Support Solution

K65271370: Most Common SSL Methods for LTM: SSL Offload, SSL Pass-Through and Full SSL Proxy

Published Date: **May 7, 2020** Updated Date: **Feb 21, 2023**

AI Recommended Content

Applies to:

Description

BIG-IP is built to handle SSL traffic in load balancing scenario and meet most of the security requirements effectively. The 3 common SSL configurations that can be set up on LTM device are:

- SSL Offloading
- SSL Passthrough
- Full SSL Proxy / SSL Re-Encryption / SSL Bridging / SSL Terminations

Environment

- Configuration objects and settings: Virtual Server, Client SSL and Server SSL profiles
- BIG-IP, LTM

Cause

None

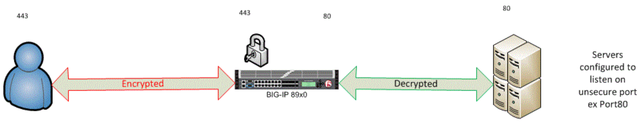
Recommended Actions

None

Additional Information

Typical load balancing infrastructure setup would be Client--->BIG-IP VIP ---->Servers hosting applications i.e. client traffic will be directed to a load balancer like BIG-IP which in return (using complex algorithm) send the traffic to an appropriate server.

SSL Offloading - In this method the client traffic to BIG-IP is sent as encrypted. Instead of the server decrypting and re-encrypting the traffic BIG-IP would handle that part. So the client traffic is decrypted by the BIG-IP and the decrypted traffic is sent to the server. The return communication from the server to client is encrypted by the BIG-IP and sent back to the client. Thus sparing the server additional load of encryption and decryption. All the server resources can now be fully utilized to serve the application content or any other purpose they are built to do.



Note:

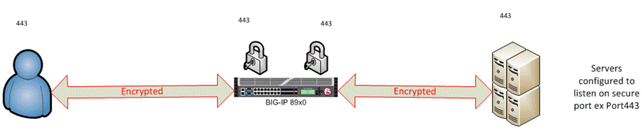
1. The communication between the server BIG-IP and server is in clear txt.
2. Servers are setup to listen on unsecure ports ex Port 80.
3. Since the BIG-IP decrypts the HTTP traffic it has now the ability to read the content (header, txt, cookies etc.) and all the persistence options can be applied. (Source address, Destination address, Cookies, SSL, SIP, Universal, MSRDP)

SSL Pass through - As the name suggests the BIG-IP will just pass the traffic from client to servers absolving itself from any SSL related workload. Instead of forwarding SSL handshakes and connections to the servers directly it will just pass the client traffic to the servers. Usually this setup is used if the applications being served are anti SSL proxy or cannot consume decrypted traffic.

Note -

1. Since it's just pass through LTM cannot read the headers which introduces limitations on persistence. Only non SSL information in the packet can be used to maintain persistence like source ip address, destination ip address.

SSL Full Proxy - This method goes by a few names such as SSL Re-Encryption, SSL Bridging and SSL Terminations. In this method the BIG-IP will re-encrypt the traffic before sending it to the servers. Client sends encrypted traffic to BIG-IP , BIG-IP then decrypts it and before send it to the servers or pool members re-encrypts it again. This method is generally used to satisfy the requirement of traffic to be encrypted between the LTM and Servers as well. This requirement might be put in place for additional security or prevent intrusion from within the network. When this method is used the servers will also have to decrypt and encrypt the traffic.



Note –

1. The communication between the server LTM and server is secure.
2. Servers are setup to listen on secure ports ex Port 443.
3. Since the LTM initially decrypts the HTTP traffic it still has the ability to read the content (header, txt, cookies etc.) and all the persistence options can be applied same as SSL Offloading. (Source address, Destination address, Cookies, SSL, SIP, Universal, MSRDP)

Related Content

DevCentral: SSL Passthrough, SSL Offloading and SSL Bridging

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

Support Solution articles are written by F5 Support engineers who work directly with customers; these articles give you immediate access to mitigation, workaround, or troubleshooting suggestions.

Return to Top