Knowledge

AI Recommended Content

K14343463: Configuring the BIG-IP system to pass through SSL traffic

Published Date: **Aug 28, 2019** Updated Date: **Apr 18, 2024**

Applies to:

Topic

This article discusses how to configure the BIG-IP system to pass through SSL connections.

Description

In this configuration, the BIG-IP system forwards encrypted SSL traffic to the back-end servers without decryption. This type of configuration is preferable when you do not want the BIG-IP system to do anything with encrypted traffic but simply load balance it to a pool of destination server(s) for processing. The BIG-IP system processes SSL traffic at the TCP layer and does not interact with the contents of the packet. You are not required to configure Client SSL or Server SSL profiles since your virtual server does not decrypt or encrypt the SSL traffic.

You can use the following virtual server types when configuring the BIG-IP system as an SSL pass-through:

- Performance (Layer 4)
- Forwarding (Layer 2)
- Forwarding (IP)
- Standard

Note: *Forwarding (Layer 2) and Forwarding (IP) are used when directly routing to a destination SSL server. This style of virtual server type does not offer load-balancing options.*

Configure the BIG-IP system to pass through SSL connections

For a basic SSL pass through configuration, you must define the following local traffic objects:

- A SSL load-balancing pool with HTTPS monitor
- A Standard SSL virtual server

Note: *When configuring persistence for a SSL pass-through virtual server, you can only use IP-based and/or SSL persistence profiles.*

Configure a SSL load-balancing pool with HTTPS monitor

1. Log into the Configuration utility.
2. Go to **Local Traffic** > **Pools**.
3. Select **Create**.
4. Enter a name for the pool.
5. For **Health Monitors**, move **https** to **Available**.
6. Select a load-balancing method such as **Round Robin**.
7. For **New Members**, complete the following:
   - **Node Name**: Enter the name for the member you are adding to the pool.
   - **Address**: Enter the IP address for the member you are adding to the pool.
   - **Service Port**: Select **HTTPS** or enter the port number associated with your SSL application.
8. Select **Add**.
9. Repeat step 7 for each pool member you want to add to the pool.
10. Select **Finished**.

Configure a SSL pass-through virtual server

1. Log into the Configuration utility.
2. Go to **Local Traffic** > **Virtual Servers**.
3. Select **Create**.
4. Enter a name for the virtual server.
5. For **Type** select **Standard**, or one of the other virtual server types listed above.
6. For **Destination Address/Mask**, enter the IP address of the virtual server.
7. For **Service Port**, select **HTTPS** or enter the port number associated with your SSL application.
8. Under **Resources**, select the pool object you created in the previous procedure from **Default Pool**.
9. For **Default Persistence**, select a IP-based or SSL persistence if desired.
10. Select **Finished.**

For example, after you have completed the above procedures your SSL pass-through configuration may appear similar to the following configuration:

```
ltm virtual sslpassthrough_vs_standard {
    destination 172.16.1.101:https
    ip-protocol tcp
    mask 255.255.255.255
    persist {
        hash {
            default yes
        }
    }
    pool sslpassthrough_pool
    profiles {
        tcp { }
    }
    source 0.0.0.0/0
    source-address-translation {
        type automap
    }
    translate-address enabled
    translate-port enabled
}
ltm pool sslpassthrough_pool {
    members {
        10.0.0.12:https {
            address 10.0.0.12
            session monitor-enabled
            state up
        }
    }
    monitor https
}
```

Related Content

- K12015: Configuration requirements for SSL virtual servers, profiles, pools, and monitors
- K65271370: Most Common SSL Methods for LTM: SSL Offload, SSL Pass-Through and Full SSL Proxy
- K55185917: Overview of BIG-IP virtual server types (12.x - 17.x)

AI Recommended Content

- **Security Advisory** - K000141008: RADIUS authentication vulnerability CVE-2024-3596
- **Security Advisory** - K000148609: Intel vulnerabilities CVE-2024-28885 and CVE-2024-31074
- **Security Advisory** - K000148582: Intel Server Board vulnerabilities CVE-2024-31154, CVE-2024-31158, CVE-2024-39609, CVE-2024-40885, and CVE-2024-41167
- **Known Issue** - K000148566: F5 rSeries systems may silently reboot after upgrading to F5OS-A 1.8.0

Return to Top