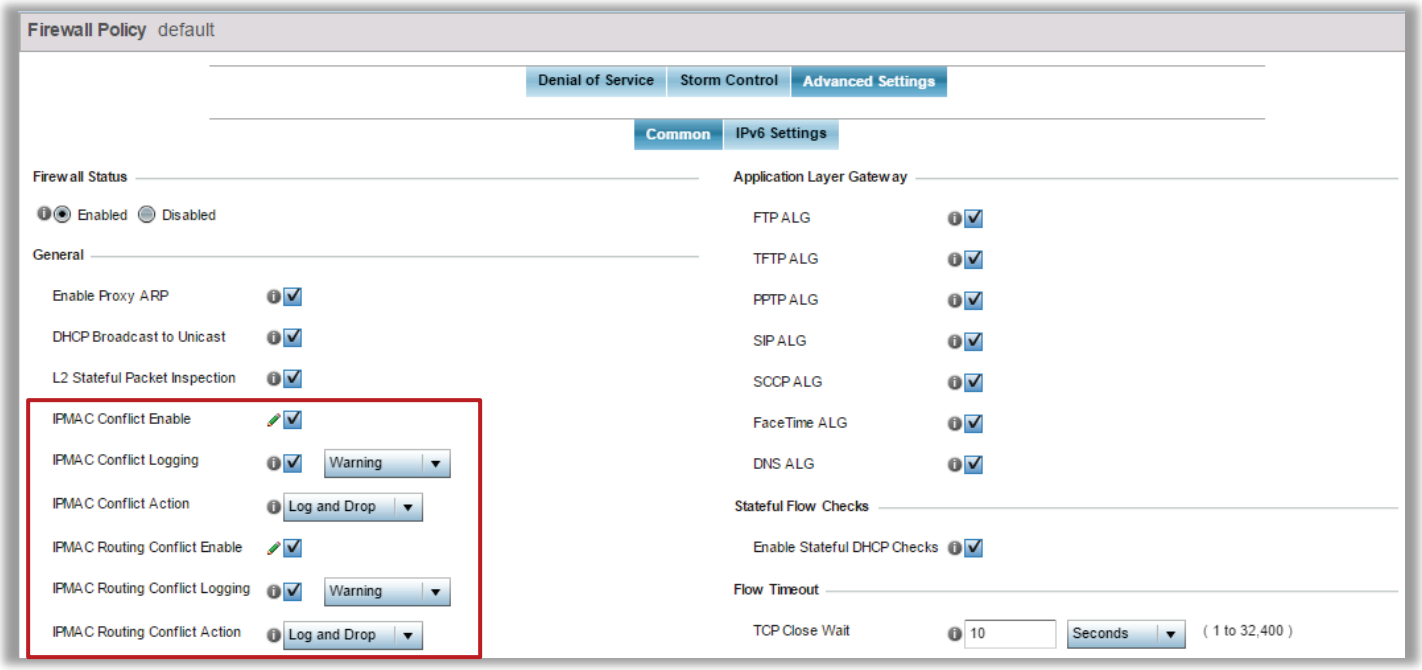
This feature is disabled by default and is only applicable when the DHCP server resided on the same VLAN as the client for which the offers are intended. It is recommended to enable this feature whenever possible.



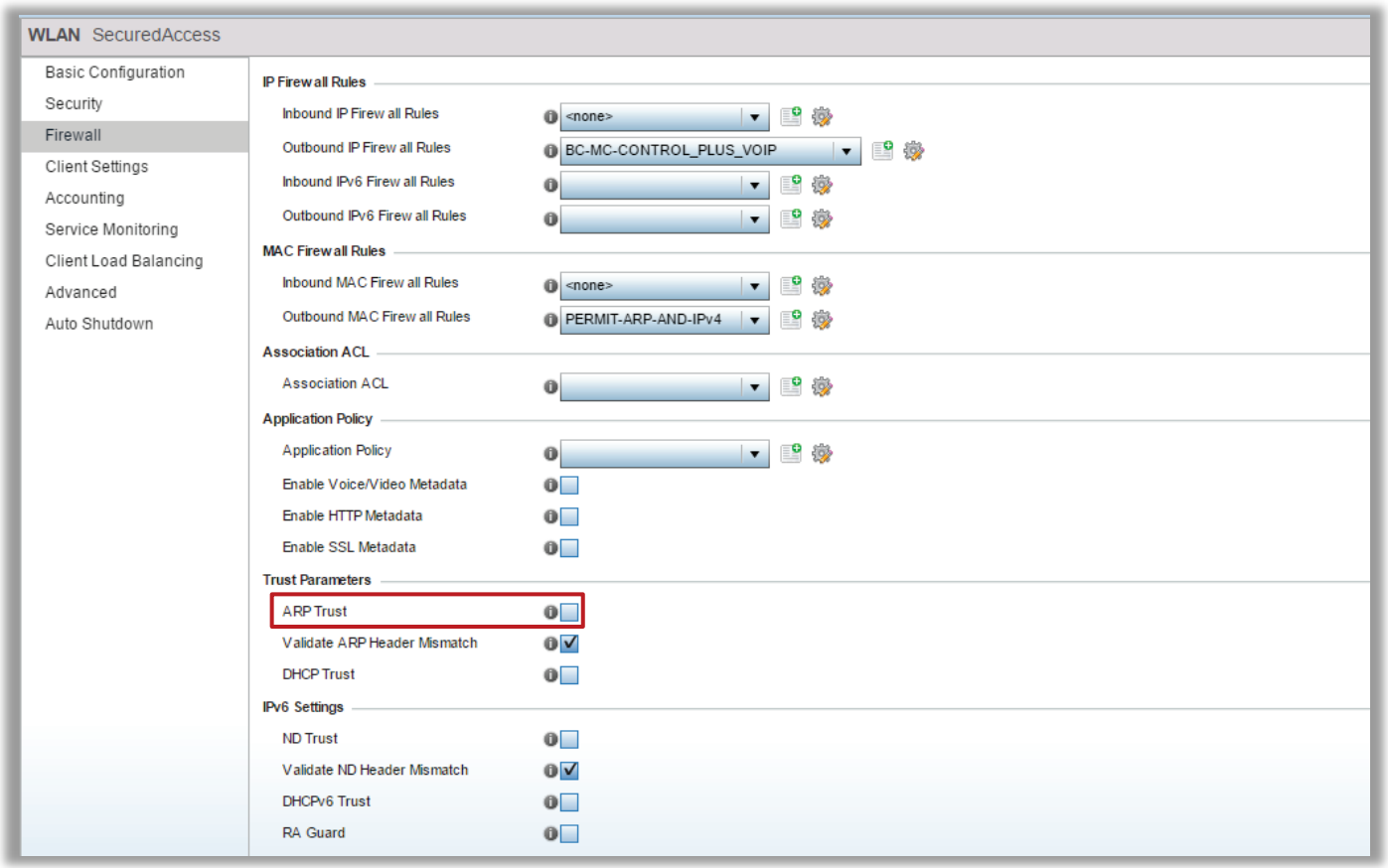
IP / MAC Conflict Detection

This feature mitigates various man-in-the-middle and other spoofing attacks. It allows an AP to intercept and log packets with IP / MAC bindings and build a table recording the information, by snooping DHCP offer and acknowledgement packets.

- The binding table includes IP and MAC addresses for all DHCP servers, routers virtual IP interfaces
- Requires that clients use DHCP; statically address clients will not be added to the table as there is no DHCP snooping possible for those.

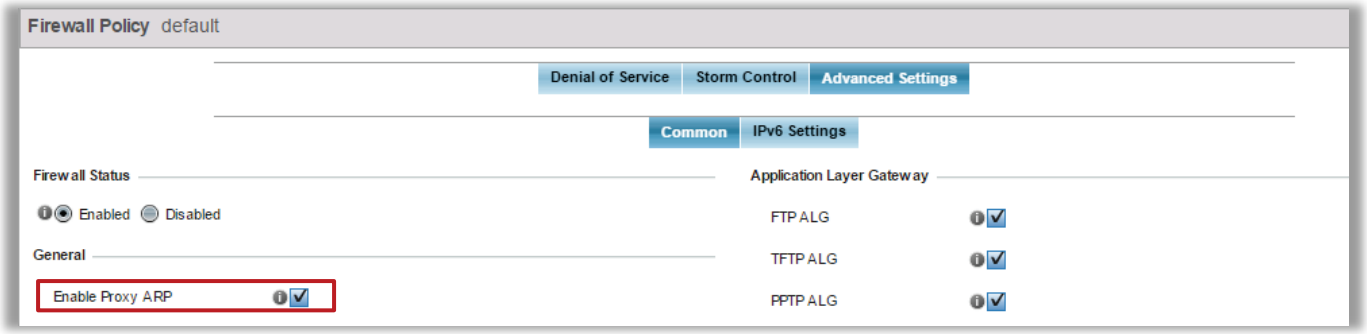


Each physical port and WLAN can be configured to trust or un-trust ARP and DHCP packets and drop suspicious packets upon arrival. One typically does not expect to see DHCP server packets initiating on a WLAN and thus finding them may indicate a rogue device on the network for malicious purposes. These packets would be un-trusted on the WLAN and therefore dropped by the access points when discovered.



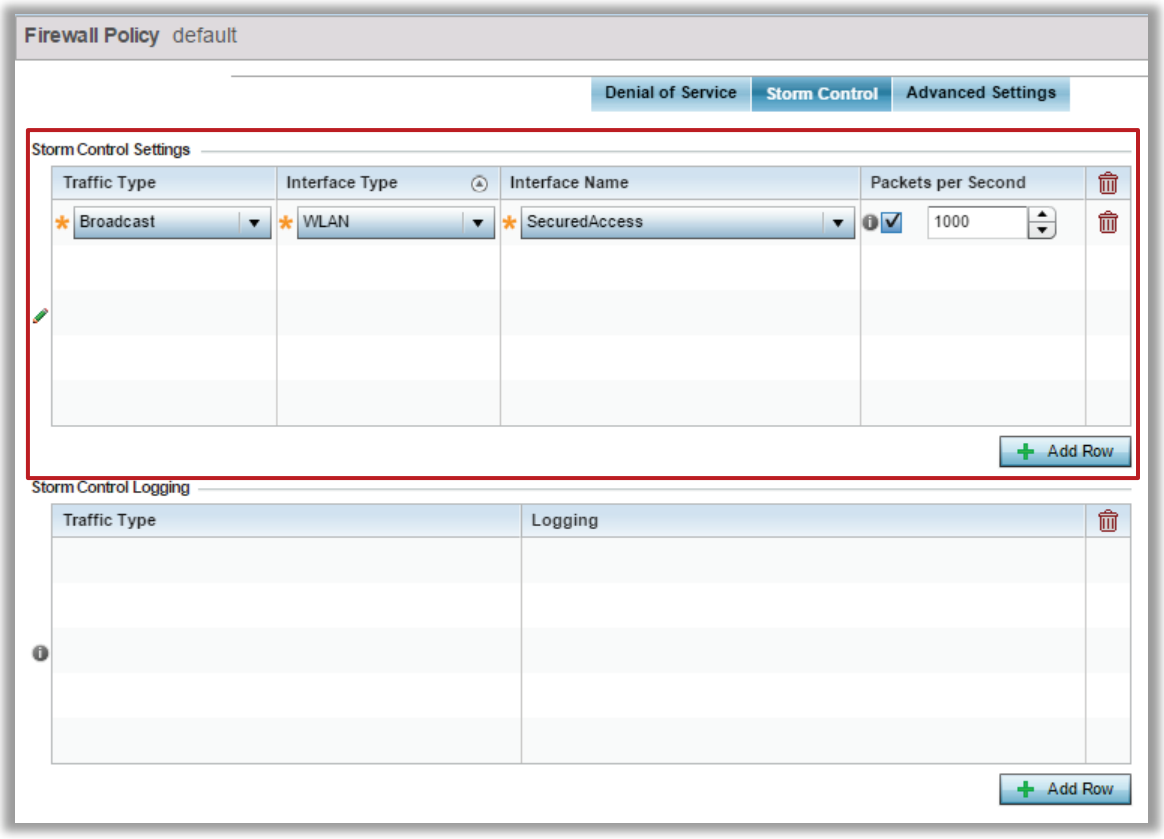
Proxy ARP

Proxy ARP allows wireless controllers and access points to respond to ARP requests on behalf of wireless clients. In this way, clients do not have to wake up to respond, and also ARP requests will not be forwarded to the air, which will dramatically improve overall airtime. It is enabled by default in the default and user defined firewall policies. It is strongly recommended to keep this option enabled.



Storm Controls

Storm controls provides a mechanism to protect the network from flooding attacks or high rates of traffic through the wireless controller or access points and may apply to broadcast / multicast / unknown unicast packets per second through ports or WLAN's. Thresholds are defined by an administrator and traffic exceeding the thresholds is dropped and an event log is generated.



A word of caution when enabling this feature; unless there is sufficient understanding of "normal" levels of these traffic types on the network, enabling this could result in legitimate traffic being dropped and thus affecting clients on the network. A proper baseline of the traffic should be known first.

Firewall Flow Migration

WiNG5 distributed firewall allows to seamlessly migrate wireless client firewall session information upon roaming. This is referred to as firewall flow migration. The data exchanged between the APs during roaming includes firewall flows for this particular client, ALG information as well as state of the wireless client (DATA-READY, INIT, Captive Portal unauthenticated host etc). This happens automatically when firewall is enabled.

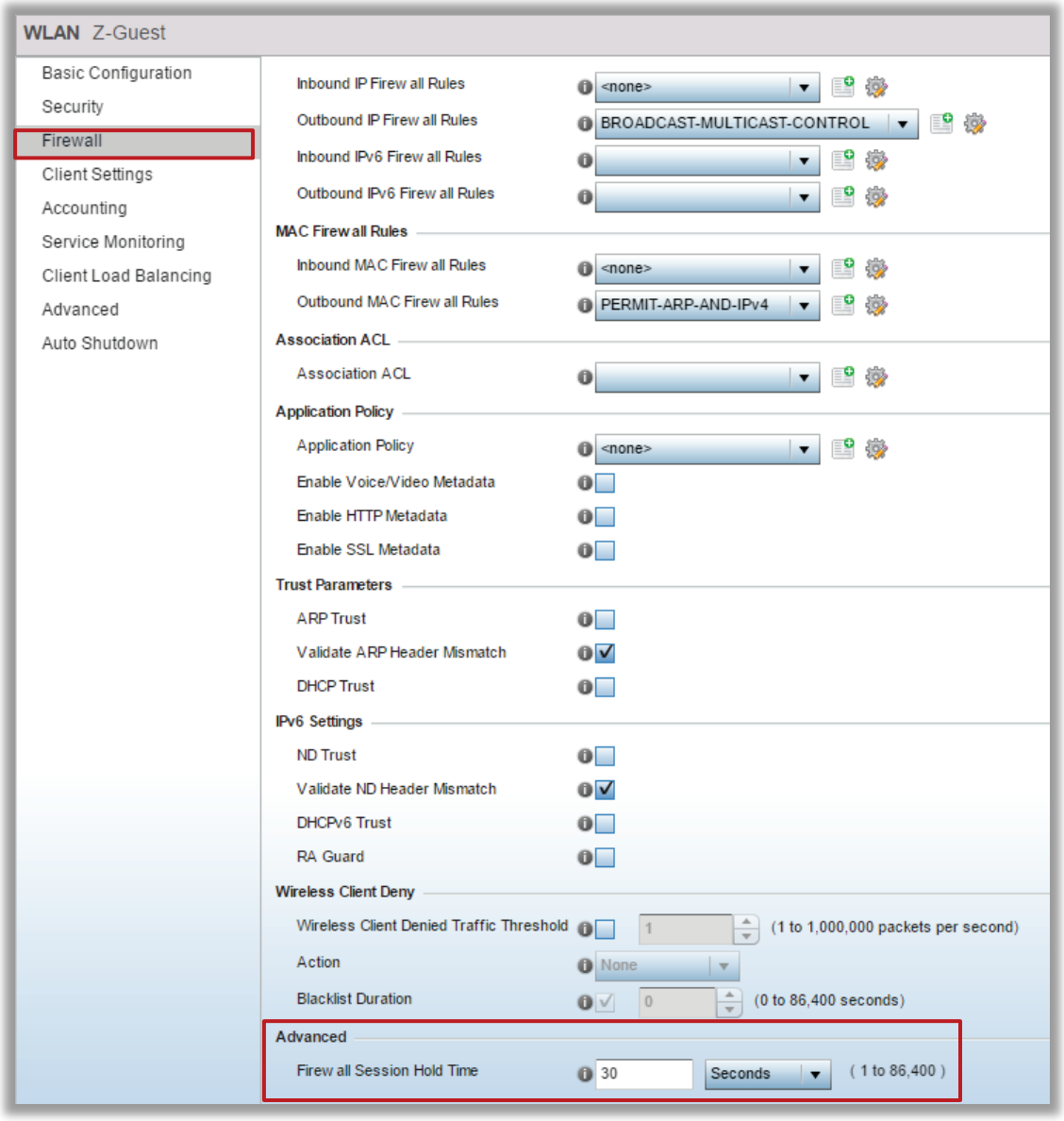
Whenever a wireless client associates to an Access Point, this AP will transmit a **WNMP** (Wireless Network Management Protocol) roaming notification inside the user VLAN (lo*cally bridge or tunneled VLANs). It serves several other purposes, one of them is also to update the **Forwarding Database** (FDB) of the wired switches or the FDB of the Controller if the VLAN is tunneled.

The WNMP message includes a MiNT ID of the Access Point, source MAC address is set to wireless client MAC address, destination address is a MAC Multicast address **01:A0:F8:F0:F0:04**, ethertype **0x8781**:

WNMP Frame	
SRC Address	Client MAC Address
DST Address	01-A0-F8-F0-F0-04

If the wireless client is roaming to a new AP, the old Access Point upon receiving WNMP roaming notification will initiate a firewall flow migration to the new AP via MiNT protocol (identified by MINT ID in WNMP message).

It is important to note that flow migration will occur if a wireless client roams within the `wireless-client hold-time`. Default `wireless-client hold-time` is 30 seconds:



Firewall Rules

Access control lists have been enhanced in WiNG 5 to simplify deployments. Standard and Extended rules have been deprecated and replaced with a single type of ACL. These ACL's no longer get numeric value ID's, but rather unique names. The rules can be applied to physical ports or virtual interfaces on individual devices (as device overrides) or across groups of devices through hardware profile. WiNG5 differentiates between IPv4 and IPv6 Access Lists.

IP firewall rules can contain up to 500 entries and are made of various configuration elements as listed below.

Policy Use and Configuration:

Firewall policies are used on hardware devices; controllers or access points. The “default” firewall policy is applied to all devices automatically – even new user-defined profiles, unless a user-defined firewall policy has been created and applied to a device or profile.

The default policy enables all pre-defined denial-of-service event types except for “TCP Packet Sequence” attacks. Additionally, services such as Proxy ARP and some of the Application Layer Gateways (ALG’s) are enabled and are applied globally on the WiNG 5 devices that the policy is applied to.

A capture of the default policy DoS events is shown below.

New Policy Creation

In most cases utilizing the default policy will be sufficient for all devices. An administrator may wish to create additional policies for various reasons; perhaps while performance testing and / or establishing baselines of the WLAN infrastructure, utilizing a minimal policy or to create custom properties separate from the working default policy. Whatever the reason, it is a simple process:

CLI Firewall Policy Creation

CLI Firewall Policy Creation:

```
vx9000#conf t
vx9000(config)#firewall-policy test-fw-policy
vx9000(config-fw-policy-test-fw-policy)#commit write
```

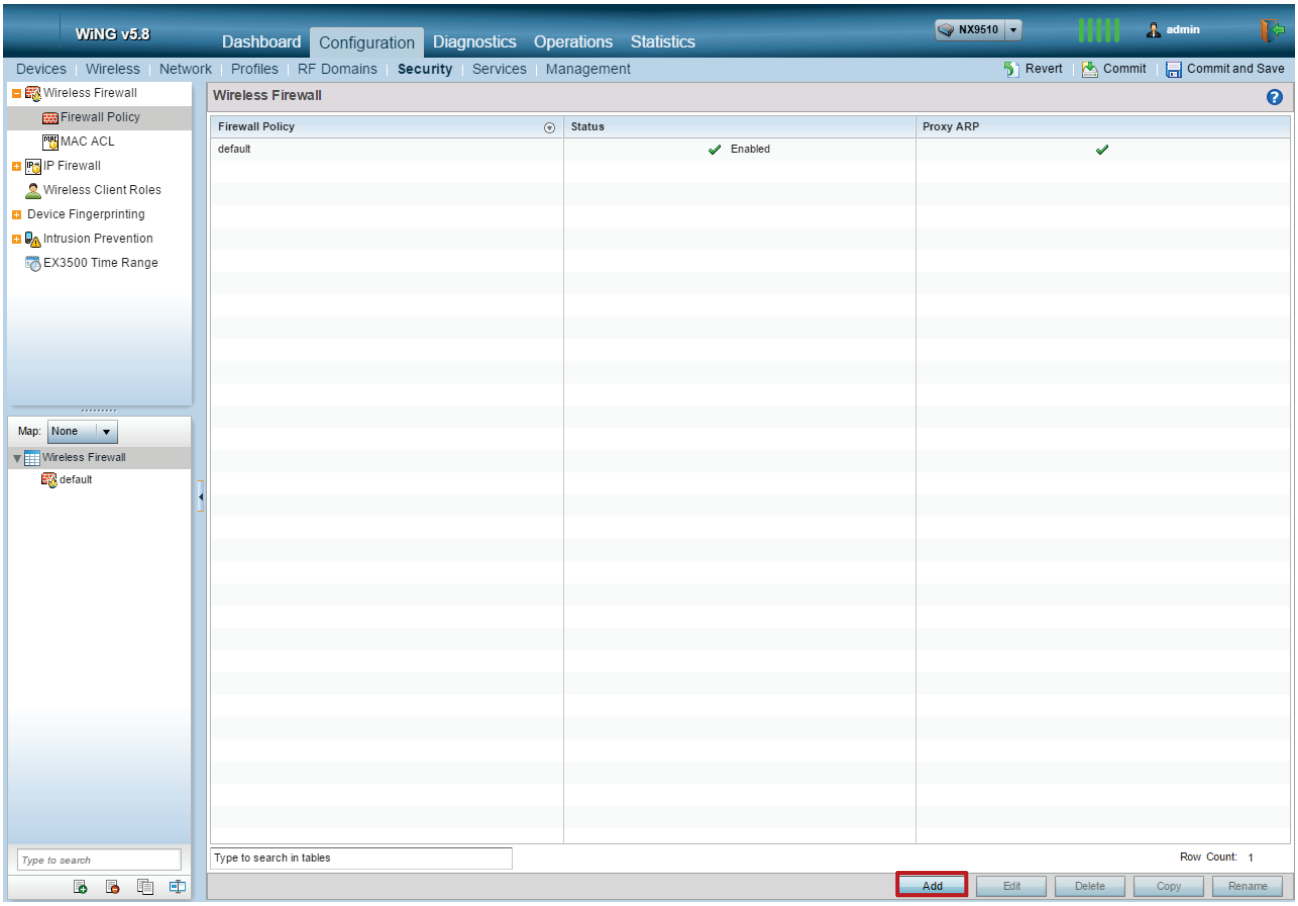
Firewall Policy Defaults:

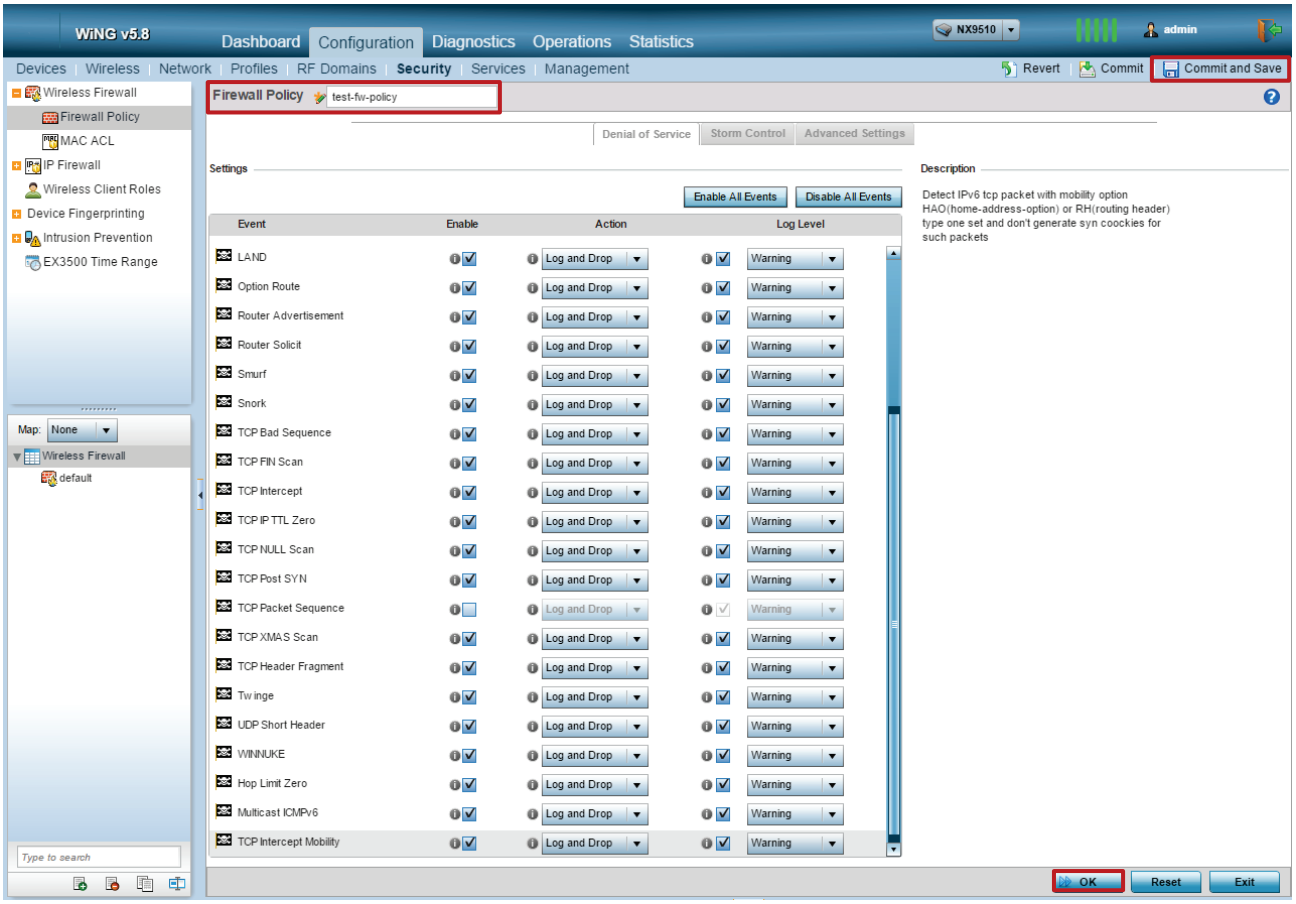
```
vx9000(config-fw-policy-test-fw-policy)#show context include-factory

firewall-policy test-fw-policy
 ip dos smurf log-and-drop log-level warnings
 ip dos twinge log-and-drop log-level warnings
 ip dos invalid-protocol log-and-drop log-level warnings
 ip dos router-advt log-and-drop log-level warnings
 ip dos router-solicit log-and-drop log-level warnings
 ip dos option-route log-and-drop log-level warnings
 ip dos ascend log-and-drop log-level warnings
 ip dos chargen log-and-drop log-level warnings
 ip dos fraggle log-and-drop log-level warnings
 ip dos snork log-and-drop log-level warnings
 ip dos ftp-bounce log-and-drop log-level warnings
 ip dos tcp-intercept log-and-drop log-level warnings
 ip dos broadcast-multicast-icmp log-and-drop log-level warnings
 ip dos land log-and-drop log-level warnings
 ip dos tcp-xmas-scan log-and-drop log-level warnings
 ip dos tcp-null-scan log-and-drop log-level warnings
 ip dos winnuke log-and-drop log-level warnings
 ip dos tcp-fin-scan log-and-drop log-level warnings
 ip dos udp-short-hdr log-and-drop log-level warnings
 ip dos tcp-post-syn drop-only
 ip dos tcphdrfrag log-and-drop log-level warnings
 ip dos ip-ttl-zero log-and-drop log-level warnings
 ip dos ipspoof log-and-drop log-level warnings
 ip dos tcp-bad-sequence drop-only
 no ip dos tcp-sequence-past-window
 ip tcp validate-rst-seq-number
 ip tcp validate-rst-ack-number
 ip tcp validate-icmp-unreachable
 ip tcp recreate-flow-on-out-of-state-syn
 ip tcp optimize-unnecessary-resends
 ip dos tcp-max-incomplete high 500
 ip dos tcp-max-incomplete low 200
 ip-mac conflict log-and-drop log-level warnings
 ip-mac routing conflict log-and-drop log-level warnings
 flow timeout icmp 30
```

```
flow timeout udp 30
flow timeout tcp setup 10
flow timeout tcp established 5400
flow timeout tcp close-wait 10
flow timeout tcp reset 10
flow timeout tcp stateless-general 90
flow timeout tcp stateless-fin-or-reset 10
flow timeout other 30
no dhcp-offer-convert
proxy-arp
firewall enable
ipv6 firewall enable
no ipv6 rewrite-flow-label
ipv6 strict-ext-hdr-check log-and-drop log-level warnings
ipv6 unknown-options log-and-drop log-level warnings
ipv6 duplicate-options log-and-drop log-level warnings
no ipv6 option end-point-identification
no ipv6 option router-alert
no ipv6 option network-service-access-point
ipv6 option strict-hao-opt-check log-and-drop log-level warnings
ipv6 option strict-padding log-and-drop log-level warnings
no ipv6 routing-type one
no ipv6 routing-type two
ipv6 dos multicast-icmpv6 log-and-drop log-level warnings
ipv6 dos hop-limit-zero log-and-drop log-level warnings
ipv6 dos tcp-intercept-mobility log-and-drop log-level warnings
acl-logging
stateful-packet-inspection-l2
flow dhcp stateful
alg ftp
alg tftp
no alg sip
alg dns
no alg facetime
no alg sccp
alg pptp
no logging icmp-packet-drop
no logging malformed-packet-drop
no logging verbose
no ip tcp adjust-mss
clamp tcp-mss
virtual-defragmentation
no virtual-defragmentation minimum-first-fragment-length
virtual-defragmentation maximum-fragments-per-datagram 140
virtual-defragmentation maximum-defragmentation-per-host 8
virtual-defragmentation timeout 1
dns-snoop entry-timeout 1800
no 802.2-encapsulation
no vlan-stacking
dns-snoop drop-on-parserror
proxy-nd
ipv6-mac conflict log-and-drop log-level warnings
ipv6-mac routing conflict log-and-drop log-level warnings
```

Web UI Firewall Policy Creation





At this point events can be disabled as desired or the action can be changed from the default of "Log and Drop" to either "Log Only" or "Drop Only". Also Storm Controls can be created for unknown Unicast, Multicast, Broadcast or ARP traffic and for Interface Type and the Threshold. Use of the Storm Controls mechanism should be done only after careful consideration and an understanding of what "normal" network traffic is. If a proper baseline is not established and the thresholds are set too low, it may interfere with normal production traffic.

In general, firewall policies are an "all or nothing" feature. They provide the core fundamental services typically associated with a good firewall. The real functionality of the WiNG 5 firewall services is in the stateful inspection IPv4 / IPv6 and MAC firewall rules. The remainder of this How-To will cover configuration and examples.

Firewall Rules

Stateful Inspection IP Rules

Stateful inspection of IPv4 or IPv6 flows is provided for when the flows are being switched or routed by either a wireless switch or an AP, depending which device is in the data path and how close it is to where the rule should take effect. When choosing where to apply your firewall rule, think about the data flow that you are trying to police (tunnel vs local bridging, wireless:WLAN vs wired:SVI/GE, etc).

For non-IPv4/IPv6 traffic (IPX, AppleTalk, etc.), inspection is stateless.

Rules follow a common syntax with a traffic match condition, an action and logging if so configured. The firewall rules can be assigned to:

- Physical ports – inbound
- Logical interfaces (SVI, Tunnel) – inbound
- WLAN's – inbound and outbound
- Wireless clients (using Role Based Firewall)

In WiNG 5 there are no "standard" and "extended" numbered rules; there are just uniquely named rules and actions configured within them. Each uniquely defined firewall rule may have up to 500 entries, as shown below:

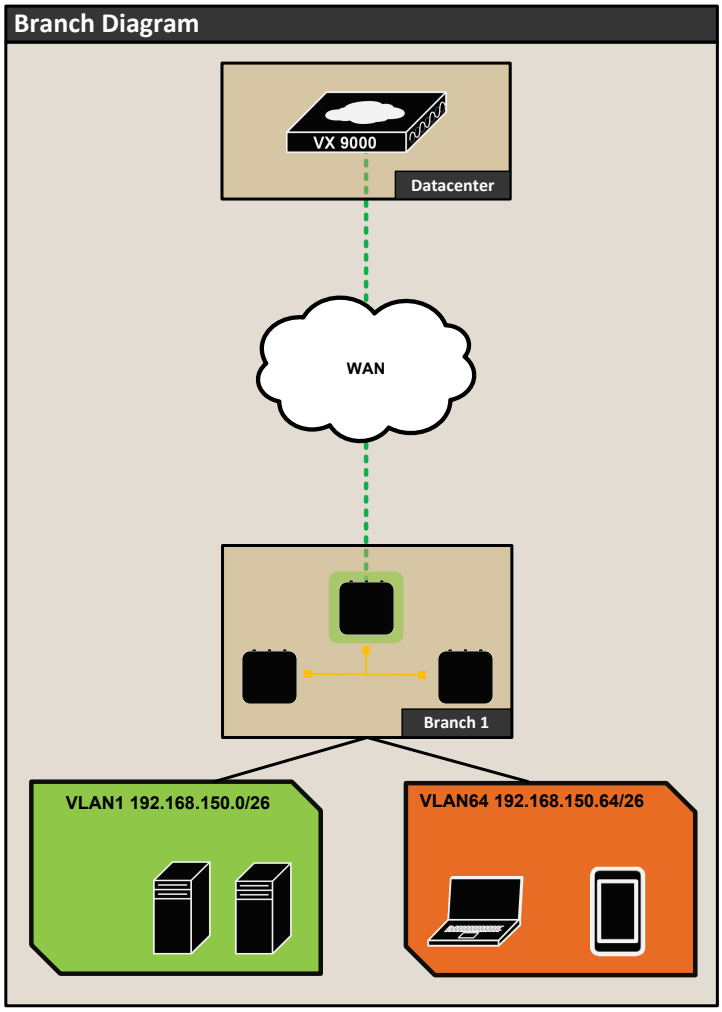
IPv4 Firewall Policy Elements	
Precedence Value	The order the rule is placed within the ACL (1-5000)
Action	Two options: Allow – permits the IP Flow Deny – blocks the IP Flow
DNS Name	DNS Name can be specified as a match criteria.
DNS Match Type	Three options: Exact for a FQDN Suffix for the Domain name or its part Contains to match a portion of the DNS or Domain Name.
Source IP	Source Host IP, Network, ALIAS, or Any.
Destination IP	Destination Host IP, Network, ALIAS, or Any.
Protocol	The service ALIAS or IP protocol number (0-254).
Source Port	Equals, Range, ALIAS or Any.
Destination Port	Equals, Range, ALIAS or Any.
Start VLAN	Source VLAN or VLAN range for IPv4 packets as a match criteria.
End VLAN	End of VLAN or VLAN range for IPv4 packets as a match criteria.
Mark	Two options: DSCP – layer 3 marking with DSCP tag (0-63) 802.1p – layer 2 marking with 802.1p tag (0-7)
Log	Log packets that match the rule

Example 1: Branch Location IP Rules

The first scenario is that of a branch location for a company, who wishes to keep all WLAN traffic local to the site. WLAN users cannot get to any other destination that is not a local address, either on the WLAN or LAN. This will be accomplished using a simple IP access-list that allows traffic from the WLAN to local network destinations; however it will block any WLAN IP traffic that is destined for any other destination that is not a local address.

The branch utilizes AP7522s, which are adopted over layer-3 to a centralized controller at Corporate. A custom profile has been created for the site. Also, a WLAN called “branch-wlan” has been created and is in use at the branch location. We must consider the following:

- There is an external DHCP server to the branch location networks
- Traffic is locally bridged by Access Points
- WLAN users will need to obtain IP addresses
- WLAN users can communicate via IP to local addresses (192.168.150.0/26 and 192.168.150.64/26)
- WLAN users cannot get to any other destinations



Configuration and Propagation

Since the AP7522 is adopted to a centralized controller, we will modify our master configuration, focusing on our branch firewall rules and profile changes so that the configuration will be pushed to the remote device. We will cover configuration at the CLI, followed by configuration via the Web UI.

IPv4 ACL – CLI Configuration

CLI IP ACL Configuration

```
vx9000#conf t
vx9000(config)#ip access-list wlan-branch-clients
vx9000(config-ip-acl-wlan-branch-clients)#permit udp any any eq dhcps rule-precedence 5
vx9000(config-ip-acl-wlan-branch-clients)#permit ip 192.168.150.0/25 192.168.150.0/25 rule-precedence 10
vx9000(config-ip-acl-wlan-branch-clients)#deny ip any any log rule-precedence 20
```

CLI IP ACL Assignment (WLAN)

```
vx9000(config)#wlan branch-wlan
vx9000(config-wlan-branch-wlan)#use ip-access-list in branch-wlan-clients
vx9000(config-wlan-branch-wlan)#commit write
```

CLI configuration is very simple; create the desired firewall rule (ACL) and then apply it. In the previous example, by applying the rule inbound on the WLAN, we catch and process the traffic at the edge, closest to the traffic source. Of course the rule could be applied to other interfaces, which would also require modification of the individual lines.

To see the statistics for our firewall rule we must go to the access-point(s), as we have applied the firewall rule inbound on the WLAN; if we attempt to view statistics at the controller, there will not be any for this particular rule. Connect to an access-point where clients are associated and view the stats, as seen below:

IPv4 ACL – Statistics CLI

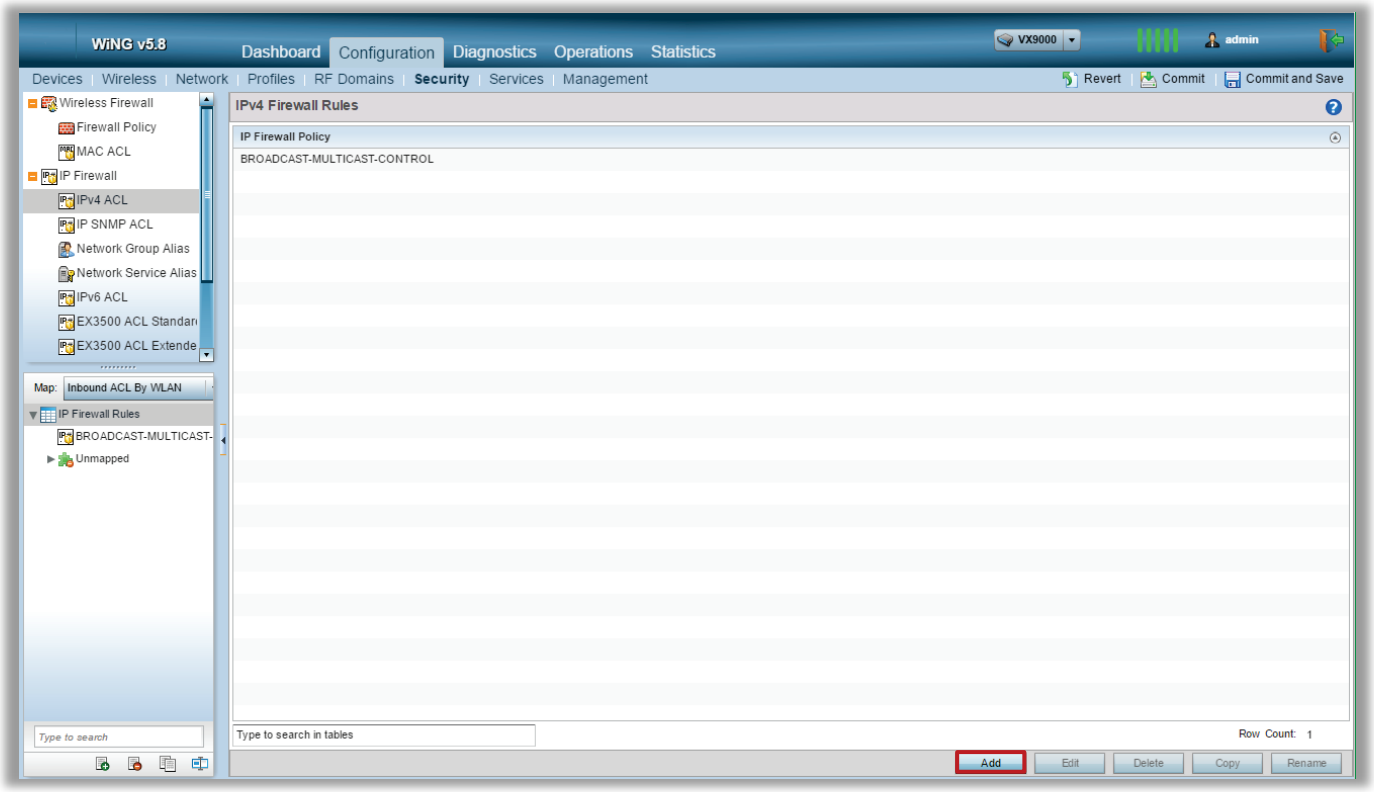
```
vx9000#show ip-access-list stats wlan-branch-clients on 8533-C0-1
IP Access-list: wlan-branch-clients
  permit udp any any eq dhcps rule-precedence 4        Hitcount: 1
  permit ip 192.168.150.0/25 192.168.150.0/25 rule-precedence 10        Hitcount: 141
  deny ip any any log rule-precedence 20        Hitcount: 88
```

IPv4 ACL – Web UI Configuration

Let's look now at the Web UI configuration. Within the web interface, navigate to "Configuration

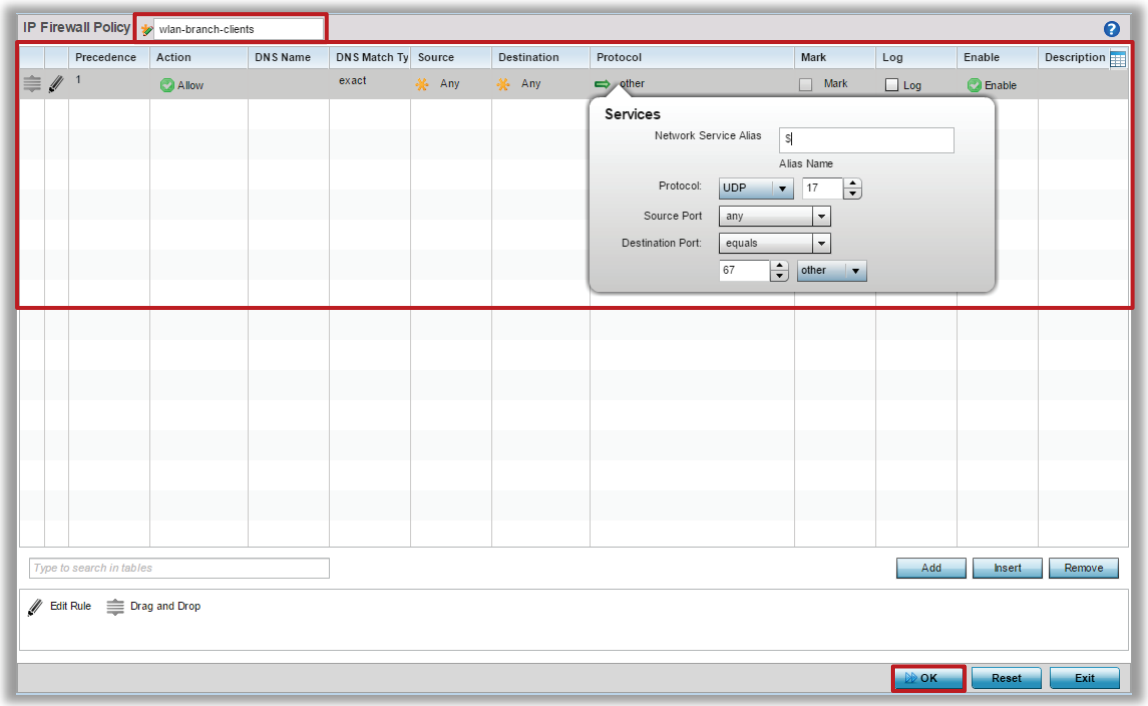
> Security > IP Firewall Rules", then click "Add" in the main working pain, as seen in the example

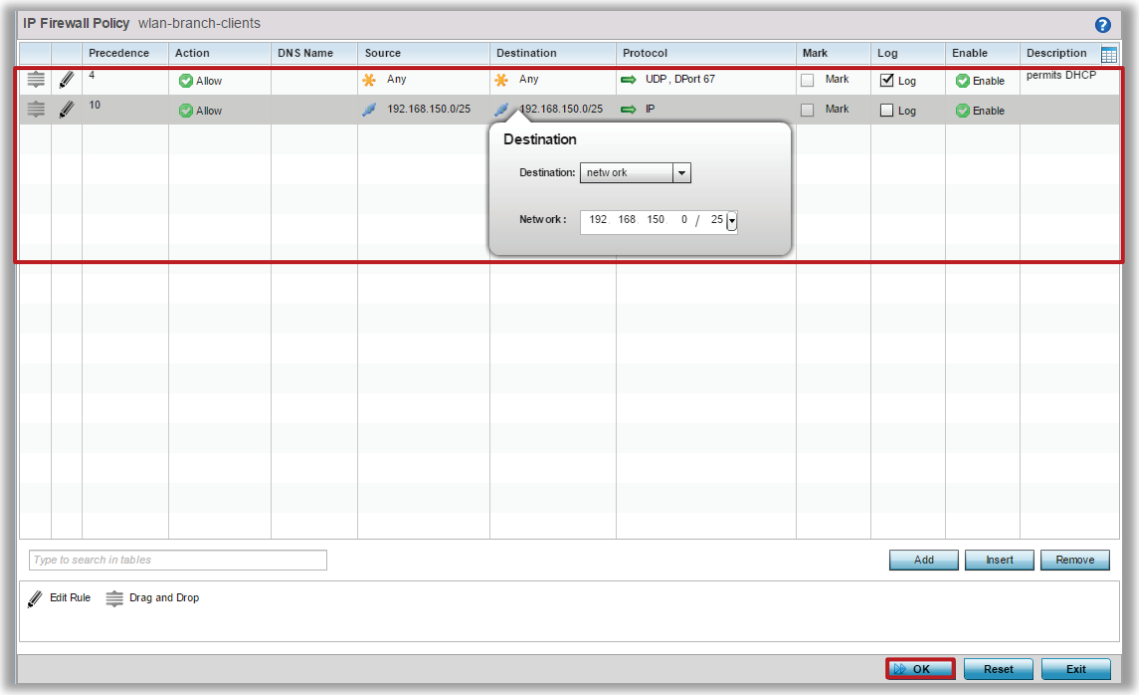
IPv4 ACL – Web UI Configuration

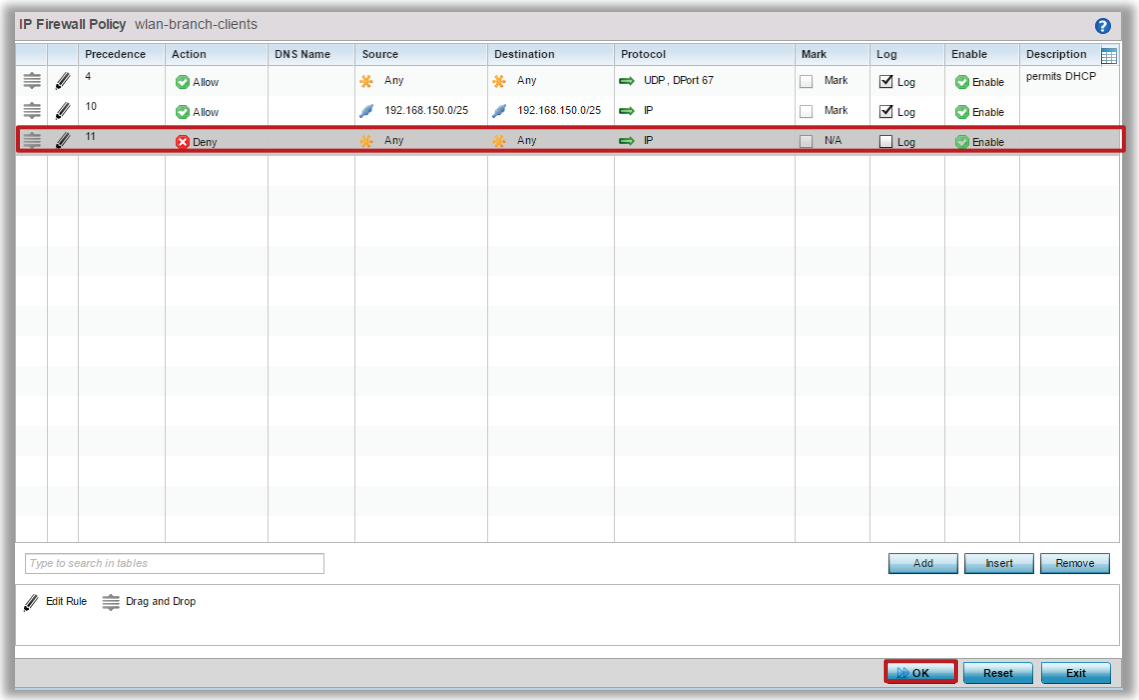


You will be presented with the IP Firewall Rules main working screen. Give your firewall rule (access-list) a unique name, click "**+Add Row**", then click on the newly added row to create your rule parameters.

IPv4 ACL – Web UI Configuration





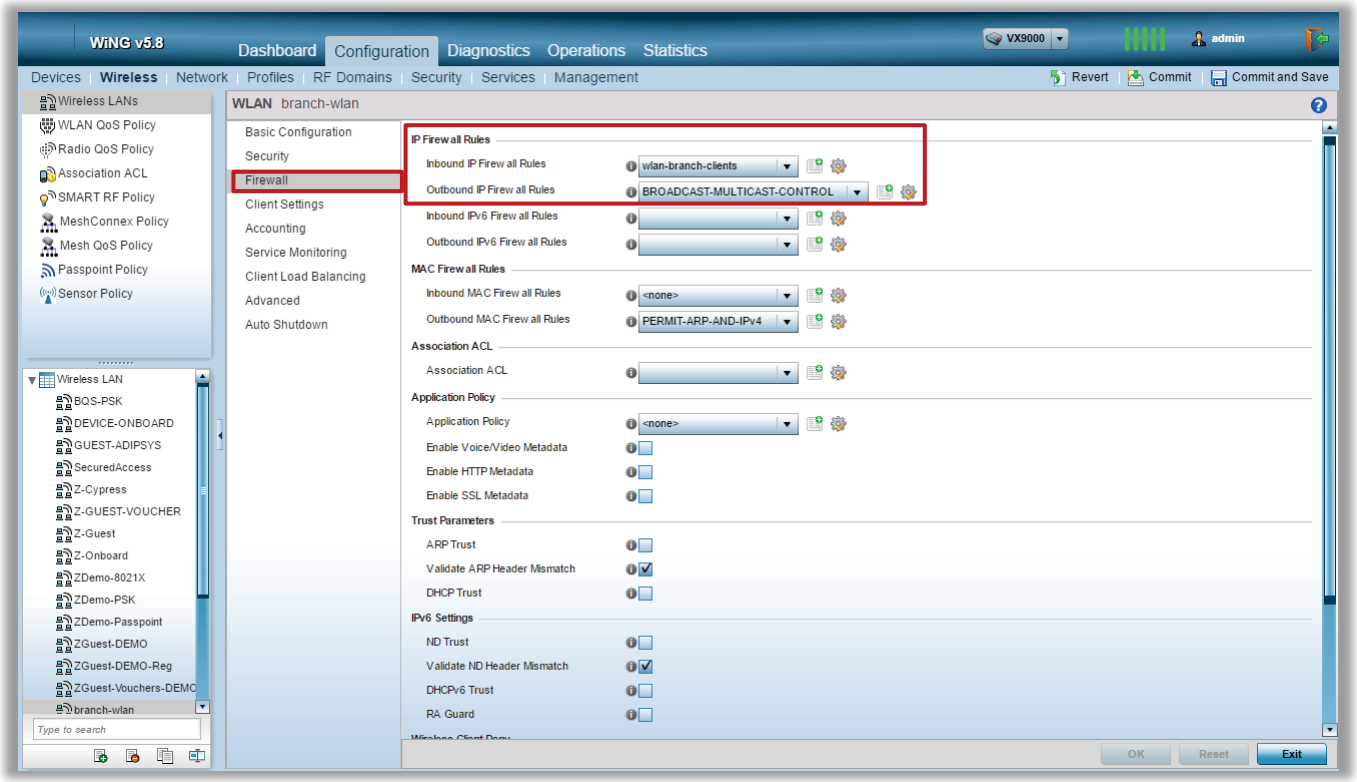


Once the rule definition is complete, don't forget to Commit and Save your work.

The next Web UI step is to apply the IP firewall rule to the WLAN. When applying rules to WLAN's, one has the option of choosing inbound or outbound directions. Inbound on a WLAN is from the wireless client "in" to the access-point / wired network. Outbound would apply from the access-points perspective "out" to the wireless clients / radio. In our example, we will apply the firewall rule inbound. We will also apply the default "BROADCAST-MULTICAST-CONTROL" Access List to the outbound direction, as a best practice to reduce the amount of unneeded traffic (IP Multicast, Netbios, ICMP Broadcast) hitting the air.

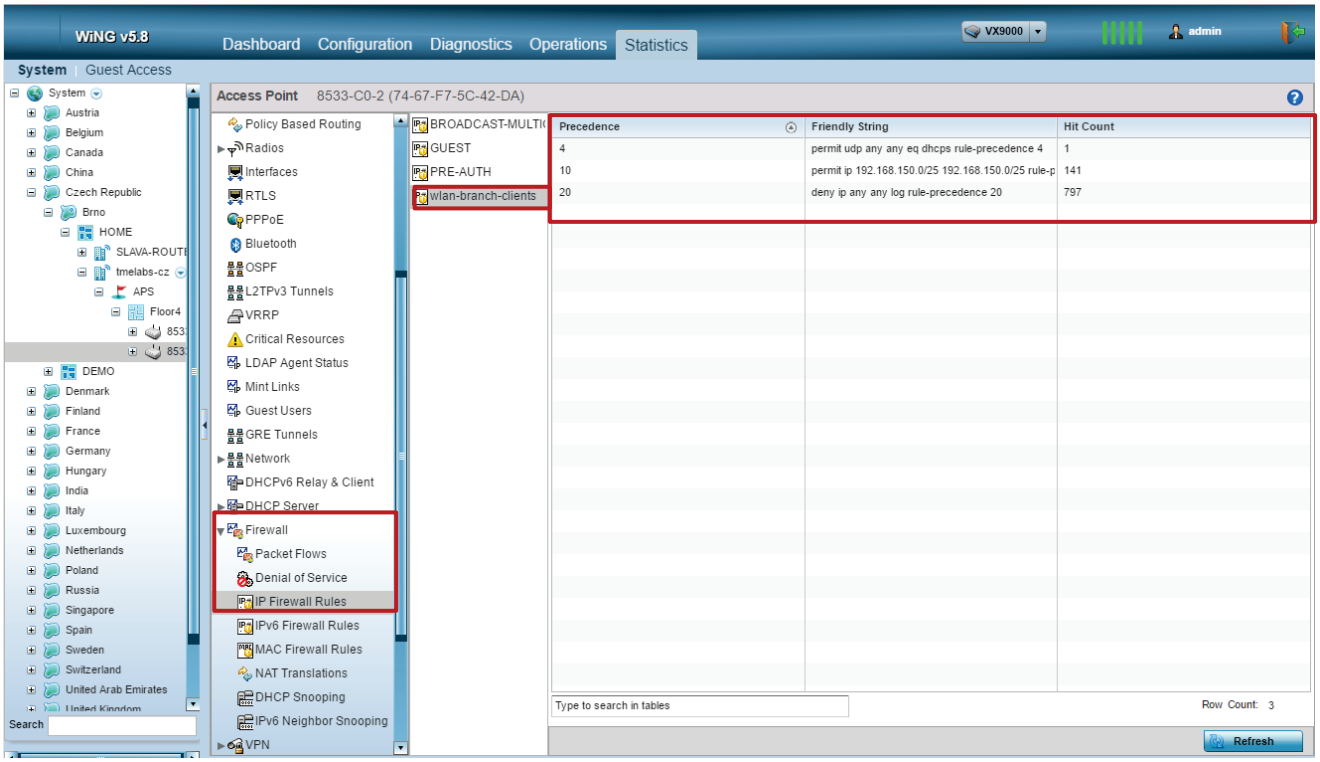
Navigate to "**Configuration > Wireless > Wireless LANs**" and select the WLAN to which the firewall rule will be applied. Then click "**Edit**".

IPv4 ACL WLAN Assignment – Web UI Configuration



To view the statistics within the web UI, navigate to "Statistics", and select an access- point. The statistics working pane will show; from here navigate to "Firewall > IP Firewall Rules" then select the firewall rule that was created. The statistics can be refreshed to confirm that the rule is in effect.

IPv4 ACL – Web UI Statistics



Stateful Inspection MAC Rules

Like the IP firewall rules, MAC firewall rules are also stateful for IP flows and stateless for non IP flows. One can specify mac-addresses in any, host and mask formats and specify source and destination, as with IP firewall rules.

As one would assume, MAC firewall rules inspect traffic at layer-2. As such, other flags within a layer-2 header can be inspected, such as 802.1q vlan tag or 802.1p priority markings. We can then apply our action based on these flags as well as the designated ethertype.

MAC firewall rules can be applied to the following types of interfaces:

- Inbound or Outbound on WLANs
- Inbound on Physical Interfaces (GE1, GE2, XGE1, etc)
- Inbound or Outbound on Wireless Clients (via Role Based Firewall)

They cannot be applied to L3 SVI's (VLAN interfaces), as these are logical L3 interfaces.

Following are the different elements of a MAC firewall rule:

IPv4 Firewall Policy Elements	
Precedence Value	The order the rule is placed within the ACL (1-5000)
Allowance	Two options: Allow – permits the IP Flow Deny – blocks the IP Flow
Source MAC	Host, Range, or Any.
Destination MAC	Host, Range, or Any.
Action	Log, Mark (802.1p / DSCP) or Traffic Class for IPv6 header
Ethertype	Ethertype (1-65535 Ethertype Protocol number). Pre-defined: 8021q VLAN Ether Type (0x8100) aarp AARP Ether Type (0x80F3) appletalk APPLETALK Ether Type (0x809B) arp ARP Ether Type (0x0806) ip IP Ether Type (0x0800) ipv6 IPv6 Ether Type (0x86DD) ipx IPX Ether Type (0x8137) mint MINT Ether Type (0x8783) rarp RARP Ether Type (0x8035) wisp WISP Ether Type (0x8783)
VLAN ID	Source VLAN or VLAN range for IPv4 packets as a match criteria.
Log	Log packets that match the rule

Branch Location MAC Rules

Continuing with our example from section 3.1.1, our company now wishes to further control VLAN 64 and the associated WLAN by ensuring only certain ethertypes are allowed on the network, for example it is not desirable to have IPv6 traffic on the network, as well as any legacy non-IP traffic like IPX This can be accomplished by using a default MAC ACL that is included in each WiNG5 configuration.

Configuration and Propagation

MAC ACL – CLI Configuration

```
VX-1#conf
Enter configuration commands, one per line.  End with CNTL/Z.
VX-1(config)#mac access-list PERMIT-ARP-AND-IPv4
VX-1(config-mac-acl-PERMIT-ARP-AND-IPv4)#show context
mac access-list PERMIT-ARP-AND-IPv4
 permit any any type ip rule-precedence 10 rule-description "permit all IPv4 traffic"
 permit any any type arp rule-precedence 20 rule-description "permit all ARP traffic"
```

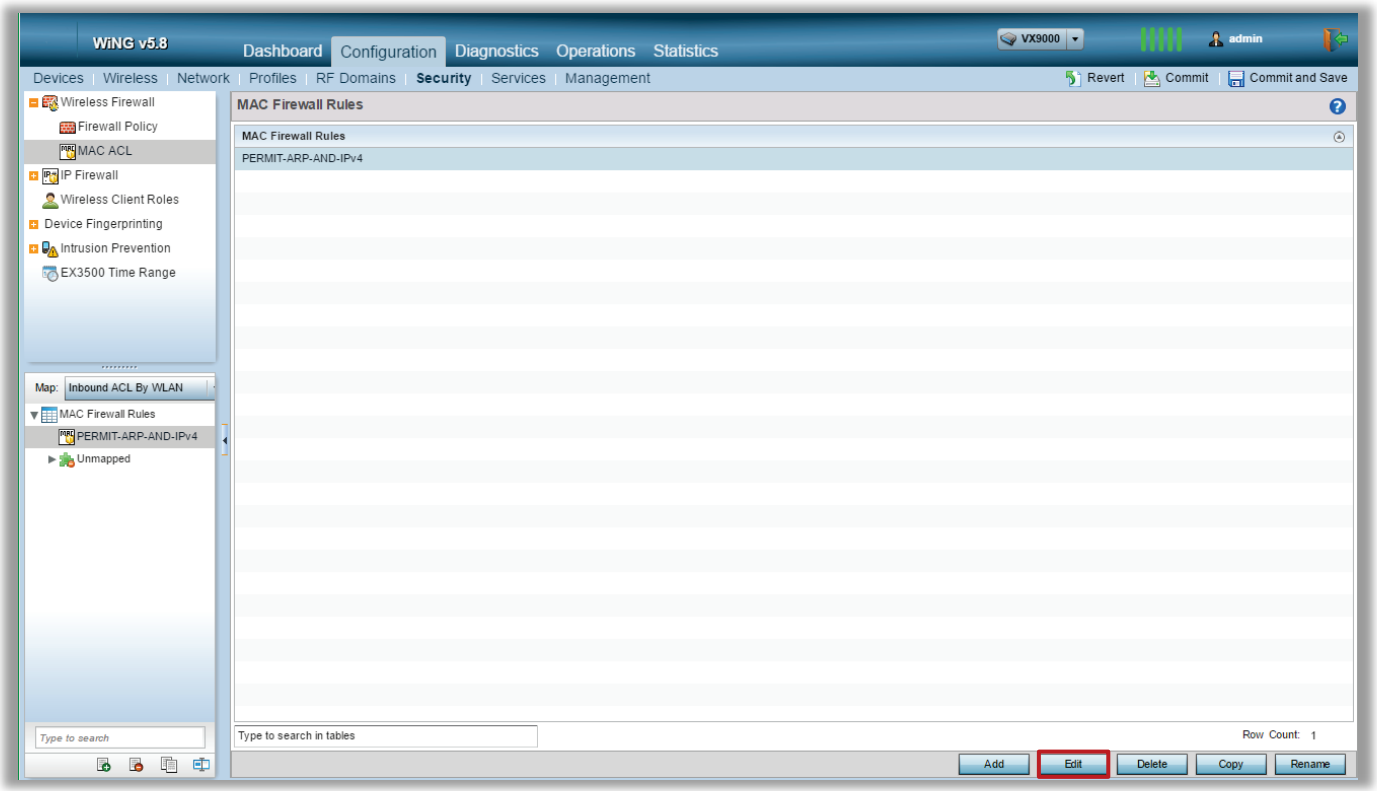
MAC ACL WLAN Assignment– CLI Configuration

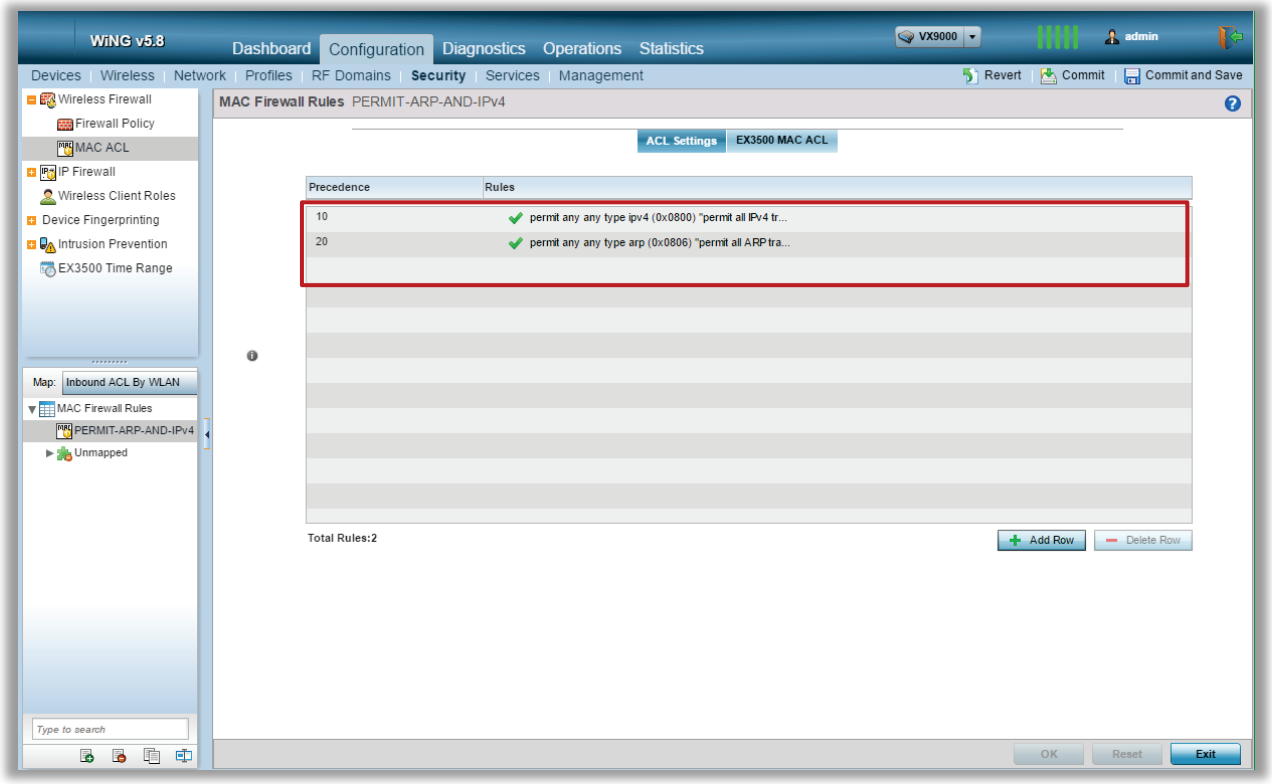
```
VX-1#conf
Enter configuration commands, one per line.  End with CNTL/Z.
VX-1(config)#wlan branch-wlan
VX-1(config-wlan-branch-wlan)#W
VX-1(config-wlan-branch-wlan)#use mac-access-list out PERMIT-ARP-AND-IPv4
```

As seen in the configuration above, it is rather simple in this example. We are allowing only ethertypes corresponding to ARP and IPv4 traffic to pass in and out to the branch WLAN. Of course, we could also specify metrics based on MAC address range or wildcard if so desired.

Configuration in the Web UI is similar to that of creating the IP Firewall rules and applying them. Navigate to "**Configuration > Security > MAC Firewall Rules**" and select already created policy "PERMIT-ARP-AND-IPv4" in the main working pane to add a new rule set.

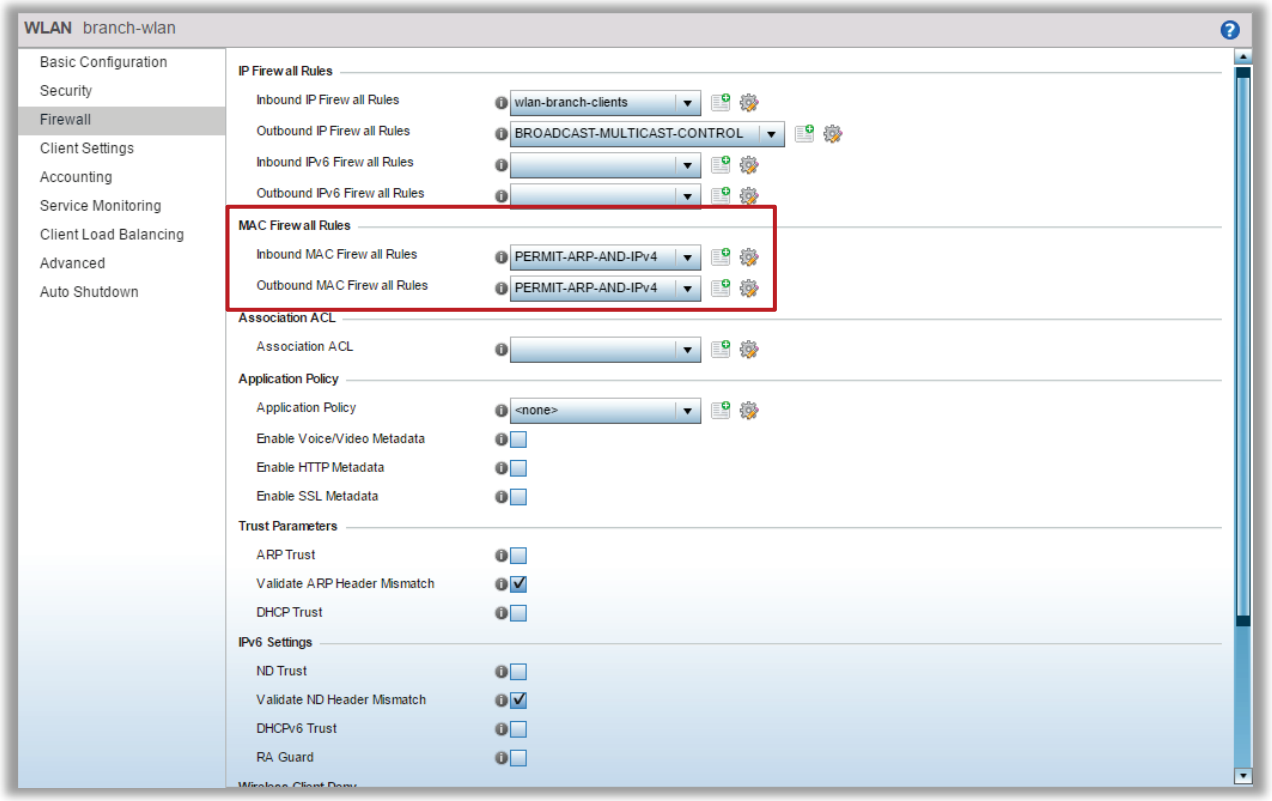
MAC ACL – Web UI Configuration





Since we already have a rule created, we don't need to commit or save any changes. We only need to apply it to the desired interface; in our example, we will be applying to WLAN "branch-wlan", both inbound and outbound direction. Navigate to "Configuration > Wireless" and select the desired WLAN; click "Edit":

MAC ACL WLAN Assignment – Web UI Configuration



Using Aliases in Firewall Rules

In WiNG 5 deployment scenarios it is common for different sites to have configuration parameters which are similar with the exception of a small number of values, for example different IP networks, host IP addresses or VLAN IDs per site.

In regards to IPv4 firewall rules instead of defining separate ACLs for each site to account for these small differences, it is much more efficient to substitute them by Alias Names which are then mapped to real values under each RF Domain or at a system level.

This permits common ACLs be shared between sites yet permits site specific parameters to be applied to a subset of sites or each individual site. It is recommended to utilize Aliases in large scale deployments to simplify configuration, limit number of configuration objects needed allowing configuration re-use.

ALIAS is a named object that can identify a host, network, protocol, port or range of ports, etc. ALIAS value is defined either under system level in global configuration or under RF Domain or Device Profile context to assign a site-specific value.

In total there are 6 different Alias types that can be used with IP Access Lists:

Alias Type	Description
Host Alias	Defines a unique IPv4 host. Example: $DNS-SERVER = 8.8.8.8
Address Range Alias	Defines an IPv4 address range. Useful for declaring DHCP scopes. Example: $DHCP-SCOPE 192.168.10.50 to 192.168.10.150
Network Alias	Defines an IPv4 subnet. Example: $CORP-DEVICES = 192.168.10.0/24
Network Group Alias	Can contain multiple hosts, subnets or address ranges. Useful to combine multiple networks or hosts into one group. Example: $FILE-SERVERS = 192.168.10.5 192.168.30.10 192.168.20.25
Network Service Alias	Can contain multiple entries of different protocol types and ports. Useful to define custom application signatures. Example: $IPSEC = alias network-service $IPSEC proto 50 proto udp 500 proto udp 4500
VLAN Alias	Defines an 802.1Q VLAN ID. Example: $GUEST-VLAN = 100

IP ACL Configuration using Aliases

Continuing with our example from section 3.1.1, our company now wishes to open a Guest WiFi on a network 192.168.100.0/24, which will require to tighten up security rules. The requirement is to allow only Web traffic (HTTP and HTTPS), as well as IPSEC to allow usage of VPN client software for end host encryption.

In case we would use ACL without Aliases the set of rules would look like this:

Precedence	Action	Source	Destination	Protocol	Log
10	Permit	Any	Any	UDP Src:67 Dst:68	No
11	Permit	192.168.100.0/24	208.67.222.222	UPD Dst:53	No
12	Permit	192.168.100.0/24	208.67.220.220	UPD Dst:53	No
20	Permit	192.168.100.0/24	Any	TCP Dst:80	No
21	Permit	192.168.100.0/24	Any	TCP Dst:443	No
30	Permit	192.168.100.0/24	Any	ESP	No
31	Permit	192.168.100.0/24	Any	UPD Dst:500	No
32	Permit	192.168.100.0/24	Any	UPD Dst:4500	No
100	Deny	192.168.100.0/24	Any	IP	Yes

By using Aliases in this scenario the set of rules can be reduced down to 5, which will provide an easy way to manage it and change rules if needed:

Precedence	Action	Source	Destination	Protocol	Log
10	Permit	Any	Any	$DHCP	No
11	Permit	$GUEST-NET	$DNS-SERVERS	$DNS	No
12	Permit	$GUEST-NET	Any	$WEB	No
20	Permit	$GUEST-NET	Any	$IPSEC	No
30	Permit	$GUEST-NET	Any	ESP	No
100	Deny	$GUEST-NET	Any	IP	Yes

Network Group Alias: $GUEST-NET
Network: 192.168.100.0/24

Network Group Alias: $DNS-SERVERS
Host: 208.67.222.222 Host: 208.67.220.220

Network Service Alias: $DHCP
Protocol: UDP Dst Port: 68

Network Service Alias $IPSEC
Protocol: ESP Protocol: UDP Dst Port: 500 Protocol: UDP Dst Port: 4500

Network Service Alias $DNS
Protocol: UDP Dst Port: 53

Network Service Alias $WEB
Protocol: TCP Dst Port: 80 Protocol: TCP Dst Port: 443

IPv4 ACL using Aliases – CLI Configuration

Aliases Definition – CLI Configuration

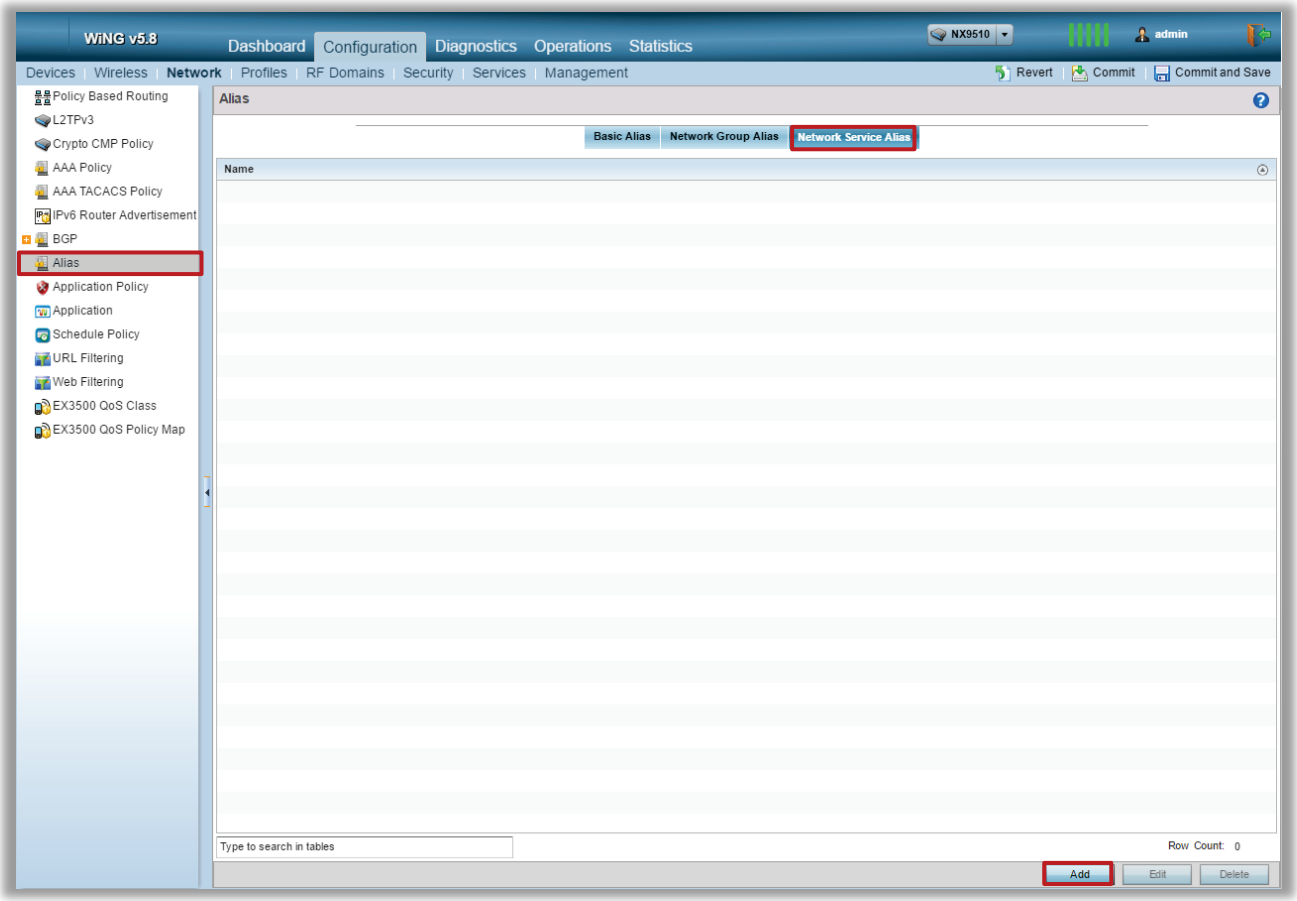
```
VX-1#conf
Enter configuration commands, one per line.  End with CNTL/Z.
VX-1(config)#alias network-service $DNS proto udp 53
VX-1(config)#alias network-service $DHCP proto udp 68
VX-1(config)#alias network-service $WEB proto tcp 80 443
VX-1(config)#alias network-service $IPSEC proto esp proto udp 500 4500
VX-1(config)#alias network-group $DNS-SERVERS host 208.67.222.222 208.67.220.220
VX-1(config)#alias network-group $GUEST-NET network 192.168.100.0/24
```

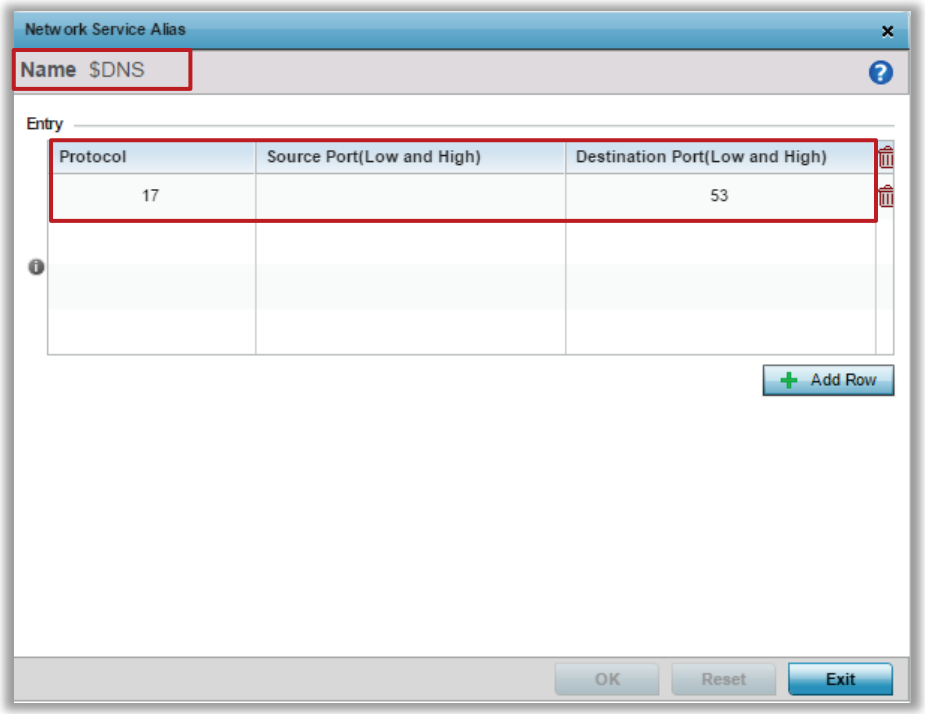
IPv4 ACL using Aliases – CLI Configuration

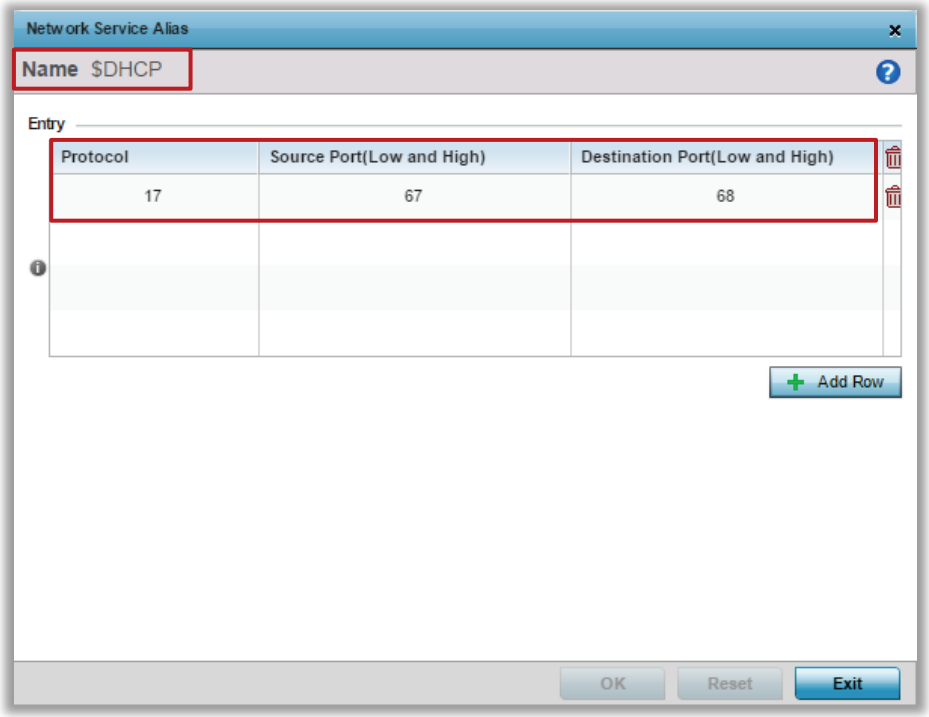
```
VX-1#conf
Enter configuration commands, one per line.  End with CNTL/Z.
VX-1(config)#ip access-list GUEST-NETWORK
VX-1(config-ip-acl-GUEST-NETWORK)#permit $DHCP any any rule-precedence 10
VX-1(config-ip-acl-GUEST-NETWORK)#permit $DNS $GUEST-NET  $DNS-SERVERS  rule-precedence 11
VX-1(config-ip-acl-GUEST-NETWORK)#permit $WEB $GUEST-NET  any rule-precedence 20
VX-1(config-ip-acl-GUEST-NETWORK)#permit $IPSEC $GUEST-NET  any rule-precedence 30
VX-1(config-ip-acl-GUEST-NETWORK)#deny ip any any rule-precedence 100
```

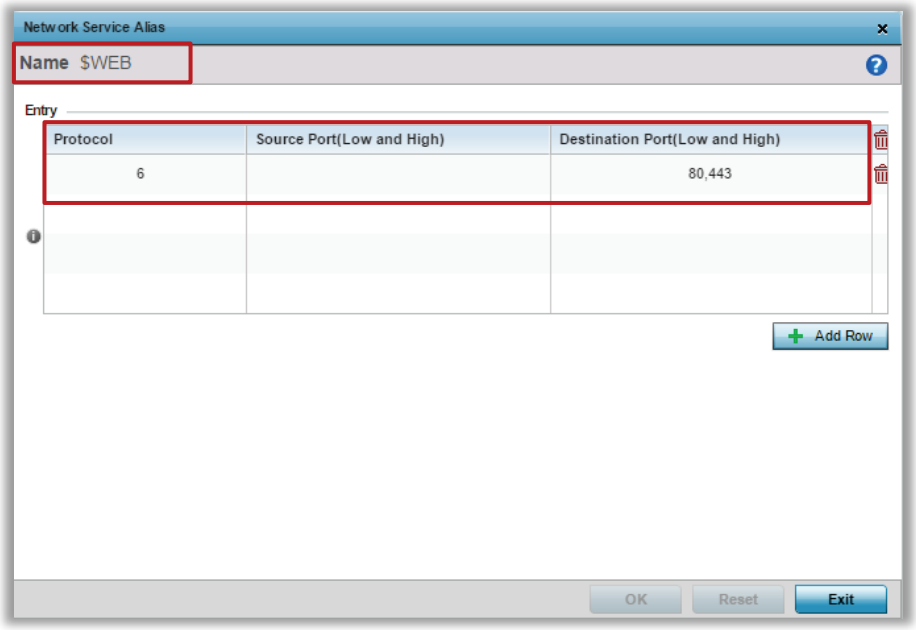
IPv4 ACL using Aliases – Web UI Configuration

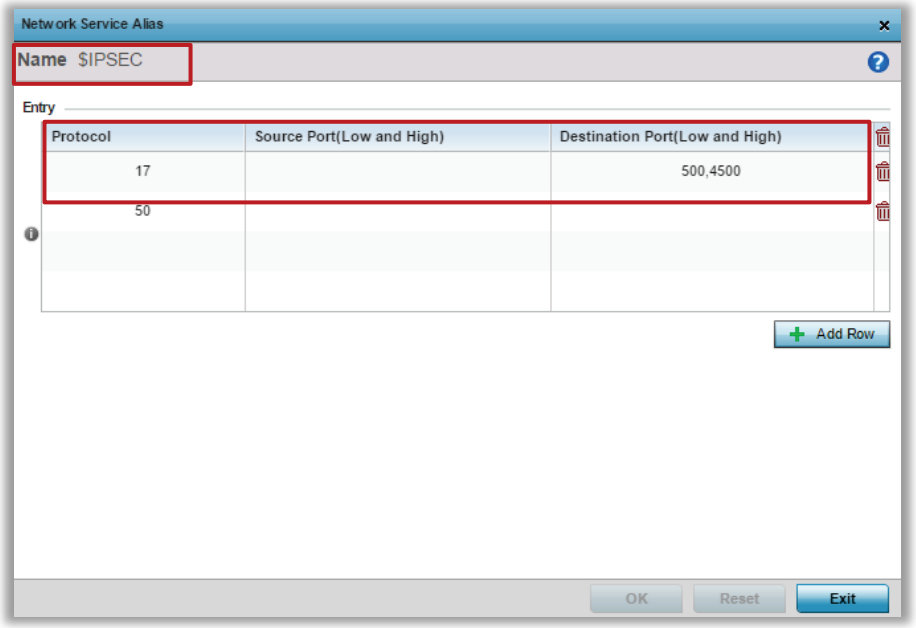
Configuration in the Web UI is similar to that of creating the IP Firewall rules and applying them. Navigate to "Configuration > Network > Alias > Network Service Alias" and click on "Add".





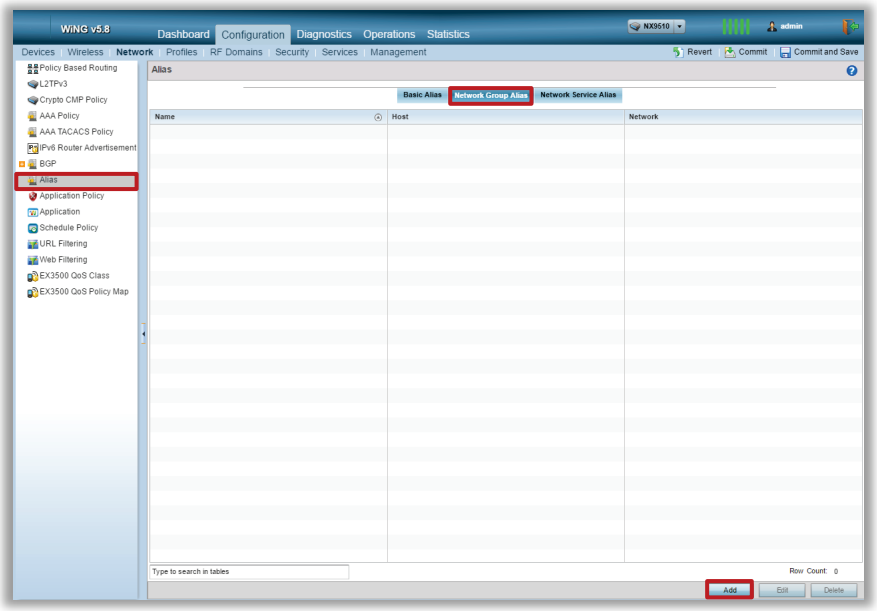


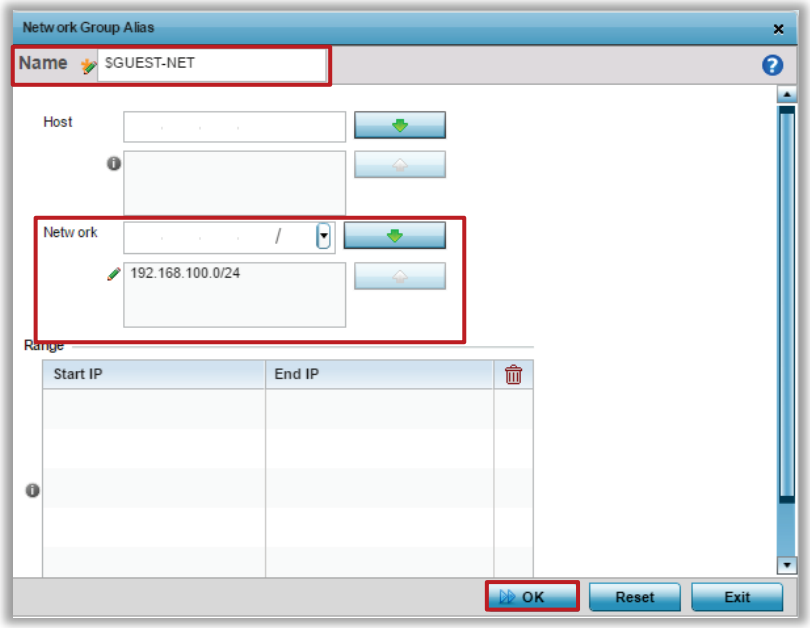


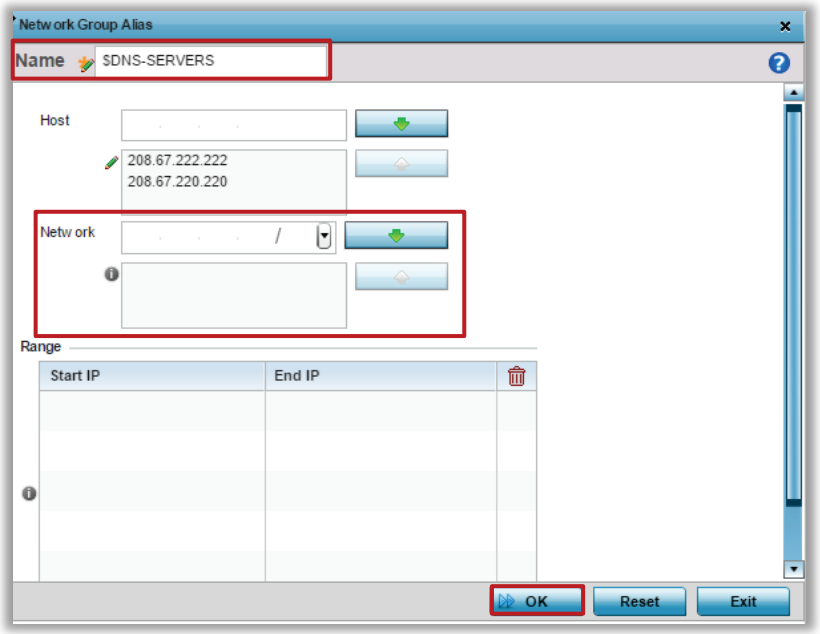


Network Group Aliases Definition – Web UI Configuration

Configuration > Network > Alias > Network Group Alias > Add







Firewall Statistics

Besides general ACL hit counts that are available for IP or MAC Access Lists, additional information about all firewall flows, dhcp snoop table or IPv6 neighbor table can be obtained from the WiNG UI or CLI.

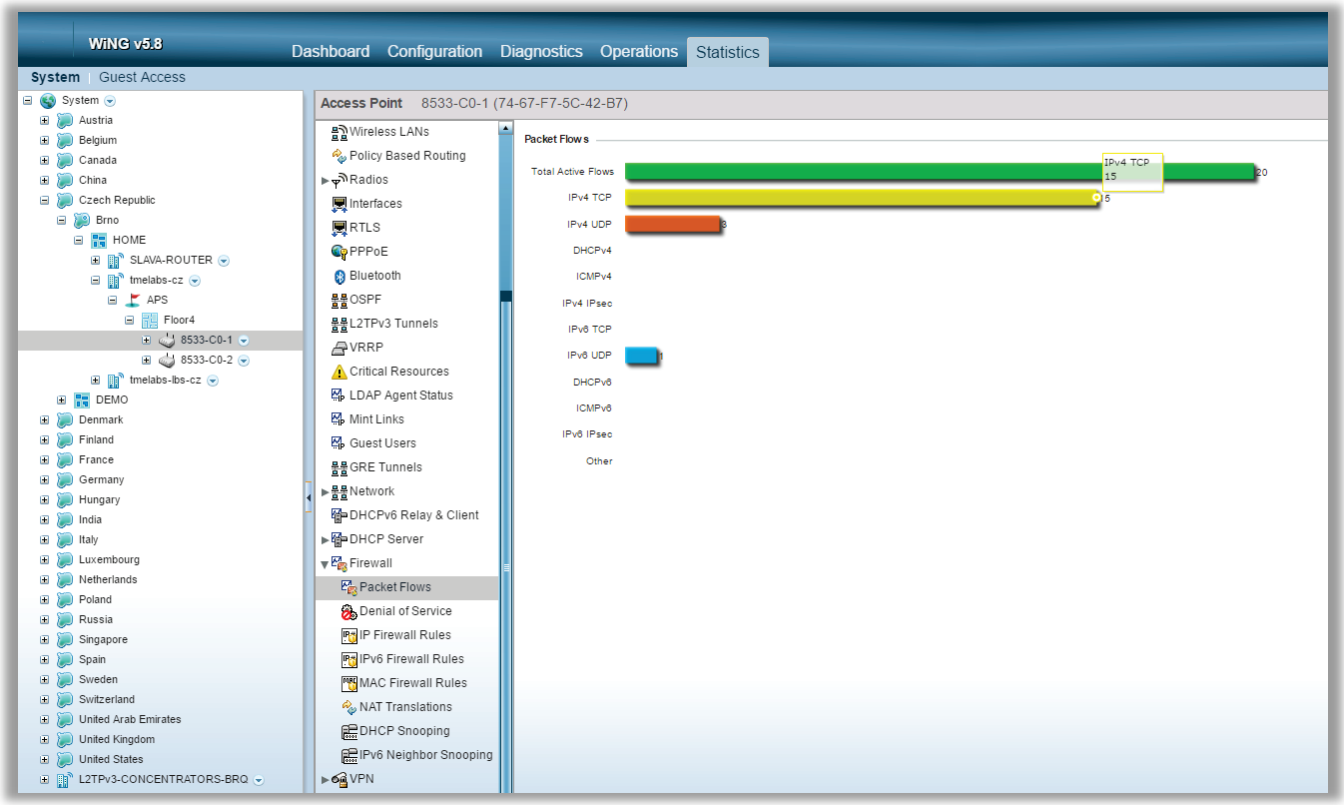
Firewall Flow Statistics – Summary

Firewall Flow information in CLI is available on a device level and can either provide detailed information for each active firewall session or a summary of this information:

Firewall Flow Statistics Summary - CLI

```
8533-C0-1#show firewall flows stats
Active Flows        18
TCP/IPv4 flows      16
UDP/IPv4 flows      1
DHCP/IPv4 flows     0
ICMP/IPv4 flows     0
IPsec/IPv4 flows    0
TCP/IPv6 flows      0
UDP/IPv6 flows      0
DHCP/IPv6 flows     0
ICMP/IPv6 flows     0
IPsec/IPv6 flows    0
L3/Unknown flows    0
```

Firewall Flow Statistics Summary – Web UI



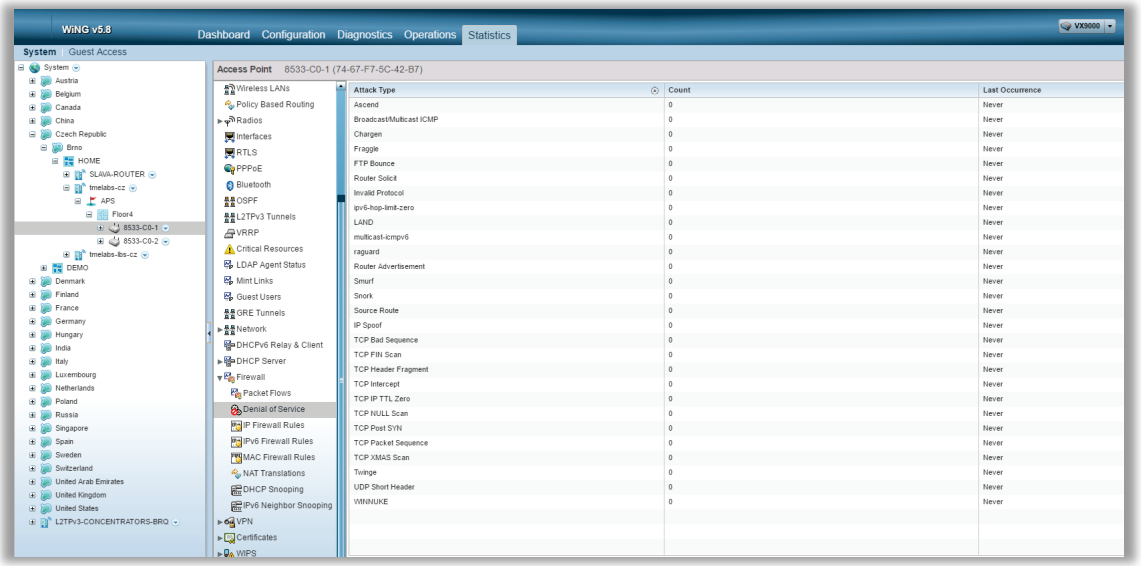
Firewall DOS Attack Summary

Firewall DoS statistics will show a number of times a particular attack was detected and what was the last time the attack occurred. Statistics are available on device level.

DOS Attack Summary - CLI

```
VX-1#show firewall dos stats on <device name>
-------------------------------------------------------------------------------
          ATTACK TYPE                    COUNT            LAST OCCURENCE
-------------------------------------------------------------------------------
  udp-short-hdr                          0                Never
  multicast-icmpv6                       0                Never
  icmp-router-solicit                    0                Never
  tcp-xmas-scan                          0                Never
  twinge                                 0                Never
  ascend                                 0                Never
  raguard                                0                Never
  tcp-bad-sequence                       0                Never
  broadcast-multicast-icmp               0                Never
  ftp-bounce                             0                Never
  spoof                                  0                Never
  source-route                           0                Never
  tcp-null-scan                          0                Never
  fraggle                                0                Never
  ipv6-hop-limit-zero                    0                Never
  land                                   0                Never
  tcp-fin-scan                           0                Never
  router-advt                            0                Never
  snork                                  0                Never
  tcp-post-syn                           0                Never
  winnuke                                0                Never
  tcp-header-fragment                    0                Never
  tcp-ip-ttl-zero                        0                Never
  chargen                                0                Never
  invalid-protocol                       0                Never
  tcp-intercept                          0                Never
  smurf                                  0                Never
  tcp-sequence-past-window               0                Never
-------------------------------------------------------------------------------
```

DOS Attack stats – Web UI

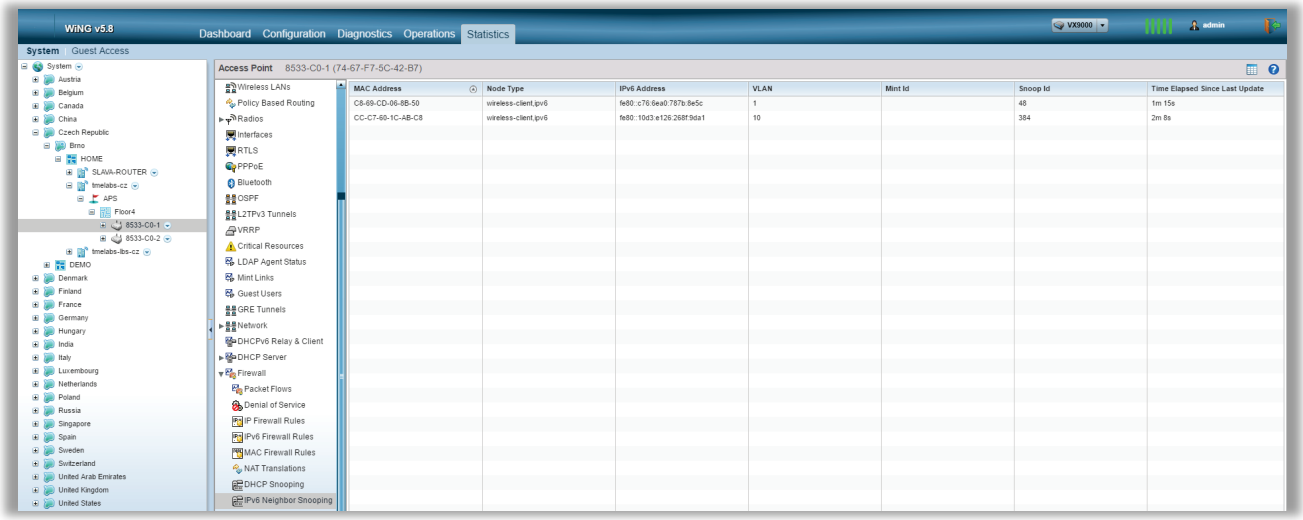


Firewall IPv6 Neighbor Snoop Table

IPv6 Neighbor Snoop Table – CLI

```
8533-C0-1#show firewall neighbors snoop-table
Snoop Binding <fe80::c76:6ea0:787b:8e5c, C8-69-CD-06-8B-50, Vlan 1>
Type wireless-client-ipv6, Touched 88 seconds ago
DAD Seen
--------------------------------------------------------------------------------
Snoop Binding <fe80::10d3:e126:268f:9da1, CC-C7-60-1C-AB-C8, Vlan 10>
Type wireless-client-ipv6, Touched 141 seconds ago
--------------------------------------------------------------------------------
```

IPv6 Neighbor Snoop Table – Web UI



Firewall Flows Detailed Statistics

Detailed firewall flow information is available under device context in CLI. It provides information like forward and reverse path of the flow, connection state (if TCP), number of packets and bytes transmitted, application associated with the flow (if DPI engine is available and enabled), as well as the flow timeout.

Firewall Flow Detailed Information – CLI Only

```
8533-C0-1#show firewall flows     | *optionally filter <match by traffic type, direction, time session is
active, etc>
========== Flow# 1 Summary ==========
Forward:
IPv4 Vlan 1, TCP 192.168.50.172 port 40456 > 52.29.20.233 port 443
 74-67-F7-5C-42-B7 > 5C-0E-8B-1A-DF-88, ingress port local
 Egress port: ge1, Egress interface: vlan1, Next hop: 192.168.50.1 (5C-0E-8B-1A-DF-88)
 755 packets, 318909 bytes, last packet 2917 seconds ago
Reverse:
IPv4 Vlan 1, TCP 52.29.20.233 port 443 > 192.168.50.172 port 40456
 5C-0E-8B-1A-DF-88 > 74-67-F7-5C-42-B7, ingress port ge1
 Egress port: <local>, Egress interface: vlan1, Next hop: <local> (74-67-F7-5C-42-B7)
 529 packets, 156617 bytes, last packet 3033 seconds ago
TCP state: Fwd FIN
Application : SSL_generic, Category : tunnel
Flow times out in 41 minutes 23 seconds

========== Flow# 2 Summary ==========
Forward:
IPv4 Vlan 1, TCP 192.168.50.1 port 44510 > 192.168.50.172 port 22
 5C-0E-8B-1A-DF-88 > 74-67-F7-5C-42-B7, ingress port ge1
 Egress port: <local>, Egress interface: vlan1, Next hop: <local> (74-67-F7-5C-42-B7)
 280 packets, 27573 bytes, last packet 0 seconds ago
Reverse:
IPv4 Vlan 1, TCP 192.168.50.172 port 22 > 192.168.50.1 port 44510
 74-67-F7-5C-42-B7 > 5C-0E-8B-1A-DF-88, ingress port local
 Egress port: ge1, Egress interface: vlan1, Next hop: 192.168.50.1 (5C-0E-8B-1A-DF-88)
 182 packets, 25721 bytes, last packet 0 seconds ago
TCP state: Established
Application : SSH, Category : remote_control
Flow times out in 1 hour 30 minutes

========== Flow# 4 Summary ==========
Forward:
IPv4 Vlan 10, TCP 192.168.10.141 port 65017 > 132.245.48.34 port 443
 CC-C7-60-1C-AB-C8 > 5C-0E-8B-1A-DF-88, ingress port radio2
Egress port: ge1
 20 packets, 3620 bytes, last packet 245 seconds ago
Reverse:
IPv4 Vlan 10, TCP 132.245.48.34 port 443 > 192.168.10.141 port 65017
 5C-0E-8B-1A-DF-88 > CC-C7-60-1C-AB-C8, ingress port ge1
Egress port: radio2
 17 packets, 10178 bytes, last packet 245 seconds ago
TCP state: Established
Application : office365, Category : business
Flow times out in 1 hour 25 minutes 55 seconds

========== Flow# 5 Summary ==========
Forward:
IPv4 Vlan 100, TCP 10.1.100.145 port 58435 > 172.217.16.101 port 443
 30-A8-DB-64-25-59 > 74-67-F7-5C-42-B7, ingress port radio2
 Egress port: ge1, Egress interface: vlan1, Next hop: 192.168.50.1 (5C-0E-8B-1A-DF-88)
 10 packets, 1854 bytes, last packet 3039 seconds ago
Reverse:
IPv4 Vlan 1, TCP 172.217.16.101 port 443 > 192.168.50.172 port 58132
 5C-0E-8B-1A-DF-88 > 74-67-F7-5C-42-B7, ingress port ge1
 Egress port: radio2, Egress interface: vlan100, Next hop: 10.1.100.145 (30-A8-DB-64-25-59)
 11 packets, 6008 bytes, last packet 3039 seconds ago
TCP state: Rev FIN
Application : gmail, Category : mail
Flow times out in 39 minutes 21 seconds
```