Deploying a Multi-Homed Forcepoint DLP Protector

A Forcepoint DLP protector can use one or more interfaces to monitor and process traffic. One interface must be defined as the management interface.

Depending on the network topology and existing security policies, a protector may have a single path or separate routes to the Internet and to other Forcepoint DLP components.

- When there is a single path, the protector can use a default route to access the Internet and management server.
- When there are multiple paths, it may be necessary to add a static route to ensure connectivity between the protector and other Forcepoint DLP components.

This document provides sample steps to configure a protector with multiple interfaces as follows:

- One interface is in a DMZ and is the default path.
- One interface is in a separate network and is used as the management interface.

The sample steps assume that:

- Forcepoint DLP is installed and working.
- All required networking information is available (default gateway, network masks, IP addresses of routers, DNS, and so on).
- em1 is an internal interface that leads to the management server and other internal components
- em2 is in the DMZ leading to the Internet.

Continue with *Configuring the protector*, page 2.

Configuring the protector

Before performing these steps, install the protector as described in the Forcepoint DLP Installation Guide.

Initial configuration

First, configure the protector to ensure that the management server can be reached via a default route:

1. Open the protector console and log on as **root**.
2. Run the wizard when prompted.
3. Configure network interfaces as prompted.
4. Register with the management server or Forcepoint DLP server.
5. After the registration completes, in the protector console, add a static route so the management server can be reachable without a default route:
    a. Create the following file:

    ```
    /etc/sysconfig/network-scripts/route-em1
    ```

    b. Add the following route entry:

    ```
    10.103.18.x/24 via 10.104.43.x dev em1
    ```

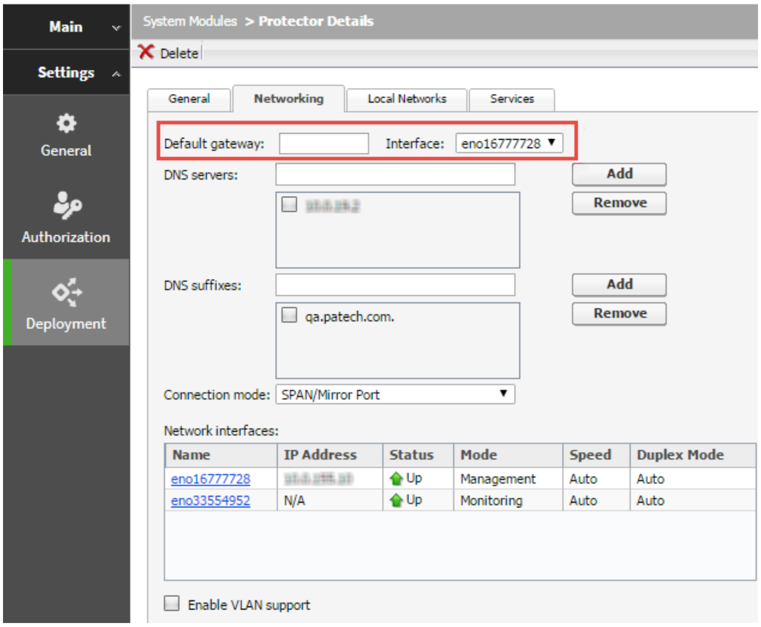
    c. Save and close the file.
6. Log on to the Data Security module of the Forcepoint Security Manager and click **Deploy**.
7. Verify that all changes have been saved, including any new interfaces.

Add the final default gateway

Configure the final default gateway in the Security Manager:

1. Go to the **Settings** > **Deployment** > **System Modules** page.
2. Select the protector instance in the System Modules tree.
3. On the Protector Details page, select the **Networking** tab.
4. Use the Interface drop-down list to select the interface corresponding to **em2**.
5. Enter the new **Default gateway**.

6. In the network section, select **em2** and enter the new **default gateway**.



Default gateway: ____ Interface: eno16777728

DNS servers:

□ [redacted]

DNS suffixes:

□ qa.patech.com.

Connection mode: SPAN/Mirror Port

Network interfaces:

Name	IP Address	Status	Mode	Speed	Duplex Mode
eno16777728	[redacted]	Up	Management	Auto	Auto
eno33554952	N/A	Up	Monitoring	Auto	Auto

□ Enable VLAN support

7. In the protector console, to make sure the **pamad** service is running, use the following command:

```
ps –ef | grep pamad
```

If the service is not started, enter the following command:

```
service pamad restart
```

For example:

```
~ root@protector8# ps -ef | grep pamad
root 22159 22153 0 Mar25 ? 00:00:10 /opt/websense/neti/
bin/pamad
root 31532 27857 0 06:25 pts/0 00:00:00 grep pamad
~ root@protector8# service pamad restart
Stopping SMTP Blocking Service... [ OK ]
Stopping PAMA Watchdog ........... [ OK ]
Starting SMTP Blocking Service... [ OK ]
Starting PAMA Watchdog... [ OK ]
~ root@protector8#
```

8. In the Security Manager, click **Deploy**.

The protector now has a new default gateway, but it can still communicate with the management server via the static route previously entered.

Rename the protector

To rename the protector:

1. In the protector console, enter the following command:

   ```
   wizard hostname
   ```

2. Set the external hostname US-XXXXDLP1-NET0.
3. Still in the protector console, enter the following command:

   ```
   wizard securecomm
   ```

4. Register with the management server.
5. In the Security Manager, click Deploy.

   The deploy process will fail due to connection failure.

6. Log off of the Security Manager.
7. Use remote desktop (RDP) to connect to the Forcepoint DLP server and use the Windows Services tool to restart the **Websense Data Security Manager** service.
8. Log on to the Security Manager.
9. Confirm that the protector object has all the saved settings, including the new name.
10. Click **Deploy** again. This time, the deploy process should succeed.