INTEGRATION GUIDE

BIG-IP SSL Orchestrator and NETSCOUT

SSL/TLS Visibility with Service Chaining

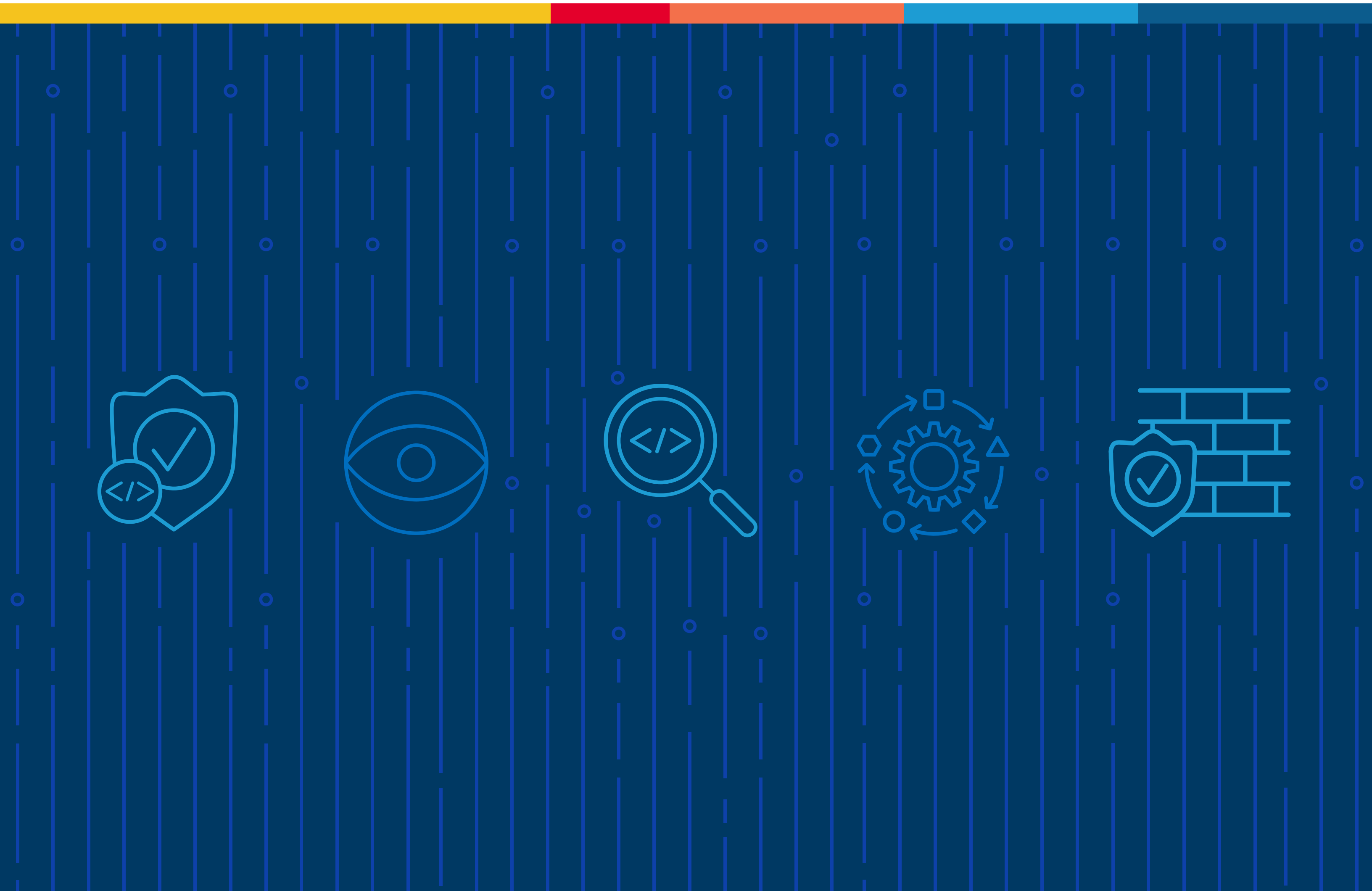


Table of Contents

The Secure Sockets Layer (SSL) protocol and its successor, Transport Layer Security (TLS), are being widely adopted by organizations to secure IP communications. While SSL/TLS provides data privacy and secure communications, it also presents challenges for inspection devices within the security stack. In short, encrypted communications can't be seen as clear text and are passed through without inspection, resulting in security blind spots. This creates serious risks for businesses: What if attackers are hiding malware inside the encrypted traffic?

However, the process of performing decryption of SSL/TLS traffic on security inspection devices, even with native decryption support, can significantly degrade the performance of those devices. This is particularly true given the demands of stronger 2048-bit certificates.

F5® BIG-IP® SSL Orchestrator® is designed and purpose-built to enhance SSL/TLS infrastructure, provide security solutions with visibility into SSL/TLS encrypted traffic, and optimize and maximize your existing security investments. BIG-IP SSL Orchestrator provides SSL/TLS encryption and decryption of live traffic, as well as the ability to send traffic to tools in a service/tool chain.

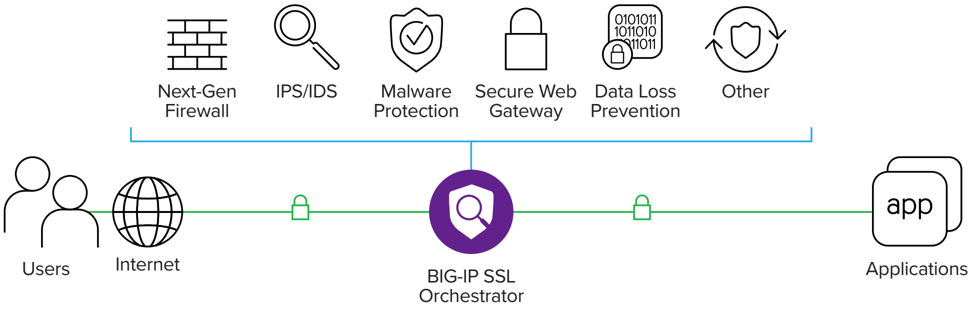


Figure 1: BIG-IP SSL Orchestrator maximizes efficiency and performance for a wide range of inspection devices while maintaining optimal security.

BIG-IP SSL Orchestrator can be deployed as a standalone appliance, a module in an F5® BIG-IP® system, or as a module in an F5® BIG-IP® Virtual Edition (VE) for cloud services such as AWS and Azure. In each deployment model the decrypted SSL/TLS traffic can be passively copied directly to NETSCOUT vSTREAM and InfiniStreamNG (ISNG) instrumentation for inspection to provide smart visibility for service and security assurance. This packet access solution eliminates the blind spots introduced by SSL/TLS and closes any opportunity for adversaries.

The integration between F5 and NETSCOUT vSTREAM/ISNG provides network operations, engineering, network security engineers, and analysts with the ability to collect, investigate, and research unencrypted and encrypted network traffic at the packet level. When used in combination with NETSCOUT nGeniusONE and Omnis security and analytics products, users can perform proactive service assurance, and service triage, analytics, and notifications can be enabled to alert network security engineers of threats to the infrastructure.

In physical environments, BIG-IP SSL Orchestrator can be added as a blade-based function. In a virtual/cloud environment, the BIG-IP SSL Orchestrator module can be enabled as a standalone or an add-on software license to BIG-IP VE. In this model, BIG-IP can provide the ISNG or vSTREAM with copies of client and/or server-side encrypted traffic, through use of clone pools, while BIG-IP SSL Orchestrator provides decrypted copies of traffic.

Figure 2: BIG-IP SSL Orchestrator deployment with BIG-IP (physical or virtual)

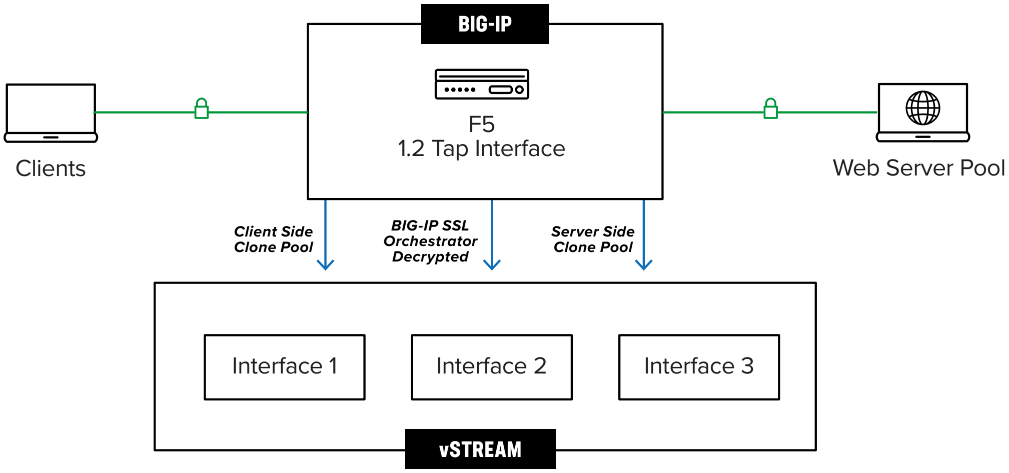
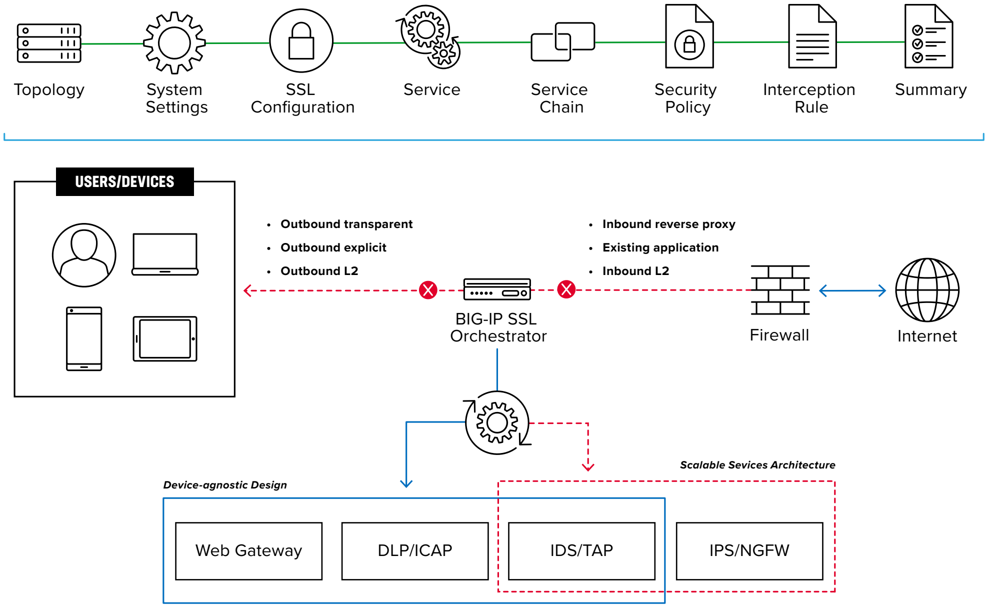


Figure 3: BIG-IP SSL Orchestrator standalone deployment (physical or virtual), where the ISNG is a TAP/ tool in the service chain to receive decrypted copies of traffic that flow through the F5 system



The F5 and NETSCOUT Integrated Solution

This section provides instructions for configuring BIG-IP SSL Orchestrator with NETSCOUT. This document is not intended to suggest optimum installations or configurations. It is assumed that the reader has both working knowledge of all products involved and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components. All BIG-IP components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Note: The configuration shown in this integration guide is for example and testing purposes only. It is not intended to be the optimal setup for the device. It is recommended that customers make sure that the BIG-IP is properly configured and secured before deploying to a production environment. For more information, please refer to BIG-IP documentation.

PREREQUISITES

Careful, advance consideration of deployment can ensure an efficient and effective implementation of the F5 integrated solution with NETSCOUT. This section helps you with information on license components, best practices, and initial steps. Once these steps are complete, you can proceed to the configuration of BIG-IP SSL Orchestrator.

LICENSE COMPONENTS

The BIG-IP SSL Orchestrator product line—the i2800, r2800, i4800, r4800, i5800, r5800, i10800, r10800, r10900, i11800, i15800, and Virtual Edition High Performance (HP)—supports this joint solution. The F5® VIPRION® platform and the F5® VELOS® platform are also supported. BIG-IP SSL Orchestrator devices ship with an installed base module that provides both SSL/TLS interception and service chaining capabilities. Please contact your local F5 representative to further understand the licensing and deployment options.

Unless otherwise noted, references to BIG-IP SSL Orchestrator and the BIG-IP system in this document (and some user interfaces) apply equally regardless of the F5 hardware or VE used. The solution architecture and configuration are identical.

Optionally, customers can add the functionality of:

- An **F5 URL filtering (URLF) subscription** to access the URL category database.
- An **F5® IP Intelligence Services subscription** for IP reputation service.
- A network **hardware security module (HSM)** to safeguard and manage digital keys for strong authentication.

- **F5® Secure Web Gateway Services** to filter and control outbound web traffic using a URL database.
- **F5® BIG-IP® Access Policy Manager® (APM)** to authenticate and manage user access.
- **F5® BIG-IP® Advanced Firewall Manager™ (AFM)** to protect against denial-of-service.
- **F5® BIG-IP® Advanced WAF®** to protect against common vulnerabilities (CVEs) and web exploits, targeted attacks, and advanced threats.
- An **F5® BIG-IP® Local Traffic Manager™ (LTM)** add-on software license mode. This solution's supported on all F5® BIG-IP® iSeries® and older F5 hardware platforms and has no specific restrictions on additional F5 software modules (including the above software services). This option's suited for environments that need to deploy BIG-IP SSL Orchestrator on an existing BIG-IP device or have other functions that must run on the same device.

Best Practices for the Joint Solution

Several best practices can help optimize the performance and reliability, as well as the security, of the joint solution.

ARCHITECTURE BEST PRACTICES

To ensure a streamlined architecture that optimizes performance, reliability, and security, F5 recommendations include:

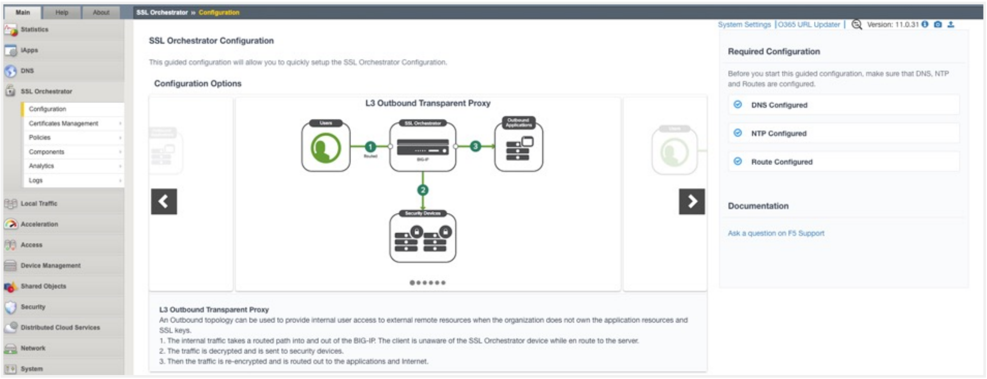
- Deploy the F5 systems in a device sync/failover device group (S/FDG), which includes the active standby pair, with a floating IP address for high availability (HA).
- Further interface redundancy can be achieved using the Link Aggregation Control Protocol (LACP). LACP manages the connected physical interfaces as a single virtual interface (aggregate group) and detects any interface failures within the group.

Unlike with some competing solutions, the F5 systems do not need physical connections to the NETSCOUT. All the F5 system requires is L3 reachability to send the copied decrypted and unencrypted traffic. In slow networks, however, we recommend deploying the NETSCOUT not more than one hop away. As a generic guideline, when inspection devices are not directly connected to the F5 system, we highly recommend use of network and VLAN controls to restrict access to the unencrypted data only to the inspection devices.

Initial Setup

Please follow this link and perform the initial configuration of the BIG-IP system, including enabling the licenses for both BIG-IP LTM and BIG-IP SSL Orchestrator.

Once the initial configuration is completed and the licenses are applied, the BIG-IP SSL Orchestrator configuration page appears with a menu displayed on the left side of the page.



SSL Orchestrator Configuration

This guided configuration will allow you to quickly setup the SSL Orchestrator Configuration.

Configuration Options

L3 Outbound Transparent Proxy

An Outbound topology can be used to provide internal user access to external remote resources when the organization does not own the application resources and SSL keys.

1. The internal traffic takes a routed path into and out of the BIG-IP. The client is unaware of the SSL Orchestrator device while en route to the server.
2. The traffic is decrypted and is sent to security devices.
3. Then the traffic is re-encrypted and is routed out to the applications and Internet.

Required Configuration

Before you start this guided configuration, make sure that DNS, NTP and Routes are configured.

✓ DNS Configured

✓ NTP Configured

✓ Route Configured

Documentation

Figure 4: BIG-IP SSL Orchestrator initial configuration page

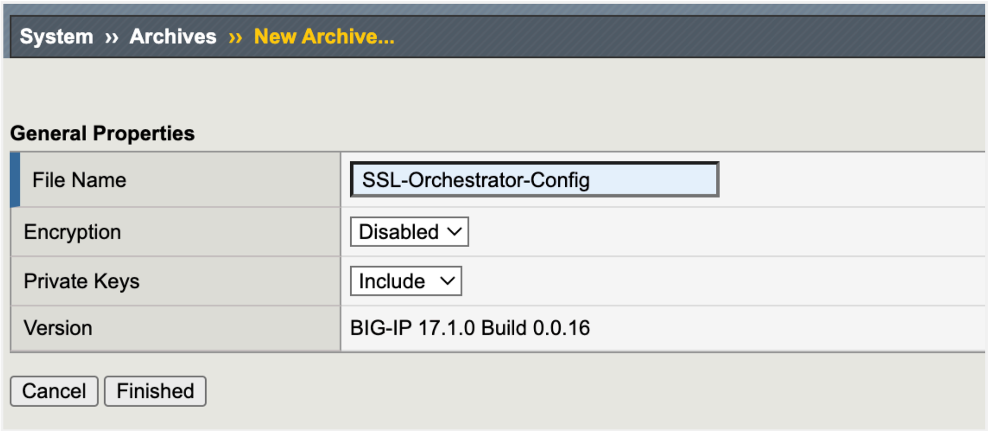
You are now ready to proceed to the second part of configuration, where you'll finalize your system for BIG-IP SSL Orchestrator.

BACK UP YOUR F5 SYSTEM CONFIGURATION

Before beginning the detailed BIG-IP SSL Orchestrator configuration, we strongly recommend you back up the F5 system configuration using the following steps. This enables you to restore the previous configuration in case any issues arise.

1. From the main tab of the F5 management interface, click **System** > **Archives**.
2. To initiate the process of creating a new UCS archive (backup), click **Create**.
3. Enter a unique **File Name** for the backup file.
4. Optional:

- If you want to encrypt the UCS archive file, from the **Encryption** menu, select **Enabled** and enter a passphrase. You must supply the passphrase to restore the encrypted UCS archive file.
- If you want to exclude SSL private keys from the UCS archive, from the **Private Keys** menu, select **Exclude**.



System ›› Archives ›› New Archive...

General Properties

File Name	SSL-Orchestrator-Config
Encryption	Disabled
Private Keys	Include
Version	BIG-IP 17.1.0 Build 0.0.16

Figure 5: System Archives page for configuration backup

5. Click **Finished** to create the UCS archive file.
6. When the backup process is done, examine the status page for any reported errors before proceeding to the next step.
7. Click **OK** to return to the **Archive List** page.
8. Copy the .ucs file to another system.

To restore the configuration from a UCS archive, navigate to **System** > **Archives**. Select the name of the UCS file you want to restore and click **Restore**. For details and other considerations for backing up and restoring the BIG-IP system configuration, reference K13132: Backing up and restoring BIG-IP configuration files with a UCS archive on MyF5.

BIG-IP SSL Orchestrator Configuration

This section covers step by step configuration of BIG-IP SSL Orchestrator to provide a packet-by-packet copy of both the unencrypted HTTP and decrypted HTTPS traffic to NETSCOUT vSTREAM configured for TAP mode.

The BIG-IP SSL Orchestrator guided configuration presents a completely new and streamlined user experience. This workflow-based architecture provides intuitive, reentrant configuration steps tailored to a selected topology.

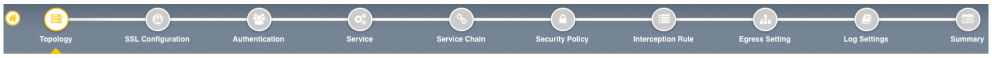


Figure 6: BIG-IP SSL Orchestrator guided configuration workflow

CONFIGURATION EXAMPLE WHERE THE SERVICE EXISTS IN BIG-IP LTM

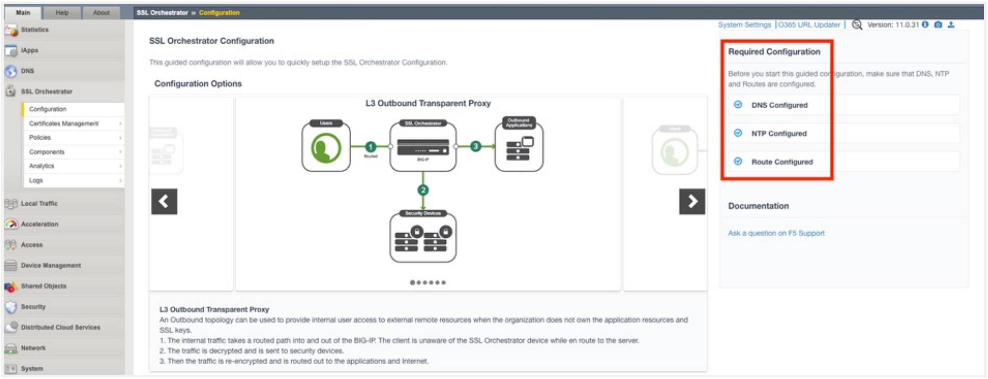
In this example, we will use the Existing Application option for a new BIG-IP SSL Orchestrator topology. This assumes you have already created a Pool and Virtual Server under Local Traffic.

To get started follow these steps:

1. Navigate to the BIG-IP SSL Orchestrator Configuration page and review the list of prerequisites on the right-hand side. Configure each prerequisite to display a blue checkmark.

Note: NTP is required for HA deployments.

Figure 7: BIG-IP SSL Orchestrator Required Configuration



SSL Orchestrator Configuration

This guided configuration will allow you to quickly setup the SSL Orchestrator Configuration.

Configuration Options

L3 Outbound Transparent Proxy

Required Configuration

Before you start this guided configuration, make sure that DNS, NTP and Routes are configured.

- DNS Configured
- NTP Configured
- Route Configured

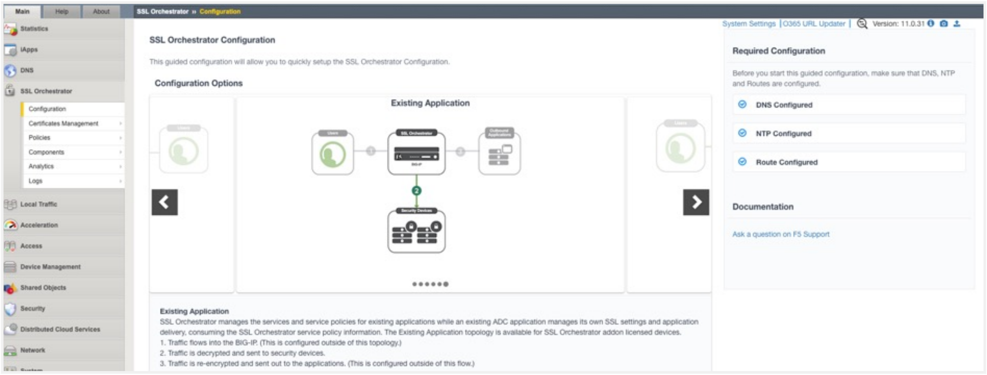
Documentation

Ask a question on F5 Support

L3 Outbound Transparent Proxy
An Outbound topology can be used to provide internal user access to external remote resources when the organization does not own the application resources and SSL keys.
1. The internal traffic takes a routed path into and out of the BIG-IP. The client is unaware of the SSL Orchestrator device while en route to the server.
2. The traffic is decrypted and is sent to security devices.
3. Then the traffic is re-encrypted and is routed out to the applications and Internet.

2. Click on the large arrows to advance through the available topologies. We will be using the Existing Application topology for this example. Select the **Next** button at the bottom of the page.

Figure 8: Review available topologies



SSL Orchestrator Configuration

This guided configuration will allow you to quickly setup the SSL Orchestrator Configuration.

Configuration Options

Existing Application

Required Configuration

Before you start this guided configuration, make sure that DNS, NTP and Routes are configured.

- DNS Configured
- NTP Configured
- Route Configured

Documentation

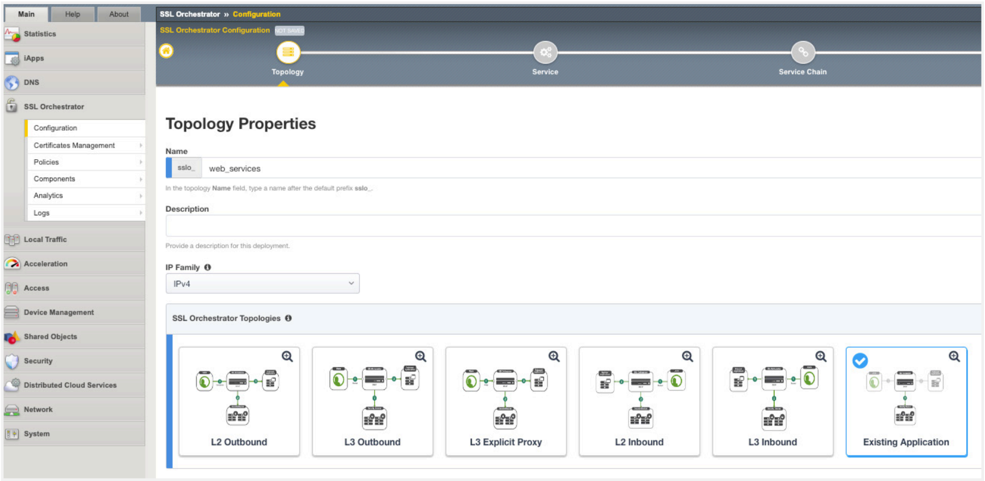
Ask a question on F5 Support

Existing Application
SSL Orchestrator manages the services and service policies for existing applications while an existing ADC application manages its own SSL settings and application delivery, consuming the SSL Orchestrator service policy information. The Existing Application topology is available for SSL Orchestrator addon licensed devices.
1. Traffic flows into the BIG-IP. (This is configured outside of this topology.)
2. Traffic is decrypted and sent to security devices.
3. Traffic is re-encrypted and sent out to the applications. (This is configured outside of this flow.)

Topology properties

1. On the **Topology Properties** page, name your topology and select **Existing Application**.
2. Click on the **Save & Next** button.

Figure 9: Configure Topology Properties



Topology Properties

Name: sslo_ web_services

In the topology **Name** field, type a name after the default prefix **sslo_**.

Description

Provide a description for this deployment.

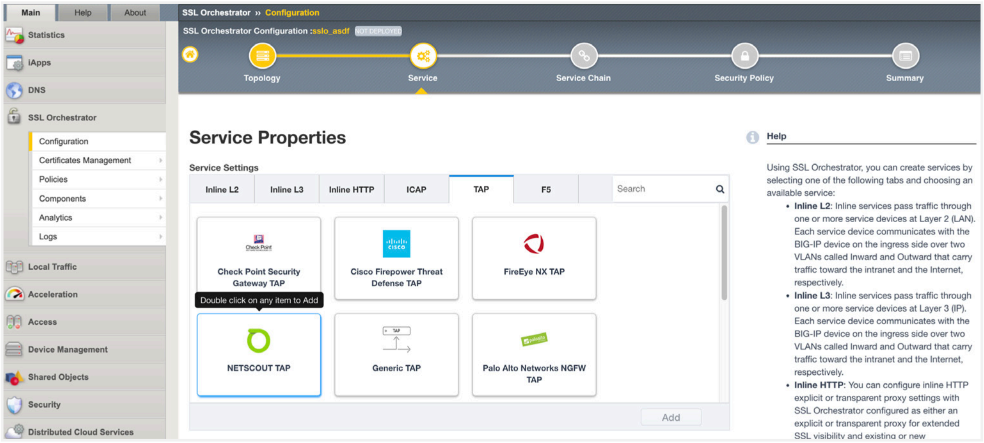
IP Family: IPv4

SSL Orchestrator Topologies

Service properties

1. In the **Service Properties** page, click on **Add Service**. Select **TAP** then **NETSCOUT TAP** and click on the **Add** button.

Figure 10: Service Properties page



Service Properties

Double click on any item to Add

Help

Using SSL Orchestrator, you can create services by selecting one of the following tabs and choosing an available service:

- **Inline L2**: Inline services pass traffic through one or more service devices at Layer 2 (LAN). Each service device communicates with the BIG-IP device on the ingress side over two VLANs called Inward and Outward that carry traffic toward the intranet and the Internet, respectively.
- **Inline L3**: Inline services pass traffic through one or more service devices at Layer 3 (IP). Each service device communicates with the BIG-IP device on the ingress side over two VLANs called Inward and Outward that carry traffic toward the intranet and the Internet, respectively.
- **Inline HTTP**: You can configure inline HTTP explicit or transparent proxy settings with SSL Orchestrator configured as either an explicit or transparent proxy for extended SSL visibility and existing or new

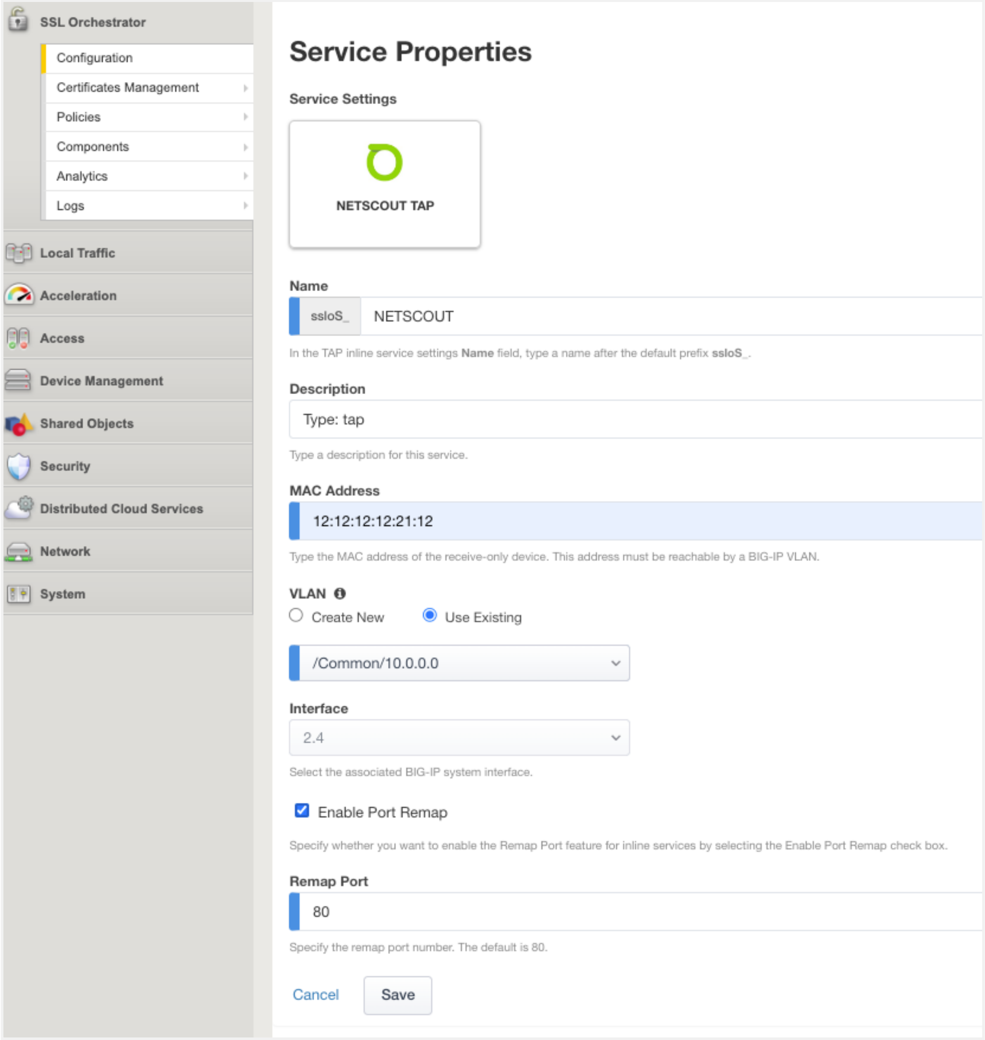
2. In the **Service Properties Service Settings** page, enter each property pertaining to the TAP service. Name your service and enter the MAC address of the ISNG/vSTREAM monitor port.

Note: For virtual deployments, the vSTREAM monitor port and the BIG-IP internal port need to be in the same subnet (broadcast domain).

3. Under **VLAN**, select **Use Existing** and in the dropdown, select the Common/Internal VLAN.

4. Under **Interface**, the internal interface that matches that VLAN will be selected for you.

5. Check the **Enable Port Remap** checkbox and enter port 80. This will send the decrypted traffic to the Monitor port as HTTP.
6. Click on the **Save** button.
7. In the **Service List** page, click **Save & Next**.



Service Properties

Service Settings

NETSCOUT TAP

Name

ssloS_ NETSCOUT

In the TAP inline service settings **Name** field, type a name after the default prefix **ssloS_**.

Description

Type: tap

Type a description for this service.

MAC Address

12:12:12:12:21:12

Type the MAC address of the receive-only device. This address must be reachable by a BIG-IP VLAN.

VLAN

○ Create New ● Use Existing

/Common/10.0.0.0

Interface

2.4

Select the associated BIG-IP system interface.

☑ Enable Port Remap

Specify whether you want to enable the Remap Port feature for inline services by selecting the Enable Port Remap check box.

Remap Port

80

Specify the remap port number. The default is 80.

Figure 11: Service Properties service settings

Services chain

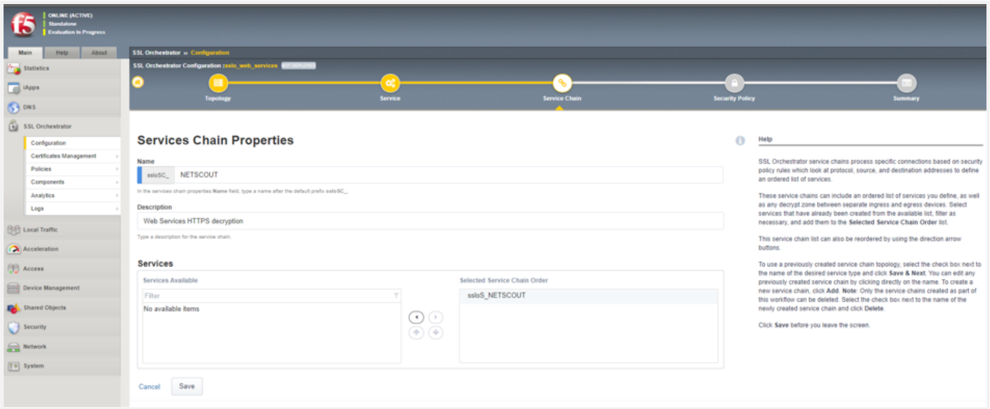
1. In the **Services Chain List** page, click on the Add button.
2. Name your service chain and under **Services**, select the new service you just created. Click on the **right arrow** to add it to the **Selected Service Chain Order**.

Even though we are not creating a chain of devices, BIG-IP SSL Orchestrator needs to have at least one service specified in the service chain.

3. Click on the **Save** button.

4. Click **Save & Next**.

Figure 12: Services Chain Properties settings



SSL Orchestrator Configuration :sslo_web_services

Services Chain Properties

Name: ssloSC_ NETSCOUT

In the services chain properties **Name** field, type a name after the default prefix ssloSC_.

Description: Web Services HTTPS decryption

Type a description for the service chain.

Services

Services Available: Filter — No available items

Selected Service Chain Order: ssloS_NETSCOUT

Help

SSL Orchestrator service chains process specific connections based on security policy rules which look at protocol, source, and destination addresses to define an ordered list of services.

These service chains can include an ordered list of services you define, as well as any decrypt zone between separate ingress and egress devices. Select services that have already been created from the available list, filter as necessary, and add them to the **Selected Service Chain Order** list.

This service chain list can also be reordered by using the direction arrow buttons.

To use a previously created service chain topology, select the check box next to the name of the desired service type and click **Save & Next**. You can edit any previously created service chain by clicking directly on the name. To create a new service chain, click **Add**. **Note**: Only the service chains created as part of this workflow can be deleted. Select the check box next to the name of the newly created service chain and click **Delete**.

Click **Save** before you leave the screen.

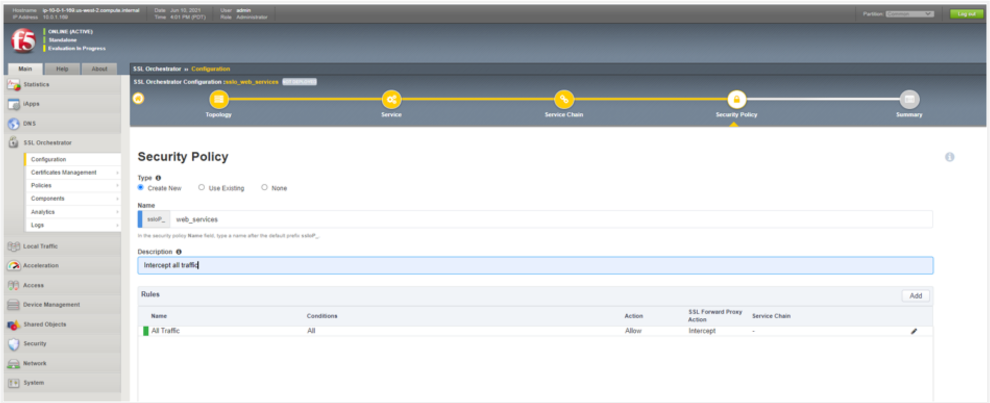
Security policy

1. In the **Security Policy** page, name the Security Policy and under **Rules**, the default is to intercept All Traffic. Edit the default All Traffic rule by clicking on the pencil and selecting the Service Chain.

2. Click **Save & Next**.

3. In the Summary screen, click **Deploy**.

Figure 13: Security Policy settings



Hostname ip-10-0-1-169.us-west-2.compute.internal Date Jun 10, 2021 User admin
IP Address 10.0.1.169 Time 4:01 PM (PDT) Role Administrator

SSL Orchestrator Configuration :sslo_web_services

Security Policy

Type: ● Create New ○ Use Existing ○ None

Name: ssloP_ web_services

In the security policy **Name** field, type a name after the default prefix ssloP_.

Description: Intercept all traffic

Rules

Name	Conditions	Action	SSL Forward Proxy Action	Service Chain
All Traffic	All	Allow	Intercept	-

4. On the **Local Traffic** menu, select **Virtual Servers**.

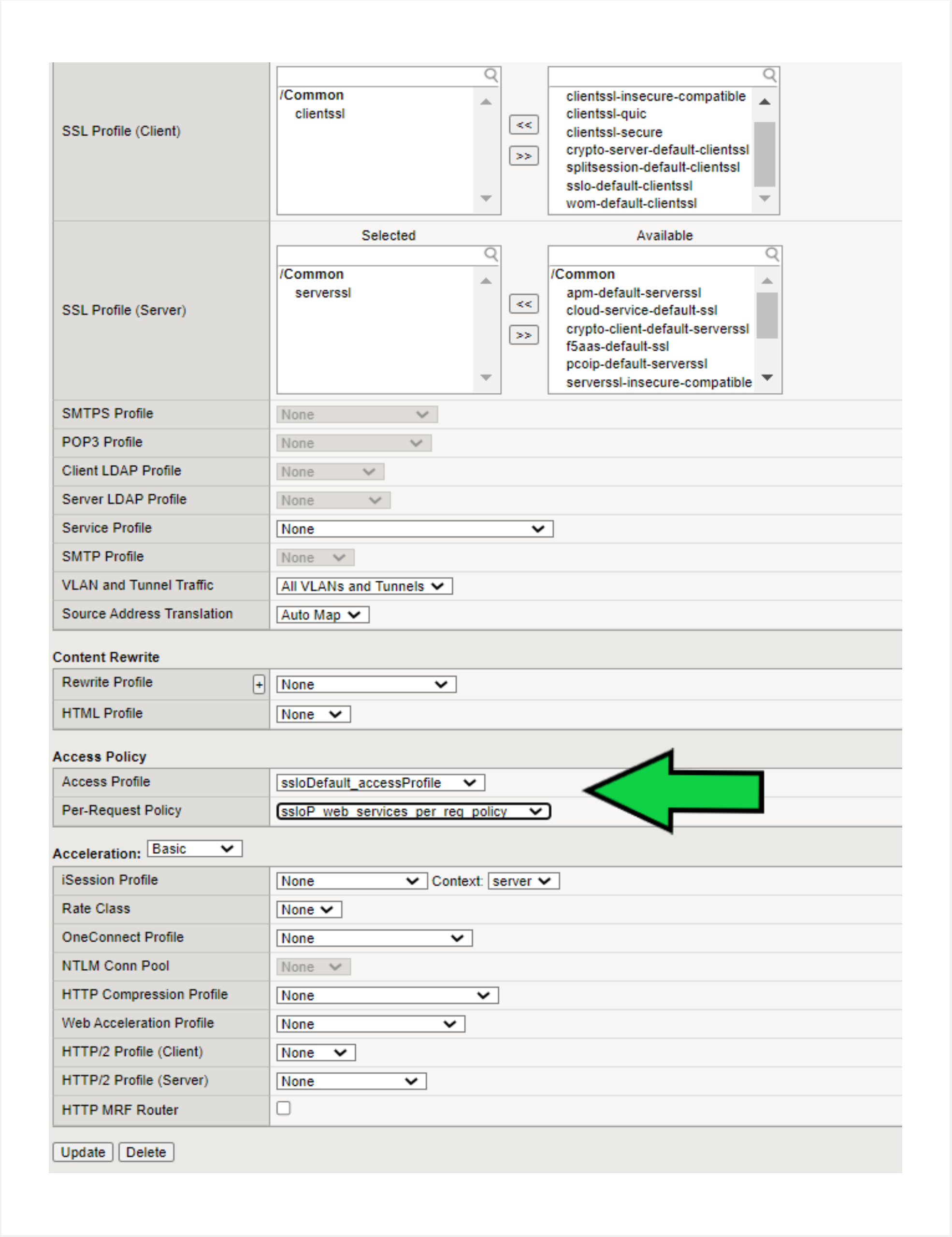
5. Click **Virtual Servers List** and click on the Virtual Server that you want BIG-IP SSL Orchestrator to decrypt.

6. On the **Properties** tab, scroll down to **Access Policy | Access Profile** and select the **ssloDefault_accessProfile**.

7. **For Access Policy | Per-Request Policy**, select the security policy that has the same name as the new BIG-IP SSL Orchestrator configuration that you just deployed.

8. Click on the **Update** button at the bottom.

Figure 14: Modify Virtual Server Access Policy settings



	Selected		Available
SSL Profile (Client)	/Common clientssl	<< >>	clientssl-insecure-compatible clientssl-quic clientssl-secure crypto-server-default-clientssl splitsession-default-clientssl sslo-default-clientssl wom-default-clientssl
SSL Profile (Server)	/Common serverssl	<< >>	/Common apm-default-serverssl cloud-service-default-ssl crypto-client-default-serverssl f5aas-default-ssl pcoip-default-serverssl serverssl-insecure-compatible

SMTPS Profile	None
POP3 Profile	None
Client LDAP Profile	None
Server LDAP Profile	None
Service Profile	None
SMTP Profile	None
VLAN and Tunnel Traffic	All VLANs and Tunnels
Source Address Translation	Auto Map

Content Rewrite

Rewrite Profile +	None
HTML Profile	None

Access Policy

Access Profile	ssloDefault_accessProfile
Per-Request Policy	ssloP_web_services_per_req_policy

Acceleration: Basic

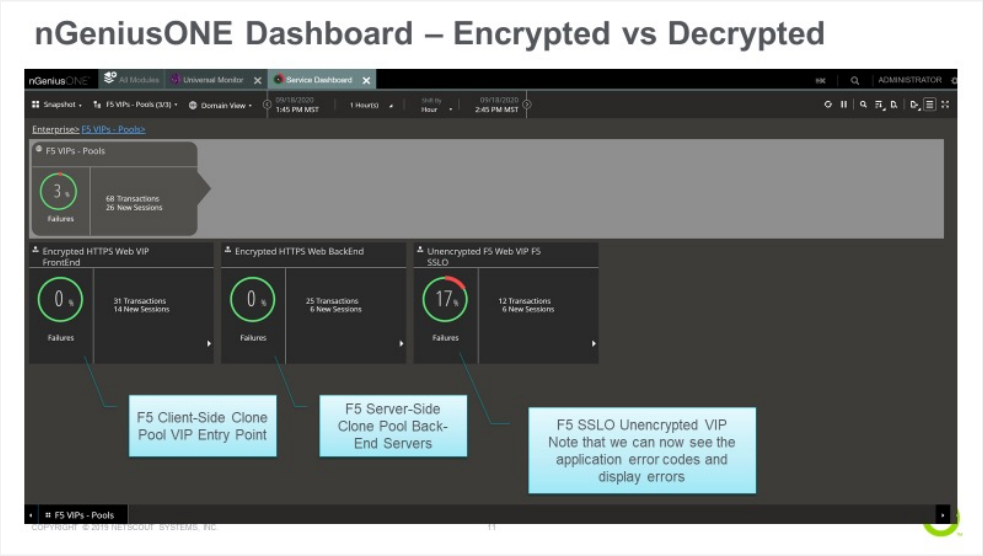
iSession Profile	None Context: server
Rate Class	None
OneConnect Profile	None
NTLM Conn Pool	None
HTTP Compression Profile	None
Web Acceleration Profile	None
HTTP/2 Profile (Client)	None
HTTP/2 Profile (Server)	None
HTTP MRF Router	□

Testing the Solution

Test the deployed solution using the following options.

1. To verify receipt of the BIG-IP SSL Orchestrator decrypted SSL packets, log onto NETSCOUT's nGeniusONE.
2. Using nGeniusONE, select the BIG-IP interfaces in the Dashboard. High level visibility in the Dashboard requires that Application Services are created for the load balanced apps. The data can be obtained without any Application Services configured in nGeniusONE by clicking on the Global Search icon (magnifying glass in the upper right corner) and searching for the load balanced application (i.e., HTTPS, HTTP, MySQL, etc.). Either method will provide a drill down into the appropriate Service Monitor to view the traffic volume, application performance, and network performance metrics.

Figure 15: nGeniusONE Dashboard



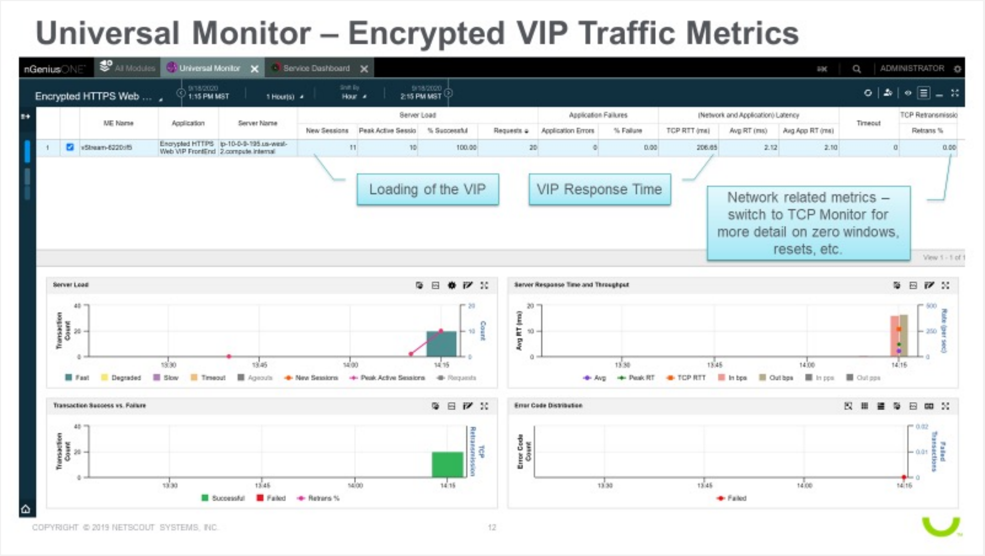
nGeniusONE Dashboard – Encrypted vs Decrypted

F5 Client-Side Clone Pool VIP Entry Point

F5 Server-Side Clone Pool Back-End Servers

F5 SSLO Unencrypted VIP Note that we can now see the application error codes and display errors

3. From nGeniusONE, drill down into the Universal Service Monitor content collected from BIG-IP SSL Orchestrator to view key performance indicators (KPIs) developed from packet traffic captured by NETSCOUT vSTREAM.



Universal Monitor – Encrypted VIP Traffic Metrics

nGeniusONE | All Modules | Universal Monitor | Service Dashboard | ADMINISTRATOR

Encrypted HTTPS Web ... | 9/18/2020 1:15 PM MST | 1 Hour(s) | Hour | 9/18/2020 2:15 PM MST

		ME Name	Application	Server Name	Server Load				Application Failures		(Network and Application) Latency			Timeout	TCP Retransmissio
					New Sessions	Peak Active Sessio	% Successful	Requests	Application Errors	% Failure	TCP RTT (ms)	Avg RT (ms)	Avg App RT (ms)		Retrans %
1	☑	vStream-6220::if5	Encrypted HTTPS Web VIP FrontEnd	ip-10-0-0-195.us-west-2.compute.internal	11	10	100.00	20	0	0.00	206.65	2.12	2.10	0	0.00

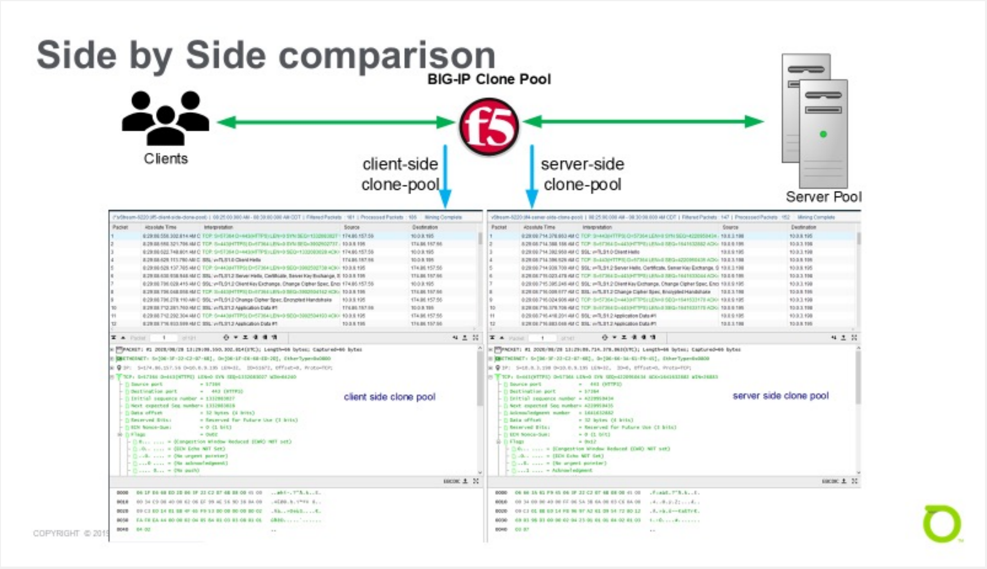
Loading of the VIP

VIP Response Time

Network related metrics – switch to TCP Monitor for more detail on zero windows, resets, etc.

Figure 16: nGeniusONE app performance analytics

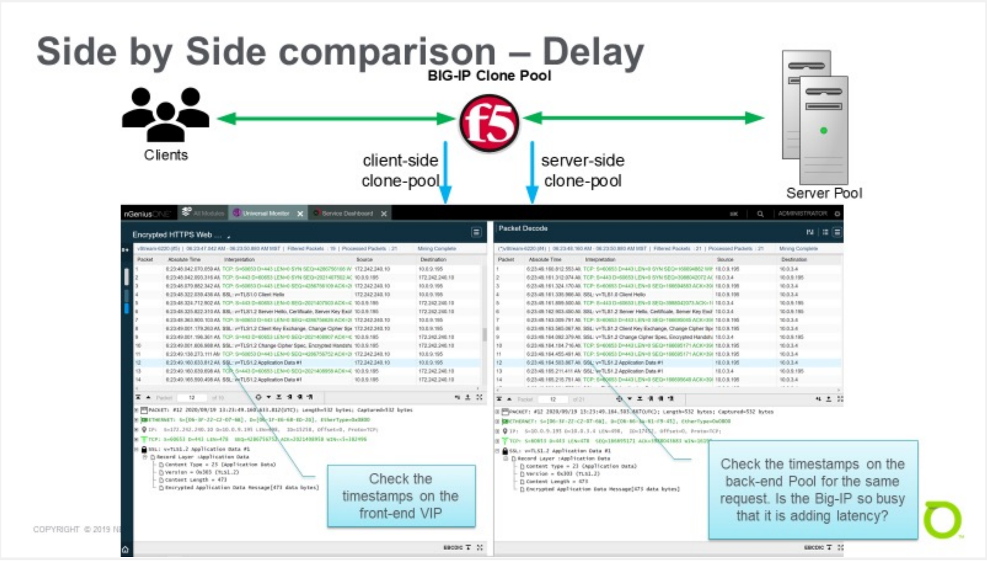
4. From the nGeniusONE Universal Service Monitor, drill down into the **Packet Analysis** function to view the packets captured by NETSCOUT vSTREAM. Compare the client-side clone pool with the server-side clone pool looking at the time stamps and/or the X-Forwarded-For original client IP addresses.



Side by Side comparison

Figure 17: Session comparison from virtual server to pool

Figure 18: Session comparison from virtual server to pool delay



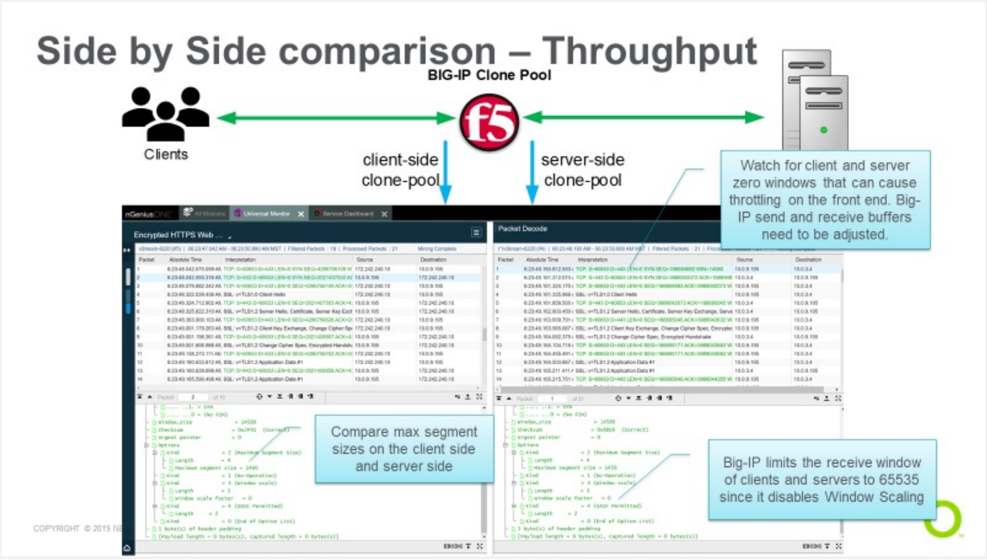
Side by Side comparison – Delay

Check the timestamps on the front-end VIP

Check the timestamps on the back-end Pool for the same request. Is the Big-IP so busy that it is adding latency?

5. Performing a side-by-side comparison of the client-side and server-side clone pools allows the user to investigate the comparative throughput, as well as the delay of the respective views, to verify the performance and understand if any tuning of the F5 configurations are in order, such as the buffer sizes or default window scaling parameters.

Figure 19: Session comparison from virtual server to pool throughput



Side by Side comparison – Throughput

Watch for client and server zero windows that can cause throttling on the front end. Big-IP send and receive buffers need to be adjusted.

Compare max segment sizes on the client side and server side

Big-IP limits the receive window of clients and servers to 65535 since it disables Window Scaling

Appendix

NOTES ON BIG-IP VE DEPLOYMENT IN AWS

To create an Amazon Elastic Compute Cloud (EC2) instance of BIG-IP VE, you deploy a version of it from the AWS Marketplace. The list of BIG-IP products (pay-as-you-go (PAYG) or bring-your-own-license (BYOL)) are available in the AWS Marketplace.

A complete example of deployment and provisioning can be seen in this CloudDocs page: Amazon Web Services: Three-NIC F5 BIG-IP Virtual Edition.

Note: The prerequisite is that you have three subnets created in your AWS Virtual Private Cloud (VPC)—one for each interface (external, internal, and management). Edit the external and management subnet route tables to include an Internet gateway.

To create an account and request a demo license key, you'll need to visit the F5 website.

To apply the license key, follow the instructions found in this F5 support article: K15055: Using tmsh to view and manage licenses for BIG-IP and BIG-IQ systems.

In order for the BIG-IP SSL Orchestrator TAP service to forward unencrypted traffic to the NETSCOUT vSTREAM monitor interface, both the F5 internal interface (Inf 1.2 in the example in Figure 20) and the vSTREAM monitor interface(s) have to be in the same 'internal' subnet (10.0.5.0/24 in the example).

In AWS under EC2 | Network Interfaces, select the BIG-IP internal interface. Click on the **Actions** button and select **Change Source/Dest. Check**. Then select **Disabled** and click the **Save** button. Repeat this step for the vSTREAM monitor network interfaces (ENIs). Make a note of the monitor network interfaces' MAC addresses. You will need these when you create your BIG-IP SSL Orchestrator deployment, the same as if you had a physical NETSCOUT ISNG connected to a physical BIG-IP system.

Clone pools

The use of BIG-IP clone pools is a method of sending specific client-side and server-side traffic to vSTREAM's monitor network interfaces. To configure BIG-IP clone pools to send traffic to vSTREAM and other security devices, please see this MyF5 article: K13392: Configuring the BIG-IP system to send traffic to an intrusion detection system.

In an AWS deployment, vSTREAM monitor interfaces will be assigned a private IP address, similar to any Elastic Network Interface (ENI). You can use this address as the target for where the clone pool should send the traffic. As in the above, you must set each vSTREAM's monitor port ENI Source/Dest. Select **Disabled**. This ensures that traffic copied to the vSTREAM's monitor port is not dropped by AWS, as it recognizes the traffic is intended for the private IP address of the monitor port.

In a physical deployment, the ISNG monitor ports will not have an IP address by default. You can use the same K13392 article to set up BIG-IP port mirrors instead to direct traffic to a physical ISNG monitor port. The major difference is that with clone pools you can selectively send certain traffic of interest to the vSTREAM, and with port mirrors you will copy all the traffic on a particular BIG-IP interface to the ISNG's monitor port.

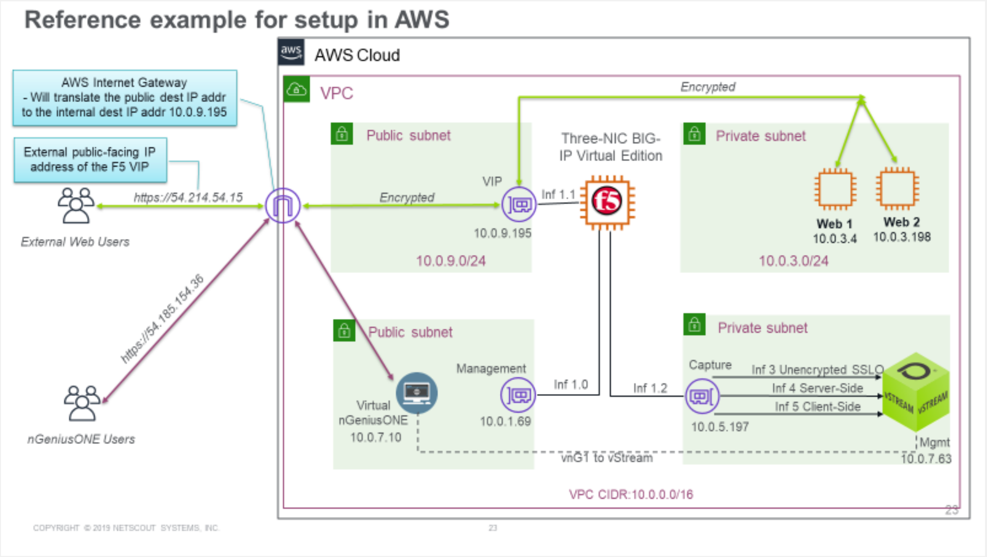


Figure 20: Reference example setup in AWS