Extra help: Transparent mode

This section provides instructions for troubleshooting connection issues when using a FortiGate in Transparent mode.

1. Use FortiExplorer if you can't connect tot he FortiGate GUI or CLI

If you can't connect to the FortiGate GUI or CLI, you may be able to connect using FortiExplorer. See your FortiGate unit's QuickStart Guide for details.

2. Check for equipment issues.

Verify that all network equipment is powered on and operating as expected. Refer to the QuickStart Guide for information about connecting your FortiGate to the network and about the information provided by the FortiGate unit LED indicators.

3. Check the physical network connections.

Check the cables used for all physical connections between the PC, the FortiGate unit, and your ISP-supplied equipment to ensure that they are fully connected and do not appear damaged. Also check the Unit Operation dashboard widget, which indicates the connection status of FortiGate network interfaces (**System > Dashboard > Status**).

4. Verify that you can connect to the management IP address of the FortiGate unit from the Internal network.

From the internal network, attempt to ping the management IP address. If you cannot connect to the internal interface, verify the IP configuration of the PC and make sure the cables are connected and all switches and other devices on the network are powered on and operating. Go to the next step when you can connect to the internal interface.

5. Verify that you can communicate from the FortiGate unit to the Internet.

Access the FortiGate CLI and use the `execute ping` command to ping an address or domain name on the Internet. You can also use the `execute traceroute` command to troubleshoot connectivity to the Internet.

6. Verify the DNS configurations of the FortiGate unit and the PCs on the internal network.

Check for DNS errors by pinging or using traceroute to connect to a domain name; for example:

```
ping www.fortinet.com
ping: cannot resolve www.fre.com: Unknown host
```

If the name cannot be resolved, the FortiGate unit or PC cannot connect to a DNS server and you should confirm the DNS server IP addresses are present and correct.

7. Verify the security policy configuration.

Go to **Policy > Policy > Policy** and verify that an internal -> wan1 security policy has been added and check the **Session** column to ensure that traffic has been processed.

8. Verify the static routing configuration.

Go to **System > Network > Routing Table** and verify that the default route is correct.

9. Disable web filtering.

A web filtering security policy may block access to the website that you are attempting to connect to. This could happen because the configuration of the default web filter profile is blocking access to the site.

It is also possible that FortiGuard Web Filtering has produced a rating error for the website, causing the web filter profile to block access. A rating error could occur for a number of reasons, including not being able to access FortiGuard. To fix this problem, go to **Security Profiles > Web Filter > Profile** and, in the default profile, enable **Allow Websites When a Rating Error Occurs**.

10. Verify that you can connect to the gateway provided by your ISP.

Try pinging the default gateway IP address from a PC on the internal network.

11. Confirm that the FortiGate unit can connect to the FortiGuard network.

Once registered, the FortiGate unit obtains antivirus and application control and other updates from the FortiGuard network. Once the FortiGate unit is on your network, you should confirm that it can reach the FortiGuard network. The FortiGate unit must be able to connect to the network from its management IP address. If the following tests provide

incorrect results, the FortiGate unit cannot connect to the Internet from its management IP address. Check the FortiGate unit's default route to make sure it is correct. Check your Internet firewall to make sure it allows connections from the FortiGate management IP address to the Internet.

First, check the **License Information** dashboard widget to make sure the status of all FortiGuard services matches the services that you have purchased. The FortiGate unit connects to the FortiGuard network to obtain this information.

Go to **System > Config > FortiGuard**. Open web filtering and email options and select **Test Availability**. After a minute, the GUI should indicate a successful connection.

12. Check the FortiGate bridge table.

The bridge table is a list of MAC addresses of devices on the same network as the FortiGate unit and the FortiGate interfaces from which each MAC address was found. The FortiGate unit uses this table to determine where to forward a packet. If a the MAC address of a specific device is getting added to the bridge table, then packets to that MAC address will be blocked. This may appear as traffic going to a MAC address but no reply traffic coming back. In this situation, check the bridge table to ensure the correct MAC addresses have been added to the bridge table. Use the following CLI command to check the bridge table:.

```
diagnose netlink brctl name host root.b
show bridge control interface root.b host.
fdb: size=2048, used=25, num=25, depth=1
Bridge root.b host table
port no device devname mac addr ttl attributes
3 4 wan1 00:09:0f:cb:c2:77 88
3 4 wan1 00:26:2d:24:b7:d3 0
3 4 wan1 00:13:72:38:72:21 98
4 3 internal 00:1a:a0:2f:bc:c6 6
1 6 dmz 00:09:0f:dc:90:69 0 Local Static
3 4 wan1 c4:2c:03:0d:3a:38 81
3 4 wan1 00:09:0f:15:05:46 89
3 4 wan1 c4:2c:03:1d:1b:10 0
2 5 wan2 00:09:0f:dc:90:68 0 Local Static
```

If your device's MAC address is not listed, the FortiGate unit cannot find the device on the network. This could indicate that the device is not connected or not operating. Check the device's network connections and make sure it is operating correctly.

13. Reset the FortiGate unit to factory defaults and try again

If all else fails, use the CLI command `execute factoryreset`. When prompted, type `y` to confirm the reset.

Resetting the FortiGate unit to factory defaults will put the unit back into NAT/Route mode.