

EdgeXOS Platform Notes

XRoads Networks

Edge Network Appliance Platform Notes

EdgeXOS Firewall Logging

Firewall Logging Setup / Overview

This document provides an overview of how you can use firewall logging to troubleshoot routing, firewall, and other network issues. The firewall logging feature enables an administrator to capture traffic in real-time and see where it is coming from and where it is going. It also shows if the traffic is being dropped or allowed.

In order to configure the firewall logging option you must first enable the firewall.

If you already have a firewall in place and/or do not want to block any traffic while performing this testing, you should first add an allow rule for all inbound traffic (outbound traffic is allowed by default).

In this example we show how to easily add an inbound allow rule:

- Step 1) Go to the NAC Firewall tab and select the L7 Firewall Rules menu
- Step 2) Click the Add Rule button
- Step 3) Enter group name ZAllow
- Step 4) Make sure WAN+ is selected for Inbound Interface
- Step 5) Make sure that the Action is ACCEPT
- Step 6) Click the Add / Update button at the bottom of the page
- Step 7) Verify this rule now appears above the default rules.



Adding Log Rules

The process for adding firewall log rules is easy:

- Step 1) Determine what rule you wish to add. If you are trying to see where specific traffic is going from a certain device on the LAN, then add a rule for that device
Example: You wish to see where traffic is going for 192.168.100.252
- Step 2) Click the Add Rule button
- Step 3) Enter group name ALog (this will place all log entries above the allow rules)
- Step 4) Select LAN from the Inbound Interface option
- Step 5) Enter the IP address where the traffic is going from
- Step 6) Enter the Mask (in this case select SINGLE HOST)
- Step 7) Make sure that the Action is ACCEPT
- Step 8) Select to Log the traffic
- Step 9) Click the Add / Update button at the bottom of the page
- Step 10) Verify this rule now appears at the top of the firewall rules.



Now that the rules have been added go ahead and enable the firewall.

Under the NAS Firewall > L7 Firewall Control menu you should click to enable the firewall and click to Update the configuration.

Firewall Enabled Firewall Disabled (Disabling will turn off all perimeter security)

Once the firewall is enabled you can view the logged traffic by going to the Reporting tab and selecting the Firewall Logs menu.

Here you will see all of data logged for the rule you created.

Time	Packet
Sat Oct 18 18:50:46 2008	ALLOWED IN=lan OUT= MAC=00:90:fb:04:85:1c:00:0c:f1:09:1:dd:08:00 Source Addr=192.168.100.252 Destination Addr= TOS=0x00 ID=55087 DF Protocol=TCP Source Port=3244 Destination Port=8088 ACK
Sat Oct 18 18:50:46 2008	ALLOWED IN=lan OUT= MAC=00:90:fb:04:85:1c:00:0c:f1:09:1:dd:08:00 Source Addr=192.168.100.252 Destination Addr=1 TOS=0x00 ID=55088 DF Protocol=TCP Source Port=3244 Destination Port=8088 ACK PSH
Sat Oct 18 18:50:46 2008	ALLOWED IN=lan OUT= MAC=00:90:fb:04:85:1c:00:0c:f1:09:1:dd:08:00 Source Addr=192.168.100.252 Destination Addr= TOS=0x00 ID=55081 DF Protocol=TCP Source Port=3244 Destination Port=8088 ACK
Sat Oct 18 18:50:46 2008	ALLOWED IN=lan OUT= MAC=00:90:fb:04:85:1c:00:0c:f1:09:1:dd:08:00 Source Addr=192.168.100.252 Destination Addr= TOS=0x00 ID=55081 DF Protocol=TCP Source Port=3242 Destination Port=8088 ACK
Sat Oct 18 18:50:46 2008	ALLOWED IN=lan OUT= MAC=00:90:fb:04:85:1c:00:0c:f1:09:1:dd:08:00 Source Addr=192.168.100.252 Destination Addr= TOS=0x00 ID=55083 DF Protocol=TCP Source Port=3242 Destination Port=8088 ACK
Sat Oct 18 18:50:46 2008	ALLOWED IN=lan OUT= MAC=00:90:fb:04:85:1c:00:0c:f1:09:1:dd:08:00 Source Addr=192.168.100.252 Destination Addr= TOS=0x00 ID=55084 DF Protocol=TCP Source Port=3242 Destination Port=8088 ACK FIN

Notice you will also see the source and destination ports and addresses:

ALLOWED IN=lan OUT=wan1 Source Addr=192.168.100.252 Destination Addr=74.125.19.103

As well as the protocol and ports being used:

Protocol=TCP Source Port=3246 Destination Port=80 ACK

Note: The IN and OUT is very helpful when trying to determine which port a particular application is being routed, especially if you have created multiple application routing, vector map, and/or best path routing rules.

If you are logging lot of information you can also use the Search tool to find specific traffic and determine how many lines you wish to view:

Search 10 (Returned Lines <500 Max>) 74.125.19.103 (Criteria - src address, port, other)

ALLOWED IN=lan OUT=wan1 Source Addr=192.168.100.252 Destination Addr=74.125.19.103 Length=40 TOS=0x00 ID=55231 DF Protocol=TCP Port=3246 Destination Port=80 ACK RST

ALLOWED IN=lan OUT=wan1 Source Addr=192.168.100.252 Destination Addr=74.125.19.103 Length=40 TOS=0x00 ID=55223 DF Protocol=TCP Port=3246 Destination Port=80 ACK

ALLOWED IN=lan OUT=wan1 Source Addr=192.168.100.252 Destination Addr=74.125.19.103 Length=40 TOS=0x00 ID=55203 DF Protocol=TCP Port=3246 Destination Port=80 ACK