Deploying a Multi-Homed TRITON AP-DATA Protector

Summary

A Forcepoint™ TRITON® AP-DATA protector can have one or more interfaces to monitor and process traffic. One of the interfaces needs to be defined as the management interface.

Depending on a company network topology and security policies, a protector may have a single path or separate routes to the Internet and the rest of the Forcepoint components.

In the case of a single path, the use of a default route is sufficient to access the Internet and TRITON management server.

In the case of multiple paths, there may be a need to add a static route in the protector to ensure connectivity between the protector and TRITON AP-DATA.

The following process describes the steps to deploy a protector with multiple interfaces, where one interface is on a DMZ and is the default path, and a second interface is in a separate network and will be used as the management interface.

Assumptions:

- TRITON AP-DATA is installed and working.
- All required networking information is available (default gateway, network masks, IP addresses of routers, DNS...)
- For the protector in this example, eth0 will be an internal interface that leads to the TRITON management server and other internal components; eth1 will be an interface in a DMZ leading to the Internet.

Details for this example:

eth0 (this is the management interface)

IP: 10.104.43.x

Netmask: 255.255.255.x

Initial default gateway: 10.104.43.x

ethX (this is located in a different network)

IP: 10.41.10.x

Netmask: 255.255.255.x

“Final” default gateway: 10.41.10.x

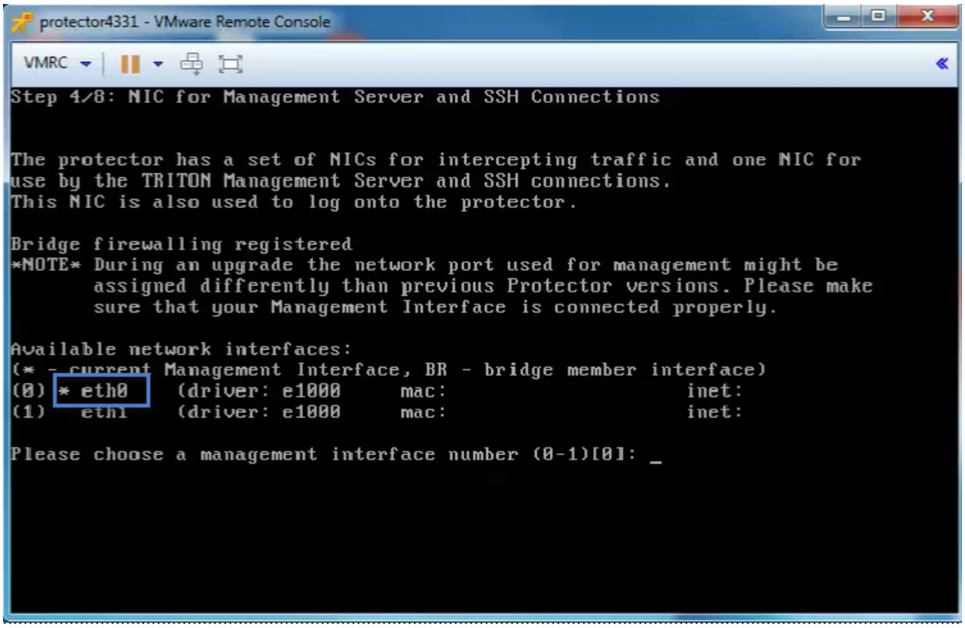
TRITON AP-DATA Triton Manager: 10.103.18.x

For the customer environment:

Initial hostname: US-XXXXDLP1-NET1

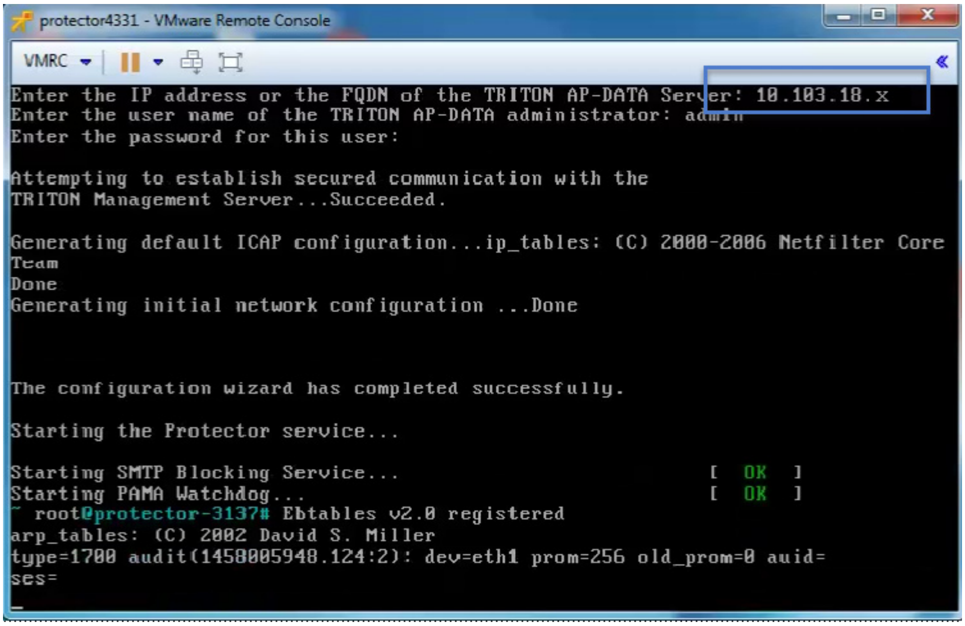
Steps:

1. Use the appropriate ISO image to install the protector.
2. From the console of the protector, log on as root (default password: admin).
3. At the prompt, **Run** the wizard.
4. Enter information into the required fields.



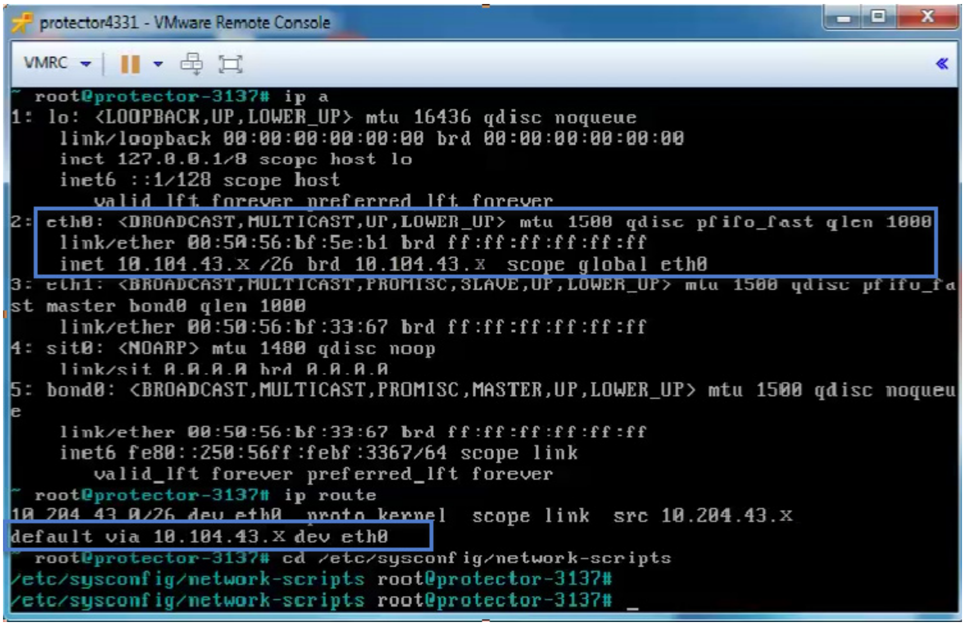
```
Step 4/8: NIC for Management Server and SSH Connections


The protector has a set of NICs for intercepting traffic and one NIC for
use by the TRITON Management Server and SSH connections.
This NIC is also used to log onto the protector.

Bridge firewalling registered
*NOTE* During an upgrade the network port used for management might be
       assigned differently than previous Protector versions. Please make
       sure that your Management Interface is connected properly.

Available network interfaces:
(* - current Management Interface, BR - bridge member interface)
(0) * eth0    (driver: e1000     mac:                        inet:
(1)   eth1    (driver: e1000     mac:                        inet:

Please choose a management interface number (0-1)[0]: _
```

5. Register with the TRITON management server or TRITON AP-DATA server.

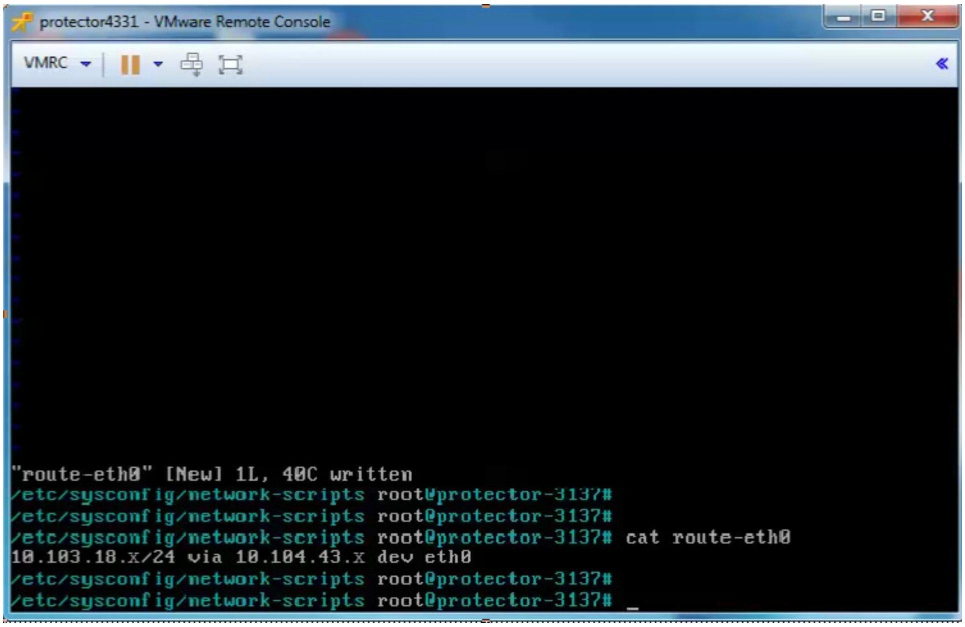


```
Enter the IP address or the FQDN of the TRITON AP-DATA Server: 10.103.18.x
Enter the user name of the TRITON AP-DATA administrator: admin
Enter the password for this user:

Attempting to establish secured communication with the
TRITON Management Server...Succeeded.

Generating default ICAP configuration...ip_tables: (C) 2000-2006 Netfilter Core
Team
Done
Generating initial network configuration ...Done


The configuration wizard has completed successfully.

Starting the Protector service...

Starting SMTP Blocking Service...                              [  OK  ]
Starting PAMA Watchdog...                                      [  OK  ]
~ root@protector-3137# Ebtables v2.0 registered
arp_tables: (C) 2002 David S. Miller
type=1700 audit(1458005948.124:2): dev=eth1 prom=256 old_prom=0 auid=
ses=
_
```

6. Once back in the command line of the protector, add a static route so the TRITON management server can be reachable without a default route. One way is to create the file `/etc/sysconfig/network-scripts/route-eth0` and add the route entry: `10.103.18.x/24 via 10.104.43.x dev eth0`

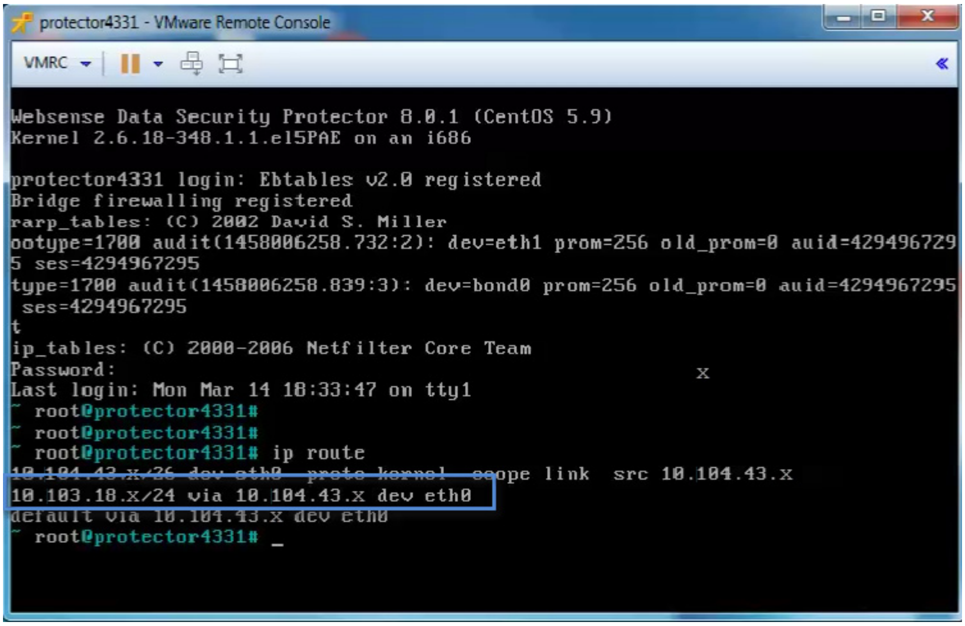


```
~ root@protector-3137# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:50:56:bf:5e:b1 brd ff:ff:ff:ff:ff:ff
    inet 10.104.43.x /26 brd 10.104.43.x  scope global eth0
3: eth1: <BROADCAST,MULTICAST,PROMISC,SLAVE,UP,LOWER_UP> mtu 1500 qdisc pfifo_fa
st master bond0 qlen 1000
    link/ether 00:50:56:bf:33:67 brd ff:ff:ff:ff:ff:ff
4: sit0: <NOARP> mtu 1480 qdisc noop
    link/sit 0.0.0.0 brd 0.0.0.0
5: bond0: <BROADCAST,MULTICAST,PROMISC,MASTER,UP,LOWER_UP> mtu 1500 qdisc noqueu
e
    link/ether 00:50:56:bf:33:67 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::250:56ff:febf:3367/64 scope link
       valid_lft forever preferred_lft forever
~ root@protector-3137# ip route
10.204.43.0/26 dev eth0  proto kernel  scope link  src 10.204.43.x
default via 10.104.43.X dev eth0
~ root@protector-3137# cd /etc/sysconfig/network-scripts
/etc/sysconfig/network-scripts root@protector-3137#
/etc/sysconfig/network-scripts root@protector-3137# _
```



```
"route-eth0" [New] 1L, 40C written
/etc/sysconfig/network-scripts root@protector-3137#
/etc/sysconfig/network-scripts root@protector-3137#
/etc/sysconfig/network-scripts root@protector-3137# cat route-eth0
10.103.18.x/24 via 10.104.43.x dev eth0
/etc/sysconfig/network-scripts root@protector-3137#
/etc/sysconfig/network-scripts root@protector-3137# _
```

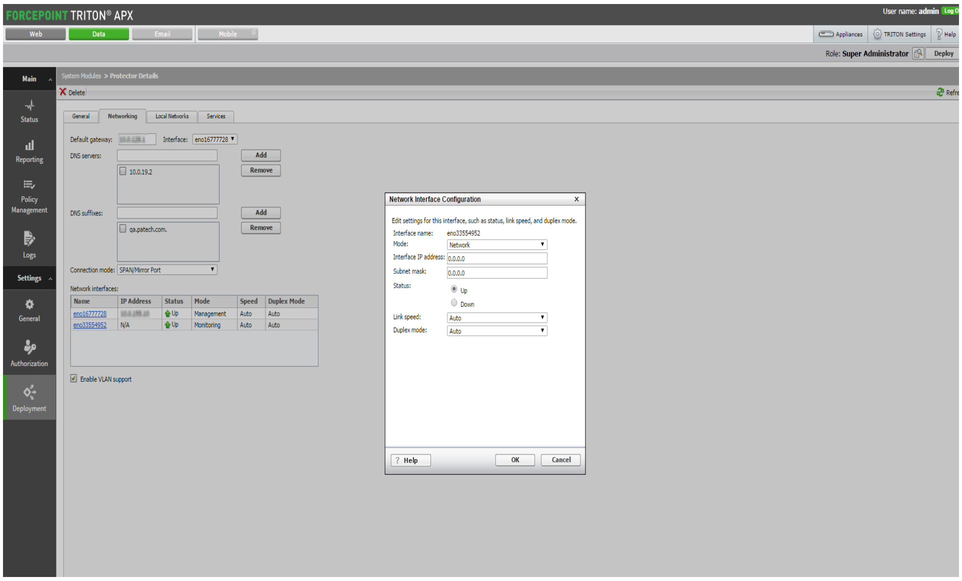
Optionally, you can reboot to confirm the route still exists.



```
Websense Data Security Protector 8.0.1 (CentOS 5.9)
Kernel 2.6.18-348.1.1.el5PAE on an i686

protector4331 login: Ebtables v2.0 registered
Bridge firewalling registered
rarp_tables: (C) 2002 David S. Miller
ootype=1700 audit(1458006258.732:2): dev=eth1 prom=256 old_prom=0 auid=429496729
5 ses=4294967295
type=1700 audit(1458006258.839:3): dev=bond0 prom=256 old_prom=0 auid=4294967295
 ses=4294967295
t
ip_tables: (C) 2000-2006 Netfilter Core Team
Password:                                                        x
Last login: Mon Mar 14 18:33:47 on tty1
~ root@protector4331#
~ root@protector4331#
~ root@protector4331# ip route
10.104.43.x/26 dev eth0  proto kernel  scope link  src 10.104.43.x
10.103.18.x/24 via 10.104.43.x dev eth0
default via 10.104.43.x dev eth0
~ root@protector4331# _
```

7. Log on to the TRITON management server.

8. Configure the protector as needed (select protocols, blocking or monitoring, additional interfaces, etc.)
   NOTE: Do not modify the default gateway at this time.



System Modules > Protector Details

Default gateway: [redacted] Interface: eno16777728

DNS servers:

□ 10.0.19.2

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

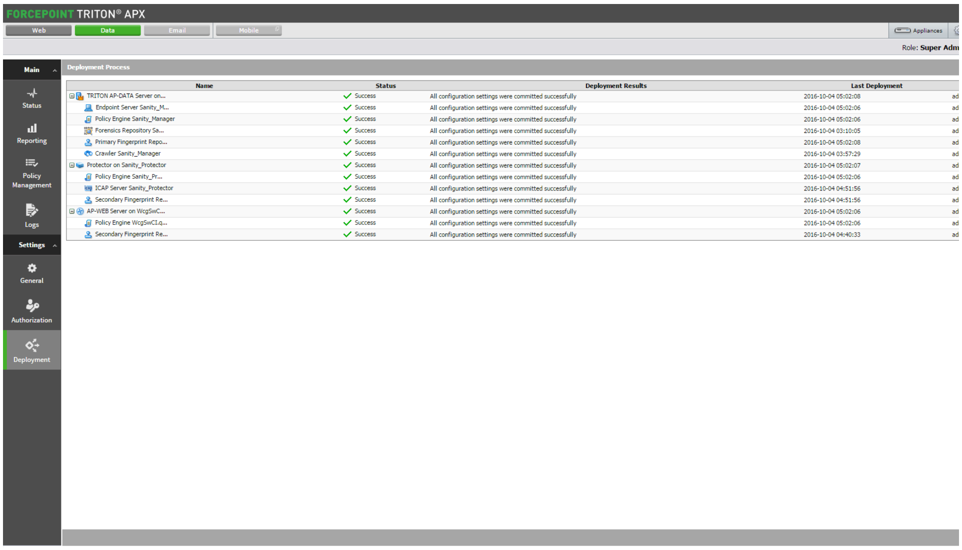
☑ Enable VLAN support

Network Interface Configuration

Edit settings for this interface, such as status, link speed, and duplex mode.

Interface name: eno33554952
Mode: Network
Interface IP address: 0.0.0.0
Subnet mask: 0.0.0.0
Status: ● Up ○ Down
Link speed: Auto
Duplex mode: Auto

9. Deploy the policy.

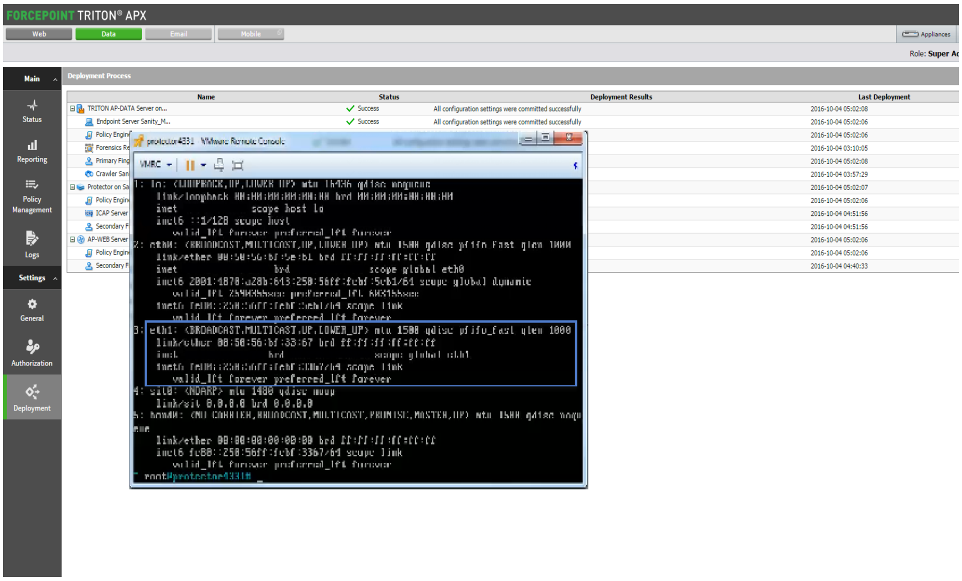


Role: Super Adm

Deployment Process

Name	Status	Deployment Results	Last Deployment	
TRITON AP-DATA Server on...	✓ Success	All configuration settings were committed successfully	2016-10-04 05:02:08	ad
Endpoint Server Sanity_M...	✓ Success	All configuration settings were committed successfully	2016-10-04 05:02:06	ad
Policy Engine Sanity_Manager	✓ Success	All configuration settings were committed successfully	2016-10-04 05:02:06	ad
Forensics Repository Sa...	✓ Success	All configuration settings were committed successfully	2016-10-04 03:10:05	ad
Primary Fingerprint Repo...	✓ Success	All configuration settings were committed successfully	2016-10-04 05:02:08	ad
Crawler Sanity_Manager	✓ Success	All configuration settings were committed successfully	2016-10-04 03:57:29	ad
Protector on Sanity_Protector	✓ Success	All configuration settings were committed successfully	2016-10-04 05:02:07	ad
Policy Engine Sanity_Pr...	✓ Success	All configuration settings were committed successfully	2016-10-04 05:02:06	ad
ICAP Server Sanity_Protector	✓ Success	All configuration settings were committed successfully	2016-10-04 04:51:56	ad
Secondary Fingerprint Re...	✓ Success	All configuration settings were committed successfully	2016-10-04 04:51:56	ad
AP-WEB Server on WcgSwC...	✓ Success	All configuration settings were committed successfully	2016-10-04 05:02:06	ad
Policy Engine WcgSwCI.q...	✓ Success	All configuration settings were committed successfully	2016-10-04 05:02:06	ad
Secondary Fingerprint Re...	✓ Success	All configuration settings were committed successfully	2016-10-04 04:40:33	ad

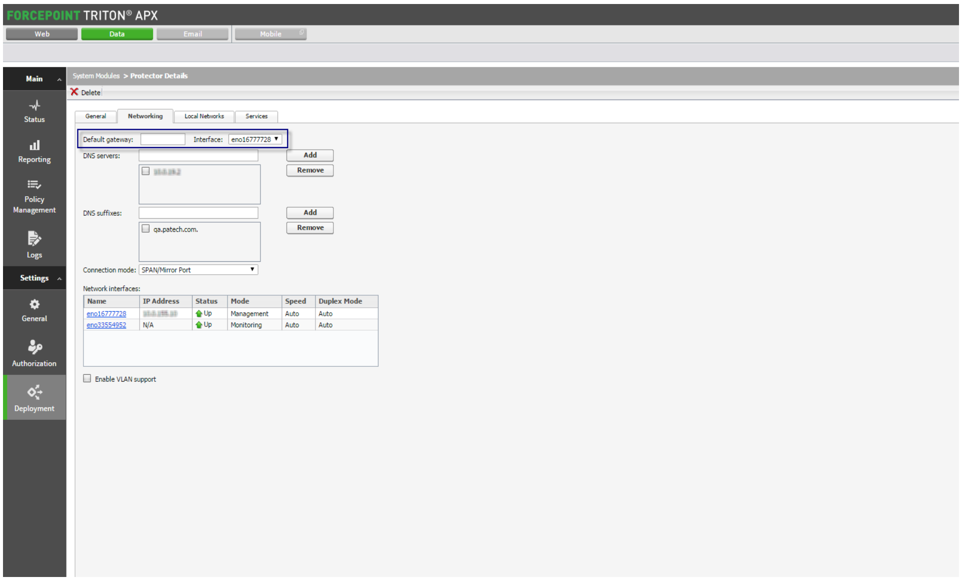
10. Check that the changes have been saved, including any new interfaces.



Name	Status	Deployment Results	Last Deployment
TRITON AP-DATA Server on...	✓ Success	All configuration settings were committed successfully	2016-10-04 05:02:08
Endpoint Server Sanity_M...	✓ Success	All configuration settings were committed successfully	2016-10-04 05:02:06
Policy Engin			2016-10-04 05:02:06
Forensics Re			2016-10-04 03:10:05
Primary Fing			2016-10-04 05:02:08
Crawler San			2016-10-04 03:57:29
Protector on Sa			2016-10-04 05:02:07
Policy Engin			2016-10-04 05:02:06
ICAP Server			2016-10-04 04:51:56
Secondary F			2016-10-04 04:51:56
AP-WEB Server			2016-10-04 05:02:06
Policy Engin			2016-10-04 05:02:06
Secondary F			2016-10-04 04:40:33

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet             scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:50:56:bf:5e:b1 brd ff:ff:ff:ff:ff:ff
    inet                 brd                scope global eth0
    inet6 2001:1878:a28b:613:250:56ff:febf:5eb1/64 scope global dynamic
       valid_lft 2590955sec preferred_lft 603155sec
    inet6 fe80::250:56ff:febf:5eb1/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:50:56:bf:33:67 brd ff:ff:ff:ff:ff:ff
    inet                brd               scope global eth1
    inet6 fe80::250:56ff:febf:3367/64 scope link
       valid_lft forever preferred_lft forever
4: sit0: <NOARP> mtu 1480 qdisc noop
    link/sit 0.0.0.0 brd 0.0.0.0
5: bond0: <NO-CARRIER,BROADCAST,MULTICAST,PROMISC,MASTER,UP> mtu 1500 qdisc noqu
eue
    link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::250:56ff:febf:3367/64 scope link
       valid_lft forever preferred_lft forever
~ root@protector4331# _
```

11. Add the final default. In the network section, select **eth1** 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

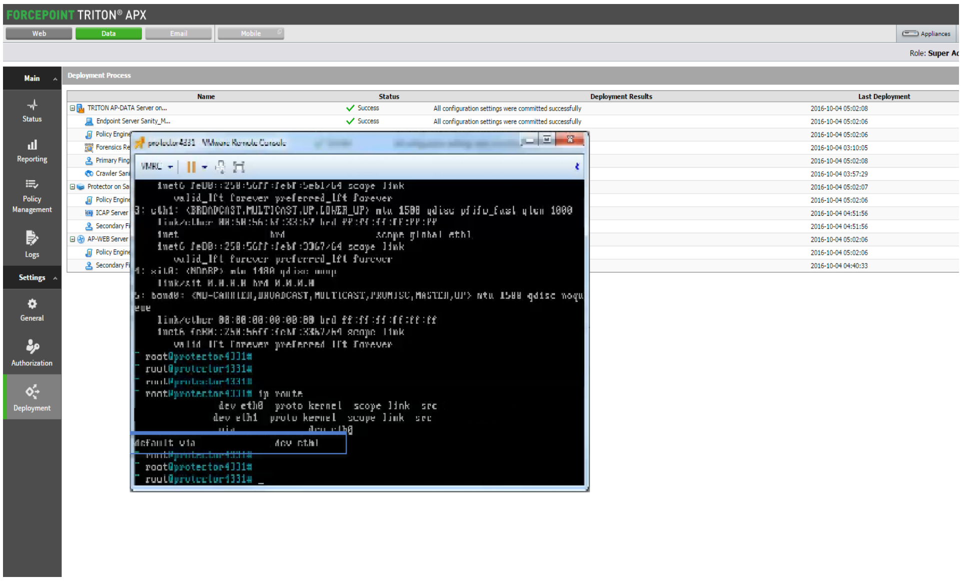
□ Enable VLAN support

12. Check to ensure the pamad service is running.

13. Run `ps -ef | grep pamad`. If the service is not started, run service pama restart.

```
~ 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 pama restart
Stopping SMTP Blocking Service... [ OK ]
Stopping PAMA Watchdog .......... [ OK ]
Starting SMTP Blocking Service... [ OK ]
Starting PAMA Watchdog... [ OK ]
~ root@protector8#
```

14. Deploy the policy.



Deployment Process

Name	Status	Deployment Results	Last Deployment
TRITON AP-DATA Server on...	✓ Success	All configuration settings were committed successfully	2016-10-04 05:02:08
Endpoint Server Sanity_M...	✓ Success	All configuration settings were committed successfully	2016-10-04 05:02:06
Policy Engine			2016-10-04 05:02:06
Forensics Re			2016-10-04 03:10:05
Primary Fing			2016-10-04 05:02:08
Crawler Sani			2016-10-04 03:57:29
Protector on Sa			2016-10-04 05:02:07
Policy Engine			2016-10-04 05:02:06
ICAP Server			2016-10-04 04:51:56
Secondary Fi			2016-10-04 04:51:56
AP-WEB Server			2016-10-04 05:02:06
Policy Engine			2016-10-04 05:02:06
Secondary Fi			2016-10-04 04:40:33

```
    inet6 fe80::250:56ff:feb1:5eb1/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:50:56:b1:33:67 brd ff:ff:ff:ff:ff:ff
    inet              brd                 scope global eth1
    inet6 fe80::250:56ff:feb1:3367/64 scope link
       valid_lft forever preferred_lft forever
4: sit0: <NOARP> mtu 1480 qdisc noop
    link/sit 0.0.0.0 brd 0.0.0.0
5: bond0: <NO-CARRIER,BROADCAST,MULTICAST,PROMISC,MASTER,UP> mtu 1500 qdisc noqu
eue
    link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::250:56ff:feb1:3367/64 scope link
       valid_lft forever preferred_lft forever
~ root@protector4331#
~ root@protector4331#
~ root@protector4331#
~ root@protector4331# ip route
              dev eth0  proto kernel  scope link  src
             dev eth1  proto kernel  scope link  src
     via              dev eth0
default via               dev eth1
~ root@protector4331#
~ root@protector4331#
~ root@protector4331# _
```

15. The protector should now have a new default gateway, but it should still be able to communicate with the management server via the static route previously entered.

16. Rename the protector:

    a. On the protector, run wizard hostname. Set the external hostname US-XXXXDLP1-NET0.

    b. On the protector, run wizard securecomm. Register with the TRITON management server.

    c. On the TRITON Manager, deploy a policy. It will fail due to connection failure.

    d. Exit the TRION Manager.

    e. RDP to the TRITON server and restart the Websense Data Security Manager service.

    f. Log on to the TRITON manager.

    g. Confirm that the protector object has all the saved settings, including the new name.

    h. Deploy policy should now succeed.

Setup certificates for customer specific configuration

17. Copy the host cert file extracted from the p7b file to `/etc/pki/tls/certs/CustomerHostb64.cer`

18. Copy the `/etc/pki/tls/CustomerChainb64.cer` file from `US-XXXXDLP1-NET0-Cx.COM` to `/etc/pki/tls/`

19. Build the AllCerts file.
    The AllCerts file that goes in `/opt/websense/PolicyEngine/` must be created with the previous files, plus the private key:

    ```
    cp /etc/pki/tls/private/dlp00X.key /opt/websense/
    PolicyEngine/CustomerAllCerts.pem
    cat /etc/pki/tls/certs/CustomerHostb64.cer >> /opt/
    websense/PolicyEngine/CustomerAllCerts.pem
    cat /etc/pki/tls/CustomerChainb64.cer >> /opt/websense/
    PolicyEngine/CustomerAllCerts.pem
    ```

20. The AllCerts file must have all the x509 certs in the following order:
    a. Host
    b. Intermediates
    c. Root CA
    d. Private Key can go anywhere

Copy certificates to appropriate path

21. Copy `CustomerHostb64.cer` to `/etc/pki/tls/certs/`
22. Copy `CustomerChainb64.cer` to `/etc/pki/tls/`
23. Copy `CustomerAllCerts.pem` to `/opt/websense/PolicyEngine/`
24. Edit /`etc/postfix/main.cf` as follows:
    a. `smtpd_tls_security_level` = may
    b. `smtp_tls_security_level` = verify
    c. `smtp_tls_cert_file` = `/etc/pki/tls/certs/CustomerHostb64.cer`
    d. `smtp_tls_CAfile` = `/etc/pki/tls/CustomerChainb64.cer`
    e. `smtpd_tls_cert_file` = `/opt/websense/PolicyEngine/CustomerAllCerts.pem`. ### this will tell smtpd to use the new certs.
25. Add this line in the tls_policy map in `/etc/postfix/tls_policy`:
    a. 127.1.0.x:10025 may
26. Restart postfix with postfix reload.
27. Tail –f /var/log/maillog
28. Send a test email.