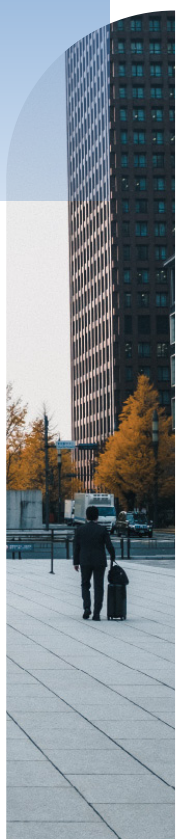
DEPLOYMENT GUIDE

Arista Macro Segmentation Service Integration With Fortinet



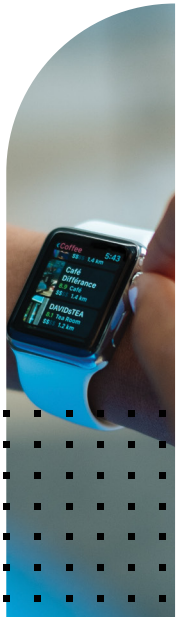


Table of Contents

Description

This document explains how to configure and deploy Arista Macro Segmentation Service (MSS) with Fortinet FortiGate firewalls (also called FortiGate next-generation firewalls or NGFWs). The feature requires use of FortiManager, a security management platform by Fortinet, that allows central management of Fortinet Network Security devices such as FortiGate firewalls.

Platform Capability

The feature has been tested with the following FortiManager and FortiGate versions:

1. FortiManager Versions: FortiManager 5.6.2 and 6.0.1 (and above)
2. FortiGate Versions: FortiGate 5.6.3, 5.6.4, and 6.0.0 build 5056 (interim) (and above)
3. FortiGate Hardware Types: Arista MSS has been designed to provide security integration with data-center class firewalls. FG100E and the higher-performance firewalls in the family are capable of supporting this feature.

Requirements for Deployment

1. VXLAN is enabled and configured on CVX and leaf switches
2. For Layer 2 virtual wire policies:
   - FortiGate virtual wires carry all 802.1Q VLAN tags 1-4094
   - A new Layer 2 (transparent mode) VDOM is created and used for Layer 2 virtual wire pair interfaces. We do not support configuring the virtual wire interfaces in the “root” VDOM.
3. For Layer 3 policies:
   - A new Layer 3 (NAT mode) VDOM is created and used for Layer 3 interfaces. We do not support configuring the routed interfaces in the “root” VDOM.
   - The firewall needs to have routes back to the original subnets in which the end hosts reside. Only static routes in default VRF are supported in the current release.

Configuration

This section describes the configuration requirements on four different components, viz., FortiGate firewalls, FortiManager, Arista leaf switches, and CVX.

Configuration on FortiGate firewalls

High-availability mode with LAGs/MLAGs: On FortiGate firewalls, configure LAG interfaces so that the passive/standby high-availability device doesn’t join the LAG and LACP converges fast on failover. If you have a FortiOS image on the FortiGate that supports LLDP, enable it:

```
config vdom edit <vdom-name>
  config system interface edit
  <lag-name> set lacp-mode active
  set lacp-ha-slave disable
end
```

If you have a FortiOS image on the FortiGate that supports LLDP, enable it:

```
config global config system global
  set lldp-reception enable set lldp-
  transmission enable
end
```

or, alternatively:

```
config system settings
  set lldp- transmission enable
end
```

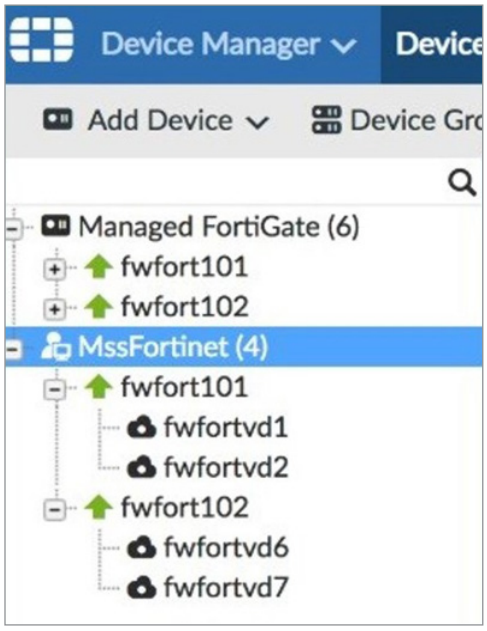
Configuration on FortiManager

The FortiGate firewall devices intended to be used with Arista MSS should be registered and fully manageable via a FortiManager.

- Enable API read access on FortiManager:

```
config system admin user edit admin
  set-rpc-permit read
end
```

- Define a device group in FortiManager Device Manager with the FortiGate firewall devices to be used as members.



  Here, 'MssFortinet' is the device group, which has the following VDOMs as members:

  - fwfortvd1, fwfortvd2 (residing on physical firewall fwfort101)
  - fwfortvd6, fwfortvd7 (residing on physical firewall fwfort102)

- Create policies between interfaces (Virtual Wire Pair or L3) attached to the Arista leaf
- Create a firewall policy (to be used by Arista MSS)
  - Add a host IPv4 address to one of the policy security zones
  - Add tags in the policy comments/description field in this format: "tags(<tag1>, <tag2>, ...)", e.g., "tags(MSS1, MSS2)"

    Arista MSS inspects FortiGate policies that have an embedded "tags( )" string in the comments field. Individual tags are extracted from within the enclosing parentheses and compared with the tags configured in the Arista MSS device-set on CVX.

    The following example CLI shows a policy configuration template with tags specified in the comments field:

```
config firewall policy
  edit <policy_id>
    set name <>
    set srcintf <>
    set dstintf <>
    set srcaddr <>
    set dstaddr <>
    set schedule always set service ALL
    set logtraffic all set action <>
    set comments "tags( MSS1, MSS2 )"
  next
end
```

Configuration on Arista Leaf Switches

High-availability mode with LAGs/MLAGs: On switch interfaces to firewall:

```
switchport mode trunk
switchport trunk allowed vlan none
channel-group <port-channel-number> mode active
```

Configuration on CVX

A sample CVX configuration with standalone FortiGate firewall is as follows:

```
!! Standalone FortiGate firewall
cvx
  no shutdown service mss
  no shutdown
  vni range 30000-40000
  !
  dynamic device-set fnet
  device <fortimgr-ip-or-dnsName>
   username admin password 7 PKigsm//o3IcnW5rqoZXWQ==
   group <fortimgr-device-group-name>
   !
  device member <fortigate-device-name>
   map device-interface port29 switch 00:1c:73:7e:28:11 interface Ethernet39
   map device-interface port30 switch 00:1c:73:7e:28:11 interface Ethernet40
   map device-interface port31 switch 00:1c:73:7e:28:11 interface Ethernet41
   map device-interface port32 switch 00:1c:73:7e:28:11 interface Ethernet42
   management virtual domain root
type fortinet fortimanager
tag MSS1 MSS2
admin domain root
virtual domain <vdom_name>
state active
```

Note that the fortigate-device-name used in the “device member <fortigate-device-name>” command must be the name used in the Device Manager of FortiManager to identify that firewall. This name can also be seen from the following Arista MSS command:

```
show service mss dynamic device-set fnet device <fortimgr> group-members
```

A sample CVX configuration with FortiGate firewalls in high-availability configuration is as follows:

```
!! HA Active/Passive FortiGate firewall pair
cvx
  no shutdown
  service mss
   no shutdown
   vni range 30000-40000
   !
   dynamic device-set fnetHA
    device <fortimgr-ip-or-dnsName>
     username admin password 7 PKigsm//o3IcnW5rqoZXWQ==
     group <fortimgr-device-group-name>
   !
   device member <fortigate-device-name>
    map device-interface port13 switch 00:1c:73:7e:21:e1 interface Port-Channel60
    map device-interface port14 switch 00:1c:73:7e:28:11 interface Port-Channel60
    map device-interface port15 switch 00:1c:73:7e:21:e1 interface Port-Channel65
    map device-interface port16 switch 00:1c:73:7e:28:11 interface Port-Channel65
   management virtual domain root
type fortinet fortimanager
tag MSS1 MSS2
exception device unreachable redirect
admin domain root
virtual domain L2_FW
state active
```

FortiGate Commands

Some helpful FortiGate CLI commands are as follows:

1. Checking system versions

```
get system status
```

2. Enabling VDOM configuration

```
config system global
  set vdom-admin enable
end
```

3. Creating a new VDOM

```
config system global
  set vdom-admin enable
end
```

4. Setting VDOM mode to transparent for L2 vwire or nat for L3

```
config vdom
  edit <vdom>
   config system settings
    set opmode transparent (or nat)
    set inspection-mode flow
    set manageip <ip/netmask>
end
```

5. Add interfaces to VDOM

```
config global
  config system interface
   edit <port>
   set vdom <vdom>
```

6. For L2 policies, create a virtual wire pair on a VDOM

```
config vdom
  edit fwfortvd1
   config system virtual-wire-pair
    edit "vd1-vwire"
     set member "port1" "port2"
     set wildcard-vlan enable
    next
end
```

7. Adding a host IPv4 object on the FortiGate firewall

```
config vdom
  edit fwfortvd1
   config firewall address
    edit TestHost11
     set subnet 10.10.100.1 255.255.255.255
   next
end
```

8. Adding a static route on the FortiGate firewall

```
config router static
  edit 1
   set destination <ip address/netmask>
   set gateway <ip address>
   set distance <value>
end
```

Troubleshooting

Some helpful CVX CLI commands are as follows:

```
trace monitor msspolicymonitor
show service mss policy
show service mss internal policy
show service mss internal policy detail
show service mss dynamic
show service mss dynamic status
show service mss dynamic device-set fnet device <fortimgr> group-members
show service mss dynamic device-set fnet device <fortigate> policies
show service mss dynamic device-set fnet device <fortigate> network
show service mss dynamic device-set fnet device <fortigate> neighbors
show service mss dynamic device-set fnet device <fortigate> resources
```

Helpful switch CLI:

```
show vxlan vni
show directflow detail
show arp
```

If “IPv4 Virtual Wire Pair Policy” option is not visible under “Policy & Objects” tab in FortiManager, then enable it as follows:

1. Go to Tools > Display Options
2. Select the “IPv4 Virtual Wire Pair Policy” option in the ‘Policy’ settings
3. Click OK

Tracing

To see how Arista MSS is accessing information from FortiManager, add the following config to CVX:

```
trace MssPolicyMonitor setting MssPolicyMonitor*/0-2
```

Then use the following command:

```
trace monitor msspolicyMonitor
```

Limitations

1. Arista MSS supports one device-set with “state active” per FortiManager instance and VDOM.
2. root is not supported as Arista MSS vdom.

Resources

1. CloudVision—Configuration Guide (https://www.arista.com/cg-cv)
   - CloudVision eXchange (chapter 2)
   - Macro-Segmentation Service (chapter 3)
2. Refer to the Arista MSS Design Guide and other CloudVision documentation for any general limitations. Arista MSS Design Guide (“Arista Networks Macro-Segmentation Service [MSS™] Design & Deployment Guide”) can be located at: https://www.arista.com/en/solutions/design-guides
3. For Fortinet firewall queries, please refer to firewall documentation/technical specifications at www.fortinet.com.

Miscellaneous Notes

When policy updates are being pushed from FortiManager to the FortiGate (FW) devices, FortiManager may not return the correct information to MssPolicyMonitor, which will trigger the below syslog. It can be safely ignored if seen at this time only.

```
MssPolicyMonitor: %MSSPM-4-WARN: fortinet2 FortiGate API url /api/v2/cmdb/system/ha returned status
{u'message': u'Invalid url', u'code': -6} target ['adom/root/device/fortinet2']

MssPolicyMonitor: %MSSPM-3-DEVICE_ACCESS_ERROR: Device: fortinet2 Msg: FortinetApi Error accessing device
172.24.72.252 check protocol, IP address, username and password.
```


July 7, 2021 3:17 AM
614051-A-0-EN