

Configuring EpiForce with Big-IP LTM Technical Note

Apani® EpiForce® version 2.5 or later allows you to manage clear and secure traffic passing through the F5 Big-IP® Local Traffic Manager (LTM) v9 Series Load Balancers.

Big-IP LTM transparently distributes incoming network traffic between multiple servers to increase capacity and reliability. The LTM operates by replacing a virtual destination IP address used by clients with an actual server IP address. This redirects each incoming packet and reverses the address replacement for any replies.

EpiForce relies on IP addresses to enforce segmentation and security. Deploying EpiForce in an environment with LTMs requires the following configuration adjustments to the EpiForce Agent, Admin Console, Admin Server and Big-IP LTM.

Configuration

Figure 1 shows a sample Logical Network Diagram.

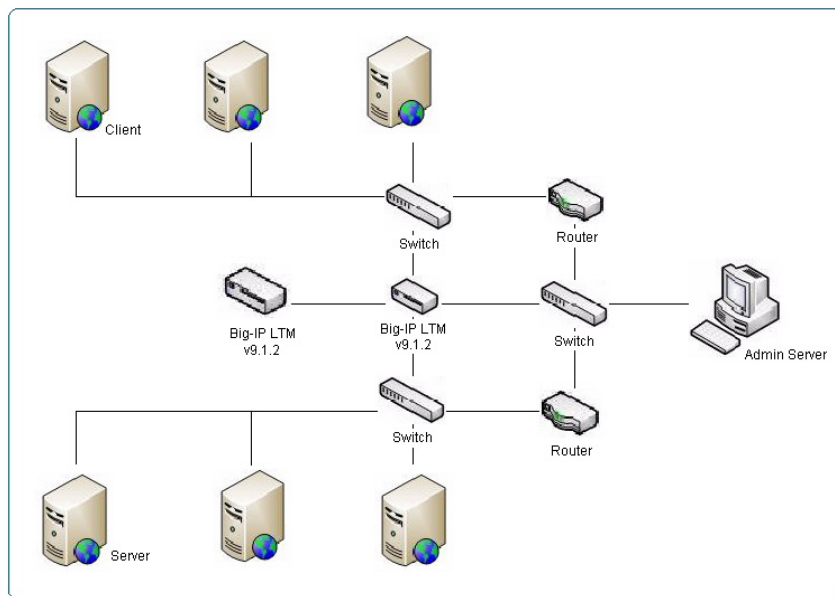


Figure 1 Logical Network Diagram

To configure Big-IP LTM with EpiForce:

1. Install and configure F5 Big-IP LTM using the vendors' documentation.
2. Install and configure the EpiForce Admin Console, Admin Server and Agent using the Apani EpiForce Installation Guide and EpiForce User Guide.

Configuring EpiForce

To configure EpiForce:

1. Access the Admin Console, then select **Zones**. The Zones panel displays.

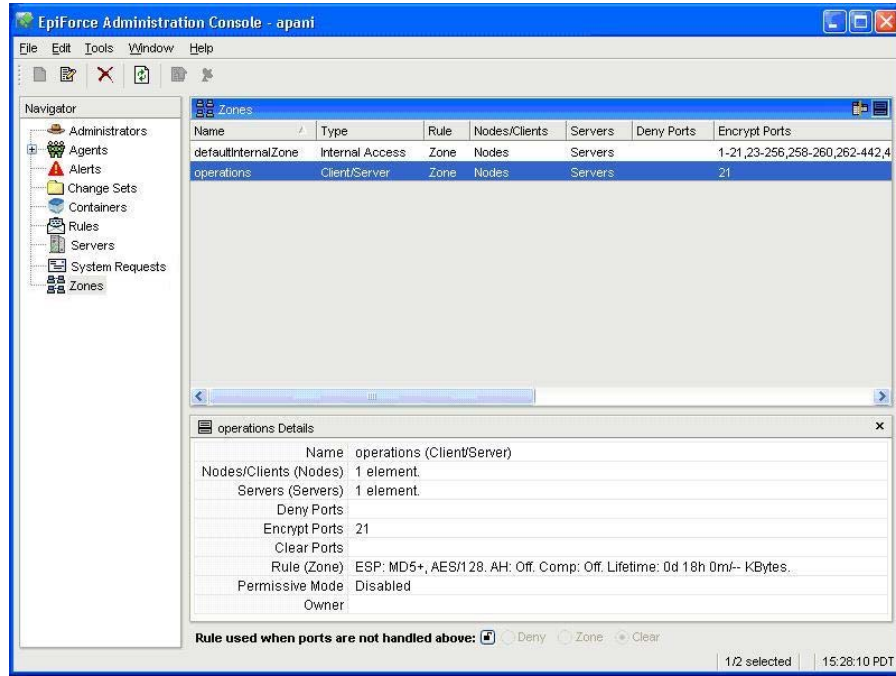


Figure 2 Admin Console Zones

2. Select or create an Internal Access Zone (IAZ).
3. Configure the IAZ as follows:
 - Add all Agents representing Servers in the Server Pool and their Clients.
 - Add the Virtual IP address of the service as a range with a netmask 255.255.255.255.
 - Define Application Ports in the Zone as Clear or Protect (Encrypt), as needed. For example, Encrypted Port – 80, 8080, Clear Port – 9090 and Deny Port – 9191.
4. Select the **Key Lifetimes** tab. The Key Lifetime page displays.

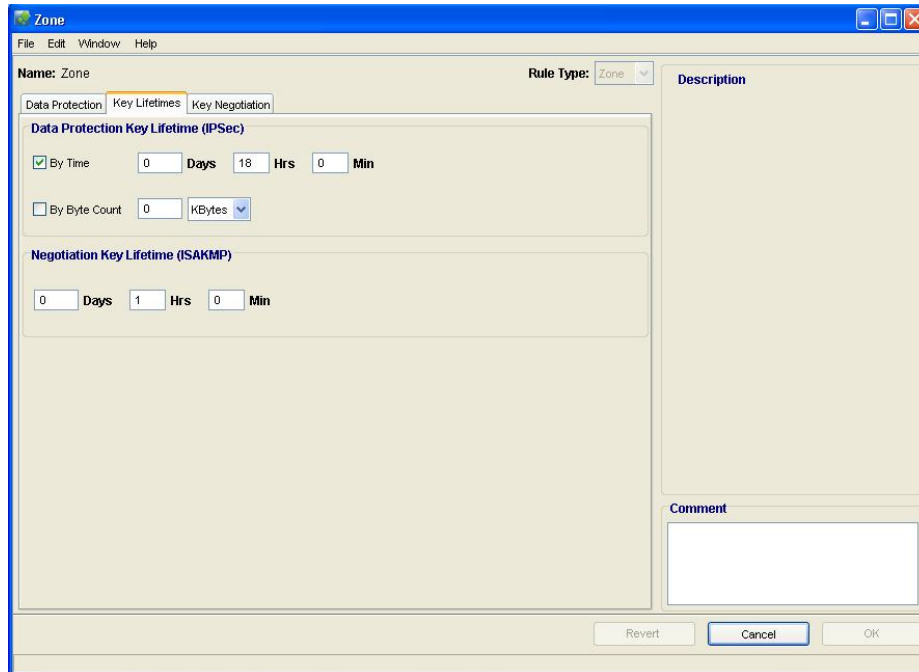


Figure 3 Key Lifetimes

5. In the **Data Protection Key Lifetime (IPSec)** field, set the time to match the Big-IP LTM **Source Address Persistence Timeout** setting.
6. In the **Negotiation Key Lifetime (ISAKMP)** field, verify the time is set to less than the **Data Protection Key Lifetime (IPSec)** field.

Configuring Big-IP LTM

To configure Big-IP LTM:

1. Access the Big-IP LTM.
2. Access the Virtual Servers.

Specify the following parameters:

- Set **Service Port** and **Protocol** to All.
These parameters must include both UDP 500 and ESP protocol 50.
- Specify **Service Type** as Performance (Layer 4).
- Set **Address Translation** to Enabled.
- Set **Port Translation** to Disabled.

3. Access Virtual Server Resources.

Set the Default Persistence Profile to source_addr.

4. Access Virtual Server Profiles Persistence.

Verify the **Persistence Type** is Source Address Infinity.

Set the **Source_addr Timeout** to the identical time specified in the EpiForce **Data Protection Key Lifetime (IPSec)** setting.

5. Access the Virtual Servers Pools Members.

Verify all servers listed in the Server Pools that are being protected have Agents and are listed in the EpiForce IAZ.



1800 East Imperial Highway
Brea, California 92821 USA

Customer Support

Voice: 714.674.1700

Fax: 714.674.1770

Email: support@apani.com

www.apani.com