

MOCK - Firewall Rule Matching

Last updated: December 1st, 2023

Introduction

Firewall Test Policy Matching is a feature that allows you to view the expected traffic flow of packets as they are processed by the firewall. This tool can be used to ensure expected behavior of firewall policies and help troubleshoot traffic flow related issues. This feature is currently only available for Layer 3 firewall policies. This tool also allows for a bulk importation from a .CSV file in order to test multiple parameters on a single network. This tool is available with on MX firmware release 10.10T and newer.

Quick Start Guide

To use Firewall Test Policy Matching Tool:

1. Navigate to [ideoproject.net](#)
2. Click on "Begin"
3. Enter API Key & Serial Number.
***Wait for tool to display desired network*
4. Click on "Go to Device" and click "Test Firewall Policy"
5. Enter desired parameters and then click the "Start" button.
***Source & Destination IP are required*
6. Click "Check Firewalls" and wait for the browser to produce desired results.



Device

Firewall Info

Firewall Check

Enter your API Key:

Enter your serial number:

Go To Device

Please Enter Source IP:

Please Enter Destination IP:

Enter Source port:

Enter Destination Port:

Enter Protocol:

Import CSV:

Choose File

No file chosen

Check Firewalls

Display ALL Rules

To review current policies , enter API Key and Serial Number to retrieve the desired network. Once the

network name has populated choose "Display All Rules". To return to policy matching tool click "Go to Device"

comment	policy	protocol	srcPort	srcCidr	destPort	destCidr	syslogEnabled
VLAN tag testing	deny		Any	[IPv4Network(172.16.1.0/24), IPv6Network(2001:1111:1000::0/4)]	Any	[IPv4Network(172.16.1.0/24), IPv6Network(2001:1111:1000::0/4)]	false
Protocol/Port testing	allow		80	[IPv4Network(172.16.1.0/24)]	80	[IPv4Network(172.16.1.0/24)]	false
Protocol/Port testing 2	deny		80	[IPv4Network(172.16.1.0/24)]	80	[IPv4Network(172.16.1.0/24)]	false
ICMPv4 test	deny		Any	[IPv4Network(172.16.1.0/24)]	Any	[IPv4Network(172.16.1.0/24)]	false

Import CSV

Import CSV:

Choose File FileTest1.csv

1. Format .csv file with the following parameters "description, src_port, src_ip, dest_ip, dest_port, protocol"
2. Upload file into browser using the "Import CSV" section
3. The program returns the .csv file with verdicts for all of the parameter sets after the last parameter column

ICMP traffic	172.16.1.1	172.16.2.1	icmp	allow
VLAN 2 to 3 isolation	172.16.1.2	172.16.2.2		deny
HTTP	80 172.16.1.3	172.16.2.3	80 tcp	allow
IPv6 Test	2001::1111:1001::1	2001::1111:1002::1		allow

Filtering & Parameters

For the best results with the Firewall Test Policy Matching tool, it is important to filter for a specific traffic flow you are targeting. The following filters can be configured:

Filter	Accepted Parameters
Source IP	Address to test traffic flow FROM (e.g. 192.168.1.0) (IPv6 supported)
Destination IP	Address to test traffic flow TO (e.g 172.16.1.0) (IPv6 supported)
Source Port	Port number (e.g. 80)
Destination Port	Port number (e.g. 80)
Protocol	Protocol used
Decision	Definition
Allowed	The flow has been allowed
Denied	The flow has been denied



COMPANY

[About Meraki](#)
[Careers](#)
[Privacy](#)
[Trust](#)
[GDPR](#)
[Terms of Use](#)

PARTNERS

[Partner Portal Login](#)
[Become a Partner](#)
[Manage Service Providers](#)
[Service Providers](#)

GET STARTED

[Contact Us](#)
[Get a Demo](#)
[Start Your Trial](#)

RESOURCES

[Webinars](#)
[Documentation](#)
[Community](#)
[Learning Hub](#)