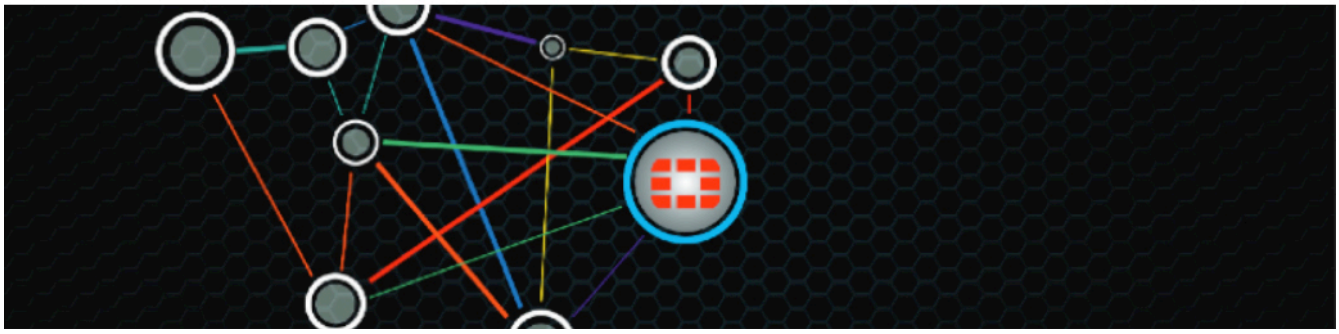
Solution Guide



Fortinet Solutions for Transparent Mode (Layer-2)

Authors: Bryan Feng, Tom Yamada
Network Security Architects

Contents

Introduction

FortiGate supports NAT/Route mode (Layer-3) and Transparent (TP) mode (Layer-2). In Transparent mode there are some optional features available based on the network environment. This document describes best practice in Transparent mode and provides sample configurations.

Deployment Considerations

The following are important aspects that need to be considered prior to using Transparent mode:

- **Using out of band management. Management access to the FortiGate on a different network than the data traffic.**
- **Multiple broadcast domains on the FortiGate.**
- **VLAN tagging.**
- **Spanning tree BPDUs.**
- **VRRP, HSRP or Network Load Balancer.**
- **Other than Ethernet II Layer 2 frame like IPX.**
- **Multicast traffic.**
- **Asymmetric forwarding.**
- **Port-pair. (logical wire connection)**

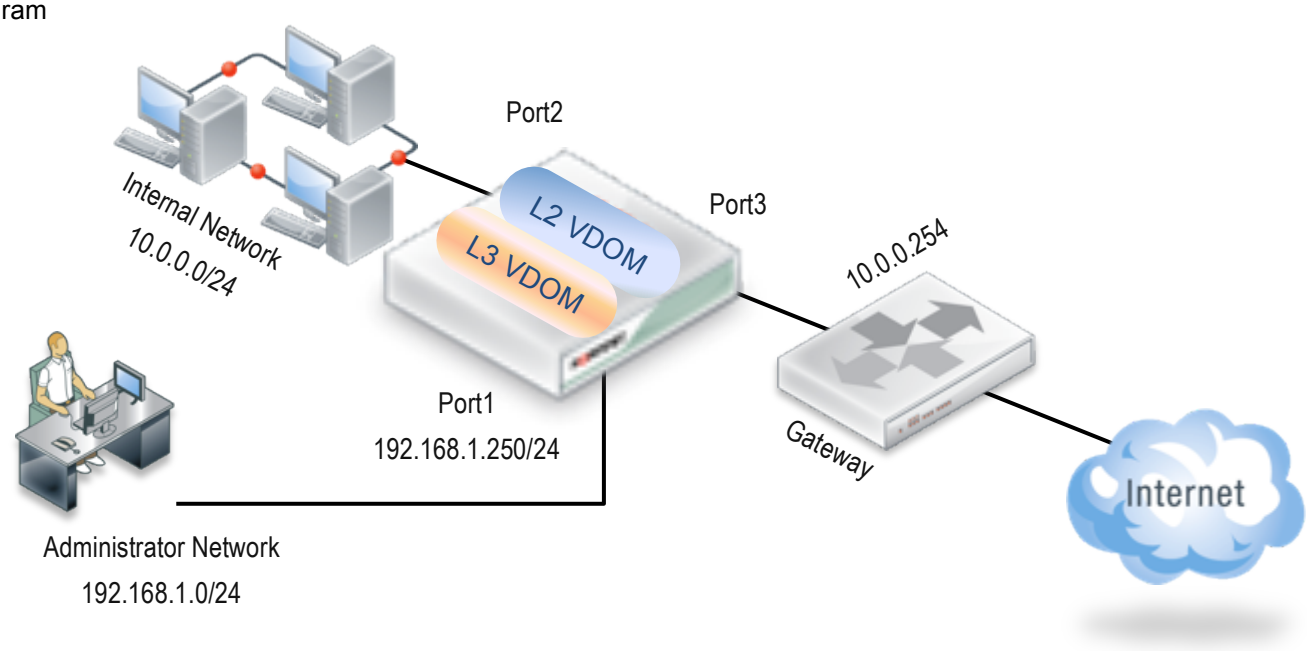
Requirements

FortiOS 5.0.6.This configuration example uses FortiOS 5.0.6

Management Access Consideration.

Description
Transparent mode management access is provided by assigning a management-ip. All the interfaces on the FortiGate are on the same network by default. The problem with this is that user traffic and management traffic are in the same broadcast domain.
By utilizing a Transparent mode VDOM (L2 VDOM) and NAT/Route mode VDOM (L3 VDOM) on the same FortiGate, a dedicated management broadcast domain and interface can be created.

Diagram



Resolution
Enable VDOM, configure a Transparent mode VDOM for data traffic and a NAT/Route mode VDOM for administrator access.

Steps and Related CLI / Configuration Example
Step 1 – Configure Management Interface
“set allow access <access_types>” command under config system interface, based on access type you want allow on the interface.
“set ip <interface_ipv4mask>” command under config sys interface to assign ip address on the interface.

Syntax

```
config system interface
    edit <interface_name>
        set allow access <access_types>
```

Variable	Description	Default
allowacces <access_types>	Enter the types of management access permitted on this interface or secondary IP address. Separate types with spaces. Use the append or clear commands (instead of set) to add or remove an option from the list. Valid types are: auto-ipsec — required for IPsec auto-configuration capwap — required for interfaces that carry CAPWAP control traffic. Interfaces dedicated for FortiAP unit use have this option enabled automatically. fgfm — FortiManager management access http — enable HTTP admin access https — enable HTTPS admin access ping — allow ping response. Useful for testing. probe-response — allow access by config system server-probe command radius-acct — RADIUS Accounting server access snmp — SNMP management access ssh — enable admin access via SSH telnet — enable admin access via Telnet	Varies for each Interface

Syntax

```
config system interface
    edit <interface_name>
        set ip <interface_ipv4mask>
```

Variable	Description	Default
ip <interface_ipv4mask>	Enter the interface IP address and netmask. This is not available if mode is set to dhcp or pppoe. You can set the IP and netmask, but it will not display. This is only available in NAT/Route mode. The IP address cannot be on the same subnet as any other FortiGate unit interface.	Varies for each interface.

Figure 1 – Configure Management Interface.

```
FGT_60C_B # config sys int
FGT_60C_B (interface) # edit port1
FGT_60C_B (port1) # set allowaccess https ssh
FGT_60C_B (port1) # set ip 10.1.1.1/24
FGT_60C_B (port1) # next
FGT_60C_B # end
```

Step 2 – Enabling VDOM

"set vdom-admin enable" command under config system global enable VDOM.

Syntax

```
config system global
    set vdom-admin {enable | disable}
```

Variable	Description	Default
vdom-admin {enable | disable}	Enable to configure multiple virtual domains	disable

Note: Changing this value requires logout/login.

Figure 2 – Enable VDOM.

```
FGT_60C_B # config sys global
FGT_60C_B (global) # set vdom-admin ena
FGT_60C_B (global) # end
You will be logged out for the operation to take effect
Do you want to continue? (y/n)n
```

Step 3 – Create a VDOM

"edit vdom <vdom_name>" command under config vdom create a VDOM.

Syntax

```
config vdom
    edit vdom <vdom_name>
```

Figure 3 – Create a VDOM

```
FGT60C_B # config vdom
FGT60C_B (vdom) # edit L2vdom
current vf=L2vdom:4
FGT60C_B (L2vdom) #
```

Step 4 – Change Operational Mode to Transparent

"set opmode {nat | transparent } " command under config system setting in the VDOM set operational mode.

Syntax

```
config vdom
    edit vdom <vdom_name>
        config system setting
            set opmode {nat | transparent}
```

Variable	Description	Default
opmode {nat | transparent}	Set operational mode nat (Layer 3 mode) or transparent (Layer 2 mode)	nat

Note: Configuring "manageip" is required opmode "transparent".

Figure 4 – Change Operational Mode to Transparent

```
FGT60C_B (L2vdom) # config system settings
FGT60C_B (settings) # set opmode transparent
```

Step 5 – Configure Manageip

"set manageip <manage_ipv4>" command under config system setting in the VDOM set management ip.

Syntax

```
config vdom
    edit vdom <vdom_name>
        config system setting
            set manageip <manage_ipv4>
```

Variable	Description	Default
manageip <manage_ipv4>	Set the IP address and netmask of the Transparent mode management interface. You must set this when you change opmode from nat to transparent.	No default

Figure 5 – Configure Manageip

```
FGT60C_B (settings) # set manageip 10.0.0.253/24
FGT60C_B (settings) # end
Changing to TP mode
FGT60C_B (L2vdom) # end
FGT60C_B # end
```

Step 6 – Import Interface to the VDOM

"set vdom <vdom_name>" command under config system interface in global assign the interface to VDOM

Syntax

```
config global
    config system interface
        edit <interface_name>
            set vdom <vdom_name>
```

Variable	Description	Default
Vdom <vdom_name>	Enter the name of the virtual domain to which this interface belongs. When you change this field, the physical interface moves to the specified virtual domain. Virtual IP previously added for this interface are deleted. You should also manually delete any routes that include this interface as they may now be inaccessible.	root

Figure 6 – Assign Interfaces to the VDOM.

```
FGT60C_B # config global
FGT60C_B (global) # config sys interface
FGT60C_B (interface) # edit port2
FGT60C_B (port2) # set vdom L2vdom
FGT60C_B (port2) # next
FGT60C_B (interface) # edit port3
FGT60C_B (port3) # set vdom L2vdom
FGT60C_B (port3) # next
FGT60C_B (interface) # end
FGT60C_B (global) # end
FGT60C_B #
```

NOTE: It is highly recommended to use the default root VDOM for the L3/out of band/management VDOM and to leave this VDOM as the management VDOM, there are some services such as FortiGuard updates and other management related that will use this VDOM for communication so network design considerations for this apply.

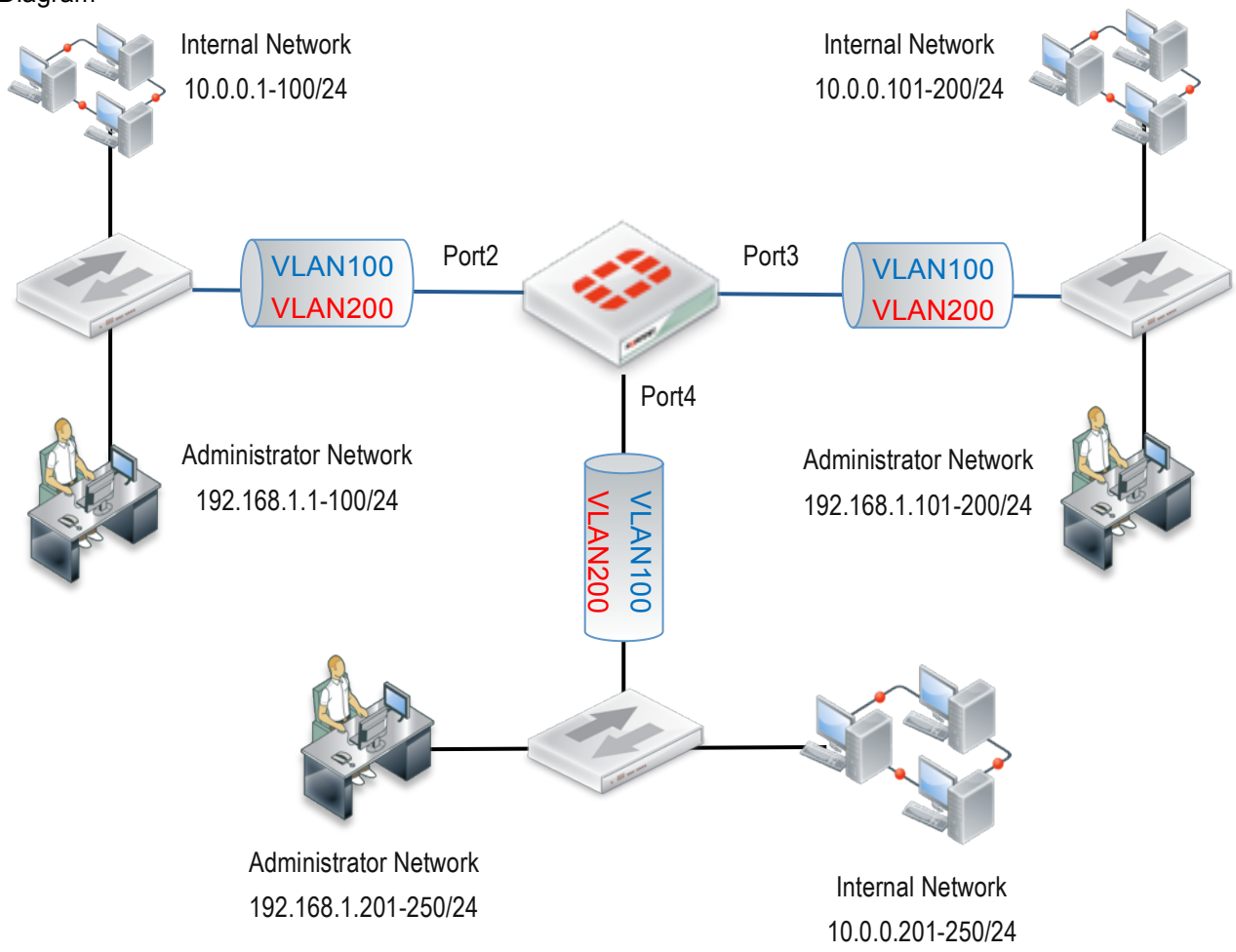
Transparent Mode with VLAN trunking

Description
Without VLAN tagging configuration on FortiGate in Transparent mode, VLAN tagged packets are treated as non-IP packets. This means that VLAN tagged packets won't be inspected by security policies.
With configuring VLAN interface (logical interface) on the FortiGate and appropriate security policy, packets will be inspected but all packets will be passed on the same broadcast domain.

Note: Broadcast packets will be flooded to all ports even if the VLAN ID is different. This is a common cause of broadcast storms and/or packet of death spirals in L2 deployments.

Resolution
For inspecting VLAN tagged packets, configure VLAN tagging on the FortiGate.
In order to ensure different broadcast domains are created for deifferent VLANs, Forwardingdomains should be configured.

Diagram



Related CLI and Configuration example

Step 1 – Configure VLAN Tagging and Forward Domain on Port2

A new logical interface needs to be created for VLAN tagging. Under config system interface "edit <interfacename>" command will create the logical interface. The vdom, physical interface and vlanid are mandatory attributes within the logical interface configuration. To ensure separate broadcast domains are configured, set forwarding domain information for VLAN100 and VLAN200.

Syntax

```
config system interface
      edit <interface_name>
            set vdom <vdom_name>
            set interface <port_name>
            set vlanid <id_number>
            set forward-domain <collision_group_number>
```

Variable	Description	Default
Vdom <vdom_name>	Enter the name of the virtual domain to which this interface belongs. When you change this field, the physical interface moves to the specified virtual domain. Virtual IP previously added for this interface are deleted. You should also manually delete any routes that include this interface as they may now be inaccessible.	root
Interface <port_name>	Enter the physical or VAP interface this virtual interface is linked to. This is available only when adding virtual interfaces such as VLANs and VPNs	None.
vlanid <id_number>	Enter a VLAN ID that matches the VLAN ID of the packets to be received by this VLAN subinterface. The VLAN ID can be any number between 1 and 4094, as 0 and 4095 are reserved, but it must match the VLAN ID added by the IEEE 802.1Q-compliant router on the other end of the connection. Two VLAN subinterfaces added to the same physical interface cannot have the same VLAN ID. However, you can add two or more VLAN subinterfaces with the same VLAN ID to different physical interfaces, and you can add more multiple VLANs with different VLAN IDs to the same physical interface. This is available only when editing an interface with a type of VLAN.	No default.
forward-domain <collision_group_number>	Specify the collision domain to which this interface belongs. Layer 2 broadcasts are limited to the same group. By default, all interfaces are in group 0. Collision domains prevent the forwarding of ARP packets to all VLANs on an interface. Without collision domains, duplicate MAC addresses on VLANs may cause ARP packets to be duplicated. Duplicate ARP packets can cause some switches to reset. This command is only available in Transparent mode.	0

Figure 1 – Configure VLAN Tagging and Forward Domain on Port2

```
FGT60C_B (interface) # edit vlan100
new entry 'vlan100' added
FGT60C_B (vlan100) # set vdom L2-test
FGT60C_B (vlan100) # set interface port2
FGT60C_B (vlan100) # set vlanid 100
FGT60C_B (vlan100) # set forward-domain 100
FGT60C_B (vlan100) # next
FGT60C_B (interface) # edit vlan200
new entry 'vlan200' added
FGT60C_B (vlan200) # set vdom L2-test
FGT60C_B (vlan200) # set interface port2
FGT60C_B (vlan200) # set vlanid 200
FGT60C_B (vlan200) # set forward-domain 200
FGT60C_B (vlan200) # next
```

Step 2 – Repeat Step1 on Port3 and Port4

Configure the same on port3 and port4. Vlanid 100 interfaces are in forward-domain 100 and vlanid 200 interfaces are in forward-domain 200. Broadcast packet won't be forwarded to each other once this configuration is complete.

NOTE: In some deployments there are many VLAN's on the trunk interface passing through the FortiGate but security enforcement and inspection are only required on a small number of VLAN's, as mentioned above packets received with VLAN tags that don't correspond to a configured VLAN interface are forwarded by default, this behaviour can be changed by disabling VLAN forwarding on the interface "set vlanforward <enable/disable>"

Syntax

```
config system interface
      edit <interface_name>
            set vlanforward {enable | disable}
```

Variable	Description	Default
vlanforward {enable | disable}	Enable or disable forwarding of traffic between VLANs on this interface. When disabled, all VLAN traffic will only be delivered to that VLAN only.	enable

It is also important to keep in mind the traffic flow for the actual interface as well, this is the interface for all untagged packets, so even though you may have been diligent and put all the VLAN interfaces into forward-domains you may end up with a bridge loop on the physical interfaces for non VLAN tagged packets.

UTM and Hardware Acceleration Deployment Consideration

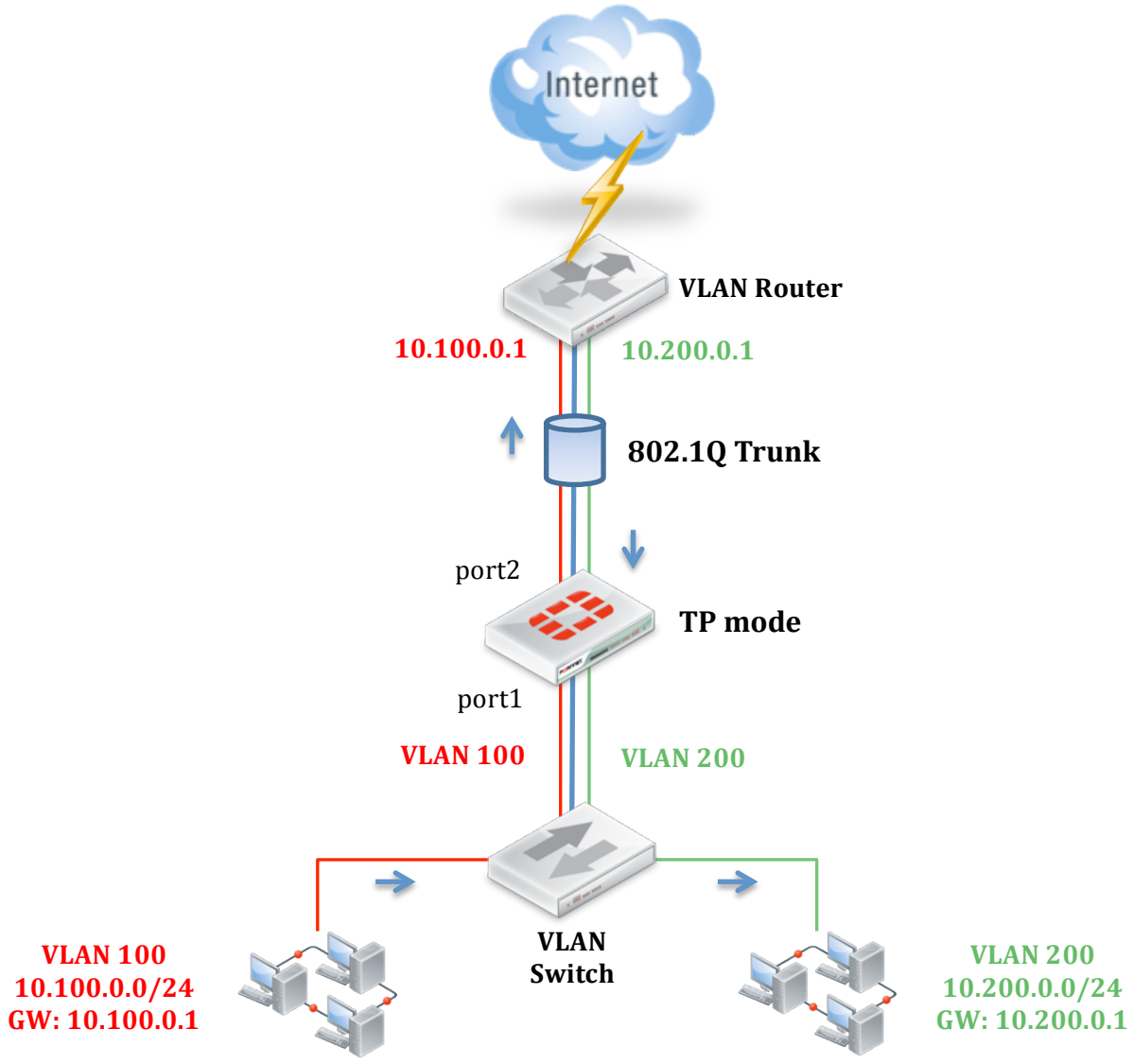
Avoiding the Same Session Traversing the Same VDom Twice

Description

When the same session traverses the same TP vdom twice from different source interface, ASIC hardware acceleration and UTM operations will NOT work.
If possible, avoid a situation where the FortiGate TP vdom is located in the data path where the same session must traverse the same TP vdom more than once if the session needs to be either hardware accelerated or subject to UTM protection.

ASIC acceleration behavior may be different on variant NPx based hardware platforms
1. some platforms such as platforms based on the NP2: traffic will be blocked with the default setting of asic offloading enabled. As a workaround, disable ASIC offloading.
2. other platforms such as NPLite/NP4 based: ASIC will not offload the traffic even if ASIC offloading is enabled.
For example, in the following TP mode deployment:
FortiGate in TP mode and internal(port1) and external(port2) trunk carries traffic from internal vlan 100, 200 at the bottom of the diagram to the VLAN Router on the top and to the Internet. There is no problem for such traffic.
But consider the traffic from VLAN 100 to VLAN 200:

Diagram



Traffic between the 2 internal VLANs, for example VLAN100 > VLAN200, data flow will be from the source VLAN100 going up through the FortiGate to reach the gateway(10.100.0.1) at the VLAN Router on the top then routed back down through the FortiGate again to the VLAN 200 at the lower right corner.
If the VLAN Router does not NAT between VLAN100 and VLAN200, the same session will traverse the TP mode vdom twice:

1st traverse: vlan100.port1 > vlan100.port2,
2nd traverse: vlan200.port2 > vlan200.port1

In this situation, the firewall is limited to performing Firewalling functions ONLY(no UTM), and the session cannot be hardware accelerated.

Solution
If this type of configuration cannot be avoided, there are 2 options to avoid the impact:

1. Configure the VLAN router to perform NAT for traffic between the VLAN100 and VLAN 200.
for the example that traffic initiated from VLAN100 > VLAN200, setup VLAN Router to NAT the src address from 10.100.0.x to 10.200.0.1
With this option in place, from the FortiGate's perspective the communication consists of 2 separate sessions:
vlan100.port1: 10.100.0.x > vlan100.port2: 10.200.0.x
vlan200.port2: 10.200.0.1 > vlan200.port1: 10.200.0.x

2. Configure FortiGate using 2 vdoms, one for each corresponding vlan. So effectively, the same session only traverses a particular vdom once.

Related CLI and Configuration example:

Syntax

```
config firewall policy
    edit <index_int>
        set auto-asic-offload {enable | disable}
```

Variable	Description	Default
Auto-asic-offload {enable | disable}	Enable or disable session offload to NP or SP processors. This is available on models that have network processors.	enable

Figure 1 – Configure Disable ASIC Offloading

```
FGT60C_B # config firewall policy
FGT60C_B (policy) # edit 1
FGT60C_B (1) # set auto-asic-offload disable
FGT60C_B (1) # show
config firewall policy
  edit 1
    set srcintf "any"
    set dstintf "any"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set auto-asic-offload disable
  next
end
```

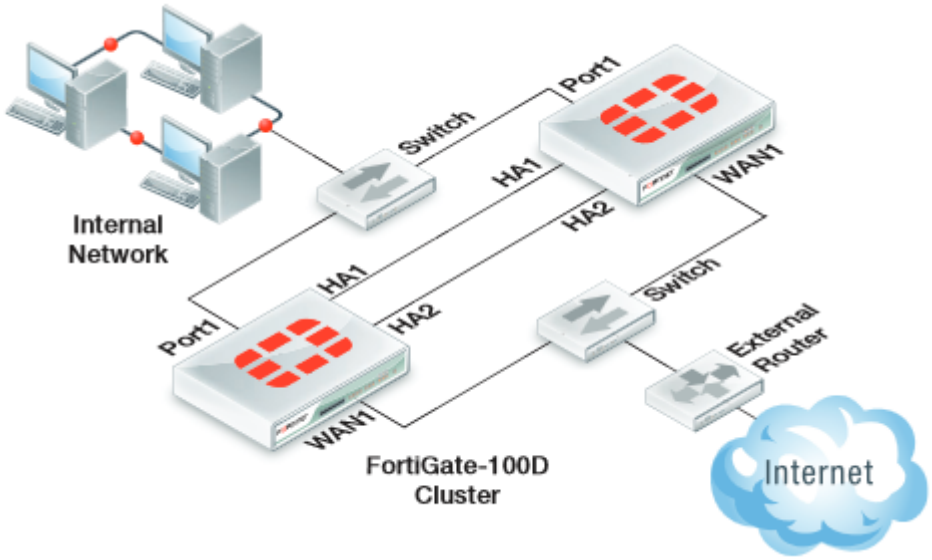
Transparent Mode VDom with STP (Spanning Tree Protocol)

Description

Spanning tree BPDUs are not forwarded by default. Please take caution when introducing a TP mode FortiGate/vdom in the network as L2 loops might be introduced if STP is broken due to STP BPDU being blocked by the FortiGate.

The example shows a TP mode HA a-p configuration. In normal state only the primary unit will be passing traffic ensuring that there is no loop in the network. However if for any reason the HA heartbeat is lost and the cluster ends up in a split brain situation both units may start forwarding packets. In this situation if the FortiGate does not forward STP BPDUs, there will be a network loop. If the FortiGate is configured to forward STP BPDUs the switch will be able to detect the loop and block one of the links as result of STP, and maintain the network loop free.

Diagram



Solution

Forward spanning tree BPDUs on all interfaces that are in the TP vdom that need traffic passing through.
Related CLI and Configuration example:

```
config system interface
  edit <interface name>
    set stpforward enable
  next
end
```

Syntax

```
config system interface
      edit <interface_name>
            set stpforward {enable | disable}
```

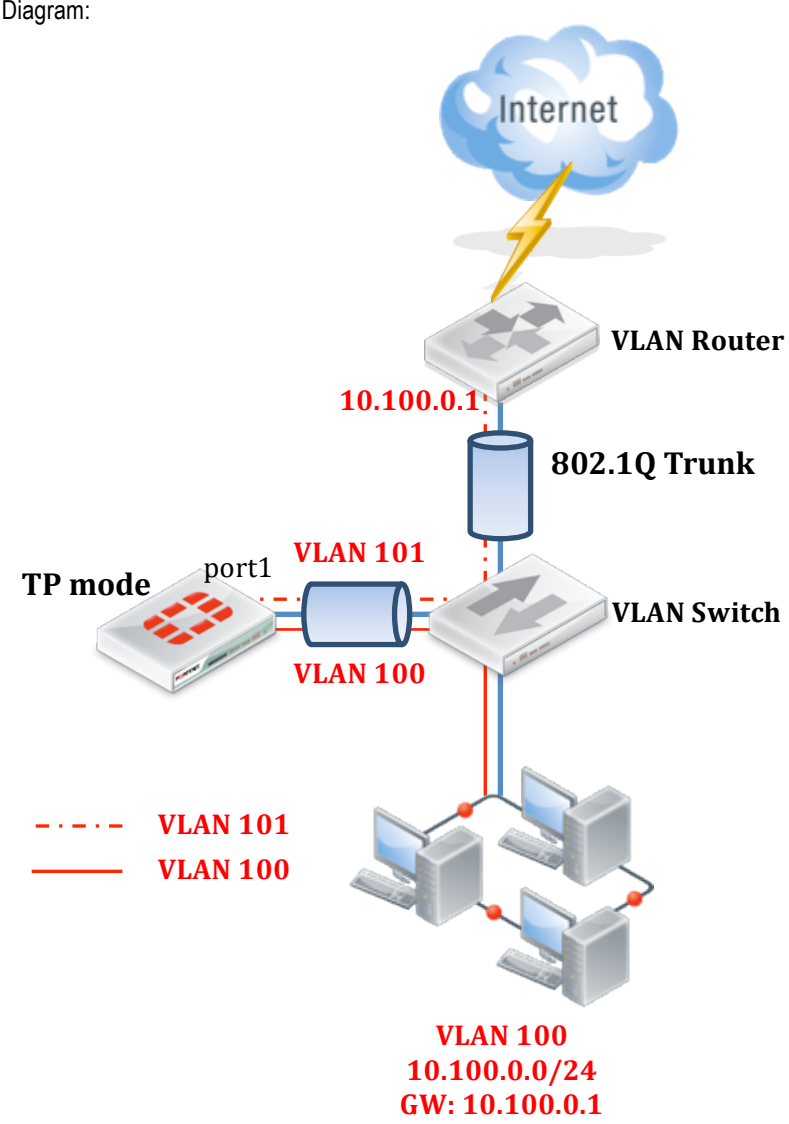
Variable	Description	Default
stpforward {enable | disable}	Enable to forward Spanning Tree Protocol (STP) packets through this interface. STP maps the network to provide the least-cost-path from point	disable

	to point while blocking all other ports for that path. This prevents any loops which would flood the network. If your network uses layer-2 protocols, and has looping issues STP will stop this. For more information, see *FortiGate VLANs and VDOMs*.	

NOTE: There is a special scenario described below needs an additional option for STP handling, stpforward-mode rpl-all-ext-id | rpl-bridge-ext-id.

Special STP Handling When internal and External VLAN Are on the Same Physical Interface (Also Known as One Arm or Firewall on a Stick)

Diagram:



The above diagram showing a scenario that the layer 2 traffic traverse TP mode firewall/Vdom, AND the source and destination VLAN interface are binded to the same physical interface.

In this scenario, in order to have TP mode firewall/Vdom to forward STP without tiggering the VLAN Switch to block the destination vlan interface, STP forwarding mode need to be changed from the default of rpl-all-ext-id to **rpl-bridge-ext-id** via CLI.

Syntax

```
config system interface
      edit <interface_name>
            set stpforward-mode {rpl-all-ext-id | rpl-bridge-ext-id}
```

Variable	Description	Default
stpforward-mode {rpl-all-ext-id | rpl-bridge-ext-id}	Choose the STP forwarding mode; rpl-all-ext-id Replace all extension IDs (root, bridge). rpl-bridge-ext-id Replace bridge extension ID only.	rpl-all-ext-id

Transparent Mode with VRRP, HSRP or Network Load Balancer

(Masked Virtual MAC address)

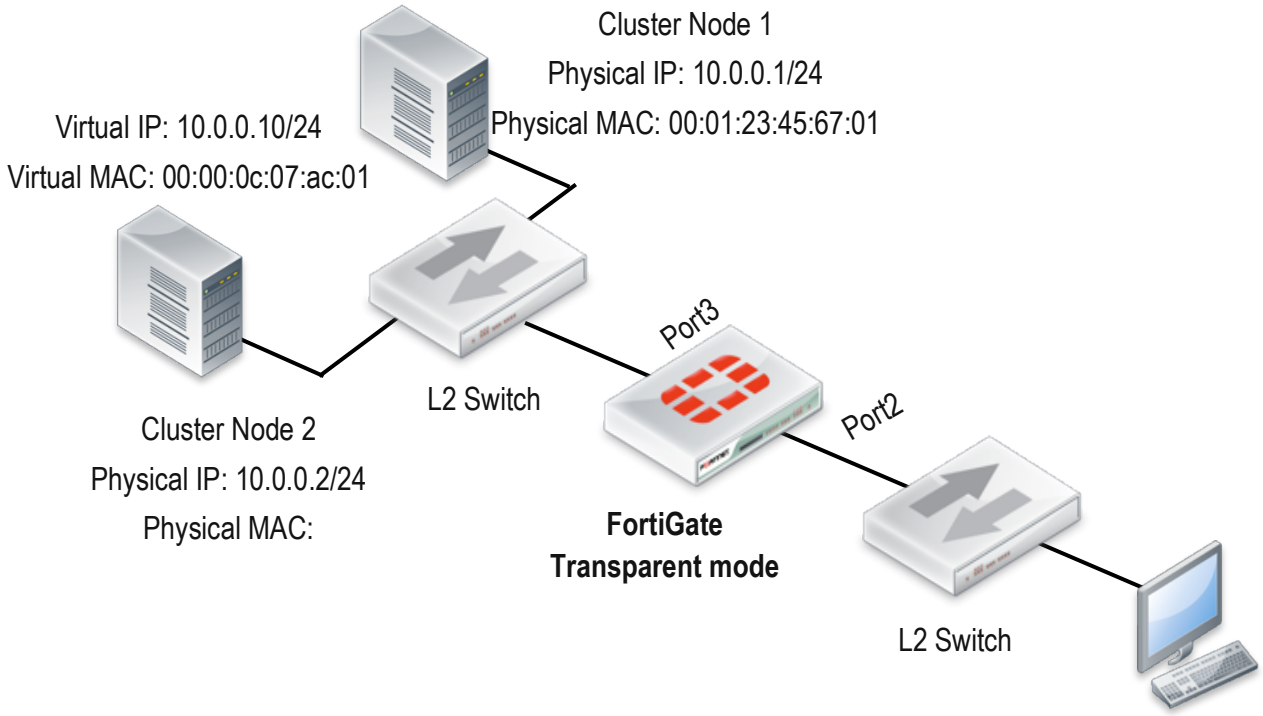
Description

In the case of VRRP, HSRP or Network Load Balancer existing in your network with a FortiGate in Transparent mode, a Static MAC entry may be required.

When a client sends an ARP request to retrieve a MAC address, those servers may respond with an ARP reply that indicates the Virtual MAC address in the payload. However, the source MAC address is the physical unit. This is accomplished to prevent switches from learning and forcing them to flood packets to all ports.

FortiGate does not create a session in this case because it has flooded a packet to all ports, so there is no stateful firewall session entry which can cause issues (i.e… reply packet drop, inability to antivirus scan, and others).

Diagram



Resolution

Configure a static MAC entry on the FortiGate. This will inform the FortiGate where the virtual MAC is connected.

Related CLI and Configuration example

"config system mac-address-table" command allows to configure static MAC entry.

Syntax

```
config system mac-address-table
      edit <mac-address_hex>
            set interface <if_name>
            set reply-substitute <mac-address_hex>
      end
```

Variable	Description	Default
edit <mac-address_hex>	Enter the MAC address as six pairs of hexadecimal digits separated by colons, e.g.: 11:22:33:00:ff:aa	No default.
interface <if_name>	Enter the name of the interface to which this MAC table entry applies.	No default.
reply-substitute <mac-address_hex>	Optionally, define a substitute MAC address to use in reply. Then define a MAC address table entry for the reply-substitute MAC address, specifying the interface to which it applies.	No default.

Note: This command is available only if the VDOM is in Transparent mode and is only allowed if the interface is in forward domain 0 which is by default.

Figure 1 – Static MAC Entry Example.

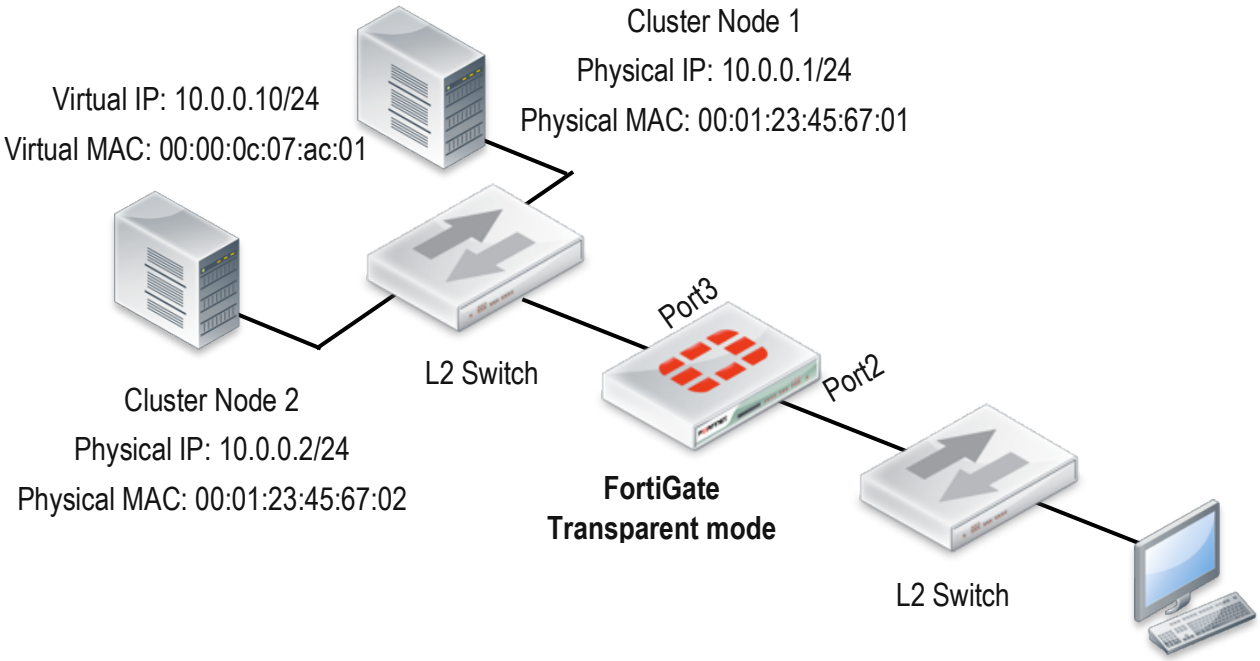
```
config system mac-address-table
    edit 00:00:0C:07:AC:01
        set interface "port3"
    next
end
```

Port-pairing

Description

Another way to solve the issue with VRRP, HSRP or a Network Load Balancer with FortiGate Transparent mode is port-pairing. Port-pairing provides a logical wire function, it forwards packets from one to another, and a session will be created even if the dst-mac is not learned.

Diagram



Related CLI and Configuration example

Step 1 – Configure Port-pair

Configuring port-pair is simple. Under config system port-pair, do edit <port-pair_name> then set port name of this port pair member.

Following the example put port2 and port3 on the same port-pair.

Syntax

```
config system port-pair
    edit <port-pair_name>
        set member <portname1> <portname2>
```

Variable	Description	Default
Edit <port-pair_name>	Enter a name for the port pair.	No default.
member <portname1> <portname2>	Enter the two port names that comprise the pair.	No default.

Figure 1 – Configure Port-paring Port2 and Port3 as Member.

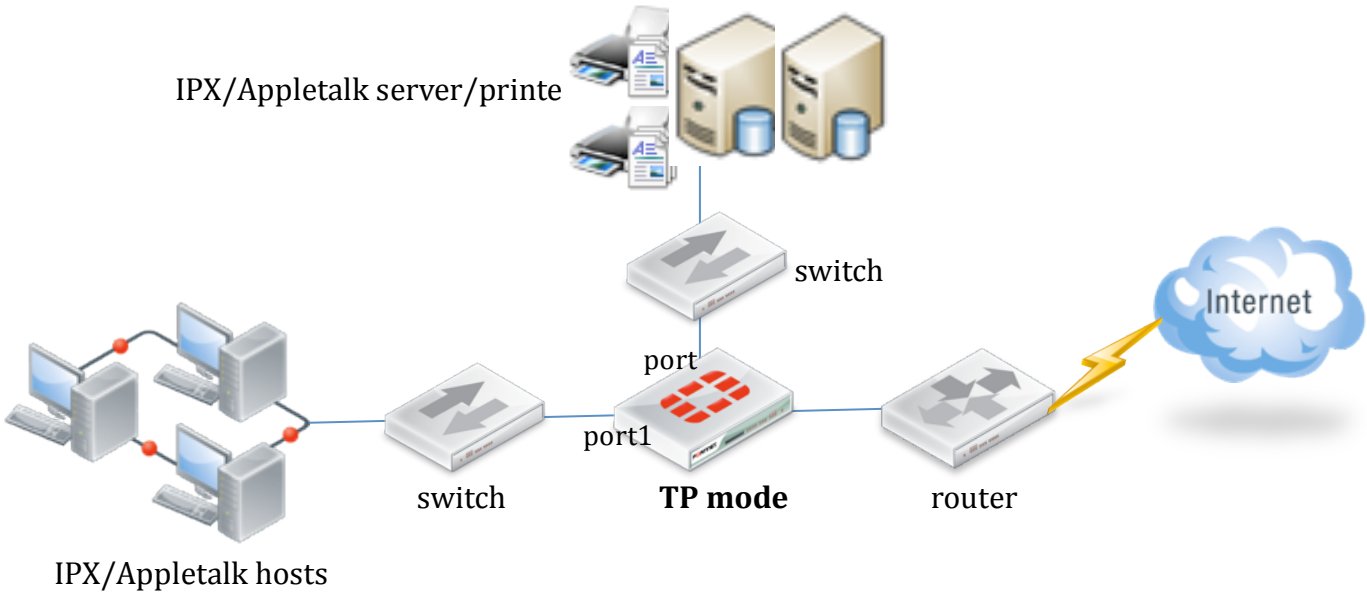
```
FGT60C_B # config sys port-pair
FGT60C_B (port-pair) # edit 1
FGT60C_B (1) # set member port2 port3
FGT60C_B (1) # next
FGT60C_B (port-pair) # end
FGT60C_B # show sys port-pair
config system port-pair
    edit "1"
        set member “port2" “port3"
    next
end
FGT60C_B #
```

Transparent Mode VDom with L2 Protocols that FortiGate Does Not Recognize.

Description

If there is any traffic or protocols that the FortiGate does not recognize, enabling l2forwarding may be appropriate. In most cases, the firewall is used to control and protect ip-based traffic. By default, a FortiGate in transparent mode, with proper settings and policy configurations, will provide firewalling or forwarding for Ethernet/EthernetII frames:
eth.type == IPv4: 0x0800, ARP: 0x0806, IPv6 0x86DD, 802.1Q 0x8100,
However, there are also cases where other L2 protocols, such as IPX AppleTalk, that need to pass through the TP mode FortiGate/vdom.

Diagram



Solution

Enable l2forward setting under the interface configuration.

Syntax

```
config system interface
      edit <interface_name>
            set l2forward {enable | disable}
```

Variable	Description	Default
l2forward {enable | disable}	Enable to allow layer-2 forwarding for this interface. If there are layer-2 protocols such as IPX, PPTP or L2TP in use on your network, you need to configure your FortiGate unit interfaces to pass these protocols without blocking. Enabling l2forward may cause packets to repeatedly loop through the network, much like a broadcast storm. In this case either disable l2forward, or enable Spanning Tree Protocol (STP) on your network's switches and routers. For more information, see *FortiGate VLANs and VDOMs*.	disable

Figure 1 – Configure l2forward Enable

```
config system interface
    edit "port1"
        set l2forward enable
    next
    edit "port2"
        set l2forward enable
    next
end
```

TP Mode FortiGate/VDom with Multicast Traffic

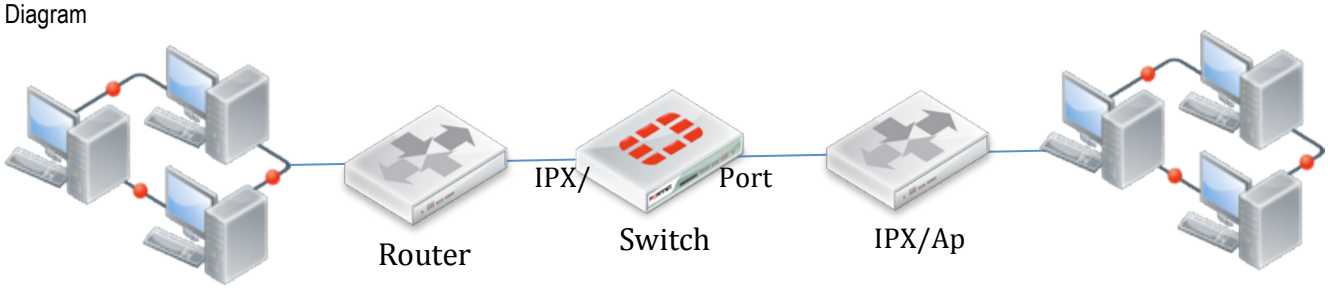
Description

By default, when a FortiGate/vdom is changed to transparent mode, a multicast firewall policy is automatically created as below to avoid interrupting possible multicast network services like RIP/ospf.

```
config firewall multicast-policy
   edit 1
      set srcintf "any"
      set dstintf "any"
      set srcaddr "all"
      set dstaddr "all"
   next
end
```

However the default any<->any multicast policy may not be desired. The actual multicast traffic needs to be passed through a TP mode FortiGate, but the FortiGate should be configured with more specific multicast address objects and multicast policies to only allow the necessary multicast traffic through the firewall.
For example, in a TP mode deployment like below:
TP mode FortiGate is inserted into an Ethernet segment between router1 and router2 that run OSPF between them.

Diagram



In this case, multicast IP 224.0.0.5 and 224.0.0.6 should be allowed in both directions.

Syntax

```
config firewall multicast-address
      edit <name_str>
            set end-ip <address_ipv4>
            set start-ip <address_ipv4>
```

Variable	Description	Default
<name_str>	Enter the name of the address. There are also predefinedaddresses: Bonjour, EIGRP, OSPF, all_hosts, all_routers.	No default
end-ip <address_ipv4>	If type is iprange, enter the last IP address in the range.	0.0.0.0
start-ip <address_ipv4>	If type is iprange, enter the first IP address in the range.	0.0.0.0

```
config firewall multicast-policy
      edit <index_int>
```

```
set action {accept | deny}
set dstaddr <addr_name_list>
set dstintf <name_str>
set srcaddr <addr_name_list>
set srcintf <name_str>
set status {enable | disable}
```

Variable	Description	Default
<index_int>	Enter the unique ID number of this multicast policy.	No default.
action {accept | deny}	Enter the policy action.	accept
dstaddr <addr_name_list>	Enter the names of multicast destination addresses for this policy. Separate address names with spaces. These addresses are defined in firewall multicast-address.	No default.
dstintf <name_str>	Enter the destination interface name to match against multicast NAT packets.	No default.
srcaddr <addr_name_list>	Enter the names of source IP addresses for this policy. Separate address names with spaces. These addresses are defined in firewall address, address6.	No default.
srcintf <name_str>	Enter the source interface name to match against multicast NAT packets.	No default.
status {enable | disable}	Enable or disable this policy.	enable

Configuration

Figure 1 – Configure Multicast Address Object and Multicast Policy.

```
config firewall multicast-address
    edit "OSPF"
        set start-ip 224.0.0.5
        set end-ip 224.0.0.6
    next
end

config firewall multicast-policy
    edit 1
        set srcintf "port1"
        set dstintf "port2"
        set srcaddr "all"
        set dstaddr "OSPF"
    next
    edit 2
        set srcintf "port2"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "OSPF"
    next
end
```

NOTE : In TP mode vdom, another setting related to multicast forwarding behavior is shown below.

Syntax

```
config system settings
      set multicast-skip-policy {enable | disable}
```

Variable	Description	Default
multicast-skip-policy {enable | disable}	Enable/disable skip policy check and allow multicast through.	disable

When multicast-skip-policy is enabled, multicast will not be controlled by the firewall multicast policy.
To avoid undesired flooding, it is best practice is to leave this setting disabled and use proper firewall multicast-policy to allow appropriate multicast traffic through FortiGate.

Asymmetrical packet forwarding in Transparent Mode

Description

Asymmetrical packet forwarding through UTM/Firewall is always chanllenging. It is best practice to NOT enable Asymmetrical packet forwarding on a FortiGate.
In FOS there is a setting that provides the option to enable asymmetrical packet forwarding using the CLI. Syntax is below:

Syntax

```
config system settings
      set asymroute {enable | disable}
```

Variable	Description	Default
asymroute {enable | disable}	Enable to turn on IPv4 asymmetric routing on your FortiGate unit, or this VDOM if you have VDOMs enabled. This feature should only be used as a temporary check to troubleshoot a network. It is not intended to be enabled permanently. When it enabled, many security features of your FortiGate unit are not enabled. **Note:** Enabling asymmetric routing disables stateful inspection. Your FortiGate unit can only perform stateless inspection in this state.	disable

There is a KB article discussing an example of how this parameter is used. Refer to:
http://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD31800&sliceId=1&docTypeID=DT_KCARTICLE_1_1&dialogID=57714254&stateId=0%200%2057712898

However, the consequences of enabling the asymroute setting is to make the FortiGate skip stateful inspection as a regular firewall, and start acting as a packet filtering device based on ACL(access control list). This should not be used in any production setting except for temporary diagnostic purposes.

Related Information

FortiOS and FortiGate Technical Documentation
http://docs.fortinet.com/fgt.html

Fortinet Knowledge Base
http://kb.fortinet.com/

FortiGate appliances
http://www.fortinet.com/products/fortigate/