AppSentinels.ai
Application Security Re-invented

AppSentinels API Security Platform

NSX Avi Load Balancer Integration

Contents

Revision	Date Modified	Author	Comments
1.0	03-Feb-25		Initial Draft

Introduction

VMware NSX Avi Load Balancer, also known as Advanced Load Balancer, is a sophisticated application delivery controller designed to optimize load balancing across multi cloud environments. It enables seamless load balancing across on-premises data centers and various cloud platforms. This flexibility supports modern application architecture, including virtual machines, containers, and bare metal servers.

This document describes the integration of AppSentinels API security platform with NSX Avi Load Balancer. This integration enables AppSentinels API security platform to capture API request and response data from NSX Avi Load Balancer for security analysis.

The AppSentinels API security platform integration with NSX Avi Load Balancer is based on the *Traffic Cloning* feature supported by NSX Avi Load Balancer. In all cloud and on-premises platforms where traffic cloning is supported by NSX Avi Load Balancer, this integration works even when the traffic is encrypted end-to-end (NSX Avi Load Balancer decrypts and encrypts the traffic before sending it to backend server). This document covers integration details in both scenarios, when backend traffic is encrypted and when backend traffic is decrypted.

Traffic Cloning in NSX Avi Load Balancer

The following points summarize the traffic cloning feature in NSX Avi Load Balancer.

- NSX Avi Load Balancer supports cloning (or mirroring) of virtual service traffic between an SE (Service Engine or Data plane) group and backend pool to a server.
- This feature mimics the behavior of SPAN port.
- Bi-directional traffic is cloned, that is, both request and response are cloned to the server.
- The clone server must be L2 connected with the NSX Avi Load Balancer.
- Traffic cloning is completely stateless and so the SE does not perform any TCP handshake and does not expect any responses to the traffic sent to the configured cloned-traffic server pool.
- Traffic cloning configuration includes traffic cloning profile creation and attaching that profile to a virtual service for which traffic needs to be mirrored.
- Traffic cloning profile includes the definition of the traffic cloning server.
- NSX Avi Load Balancer forwards decrypted traffic to the Traffic cloning server.
- If traffic is encrypted between SE and backend pool, an additional virtual service is required to act as a pool server for the main virtual service, so that decrypted traffic can be cloned.
- It is possible to preserve the original client IP address by enabling ‘Preserve Client IP’ checkbox in Traffic Clone profile.
- Traffic can be cloned to a pool of servers in round robin fashion.
- Traffic cloning is currently supported only on Linux server clouds, Cisco CSP 2100, AWS, OpenStack, vCenter write access and no-orchestrator clouds. It is not supported in platforms like GCP, Azure etc.

VMware Document Reference

Traffic Cloning

Deployment Steps

Clone server deployment

The following points summarize the deployment of a clone server virtual machine to which NSX Avi Load Balancer will forward the cloned traffic.

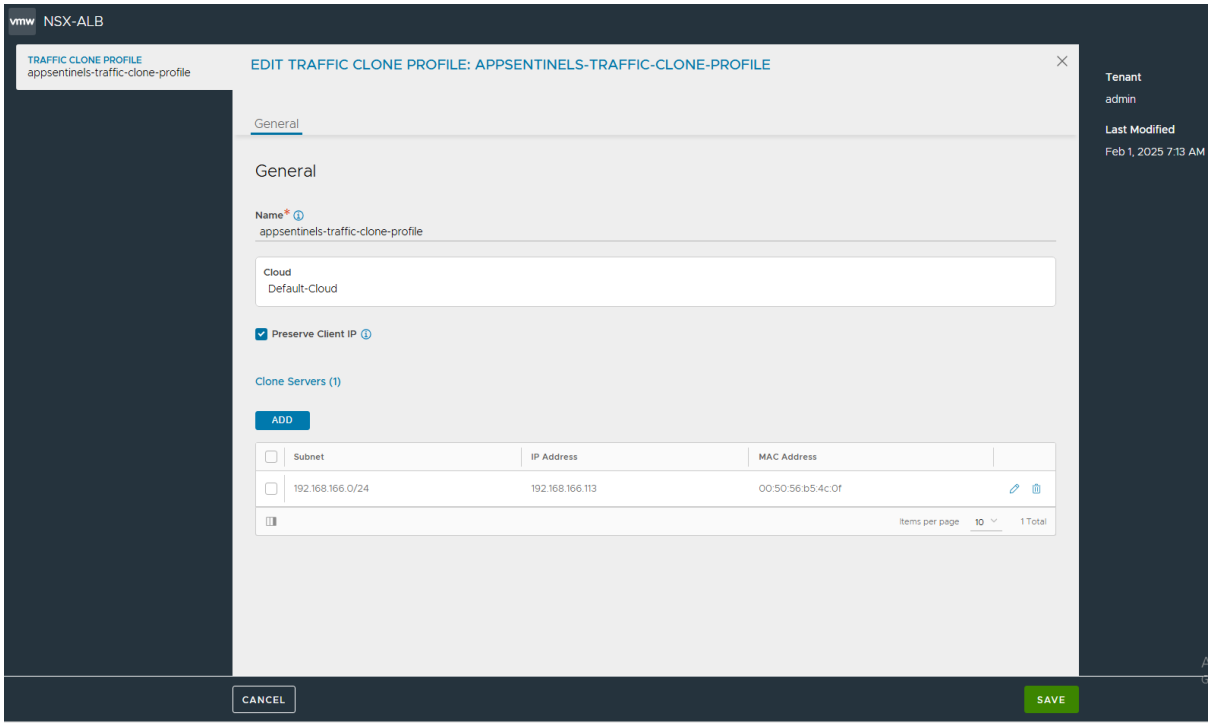
1. Deploy a clone server virtual machine in the directly connected network of Avi Load Balancer Service Engine (SE) group.
2. Allow inbound cloned traffic on the clone server virtual machine from IP addresses in the same network. Please refer to the next sections for the TCP port to be allowed.
3. Allow outbound traffic from the clone server virtual machine to the AppSentinels Controller.
4. Deploy AppSentinels sniffer sensor on the clone server. Please refer to deployment guide for sniffer sensor deployment and configuration.

Traffic Cloning profile

Please perform the following steps to create a traffic clone profile in NSX Avi Load Balancer Controller UI.

1. Go to **Templates > Profiles > Traffic Clone**.
2. Click on **CREATE** button.
3. Specify **Name** of the profile.
4. Enable **Preserve Client IP** checkbox.
5. Click on **ADD** button to add clone server IP address.
6. Select a **Network** and **Subnet** to clone the traffic to. This subnet should be same as the subnet of Service Engines.
7. Specify the **IP Address** of the clone server deployed earlier.
8. Specify the **MAC Address** of the clone server network interface. This configuration is optional.
9. Click on the **SAVE** button to save the Traffic Clone profile.

The following screenshot displays typical configuration of traffic cloning profile.

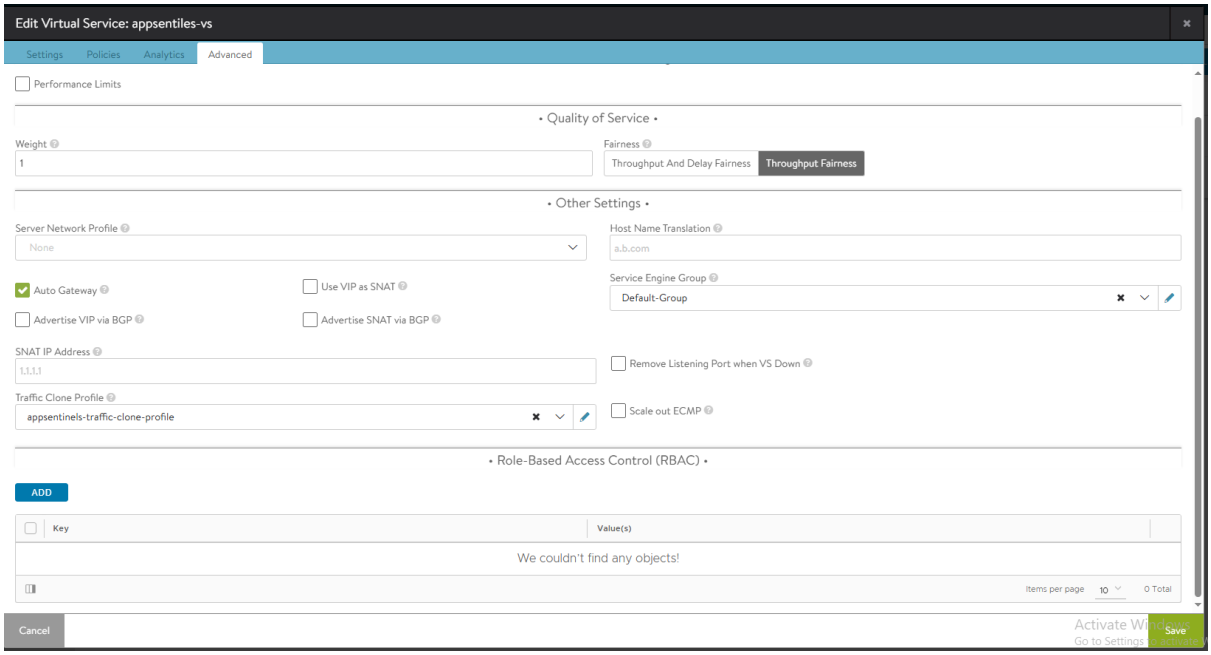


Enable Traffic Cloning – Backend traffic is decrypted

Traffic cloning configuration is simple when backend traffic is decrypted, the following points list the steps to be performed.

1. Go to Applications > Virtual Services in NSX Avi Load Balancer Controller UI.
2. Click the *edit* button for the virtual service for which traffic cloning needs to be enabled.
3. Click on the **Advanced** tab.
4. Click on **Traffic Clone Profile** drop-down and select the Traffic Clone profile created earlier.
5. Click on **Save** button to enable traffic cloning.

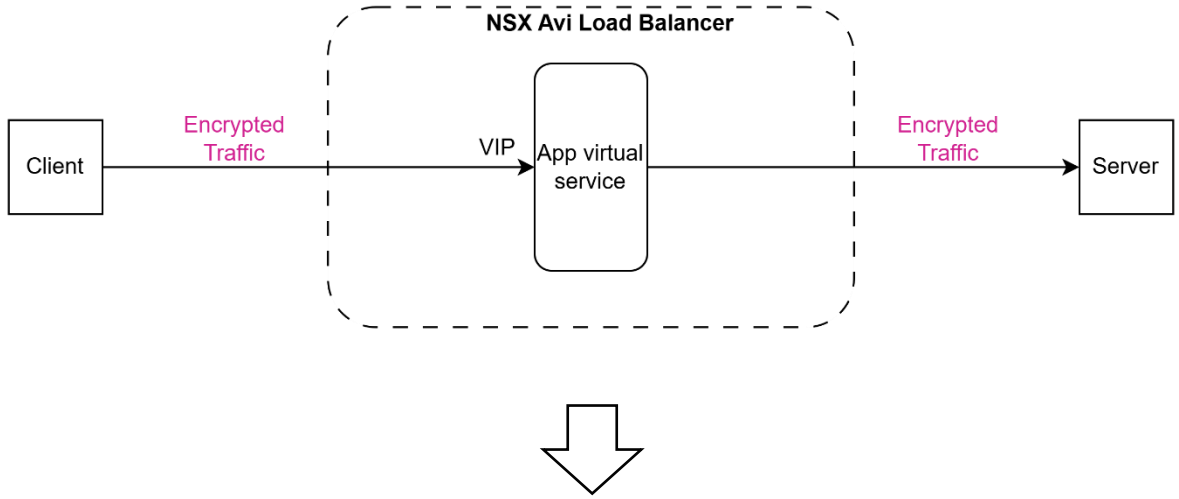
The following screenshot displays the configuration of traffic cloning profile.



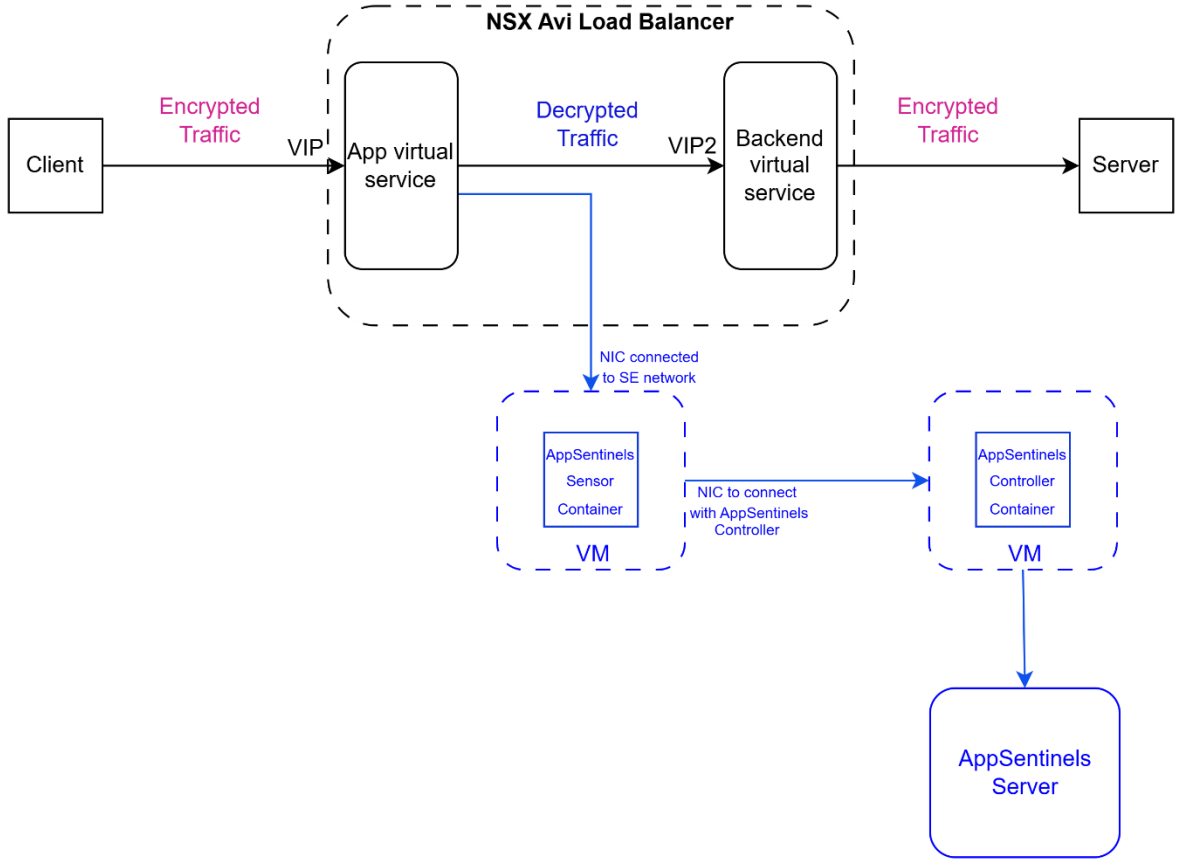
Enable Traffic Cloning – Backend traffic is encrypted

Since NSX Avi Load Balancer clones the backend server-side request and response traffic, with normal traffic clone configuration (described in previous sub-section), the clone server receives encrypted. To clone the decrypted traffic, a new virtual service is inserted between the virtual service corresponding to the application and the application server(s). The following diagram displays the changes from the original virtual service setup to the new virtual service setup with traffic cloning enabled.

Original setup



Modified setup with traffic cloning



Please note that single boxes have been used to depict clients and server pool to keep the diagrams simple. The diagram indicates that

- A new Backend virtual service with virtual IP address VIP2 has been added.

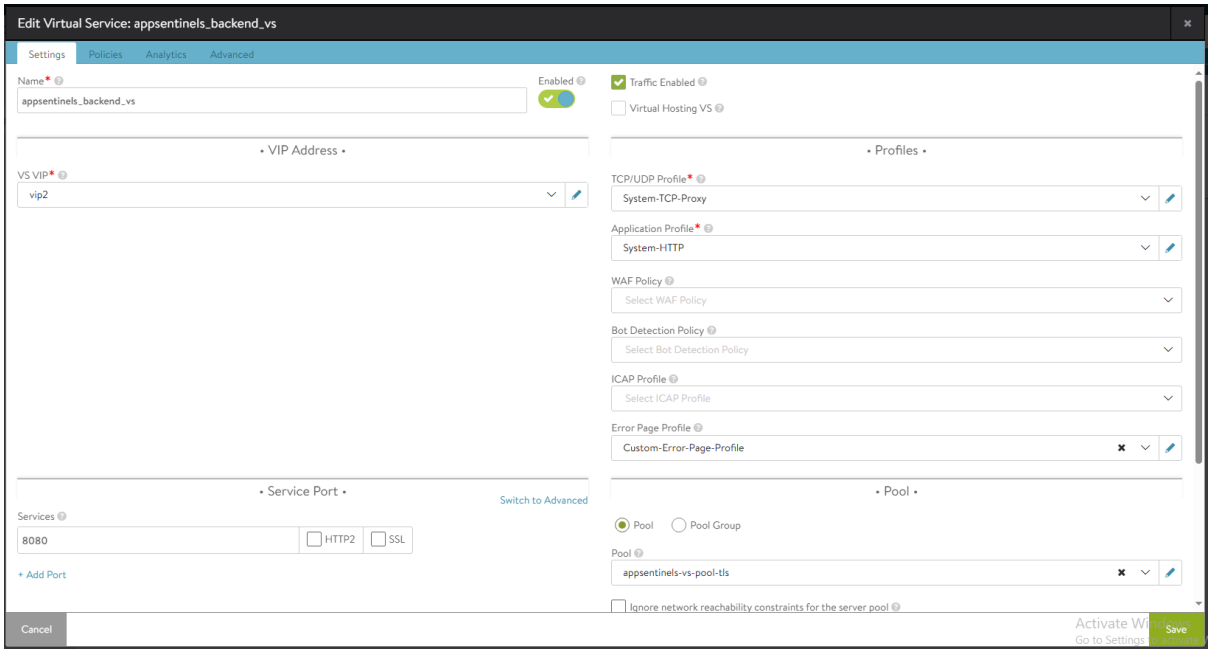
- The App virtual service backend pool has been changed to VIP2, so App virtual service forwards clear-text traffic to Backend virtual service.
- Backend virtual service forwards encrypted traffic to backend server.
- AppSentinels sniffer sensor runs on the clone server, so the clone server has been displayed as *AppSentinels Sensor*.
- The diagram displays AppSentinels Controller as a separate box connected with AppSentinels sensor, however, AppSentinels Controller and AppSentinels Sensor can be deployed as a single docker container (integrated deployment) or separate docker containers connected via the network.
- Since backend traffic from App virtual service is decrypted, the clone server (AppSentinels sensor) receives decrypted traffic.

New Backend virtual service configuration

The following steps summarize the configuration of the new backend virtual service added to enable traffic cloning.

1. Go to **Applications > Virtual Services** in NSX Avi Load Balancer Controller UI.
2. Click on **CREATE VIRTUAL SERVICE** and select **Advanced Setup**.
3. Specify the **Name** of the virtual service.
4. Assign a virtual IP address (**VS VIP**) to the virtual service.
5. Assign a **Service Port** to the virtual service. Since this port is internal to NSX Avi Load Balancer, it can be any unused port in the NSX Avi Load Balancer.
6. Do not enable **SSL** on this service port, so that the front-end (incoming) traffic to the virtual service is decrypted.
7. In the **Pool** configuration, select the same pool or pool group that is currently used in the existing application virtual service, so that the encrypted traffic is forwarded to the backend server.
8. Configure any other profiles and policies required for this virtual service.
9. Click on the **Save** button.
10. Please note the VIP and port number of this virtual service. These will be updated in the existing virtual service. Let's assume that VIP and service port for this new backend virtual service are *VIP_BACKEND* and *PORT_BACKEND* respectively. Please note that these names have been used in subsequent sections to refer to the VIP and service port of the backend virtual service.

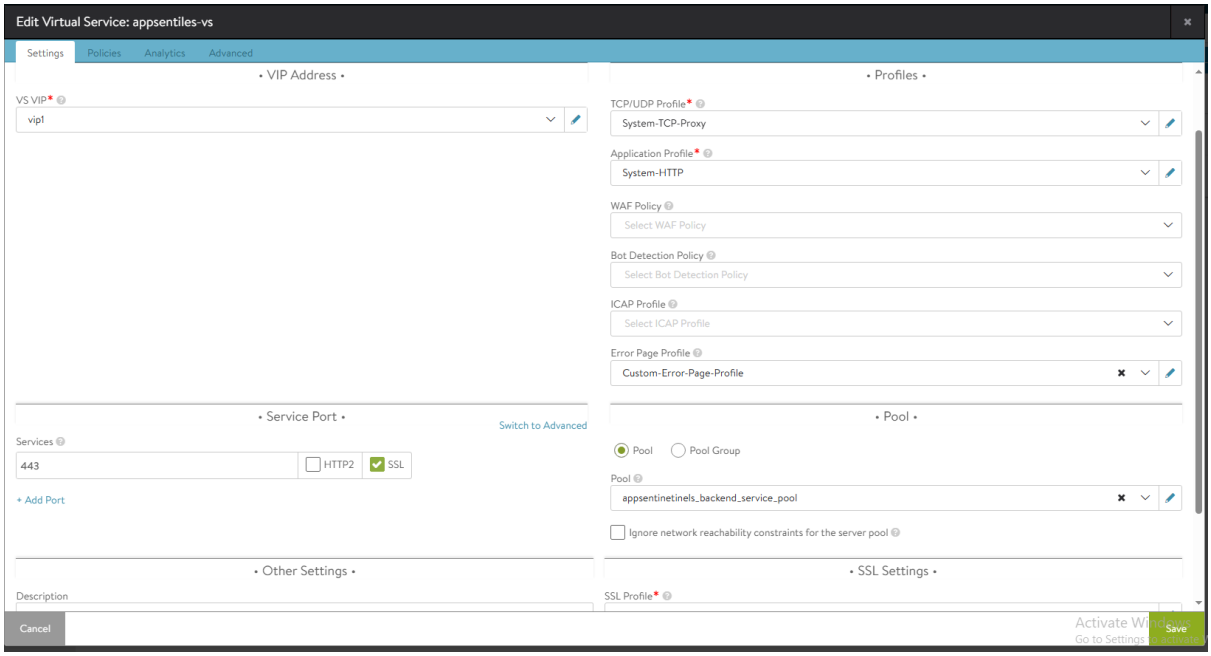
The following screenshot displays typical configuration of backend virtual service.



Modify existing application virtual service

Perform the following steps to update the existing application virtual service to enable traffic cloning.

1. Go to **Applications > Pools** in NSX Avi Load Balancer Controller UI.
2. Click on **CREATE POOL** button.
3. Specify the **Name** of the pool.
4. Select **Generic Application** as **Type**.
5. Configure *PORT_BACKEND* (service port of the new virtual service) as the **Default Server Port**.
6. In **Servers** configuration, configure *VIP_BACKEND* (VIP of the new virtual service) as the backend server IP address.
7. Perform passive health monitoring of the backend, so select **Enable Passive Health Monitor** checkbox.
8. Since decrypted traffic should be forwarded to the backend service, DO NOT enable SSL profile for this pool.
9. Click on **SAVE** button.
10. Go to **Applications > Virtual Services** in NSX Avi Load Balancer Controller UI.
11. Click on the *edit* button for the application virtual service.
12. Under **Settings** tab, select the backend pool created above in the **Pools** drop-down.



13. Click on the **Advanced** tab.
14. Click on **Traffic Clone Profile** drop-down and select the Traffic Clone profile created earlier.
15. Click on **Save** button to enable traffic cloning.

After this set up, NSX Avi Load Balancer should clone the decrypted traffic to clone server and AppSentinels dashboard should display the APIs being accessed.

Inbound traffic on clone server

- The NSX Avi Load Balancer will clone the traffic between the application virtual service and the backend virtual service, that is, the traffic with destination port as *PORT_BACKEND* and destination IP address as *VIP_BACKEND*.
- Inbound traffic on the PORT_BACKEND should be allowed on the clone server virtual machine.

Troubleshooting

1. If APIs are not visible in AppSentinels dashboard, please do a packet capture on the Service port of the backend virtual service (PORT_BACKEND) on the clone server VM.
2. If traffic is not cloned to the clone server, please make sure that NSX Avi Load Balancer supports Traffic Cloning on the given cloud or No orchestrator platform.
3. If Traffic Cloning is supported, please check the IP address and MAC address specified in Traffic Cloning profile.
4. Check Controller and Service Engine logs for errors and warnings.