Asymmetric routing and other FortiGate layer-2 installation issues

Technical Note

Asymmetric routing and other FortiGate layer-2 installation issues Technical Note	
Document Version:	Second Release
Publication Date:	September 28, 2004
Description:	This document provides information about FortiGate Antivirus Firewall Transparent Mode installation issues. Subject areas include asymmetric routing, stateful inspection, networks loops, spanning tree protocol, ARP forwarding, and using VLANs and virtual domains with Layer-2 switches with global MAC addresses.
Source:	The original version of this document was written by Bill Cormier for the Fortinet Sales Certification Lab. More information has been added in response to user comments.
Product:	FortiOS v2.80
Document Number:	01-28005-0113-20040928

Fortinet Inc.

Asymmetric routing and other FortiGate layer-2 installation issues Technical Note

September 28, 2004
01-28005-0113-20040928

Regulatory Compliance
FCC Class A Part 15 CSA/CUS

For technical support, please visit **http://www.fortinet.com**.

Send information about errors or omissions in this document or any Fortinet technical documentation to **techdoc@fortinet.com**.

Version	Date	Description of changes
First Release	July/August 2004	
Second Release	September 28, 2004	Added new section: “Layer-2 switches with global MAC addresses and ARP forwarding” on page 15.

Table of Contents

Transparent Mode 5
How it works 5
Configuration requirements 5
Considerations 6
Solutions 7
Other Asymmetric routing cases 10
Other Layer 2 Considerations 13
Network Loops 14
Spanning Tree Protocol 14
Other Layer 2 Protocols 14
Layer-2 switches with global MAC addresses and ARP forwarding 15
Check your settings 16
Conclusion 16

Transparent Mode

FortiGate units can be configured to operate in either NAT/Route or Transparent mode.

In NAT/Route mode, the FortiGate unit is a Layer 3 device. This means that each of its interfaces is associated with a different IP subnet and that it appears to other devices as a router. This is how a firewall is normally deployed.

In Transparent mode, the FortiGate unit does not change the Layer 3 topology. This means that all of its interfaces are on the same IP subnet and that it appears to other devices as a bridge. Typically, the FortiGate unit is deployed in Transparent mode when it is intended to provide antivirus and content filtering behind an existing firewall solution.

A FortiGate unit in Transparent mode can also perform firewalling. Even though it takes no part in the Layer 3 topology, it can examine Layer 3 header information and make decisions on whether to block or pass traffic.

How it works

In Transparent mode, the FortiGate unit acts invisible to the IP network. Similar to a network bridge, all of the FortiGate interfaces must be on the same subnet. In order to perform antivirus and content filtering, it performs IP packet filtering and forwarding. After applying firewall filtering rules called policies, the FortiGate unit assembles packets into content and scans for viruses and attacks, and filters out banned content from email and web traffic. The FortiGate unit then forwards packets in their original format.

Configuration requirements

Although a unit operating in Transparent mode does not alter the Layer 3 topology, it still requires basic configuration to operate as a node on the IP network. As a minimum, the unit must be configured with an IP address and subnet mask. These are used for management access and to allow the unit to receive antivirus and IPS signature file updates. Also, the unit must have sufficient route information to reach:

- the management station (such as a browser, telnet, SSH or SNMP management system),
- the FortiProtect Network servers,
- the DNS server(s).

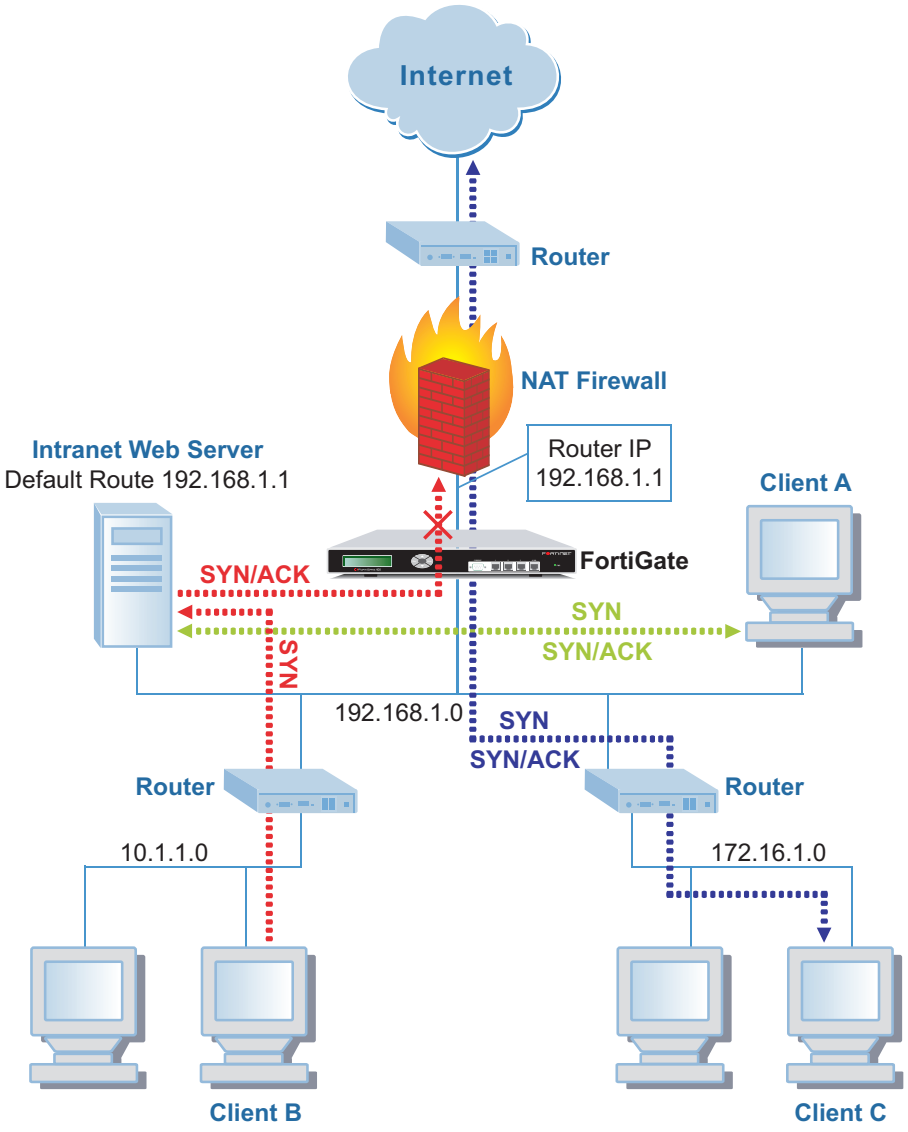
A static route is required whenever the FortiGate unit connects to a router to reach a destination. If all of the destinations are located on the external network, you may be required to enter only a single default route. If, however, the network topology is more complex, you may be required to enter one or more static routes in addition to the default route.

Considerations

In complex designs there may be more than just a default route out of the local network. In these cases it may become more difficult to place the FortiGate unit into the network in order to properly forward the traffic. If placed in the wrong position, an asymmetrical routing circumstance may cause some traffic to be blocked.

Consider the following network diagram.

Figure 1: Asymmetrical routing topology



In this network, a problem may occur where sessions from Client A work well getting to both the Intranet (internal) Web server and the Internet (external) web servers, and sessions from Client B or Client C can get to the Internet just fine, but can not get to the Intranet Web Server.

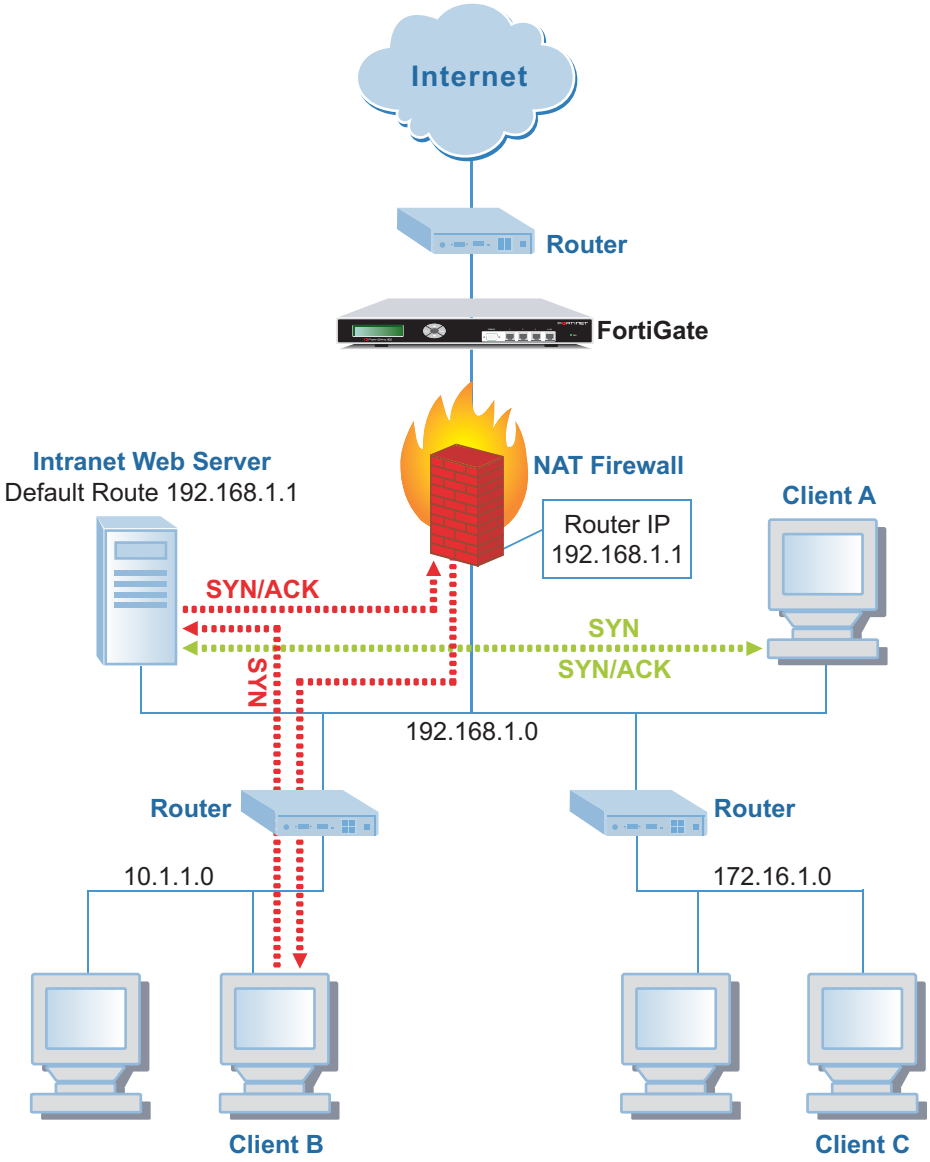
This is shown more clearly by the colored dotted lines. For Client A, which resides on the same subnet as the Intranet server, the green line shows that traffic going both to and from the server stays on the same subnet and therefore never passes through the FortiGate unit. Also for Client C, the dark blue lines, traffic going out to the Internet is symmetrical because both the send and receive traffic passes through the FortiGate unit's stateful packet inspection firewall. This works fine.

For Client B, the red line shows that traffic originates from the Client and passes through a router to get to the destination server. However, the server, not normally aware of other networks that are not directly connected, will pass the responses up to its default router, which is in front of the FortiGate unit. So the FortiGate unit being a stateful packet filter will only see the response and not the initial session request and will, therefore, block the incomplete session traffic.

Solutions

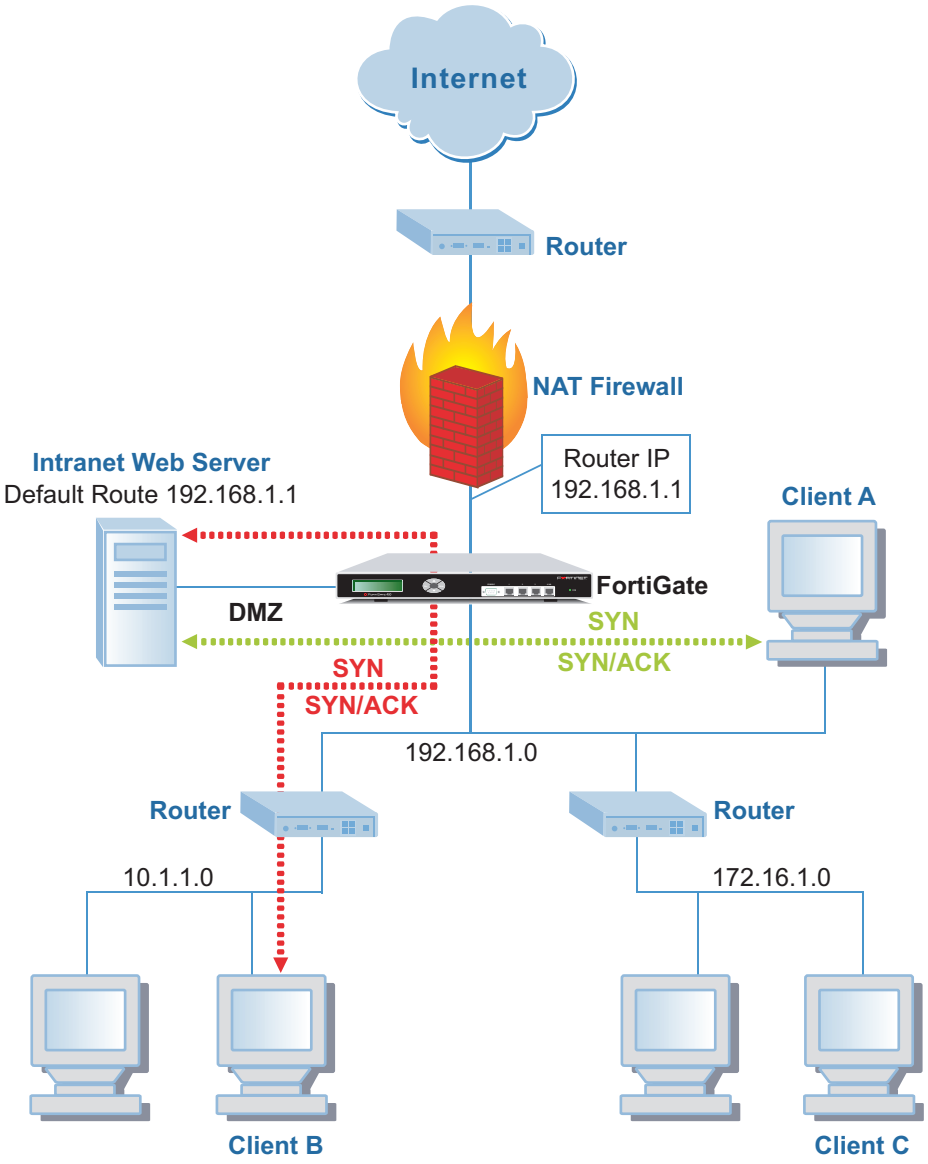
A few different workarounds can be used to correct this problem. The easiest approach may be to just move the FortiGate unit to sit in front of the firewall instead of behind it to avoid the asymmetrical routing issue. In this case sessions that are routed to the default gateway will not be filtered out. See Figure 2.

Figure 2: Solution 1 topology



Another possible solution is to add static routes to the server, so that it knows how to connect directly to other networks, without having to go through the default router. This may involve more work than above if you have a large number of servers to configure. Alternatively, if the FortiGate model has an available port, you can create a separate server DMZ network off of one of the ports on the FortiGate unit. This would allow all traffic going to and from the servers to pass through the Fortigate unit and provide the added benefit of performing antivirus and intrusion attack filtering on internal network traffic going to and from the Intranet servers. See Figure 3 below.

Figure 3: Solution 2 topology



A solution of last resort would be to turn off stateful inspection on the FortiGate unit. This would resolve the asymmetric routing problem without moving the FortiGate unit, but would cause the FortiGate unit to lose the ability to detect and prevent some hacker attacks.

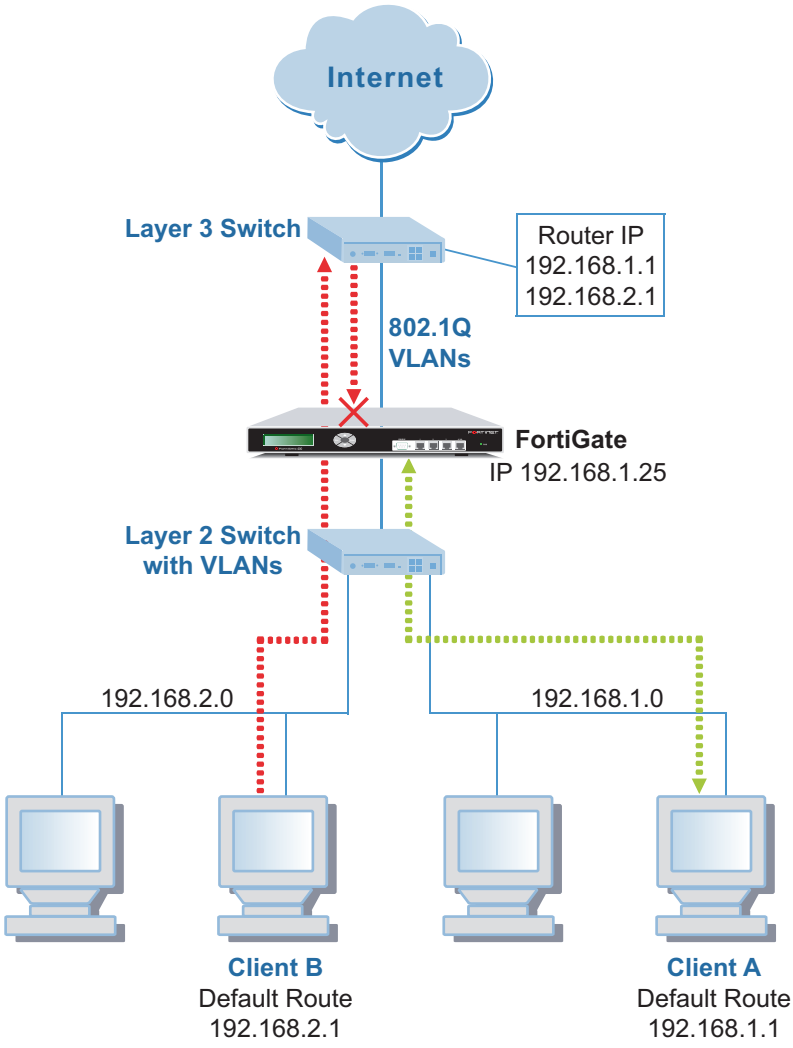
Use the following commands to turn off stateful inspection and enable asymmetric routing.

```
config system global
  set asymroute enable
  end
```

Other Asymmetric routing cases

There are many other network designs where the asymmetrical routing phenomenon occurs. Consider Figure 4.

Figure 4: Another asymmetrical routing example topology

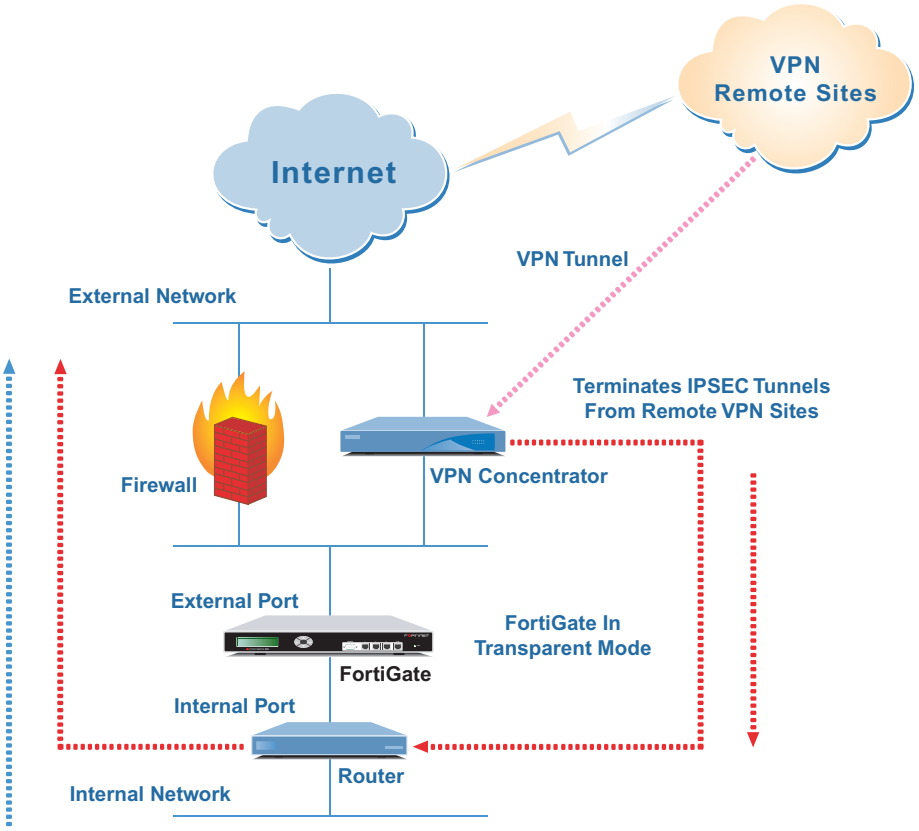


In this case both Client A and B can get out to the Internet just fine. But only Client A, the green line, can perform management functions on the FortiGate unit. Client B, the red line, is unable to PING, Telnet, or connect a Browser to the FortiGate Management agent. Again as a stateful inspection firewall, the FortiGate unit associates sessions with interfaces and when it sees an IP session request coming from one interface and then the same session request repeating back through a different interface, it assumes the second one is invalid.

In most cases, simply relocating the FortiGate unit to be in front of the default router will eliminate these problems.

Here is another design case where the stateful inspection engine breaks the traffic flow. See Figure 5.

Figure 5: Stateful inspection problem



In this case all traffic from the Internal network to the External network flows well (blue line), with or without AV scanning enabled. However, traffic from VPN users (red lines) going to the Internet, External to Internal, stops when AV scanning is enabled. The problem here is that the AV scanning engine proxy sees the same session twice, once coming into the FortiGate from the VPN concentrator and then again when the session goes back out to the Internet and comes back again. The second time it thinks that there is a session state problem and drops the session.

Unfortunately, enabling asymmetrical routing only affects the firewall stateful function, not the AV proxy engine so there is no easy fix to this issue.

There are a number of possible solutions to this problem.

- Do not AV scan the VPN traffic.
- Have the router proxy or NAT the traffic before sending it to the firewall, so that different source/destination addresses appear for each session.
- Move the FortiGate unit to be in-line with the firewall only, so that it doesn't see the VPN traffic until it goes out to the Internet (see Figure 6).
- Use two FortiGate units such that one will scan all VPN incoming traffic and one will scan all Internal to External traffic (see Figure 7).

Figure 6: A solution to the stateful inspection problem

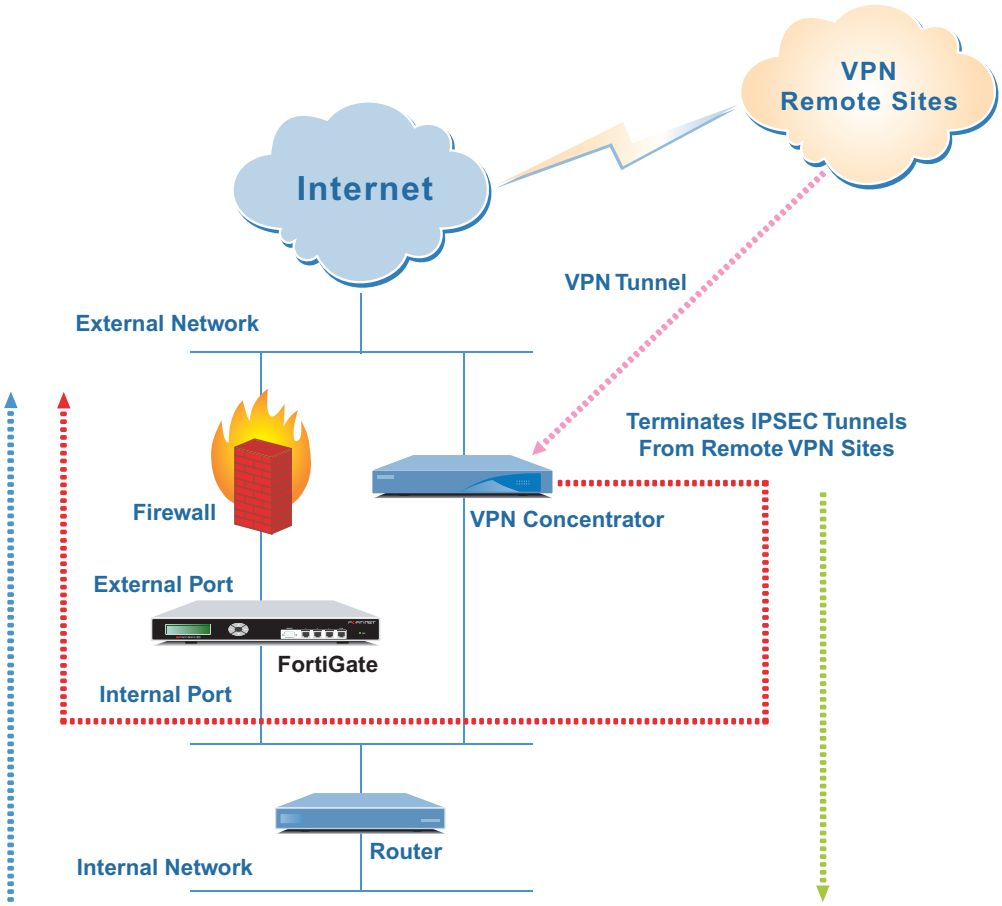
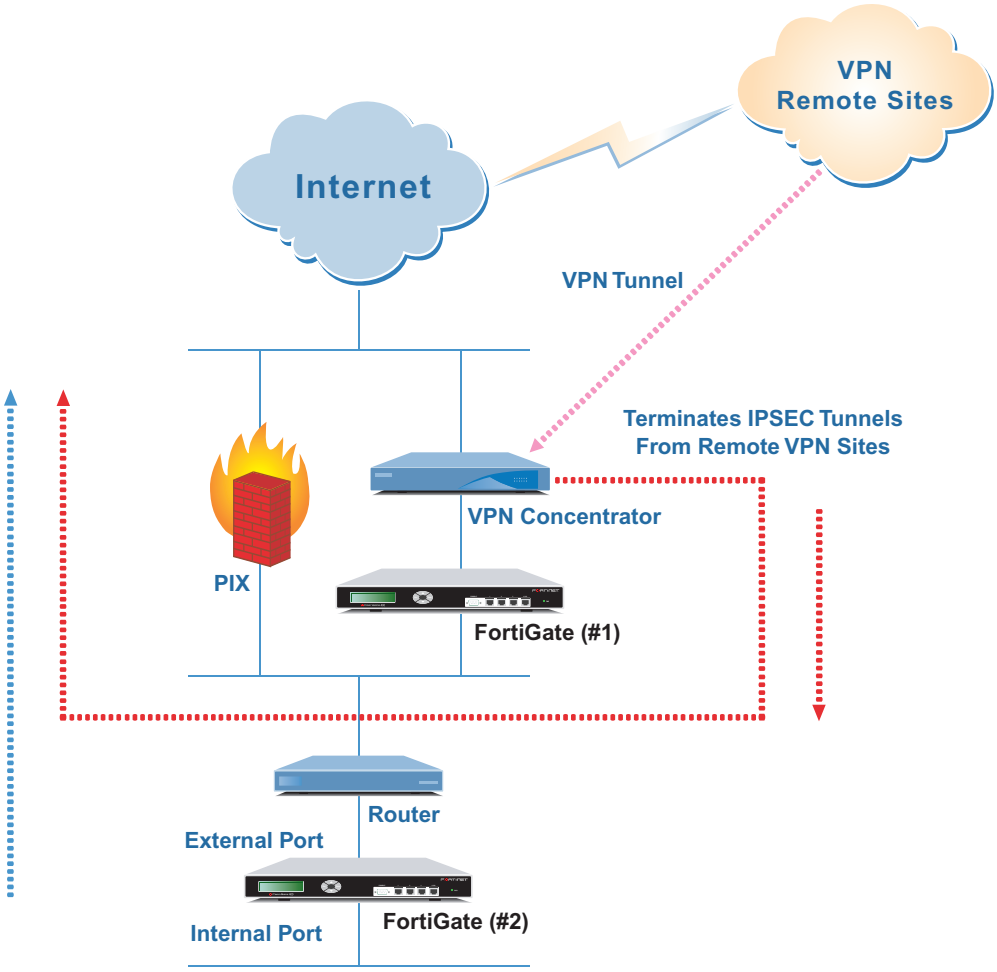


Figure 7: Another solution to the stateful inspection problem



Other Layer 2 Considerations

Even though the FortiGate unit in Transparent Mode acts as a bridge, by default its basic functionality includes only IP packet forwarding. To allow other non-IP protocols you will need to configure other options.

Network Loops

Before enabling other Layer 2 forwarding options, be sure to consider if doing so will cause any network loop conditions. A loop occurs when there are two Layer 2 paths from a source to a destination. Typically a loop condition is caused by plugging in two cables to the same switch or hub from the same Layer 2 source network. This can cause a broadcast storm. A broadcast storm occurs when a device ARPs for an address, the ARP broadcast will go out one port and loop back around through the other port and be repeated back out again rapidly over and over causing all other network traffic to be hindered. This can usually be easily detected by seeing port activity indicator lights on hubs and switches all lit up and continuously on or rapidly flashing in tandem. The Spanning Tree protocol is sometimes used to automatically detect and block network loops, and, therefore, prevent broadcast storms.

Spanning Tree Protocol

The Fortigate unit does not participate in the Spanning Tree protocol. Therefore, if used in a network topology that relies on the Spanning Tree protocol for network loop protection, you will need to make some configuration changes. Otherwise the Spanning Tree protocol will see the FortiGate unit as a blocked link and will forward the data to another path. By default the FortiGate unit will block the Spanning Tree protocol as well as other non-IP protocol traffic.

Using the Command Line Interface (CLI), you can enable the l2forward and stpforward options to allow non-IP Layer 2 protocols and the spanning tree protocol to pass through the named interface while in Transparent mode. The command is:

```
config system interface
edit <name_str>
set l2forward enable
set stpforward enable
end
```

The value `<name_str>` equals the name of the interface, which varies depending on the FortiGate model.“Layer-2 switches with global MAC addresses and ARP forwarding” on page 15

Note: You should enable `l2forward` for every interface that is receiving non-IP traffic.

Other Layer 2 Protocols

You can also enable Layer 2 ARP forwarding on each interface.

You use ARP forwarding to allow Address Resolution Protocol to pass through the FortiGate unit. ARP forwarding is enabled by default on FortiGate Antivirus Firewalls. Normally you would want ARPs to pass through the Fortigate unit, especially if it is sitting between a client and a server or between a client and a router.

The commands to set ARP forwarding are as follows:

```
config system interface
edit <name_str>
set arpforward enable
end
```

Layer-2 switches with global MAC addresses and ARP forwarding

Some layer-2 switches, when detecting the same MAC address originating on more than one switch interface or from more than one VLAN, may become unstable. This instability can occur if the layer-2 switch does not support adding separate MAC address tables for each VLAN. During normal operation, the switch keeps it own table of MAC addresses mapped to an interface or VLAN. Problems occur if the switch sees the same MAC address presented on multiple interfaces or VLANs.

In a configuration such as the one shown in Figure 8, the FortiGate unit running in Transparent mode is installed between two networks. The traffic between the two networks uses multiple VLANs. The Layer-2 switches add and remove the VLAN tags. The FortiGate unit is configured with multiple VLAN subinterfaces. VLAN-tagged traffic is received by the FortiGate unit from each Layer-2 switch, virus scanned and then forwarded to the other Layer-2 switch.

Figure 8: Example layer-2 switch network

By default, ARP forwarding is enabled on the FortiGate unit and ARP packets received by the FortiGate unit on one VLAN subinterface are forwarded out every other FortiGate VLAN subinterface. The switches can then receive multiple ARP packets from the same source MAC but tagged with different VLAN IDs.

To resolve this problem, you can configure multiple virtual domains on the FortiGate unit, 1 for each VLAN (this means one ingress and one egress VLAN added to each virtual domain). ARP packets are not forwarded between virtual domains. As a result, the switches do not receive multiple ARP packets from the same source MAC but different VLANs and the instability does not occur.

Some switches support the ability to statically configure MAC addresses to multiple ports. For example many Cisco switches that normally use a global MAC address table will allow use of the command:

```
mac-address-table static hw-addr in-port out-port-list
```

`hw-addr`	The MAC address to add to the address table.
`in-port`	The input port from which packets received with a destination address of `hw-addr` are forwarded to the list of ports in the `out-port-list`. The `in-port` must belong to the same VLAN as all the ports in the `out-port-list`.
`out-port-list`	The list of ports to which packets received on ports in `in-port` are forwarded. All ports in the list must belong to the same VLAN.

Check your settings

To view the configuration changes use the command show system interface.

You will see something similar to the display below (for a FortiGate-60 model):

```
config system interface
    edit "internal"
        set allowaccess ping https ssh
        set l2forward enable
        set stpforward enable
    next
    edit "wan1"
        set allowaccess ping
    next
    edit "wan2"
        set allowaccess ping
        set l2forward enable
        set stpforward enable
    next
    edit "dmz"
        set allowaccess ping https
    next
    edit "modem"
    next
end
```

Note: The `show system interface` command displays only commands that have been changed from the default settings. Since ARP forwarding is enabled by default the `set arpforward enable` command will not show in this display. You can confirm that ARP forwarding is enabled by typing the command `get system interface <name_str>` for each interface.

Conclusion

The FortiGate Antivirus Firewall is very flexible in its ability to work in Layer 2 or Layer 3 networks as long as you understand its capabilities and its limitations. Taking the time to diagram the network installation can help you to understand the traffic flow and avoid any pitfalls.