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

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

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.

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

11. Add the final default. In the network section, select **eth1** and enter the new default gateway.

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 ]
```
14. Deploy the policy.

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-XXXXDLPL1-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-XXXXDLPL1-NET0-Cx.COM to /etc/pki/tls/
   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.