GigaVUE V Series Applications Guide

GigaVUE Cloud Suite

Product Version: 6.2

Document Version: 1.0

Last Updated: Wednesday, February 15, 2023

(See Change Notes for document updates.)

Change Notes

When a document is updated, the document version number on the cover page will indicate a new version and will provide a link to this Change Notes table, which will describe the updates.

Product Version	Document Version	Date Updated	Change Notes
6.2.00	1.0	02/15/2023	The original release of this document with 6.2.00 GA

Contents

GigaVUE V Series Application Guide

This guide describes the list of supported V Series Applications and how to add the V Series Applications to monitoring session and configure it.

- Supported V Series Applications
- Application Metadata Exporter
- De-Duplication
- GENEVE De-encapsulation
- Header Stripping
- Load Balancing
- Masking
- Passive SSL Decryption
- PCAPng Application
- 5G-Service Based Interface Application
- Slicing

Overview of GigaVUE V Series Applications

GigaVUE V Series Node is a virtual machine running in the customer's infrastructure which processes and distributes network traffic. It plays the same role as an H Series appliance in a physical deployment, running many of the same GigaSMART applications and feeding data to tools in a similar manner. Because GigaVUE V Series nodes reside in a virtual environment, inbound and outbound traffic is tunneled (because there are no physical device ports).

GigaVUE V Series Applications run on GigaVUE V Series Nodes. All these applications use Volume- Based License. Refer to Volume-Based License for more detailed information.

You can use these applications to optimize the traffic sent from your instances to the monitoring tools. GigaVUE Cloud Suite supports the following applications:

- Application Metadata Exporter
- De-Duplication

- GENEVE De-encapsulation
- Header Stripping
- Load Balancing
- Masking
- Passive SSL Decryption
- PCAPng Application
- 5G-Service Based Interface Application
- Slicing

Refer to the Supported V Series Applications table for more information on the platforms in which these applications will be supported.

Supported V Series Applications

GigaSMART Operation	GigaVUE Cloud Suite for AWS	GigaVUE Cloud Suite for Azure	GigaVUE Cloud Suite for OpenStack	GigaVUE Cloud Suite for VMware	GigaVUE Cloud Suite for AnyCloud	GigaVUE Cloud Suite for Nutanix
Masking	✓	✓	✓	✓	✓	✓
Packet Slicing	✓	✓	✓	✓	✓	✓
De-Duplication	✓	✓	✗	✓	✗	✓
GENEVE De-encapsulation	✓	✗	✗	✗	✗	✗
Application Metadata Exporter	✓	✓	✗	✓	✗	✗
Header Stripping	✓	✓	✓	✓	✓	✓
Load Balancing (Stateless)	✓	✓	✓	✓	✗	✓
PCAPng	✓	✗	✓	✓	✗	✗
SBI-5G-Service Based Interface	✗	✗	✓	✓	✗	✗
SSL Decryption for Out-of-Band Tools (Passive SSL)	✗	✗	✗	✗	✓	✗

Application Metadata Exporter

Application Metadata Exporter(AMX) application converts the output from the Application Metadata Intelligence (AMI) in CEF format into JSON format and sends it to the cloud tools and Kafka.

```
┌──────────────┐          ┌──────────────┐                    ┌──────────────┐
│   AMI App    │          │   AMX App    │                    │              │
│ (Application │   CEF    │ (Aggregate   │  JSON File Upload  │     Tool     │
│   Metadata   │  (UDP)   │    and       │                    │              │
│ Intelligence)│          │   Export)    │                    │              │
└──────────────┘          └──────────────┘                    └──────────────┘
```

The AMX application can be deployed only on a V Series Node and can be connected to Application Metadata Intelligence running on a physical node or a virtual machine. The AMX application and the AMI are managed by GigaVUE-FM. This application is supported on VMware ESXi, VMware NSX-T, AWS and Azure.

Kafka Export

The Kafka export can be used to ingest AMI data on on-prem tools or data warehouse.

```
┌──────────────┐          ┌──────────────┐                    ┌──────────────┐
│              │  (TCP)   │ Kafka Cluster│      (TCP)         │              │
│  producers   │─────────▶│   (Brokers)  │───────────────────▶│   clients    │
│              │          │              │                    │              │
└──────────────┘          └──────────────┘                    └──────────────┘
```
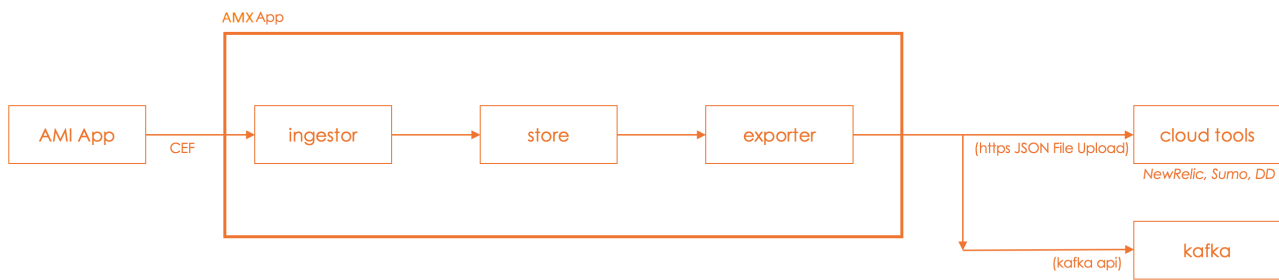
To configure an Application Metadata Exporter(AMX) application do the following:

Step No	Task	Refer the following topics
1	Create a Monitoring Domain	Create Monitoring Domain topic in the respective GigaVUE Cloud Suite Configuration Guides.
2	Deploying GigaVUE V Series Node **NOTE:** AMX application is deployed on this V Series node.	Configure GigaVUE Fabric Components in GigaVUE-FM topic in the respective GigaVUE Cloud Suite Configuration Guides.
3	• Creating Environment and Connections. • Deploy V Series Nodes. **NOTE:** This V Series Node is used for creating Application Intelligence Session. • Create Application Intelligence Session.	Configure Application Intelligence Solutions on GigaVUE V Series Nodes topic in the respective GigaVUE Cloud Suite Configuration Guides.
4	Add Application Metadata Intelligence Session	Create Metadata Intelligence by Editing Monitoring Session from Dashboard
5	Create a Monitoring Session	Create Monitoring Session topic in the respective GigaVUE Cloud Suite Configuration Guides.
6	Add Applications to the Monitoring Session	Add Application to the Monitoring Session topic in the respective GigaVUE Cloud Suite Configuration Guides.
7	View Monitoring Session Statistics	View Monitoring Session Statistics topic in the respective GigaVUE Cloud Suite Configuration Guides.

AMX Application Deployment

AMX application can be deployed on:

- On-Premises
    - Hardware
    - Virtual (VMware)

- Public Cloud

On-Premises

Hardware

In hardware deployments, the Application Metadata Intelligence (AMI) runs on a physical node/cluster, and the AMX application is deployed on a V Series 2 Node running on VMware ESXi. The output from the AMI in CEF format is sent to the AMX application in V Series Node. The performance of the device and the application is managed by GigaVUE-FM. The following devices support the integration of AMX application:

- GigaVUE-HC1
- GigaVUE-HC2
- GigaVUE-HC3
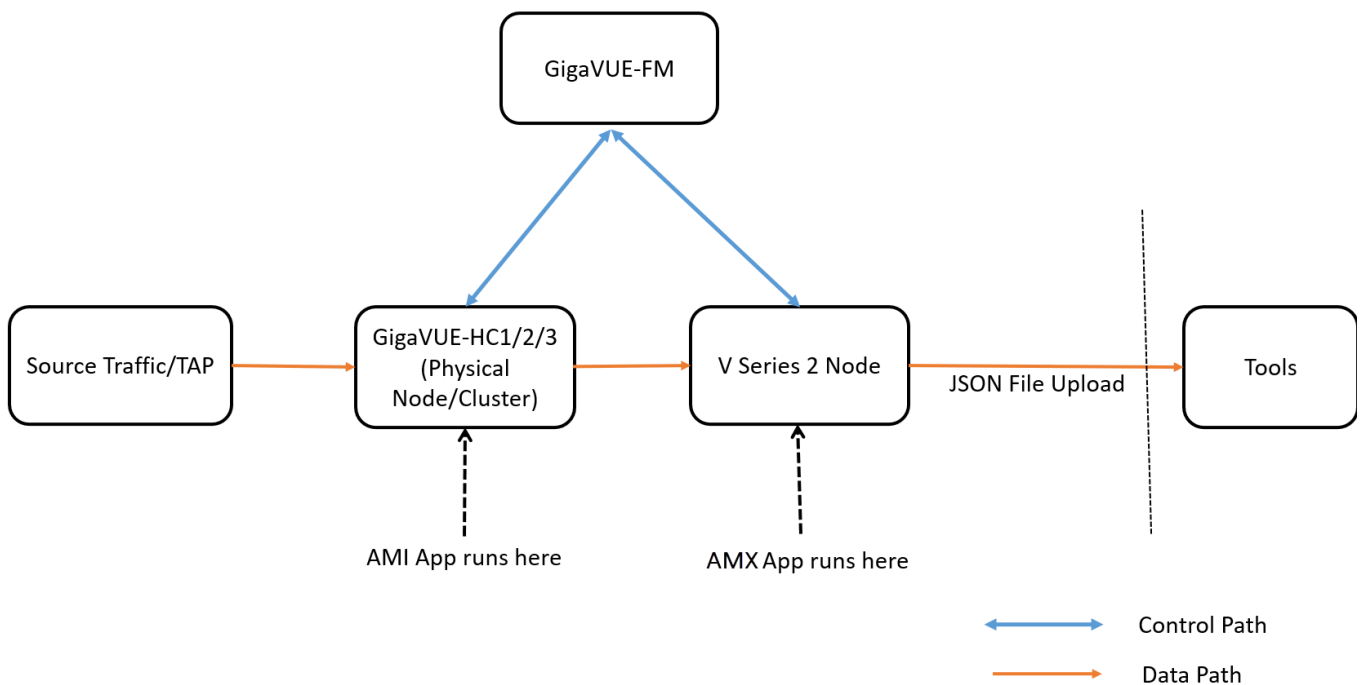
Private Cloud (VMware)

In the Private Cloud environment, the application is supported only on VMware and can be deployed in the VMware as shown in the diagram.

```
                        ┌─────────────┐
                        │ GigaVUE-FM  │
                        └─────────────┘

┌──────────────┐   ┌──────────────┐   ┌──────────────┐              ┌────────┐
│              │   │ V Series 2 Node│  │ V Series 2 Node│            │        │
│ Source Traffic/ATS│→│ (Running on  │→│ (Running on   │  JSON File  │ Tools  │
│              │   │   VMware)     │  │   VMware)     │  Upload     │        │
└──────────────┘   └──────────────┘   └──────────────┘              └────────┘

                     AMI App runs here   AMX App runs here
```

Control Path
Data Path
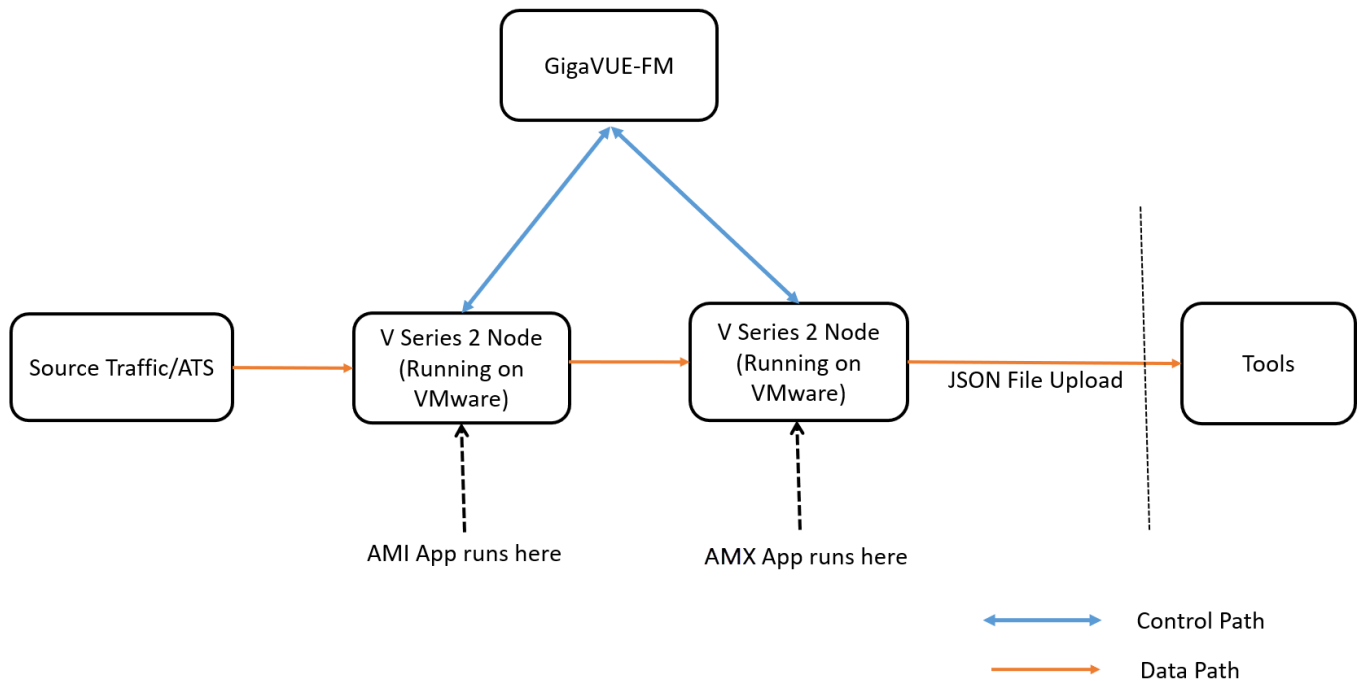
> **NOTE:** The application is not supported on Nutanix or OpenStack environment.

Public Cloud

In the Public Cloud environment, the application is supported on AWS and Azure platforms, and can be deployed as shown in the diagram:
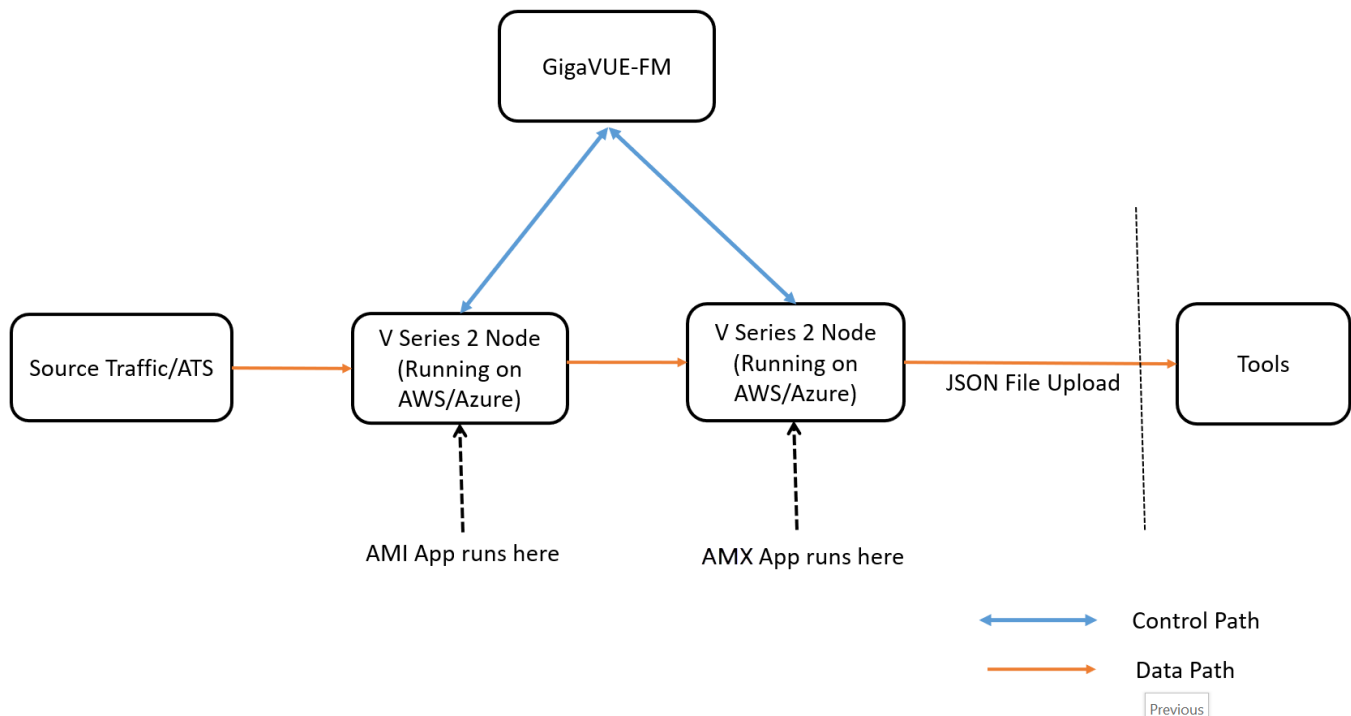
Rules

- After deploying the GigaVUE V Series Node in the monitoring domain, click on the GigaVUE V Series Node's Name, and the V Series Node quick view opens. Choose a data IP to which you wish to send CEF packets, then use the IP address of this data IP as the **Tool IP Address** when creating the Application Metadata Intelligence solution. Refer to Create Metadata Intelligence by Editing Monitoring Session from Dashboard topic in the *GigaVUE Fabric Management Guide* on how to configure AMI for AMX application.

- The GigaVUE V Series Node deployed must be entirely dedicated to the AMX application, it cannot have other applications in it.

- When multiple connections are configured under the same monitoring domain using third party orchestration, ensure to select the connection alias in which the AMX application is deployed, when deploying monitoring session.

- When multiple connections are configured under the same connection resource using third party orchestration, ensure to select the connection alias in which the Application Intelligence session is configured, when configuring Application Intelligence Session.

- When using this application for production usage, it is recommended to use large size Virtual Machines.

Prerequisites for AWS

Prerequisites to follow when creating a monitoring domain and deploying a V Series node:

- Select **Traffic Acquisition Method** as **Customer Orchestrated Source**. Refer Create a Monitoring Domain for more detailed information on how to create a monitoring domain.
- Select **Instance type** with three or more NICs. Refer Configure GigaVUE Fabric Components in GigaVUE-FM for more detailed information on how to deploy a GigaVUE V Series Node.
- When the **Traffic Acquisition Method** is selected as **Customer Orchestrated Source**, the Volume Size field appears on the **AWS Fabric Launch Configuration** page. Enter the Volume Size as 80GB.

  > **NOTE:** Check on the disk space run every 30 minutes and when the disk space reaches 50%, purge starts.

Prerequisites for Azure

Prerequisites to follow when creating a monitoring domain and deploying V Series node:

- Select **Traffic Acquisition Method** as **Customer Orchestrated Source**. Refer Create Monitoring Domain for more detailed information on how to create a monitoring domain.
- Select **Size** with three or more NICs. Refer Configure GigaVUE Fabric Components in GigaVUE-FM for more detailed information on how to deploy a GigaVUE V Series Node.
- When the **Traffic Acquisition Method** is selected as **Customer Orchestrated Source**, the **Disk Size** field appears on the **Azure Fabric Launch Configuration** page. Enter the Disk Size as 80GB.

  > **NOTE:** Check on the disk space run every 30 minutes and when the disk space

Prerequisites for VMware

Prerequisites to follow when creating a monitoring domain and deploying V Series node:

- Select **Traffic Acquisition Method** as Customer Orchestrated Source. Refer Step 2: Deploy V Series nodes on VMware ESXi for more detailed information on how to create a monitoring domain and deploy V Series nodes.
- .When deploying this application in VMware NSX-T, create a monitoring domain in the ESXi Monitoring domain. Even if your V Series node is a part of VMware NSX-T host, you can still deploy it in VMware ESXi monitoring domain. Refer to the Same Host across Different Monitoring Domains topic in the *GigaVUE Cloud Suite for VMware—GigaVUE V Series Guide* for more detailed information.

Configure Application Metadata Exporter Application

Rules to follow when using the AMX application:

The monitoring session can only have Raw End Point (REP), it cannot have other applications, maps, or tunnels when using the AMX application. Refer Create Raw Endpoint for more detailed information on how to add a REP to the monitoring session and how to configure it.

To add AMX application:

1. Drag and drop **Application Metadata Exporter** from **APPLICATIONS** to the graphical workspace. The Application quick view appears.
2. Enter the Alias for the application. Enter a port number for the **Cloud Tool Ingestor Port**. Then, click the **Add** button for **Cloud Tool Exports** or **Kafka**.

3. You can export your Application Metadata Intelligence output to either cloud tools or Kafka. Enter the following details for the Cloud tool export in the Application quick view:

Fields	Description
Alias	Enter the alias name for the cloud tool export.
Cloud Tool	Select the Cloud tool from the drop-down menu.
Account ID	Enter the account ID number of the selected Cloud Tool.
API Key	Enter the API key of the Cloud Tool.
Enable Export	Enable the box to export the Application Metadata Intelligence output in JSON format.
Zip	Enable the box to compress the output file. **NOTE:** Enable this field when using New Relic as the cloud tool.
Interval	The time interval (in seconds) in which the data should be uploaded periodically. The recommended minimum time interval is 10 seconds and the maximum time interval is 30 minutes.
Parallel Writer	Specifies the number of simultaneous JSON exports done.
Export Retries	The number of times the application tries to export the entries to Cloud Tool. The recommended minimum value is 4 and the maximum is 10.
Maximum Entries	The number of JSON entries in a file. The maximum number of allowed entries is 5000 and the minimum is 10, however 1000 is the default value.

Labels	Click **Add**. Enter the following details:
	  o Enter the **Key** .
	  o Enter the **Value**.
	
	NOTE: When New Relic is selected as the cloud tool, the key is automatically set as is **eventType** and the Value can only have alphanumeric characters, colons (:), periods (.), and underscores (_).

Enter the following details for Kafka export in the Application quick view:

Fields	Description
Alias	Enter the alias name for the Kafka Export.
Topic	The topic name to push JSON streams to, which is generally given to users part of the Kafka administration
Brokers	The URL that contains the Kafka cluster endpoints. Click ➕ to add another broker and click ➖ to remove an existing broker.
Enable Export	Enable the box to export the Application Metadata Intelligence output in JSON format.
Zip	Enable the box to compress the output file.

Fields	Description
Interval	The time interval (in seconds) in which the data should be uploaded periodically. The recommended minimum time interval is 10 seconds and the maximum time interval is 30 minutes.
Parallel Writer	Specifies the number of simultaneous JSON exports done.
Export Retries	The number of times the application tries to export the entries to Kafka. The recommended minimum value is 4 and the maximum is 10.
Maximum Entries	The number of JSON entries in a file. The maximum number of allowed entries is 5000 and the minimum is 10, however 1000 is the default value.
Labels	Click **Add**. Enter the following details: o Enter the **Key**. o Enter the **Value**.
Producer Configurations	Click **Add** to enter the authentication details if a Kafka broker needs authentication. For Example: • security.protocol=SASL_SSL • sasl.mechanism=PLAIN • sasl.username=username • sasl.password=password

4. Click **Deploy** to deploy the monitoring session. The **Select nodes to deploy the Monitoring Session** dialog box appears. Select the GigaVUE V Series Node for which you wish to deploy the monitoring session.

5. After selecting the V Series Node, select the interfaces for the REPs deployed in the monitoring session from the drop-down menu. Then, click **Deploy**.

The monitoring session configuration health can be viewed on the Monitoring Session page. Refer Cloud Health Monitoring for more detailed information on how to view cloud configuration health.

To view the application statistics on the Monitoring Session Statistics page, click **View Monitoring Session Diagram** and click on the AMX application. The Statistics appear as a quick view page. To view the exporter related statistics, select **Exporter** from the top navigation button on the quick view page.

De-Duplication

De-duplication lets you detect and choose the duplicate packets to count or drop in a network analysis environment.

Duplicate packets are common in network analysis environments where both the ingress and egress data paths are sent to a single output . They can also appear when packets are gathered from multiple collection points along a path. The Dedup application lets you eliminate these packets, only forwarding a packet once and thus reducing the processing load on your tools.

Feature Overview

There are two actions that can be specified for handling the duplicate packets detected:

- drop, which drops the duplicate packets
- count, which counts the duplicate packets, but does not drop them

A time interval can be configured within which an identical packet will be considered a duplicate. The greater the interval over which traffic can be checked for duplicates, the higher the accuracy of the de-duplication detection and subsequent elimination.

For example, if two of the same packets are seen in the specified time interval, the packets will be detected as duplicates. If one packet is seen in the time interval and another packet is seen in a later time interval, the packets will not be detected as duplicates.

For IPv4 and IPv6 packets, to determine if a packet is considered to be a duplicate, parts of the IP headers (Layer 3 and Layer 4), as well as part of the payload are compared.

For non-IP packets, a packet is considered to be a duplicate if it is identical.

Configure Dedup Application

To add a de-duplication application:

1. Drag and drop **Dedup** from **APPLICATIONS** to the graphical workspace.
2. Click the Dedup application and select **Details**. The Application quick view appears.

3. In the Application quick view, enter the information as follows:

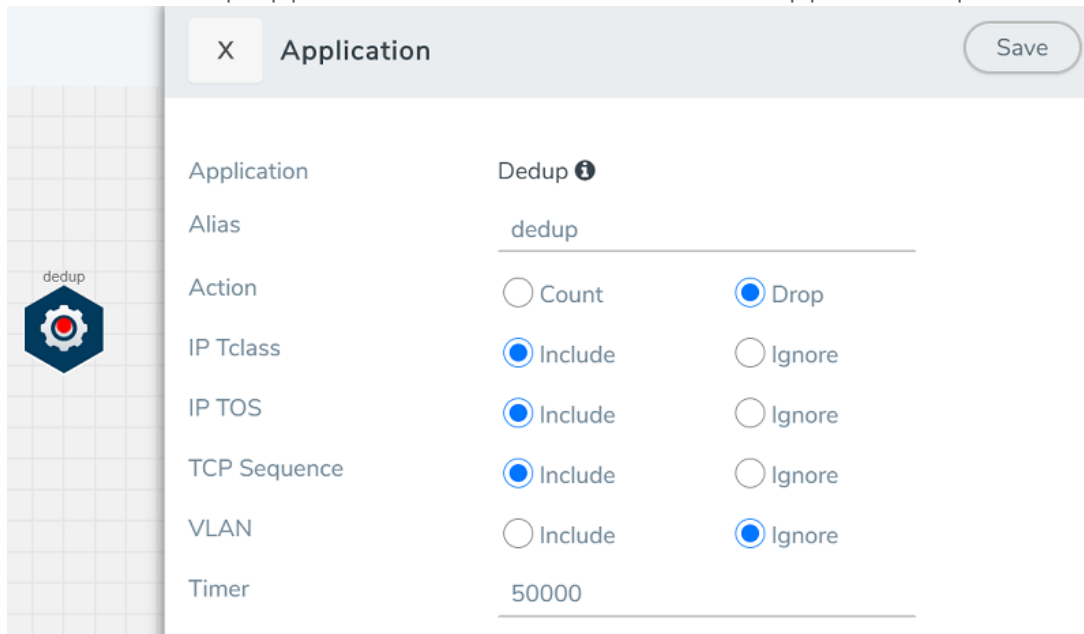| Parameter	Description
Action	Specifies whether duplicate packets are to be counted or dropped as follows: ○ **Count**– The dedup application counts the duplicate packets, but does not drop them. ○ **Drop**– The dedup application drops the duplicate packets. The default is drop.
IP Tclass **IP TOS** **TCP Sequence** **VLAN**	These options are useful when applying de-duplication operations to packets in a NAT environment. Different NAT implementations can change certain packet header fields (for example, the TCP sequence number). If you want to be able to detect duplicates without requiring that these fields match (ToS field, TCP sequence number, VLAN ID), you can disable the corresponding option. ○ **IP Tclass** – Ignore or include IPv6 traffic class. Use for IPv6. The default is include. ○ **IP TOS** – Ignore or include the IP ToS bits when detecting duplicates. Use for IPv4. The default is include. ○ **TCP Sequence** – Ignore or include the TCP Sequence number when detecting duplicates. The default is include. ○ **VLAN** – Ignore or include the VLAN ID when detecting duplicates. The default is ignore. Include means the field will be included when the application compares packets. Ignore means the field will be ignored when the application compares packets.
Timer <Value: 10-500000 μs>	Configures the time interval within which an identical packet will be considered a duplicate. The greater the interval over which traffic can be checked for duplicates, the higher the accuracy of the de-duplication detection and subsequent elimination. The default is 50,000μs. For example, if two same packets are seen in the specified time interval, the packets will be detected as duplicates. If one packet is seen in the time interval and another packet is seen in a later time interval, the packets will not be detected as duplicates. **NOTE:** Retransmissions are not counted as duplicates.

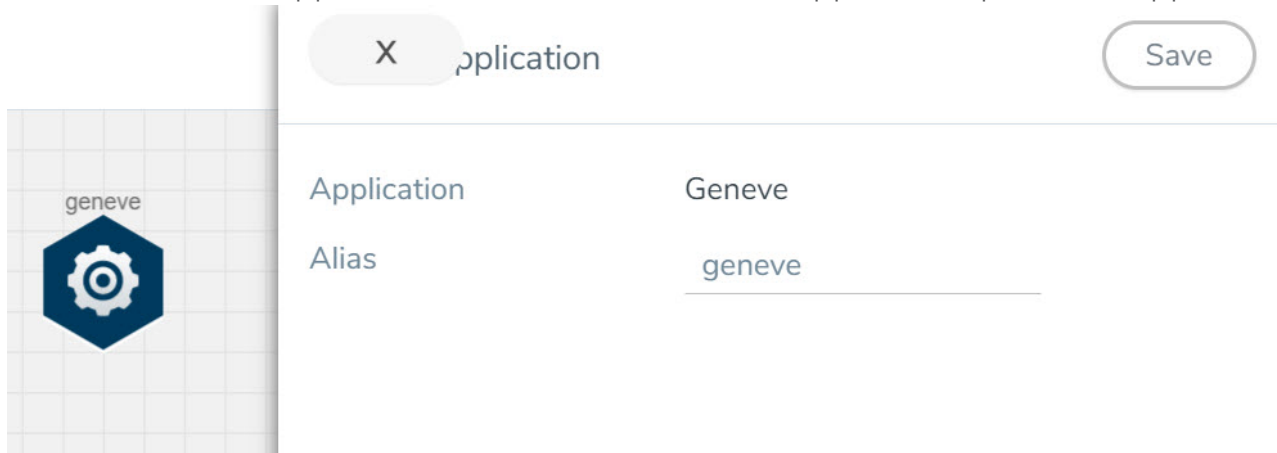4. Click **Save**.

GENEVE De-encapsulation

The GENEVE De-encapsulation application is used to acquire and strip GENEVE headers. To route the traffic through the third-party network appliances seamlessly, the AWS gateway load balancer with a VPC adds GENEVE header to packets as they are forwarded to a third-party network appliance. Each appliance is expected to terminate the GENEVE tunnel and

process the GENEVE encapsulated traffic traffic. When the GigaVUE-FM directs the acquisition of the customer traffic, the packets are encapsulated and forwarded as GENEVE tunnels that are terminated in GigaVUE V Series nodes.

To add a GENEVE application:

1. Drag and drop **GENEVE** from **APPLICATIONS** to the graphical workspace.
2. Click the GENEVE application and select **Details**. The Application quick view appears.

X	plication		Save
Application		Geneve	
Alias		geneve	

3. Enter an alias for the GENEVE application.
4. Click **Save**.

Header Stripping

Header Stripping application efficiently examines the packets for specified headers like GTP, ISL, ERSPAN, MPLS, MPLS+VLAN, VLAN, VN-Tag, VXLAN, FM6000Ts, and generic and removes them before sending the packet to the appropriate security and analysis tools. Each packet is examined for the packet forwarding addition and it also ensured that the headers are removed from the packet before sending the packet to the tools. This application is useful when working with tools that either cannot recognize these headers or have to engage in additional processing to adjust for them.

Furthermore, the presence of the protocols like GTP, ISL, ERSPAN, MPLS, MPLS+VLAN, VLAN, VN-Tag, VXLAN, and FM6000Ts in the packet can restrict or limit the ability to apply filtering and flow-based load balancing to the traffic as it is forwarded to specific tools. To address each of these challenges, header stripping of these protocols is required.

List of Protocols that are supported for stripping:

- GTP
- ISL
- ESPRAN

- MPLS
- MPLS+VLAN
- VLAN
- VN-Tag
- VXLAN
- FM6000Ts,
- Generic

Configure Header Stripping Application

To configure the header stripping application, follow the steps given below:

1. Drag and drop **Header Stripping** from **APPLICATIONS** to the graphical workspace.
2. Click the Header Stripping application and select **Details**. The Application quick view appears.

3. In the application quick view enter the following details:

Field	Description
Alias	Enter the alias name for the application
Protocol	Select the type protocol
VLAN: Use this option to strip VLAN header form the packets. You can strip only the outer VLAN header or the entire VLAN header. When choosing VLAN as your protocol for stripping, enter the following details	
VLAN Header	The VLAN Header that should be stripped. The supported minimum value is 0 and the maximum value is 16777215. The default value is 0.
VXLAN: Use this option to strip VXLAN (Virtual eXtensible Local Area Network) headers. You can strip either matching VXLAN headers or all VXLAN headers. When choosing VXLAN as your protocol for stripping, enter the following details	
VXLAN ID	The VXLAN ID that should be stripped. the default value is outer.
FM6000Ts: Use this option to strip FM6000Ts time stamp headers. Packets entering the application from other devices may contain FM6000 timestamps. FM6000 is an Intel chip used for timestamping. FM6000 has a hardware timestamp in the packet. When choosing FM6000Ts as your protocol for stripping, enter the following details.	
Time Stamp Format	The format of the time stamp you wish to be strip. Only the **None** format is supported.
ESPRAN: Use this option to strip ERSPAN Type II and Type III headers. When choosing ESPRAN as your protocol for stripping, enter the following details	
ESPRAN FlowID	Specify an ERSPAN flow ID, from 0 to 1023. A flow ID of zero is a wildcard value that matches all flow IDs.

Generic: Using this option to strip any header without having to worry about at which level header would occur. When choosing generic as your protocol for stripping, enter the following details	
Ah1	The anchor header (AH1) after which the header to be stripped is occurred.

Offset	Based on the offset value selected the enter the following details:
	
	1. **Offset Range**: If you wish to use offset range as your offset then enter the following details:
	
	   a. Offset Range Value: Offset of the header occurrence from the above anchor header. The minimum supported value is 1 and the maximum supported value is 1500.
	
	   b. Header Count: Specifies how many headers from the offset, the application should remove. The minimum supported value is 1 and the maximum is 32.
	
	   c. Custom Len: The length (in bytes) of the header that should be stripped.
	
	   d. Ah2: The next possible standard header that occurs immediately after the header
	
	2. **Start / End**: If you wish to use start or end as your offset then enter the following details:
	
	   a. Header Count: Specifies how many headers from the offset, the application should remove. The minimum supported value is 1 and the maximum is 32.
	
	   b. Custom Len: The length (in bytes) of the header that should be stripped. The minimum supported value is 1 and the maximum supported value is 1500.
	
	   c. Ah2: The next possible standard header that occurs immediately after the header

Load Balancing

Load balancing application performs stateless distribution of the packets between different endpoints. Stateless load balancing distributes the processed traffic to multiple tool ports or tunnel endpoints based on hash values generated from predefined protocol fields in the packet.

To add a load balancing application:

1. Drag and drop **Load Balancing** from **APPLICATIONS** to the graphical workspace.
2. Click the load balancing application and select **Details**. The Application quick view appears.

3. In the Application quick view, enter the information as follows:

Metric	Description
Alias	Enter a name for the load balancing application
Hash Field	• **ipOnly** : The source IP and destination IP addresses. • **ipAndPort**: The source IP and destination IP addresses, and Layer 4 source port and destination port numbers. • **fiveTupl**e: The source IP and destination IP addresses, source port and destination port numbers, and protocol field in the IP header. • **gtpuTeid**: The GTP-u tunnel identifier (ID). NOTE: There is no inner or outer field location for `GTPU-TEID`.
Field Location	• **Outer**: The first occurrence of header or field. For example, **IP Only outer** is the first IP header in the packet, which could be IPv4 or IPv6. • **Inner**: The second occurrence of header or field. The supported IP encapsulation types are: IP-in-IP, VXLAN, GTP, GRE, and ERSPAN.
Load balancing groups	Add or remove an application with the Endpoint ID and Weight value (1-100). A load balancing group can have minimum of two endpoints.

4. Click **Save**.

Masking

Masking lets you overwrite specific packet fields with a specified pattern so that sensitive information is protected during network analysis. Masking operations consist of an **offset**, **length**, and **pattern**.

To add a masking application:

1. Drag and drop **Masking** from **APPLICATIONS** to the graphical workspace.
2. Click the Masking application and select **Details**. The Application quick view appears.
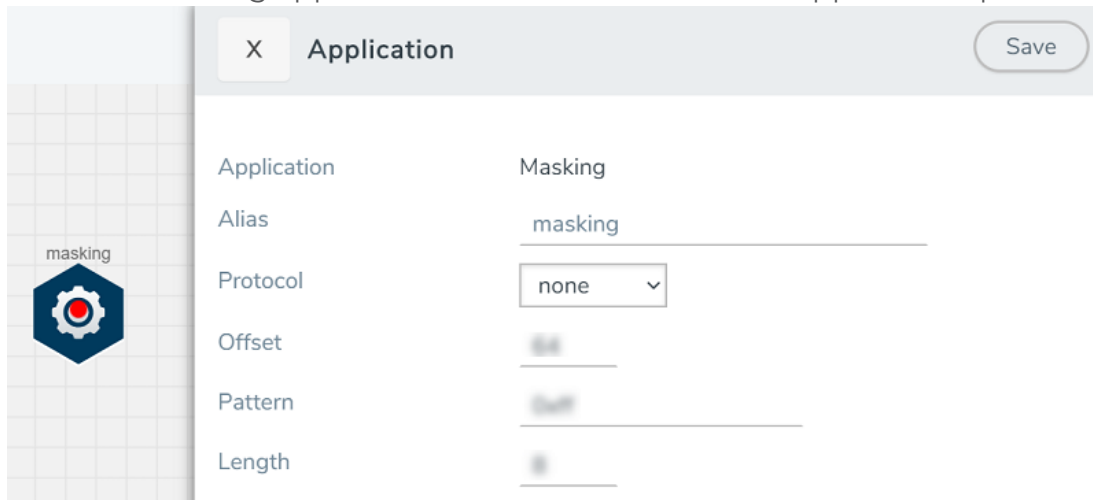
3. In the Application quick view, enter the information as follows:

Component	Description
Alias	Enter a name for the masking application.
Protocol	The following are the protocols that you can select for from the protocol drop-down list: ○ **None** – Mask starting a specified number of bytes from the start of the packet. ○ **IPV4** – Mask starting a specified number of bytes after the IPv4 header. ○ **IPV6** – Mask starting a specified number of bytes after the IPv6 header. ○ **UDP** – Mask starting a specified number of bytes after the UDP header. ○ **TCP** – Mask starting a specified number of bytes after the TCP header. ○ **ftp-data**– Identify using TCP port 20. Mask payloads using offset from the TCP header. ○ **https** – Identify using TCP port 443. Mask payloads using offset from the TCP header. ○ **SSH** – Identify using TCP port 22. Mask payloads using offset from the TCP header. ○ **GTP** – Mask starting a specified number of bytes after the outer GTP header. ○ **GTP-IPV4** – Mask starting a specified number of bytes after the IPv4 header inside the encapsulating GTP packet. ○ **GTP-UDP** – Mask starting a specified number of bytes after the UDP header inside the encapsulating GTP packet. ○ **GTP-TCP** – Mask starting a specified number of bytes after the TCP header inside the encapsulating GTP packet.
Offset	Specifies **where** the application should start masking data with the supplied pattern. You can specify this in terms of either a static offset from the start of the packet or a relative offset from a particular protocol layer. This lets you automatically compensate for variable length headers, specifying a mask target in terms of a particular packet header.
Length	Specifies **how much** of the packet should be masked. The specified one-byte pattern can be repeated to mask from 1-9600 bytes.
Pattern	Specifies **what** pattern the application should use to mask the specified portion of the packet. You can specify a one-byte hex pattern (for example, 0xFF).

4. Click **Save**.

Passive SSL Decryption

GigaVUE V Series 2 nodes support Secure Sockets Layer (SSL) decryption. SSL is a cryptographic protocol that adds security to TCP/IP communications such as Web browsing and email. The protocol allows the transmission of secure data between a server and client who both have the keys to decode the transmission and the certificates to verify trust between them. Passive SSL decryption delivers decrypted traffic to out-of-band tools that can then detect threats entering the network.

> **NOTE:** Passive SSL Decryption is called as SSL Decrypt on GigaVUE V Series 2.

Configure Passive SSL Decryption

To configure passive SSL Decryption on V Series 2, follow the steps given below:

Prerequisite: Register the nodes on the Third Party Orchestration Monitoring Domain using the VMware ESXi host. Refer Configure GigaVUE V Series Nodes using VMware ESXi for more detailed information.

Upload SSL Keys

To upload an SSL private key, do the following:

1. On the left navigation pane, select **Inventory >Resources > Security** to open the Security page. Select SSL Keys on the top navigation bar.
2. Click **Add**. The **Create SSL Key** page appears.
3. In the **Create SSL Key** page, enter the following details:
   - For **Alias**, enter an alias for the SSL key.
   - For **Description**, enter any additional information for the SSL key.
   - For **Key Upload Type**, select **PEM** or **PKCS12**.
   - (optional) For **Passphrase**, enter a passphrase for the key.
   - Select a **Private Key** by pasting the copied key in PEM format or installing from URL or installing from local directory.
   - Select a **Certificate** by pasting the copied key in PEM format or installing from URL or installing from local directory.
     > **NOTE:** Install from URL option only supports scp protocol.
4. Click **Save**.

> **NOTE:** Passive SSL Decryption on V Series 2 does not support HSM.

Delete SSL Keys

To delete a particular SSL key select the key on the SSL Keys page, and then select Delete. To delete all SSL Keys, select the **Delete All** button.

Create SSL Service

After you have uploaded a private key, you can add a service. A service maps to a physical server, such as an HTTP server. One server can run multiple services. A service is a combination of an IP address and a server port number. Also, the key and the service must be tied together.

Prerequisite

Before creating a service, upload a private key as described in Upload SSL Keys

To create a service, do the following:

1. On the left navigation pane, select **Inventory >Resources > Security** to open the Security page. Select SSL Service on the top navigation bar.The SSL Services page appears.

2. Click **Add**.

3. On the SSL Service configuration page, do the following:

   ○ Enter an alias.
   ○ Enter the information for the service: Server IP Address, Server Port.

4. Click **Save**.

Delete SSL Service

To delete a particular SSL service select the service on the SSL Services page, and then select Delete. To delete all SSL services, select the **Delete All** button.

Notes about Private Keys and Passwords

Consider the following notes about private keys and passwords:

- Encrypted private keys are stored on the node. When a private key is uploaded, it is encrypted with a password before it is stored, therefore keys are password-protected. Keychain passwords are not stored on the node.

- Because only encrypted private keys are stored on the node and because the keychain password is not stored on the node, after any node reboot you will be prompted to enter the password. Until the password is entered, Passive SSL decryption is not working.

- Key content cannot be displayed.

- Keys that are synchronized across a cluster are encrypted.

Key Mapping

After adding the SSL Service, now you map the private key with the service using Key Mapping.

To map a key with the service, follow the steps given below,

1. On the left navigation pane, select **Inventory >Resources > Security** to open the Security page. Select **SSL Key Mapping** on the top navigation bar.
2. Click **Add**.
3. Enter the Key Mapping Alias.
4. Select the SSL Service and Key Alias from the drop-down.
5. Click **Save**.

Delete SSL Key Mappings
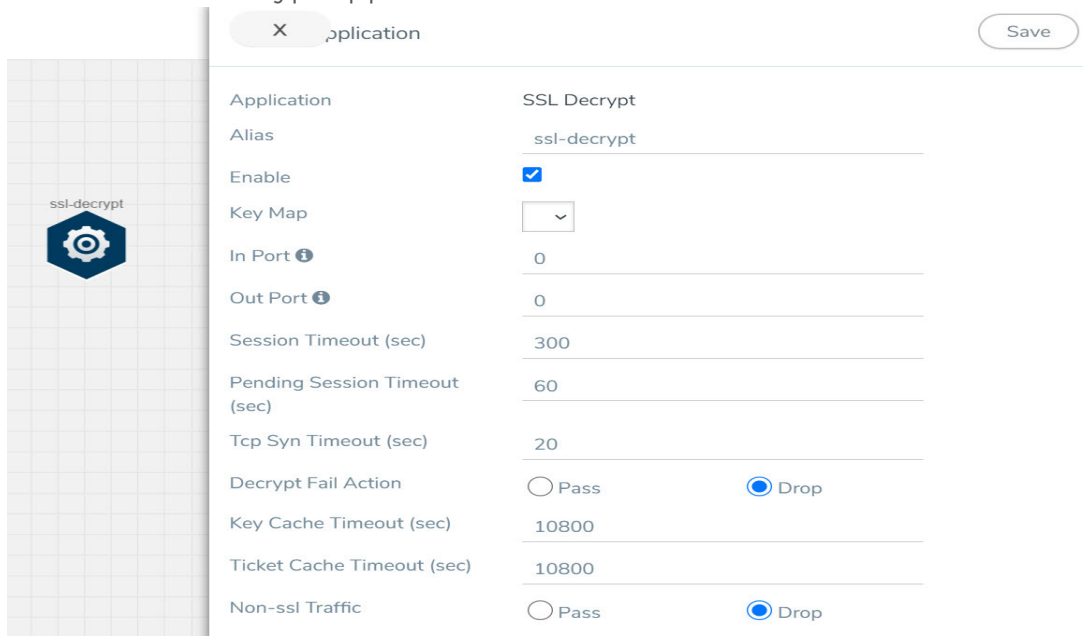
To delete a particular SSL key map select the key mapping on the SSL Key Mapping page, and then select Delete. To delete all SSL Key Mapping, select the **Delete All** button.

Add SSL Decrypt to Monitoring Session

After mapping your keys with service, to add GigaSMART applications to V series 2, follow the steps given below,

1. Create a new monitoring session. Refer to Create New Session for more detailed instructions.
2. Drag and drop **SSL Decrypt** from APPLICATIONS to the graphical workspace.

3. Click the SSL Decrypt application and select **Details**.

Application	SSL Decrypt
Alias	ssl-decrypt
Enable	☑
Key Map	⌄
In Port ⓘ	0
Out Port ⓘ	0
Session Timeout (sec)	300
Pending Session Timeout (sec)	60
Tcp Syn Timeout (sec)	20
Decrypt Fail Action	○ Pass ● Drop
Key Cache Timeout (sec)	10800
Ticket Cache Timeout (sec)	10800
Non-ssl Traffic	○ Pass ● Drop

4. Select the **Enable** checkbox to enable the application.
5. Select the **Key Map** (created in the previous step) from the drop-down.
6. Click **Save**.
7. Click **Deploy**. The Select nodes to deploy the monitoring session page appears.
8. Select the nodes you want to deploy and select an interface for each node. Then, click **Deploy**.

View Application Statistics

After adding SSL Decrypt to the monitoring session, to view the application statistics, open the **Monitoring Session Statistics** page. Refer to View Statistics for more detailed information.

1. Click **View Monitoring Session Diagram**. The monitoring session diagram appears, click the SSL Decrypt application.
2. The ssl-decrypt application statistics page appears.

3. You can view the following in the SSL application statistics page:

    - **Application**: The application statistics are displayed here.
    - **Sessions**: To view the session summary and session details of the SSL Decryption application, select the V Series Node IP and enter the Server Name and Client/ Server IP address. Then click Apply.
    - **Server Certificates**: To view the server certificate statistics, select the V Series Node IP from the drop-down and enter the Key Alias. Then, click Apply.
    - **Services**: All the service related statistics are displayed here. To view the statistics, select the V Series Node IP and the Service Alias from the drop-down and click Apply.
    - **Error Codes**: The error messages are displayed here.

Server Certificates, Services and Error Codes pages has **Refresh** and **Reset** button, which helps you to refresh and reset the statistics.

PCAPng Application

The PCAPng application reads the various blocks in the received PCAPng files and validates the blocks to be sent to the destination application or to the tools. The PCAPng file contains the following blocks:

- Mandatory Blocks
    - Section Header Block (SHB)
- Optional Blocks
    - Interface Description Block (IDB)
    - Enhanced Packet Block (EPB)
    - Simple Packet Block
    - Name Resolution Block
    - Interface Statistics Block

> **NOTE:** The PCAPng application is only applicable for the Ericsson 5G Core vTAP architecture. for detailed information.

The actual packets are present in the Enhanced Packet Block. The block data is parsed to find the start and end offset of the valid packets and the packet is sent out to the next application.

> **NOTE:** Only one EPB in a PCAPng file is supported.

The PCAPng application processes the data depending on the packet type that contains a combination of the blocks mentioned above:

Block Combination	Process
SHB+IDB+EPB+data	Packets are parsed, validated, and the data packet is sent out.
SHB+IDB	Packets are dropped.
EPB+Data	Packets are parsed, validated, and the data packet is sent out.

The PCAPng application validates if the incoming data matches any of the above three formats in the same order, and processes the packets accordingly.

The following figure shows a sample PCAPng file format that contains one section header block:
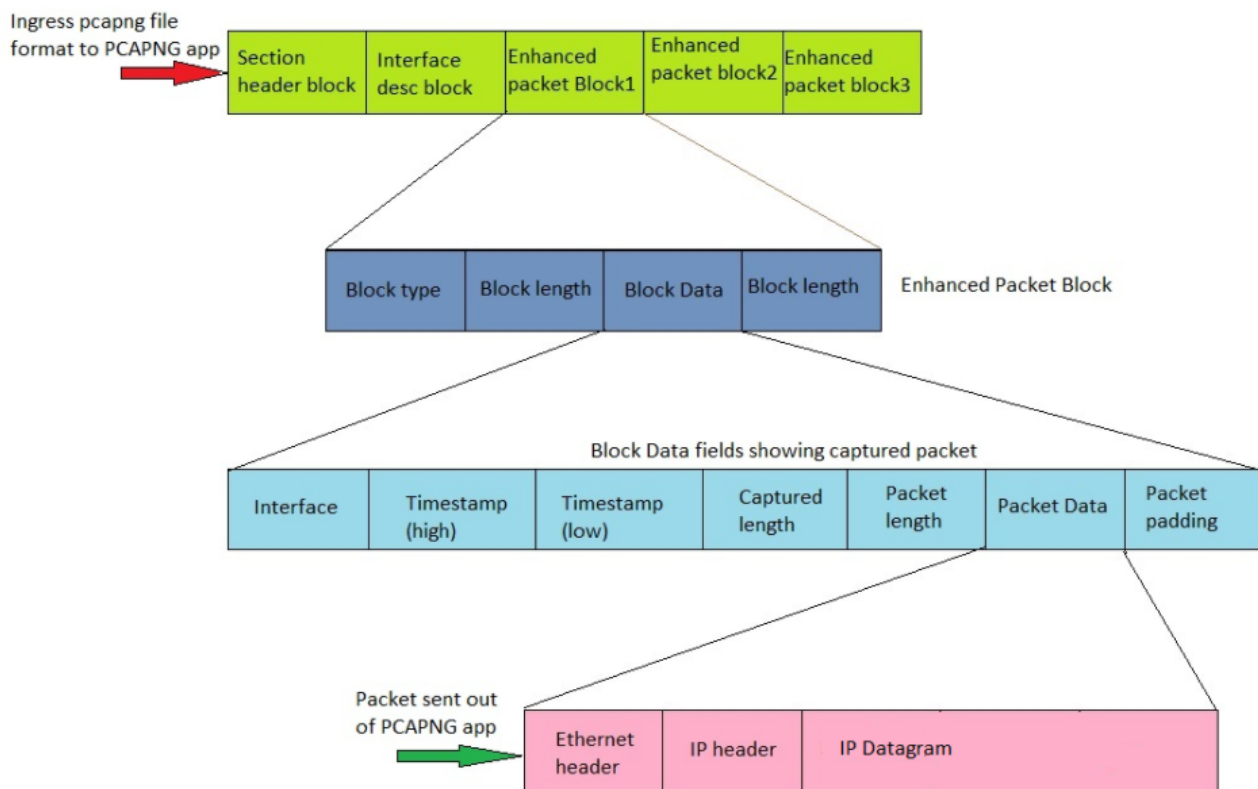
Create Link Between UDP-in-GRE Tunnel and PCAPng Application

To create a link with source as UDP-in-GRE tunnel and destination as PCAPng application:

1. In the GigaVUE-FM canvas, select **New > New Tunnel**, drag and drop a new tunnel template to the workspace. The **Add Tunnel Spec** quick view appears.

2. On the New Tunnel quick view, enter or select the required information as described in the following table.

Field	Description
Alias	The name of the tunnel endpoint **NOTE:** Do not enter spaces in the alias name.
Description	The description of the tunnel endpoint
Type	Select **UDPGRE** as the tunnel type
Traffic Direction	The direction of the traffic flowing through the V Series node • Choose **In** (Decapsulation) for creating an Ingress tunnel, traffic from the source to the V Series node
IP Version	The version of the Internet Protocol. Select IPv4 or IPv6
Remote Tunnel IP	The IP address of the tunnel source
Key	GRE key value
Source L4 Port	Layer 4 source port number
Destination L4 Port	Layer 4 destination port number. You can configure only 4754 or 4755 as the destination UDP ports

3. Click **Save**.

4. Click and drag the PCAPng application into the canvas. Configure the alias for the application.

5. Establish a link between the UDP-GRE TEP configured above and the PCAPng application.

Create Link Between PCAPng Application and Other Destinations

Create a link with source as PCAPng application and destination as one of the following:

- Other GigaSMART applications such as Slicing, Masking, etc.
- Other encapsulation TEPs.
- REP/MAP

Refer to the following image for a sample configuration.

5G-Service Based Interface Application

5G-Core is a service-based architecture, in which many control plane network functions are available and communication across these network functions happens through HTTP2 protocol. These HTTP2 transactions are mirrored using some specific network functions, which are in JSON encoded format.

5G-Service Based Interface (SBI) Application synthesizes the HTTP2 transactions with proper L2, L3, and L4 headers from the JSON encoded data that it receives from the UDP-GRE or VXLAN ingress TEPs (Tunnel End Point). Once the headers are synthesized and a complete HTTP2 transaction is formed, the packets are sent to the egress TEP and then sent to the physical or virtual probes.

In Nokia 5G core network, the traffic is mirrored between control functions using HTTP2 protocol, which is mirrored from a service called SCP (Service Control Proxy) a centralised point through which all the communications between all the control plane functions pass. Hence, it becomes the right place to mirror the traffic.

Traffic mirrored here doesn't have enough information about the entire TCP flow information between them. It only has information about request and response details between the control functions. Since the tools cannot infer much with this request and response information alone, it is required to have the entire flow information from TCP handshake to TCP connection close to form a complete TCP flow information that can be sent to the tools.

In Ericsson 5G core, there is a software probe that is used for monitoring the traffic. It captures the traffic, encapsulates it in UDP-GRE, and forwards it to V Series nodes. Here it converts the HTTP2 transactions into JSON data and a set of TCP messages are captured as PCAPng file, which is encapsulated into UDP-GRE with proto ID 0x8047 and is sent to V Series.

In either case, these are not raw packets that any tools can understand. In the case of Nokia, it doesn't have TCP session information, whereas Ericsson has the session information, but they are in a JSON encoded format. In both cases, it can't be forwarded to tools directly. Hence, we need to synthesize those packets, by adding additional information, such as TCP 3-way handshake, L2 headers and form a TCP flow information that could be forwarded to the tools.

In some versions of Nokia or Ericsson 5G Cores, the IP addresses present in the encoded message is not reliable and the SBI application converts the strings in the form of instance ID (in case of Ericsson) or producer ID (in case of Nokia) to an IP address from the string-IP mapping table.

The instance ID or producer ID must be provided in the form of CSV file. You can upload the CSV file through GigaVUE-FM.
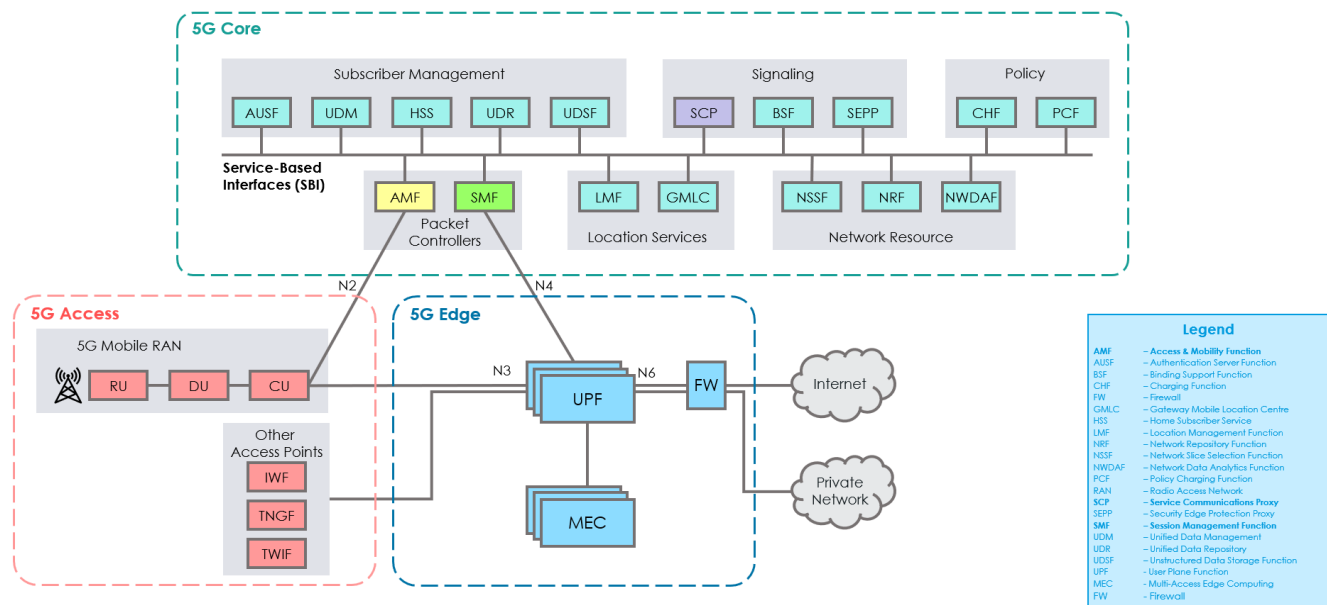

How SBI Application works

In the V series, the SBI application receives the HTTP2 transaction messages as JSON encoded data from any of the following sources:

- VxLAN TEP – In 5G-Nokia, the application receives the JSON encoded data from the VXLAN ingress TEPs

- PCAPng application - In 5G-Ericson, the application receives the JSON encoded data from the PCAPng application, whereas the PCAPng application receives the data from the UDP-GRE TEP.

In the SBI application, JSON encoded data traffic is further parsed to extract the source-destination information and is used to synthesize the complete HTTP2 transaction with proper L2, L3, and L4 headers and HTTP2 headers and HTTP2 body of the original HTTP2 transactions. Once the headers are synthesized and a complete HTTP2 transaction is formed, the packets are then given to the egress TEP to send it to the physical/virtual probes.

The following figure shows the block diagram of the data flow in the V Series containing the SBI application.
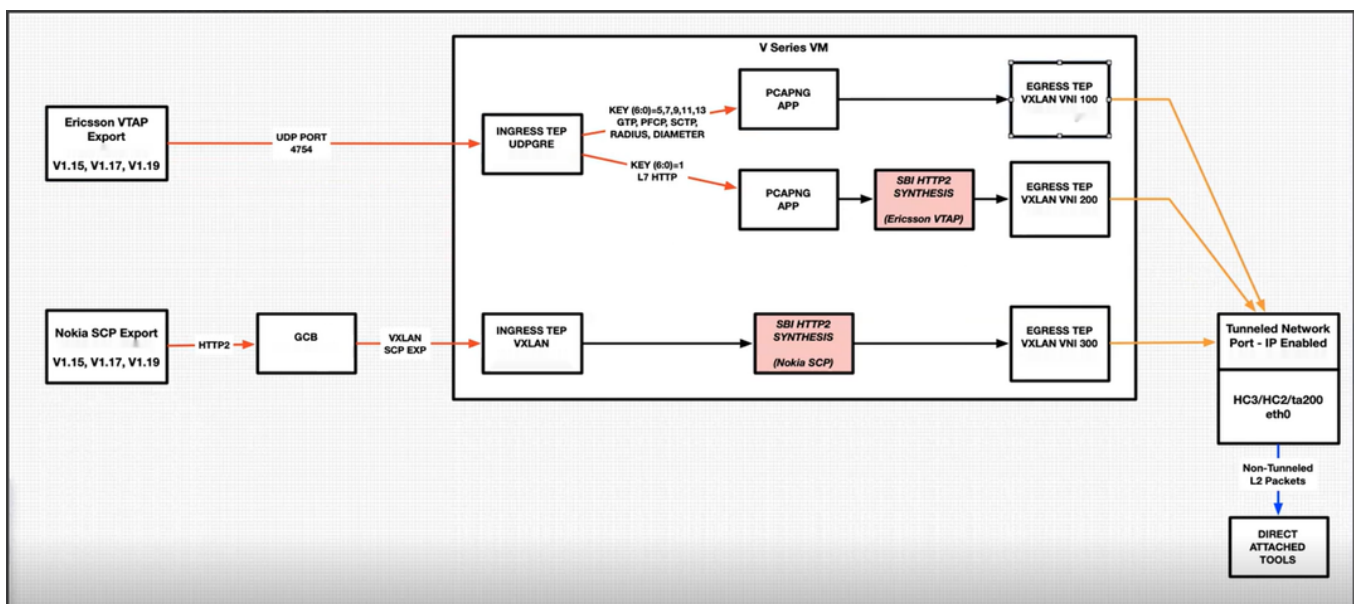
Supported Platforms:

The application is supported on the following platforms:

- VMware
- OpenStack

Rules and Notes

- The maximum number of HTTP2 headers (in the synthesized HTTP2 transactions) that is supported is 64.
- The PCAPng application that is linked to 5G-SBI application (on the right side) should only be linked to UDP-GRE TEP with key value 1 on the left side. If it is linked to other UDP-GRE TEPs(key values other than 1), then the behavior cannot be defined and leads to unexpected result.

- The maximum number of NF entries supported is 4K.

Configuration of 5G-SBI Application

In V Series, 5G-SBI application receives all the mirrored traffic from any of the following sources:

- 5G-Nokia SCP
- 5G-Ericsson

In GigaVUE-FM, the application has a field **type**, which determines whether the data is collected from 5G-Nokia or 5G-Ericsson. Based on the **type** configured, the packets received are processed.

For example, in the case of 5G-Nokia this application reads the headers (source ip/port, destination ip/port), packet type (request or response) information from the HTTP2 message. Based on the retrieved information it synthesises a TCP flow.

In the case of 5G-Ericsson, after receiving the packets from the TEP, the packets are forwarded to PCAPng application for parsing. After parsing, the JSON type data from PCAPng has the information such as source ip/port, destination ip/port, message type. Using this information HTTP2 transaction can be synthesised.

In GigaVUE-FM, to configure the 5G-SBI application refer to any of the following sections based on the source type:

- Configuration of 5G-SBI application for 5G-Nokia
- Configuration of 5G-SBI application for 5G-Ericsson

Configuration of 5G-SBI application for 5G-Nokia

In GigaVUE=FM, for 5G-Nokia, you must do the following to add the 5G-SBI application in the monitoring session of a monitoring domain in the V Series:

S.No	Steps	Refer to
1	Create VXLAN Ingress TEP to receive the HTTP2 post messages from GCB/UCT in a monitoring session.	Create Tunnel Endpoints
2	Add 5G-SBI Application (HTTP2 header synthesis) in the monitoring session.	
3	Create a link between VXLAN ingress TEP and 5G-SBI Application.	
4	Create egress TEP.	Create Tunnel Endpoints
5	Create a link between 5G-SBI Application (HTTP2 header synthesis) and Egress TEP.	
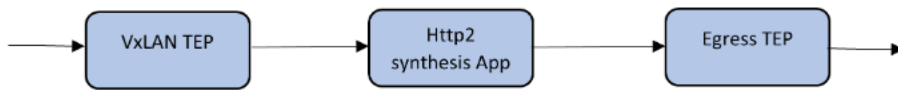
Adding 5G-SBI Application in 5G-Nokia

Prerequisites

The pre-requisite to add a 5G-SBI application in 5G-Nokia is:

- You must upload CSV file containing a valid FQDN name and a valid IPv4/IPv6 address. To upload the CSV file refer Adding CSV file for IP mapping.

You can add a 5G-SBI application for:

- New monitoring session - You can add the 5G-SBI application after creating a new monitoring session and when the canvas appears.
- Existing session - Click **Edit** on existing monitoring session, the GigaVUE-FM canvas appears.

To add a 5G-SBI application:

1. In the canvas, Drag and drop 5G-SBI application and select **Details**. The Application quick view appears.

2. On the Application quick view, enter or select the required information as described in the following table:

Field	Description
Application	The name **5g-sbi** appears by default.

Alias	The name **sbi5gAppTemplate** appears by default.
Type	Select the option **SCPviaGCB**from the drop-down list
Indexed Headers	Enable the checkbox to index the headers.
Compressed Headers	Enable the checkbox to compresss the headers.
Ip Mapping	Select the required CSV file from the drop-down list with FQDN name. Refer to Adding CSV file for IP mapping to get the required CSV file in the drop-down list. **NOTE:** In case of inadequate information (i.e., NF lookup failure), the appropriate counter is incremented and the synthesized packet is sent out with inappropriate IP address.
Mode	Nokia SCP is selected by default
Number of SCP Flows	Specify the range of SCP flow (The request ID and producer ID forms a SCP flow). The mininum value is 128. The maximum value is 16000. The default vaule is 2000.
Request Timeout	Specify the time for the request packet to wait for the response packet in the flow. The minimum value is 1 second and the maximum value is 300 seconds. The default value is 10 seconds.
Response Timeout	Specify the time for the response packet to wait for the request packet in a stream. The minimum value is 1 second and the maximum value is 300 seconds. The default value is 10 seconds.
Nokia Use 3Gpp Target API Root	When detecting Producer IP/FQDN, treat the 3GPP Target API Root to be predictive of the Producer IP if the value is non-zero. The default value is 1.
Thresholds	Specify the threshold value to configure the packet-drop settings.
Threshold Templates	Select the threshold template..
Time Interval	Select the time interval in seconds.

Rules and Notes

- The following configuration parameters are non-editable and it can be configured only during the initial configuration:
  - type
  - mode
  - eevtapVersion
  - numTCPFlows
  - numStreamsPerFlow
  - numSCPFlows

Configuration of 5G-SBI application for 5G-Ericsson

In-GigaVUE-FM, for 5G-Ericsson, you must do the following to configure the 5G-SBI application in the monitoring session of a monitoring domain in the V Series:

S.No	Steps	Refer to
1	Configure UDP-GRE Ingress TEP to receive the HTTP2/L7-JSON messages.	Create Tunnel Endpoints
2	Configure multiple other TEPs for other control protocol PDUs.	
3	Configure two instances of PCAPng application and link ingress TEPs and PCAPng application instances.	
4	Add 5G-SBI Application (HTTP2 header synthesis) in the monitoring session.	
5	Create a link between TEP and 5G-SBI Application.	
6	Create egress TEP.	Create Tunnel Endpoints
7	Create a link between PCAPng and egress TEPs or SBI and egress TEPs.	
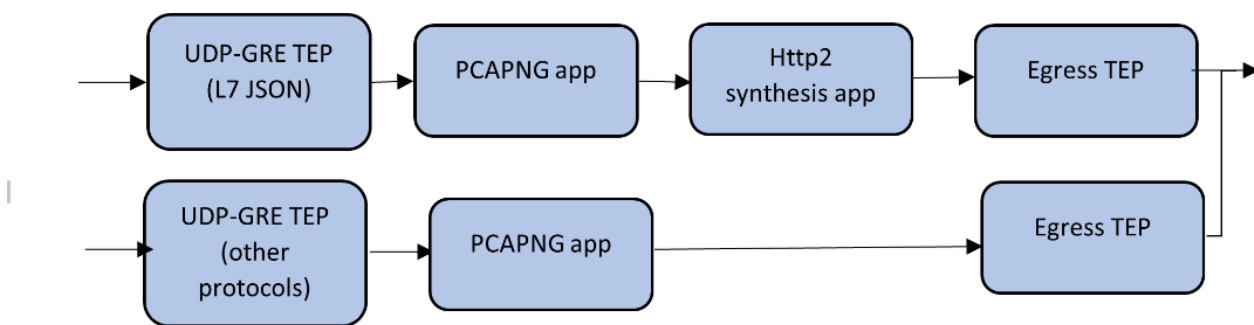
Adding 5G-SBI Application in 5G-Ericsson

Prerequisites

The pre-requisite to add a 5G-SBI application in Ericsson is:

- You must upload a CSV file containing a valid Network Function Instance ID (NFID) and a valid IPv4/IPv6 address. To upload the CSV file.

You can add a 5G-SBI application for:

- New monitoring session - You can add the 5G-SBI application after creating a new monitoring session and when the canvas appears.
- Existing session - Click **Edit** on existing monitoring session, the GigaVUE-FM canvas appears.

To add a 5G-SBI application:

1. In the canvas, Drag and drop 5G-SBI application and select **Details**. The Application quick view appears.

2. On the Application quick view, enter or select the required information as described in the following table:

Field	Description
Application	The name **5g-sbi** appears by default.
Alias	The name **sbi5gAppTemplate** appears by default.
Type	Select the option **ericssonVTap**from the drop-down list.
Indexed Headers	Enable the checkbox to index the HTTP2 headers in the 5G-SBI application.
Compressed Headers	Enable the checkbox to compress the HTTP2 headers in the 5G-SBI application.
Ip Mapping	Select the required CSV file from the drop-down list with required Network Function Instance ID (NFID) instance mapping. Refer to Adding CSV file for IP mapping to get the required CSV file in the drop-down list.
Mode	L7json is selected by default. L7native is not supported in 6.1
EEV Tap Version	Select 1 or 2 from the drop-down list box.
TCP Flows	Specify the concurrent TCP flow range. The minimum value is 128 seconds, and the maximum value is 16000 seconds. The default value is 1000 seconds.
TCP Flow Timeout	Specify the flow range for which the TCP flow should remain valid in the application. The minimum value is 0 and the maximum value is 7200 seconds. The default value is 1800 seconds
Number of Streams per Flow	Specify the Number of Streams per flow. The minimum value is 1. The maximum value is 1024. The default value is 256.
Request Timeout	Specify the time for the request packet to wait for the response packet

	in a stream. The minimum value is 1 second and the maximum value is 300 seconds. The default value is 10 seconds.
Response Timeout	Specify the time for the response packet to wait for the request packet in a stream. The minimum value is 1 second and the maximum value is 300 seconds. The default value is 10 seconds.
Threshold Templates	Select the threshold template.
Time Interval	Select the time interval in seconds.

Adding CSV file for IP mapping

To add the CSV file for IP mapping:

3. Go to **Inventory > VIRTUAL >** select your cloud platform, and then click **Settings > 5G-SBI**. The Proxy Server Configuration page appears.

4. Select any of the following from the **Type** as per the requirement:

    o   **SCPviaGCP** - Adding the CSV file containing a valid FQDN name and a valid IPv4/IPv6 address for IP mapping in 5G-Nokia.

    o   **ericcsonVTap** - Adding the CSV file containing a valid NF-instance ID and a valid IPv4/IPv6 address for IP mapping in 5G-Ericsson.

5. Enter the name for the CSV file in the **Alias** field.

6. Click **Choose File** in **FileName** field to upload the CSV file into GigaVUE-FM.

7. Click **Save** to add the CSV file.

Slicing

Packet slicing allows you to truncate packets after a specified header and slice length, preserving the portion of the packet required for monitoring purposes. Slicing operations are typically configured to preserve specific packet header information, allowing effective network analysis without the overhead of storing full packet data.

Packets can have multiple variable-length headers, depending on where they are captured, the different devices that have attached their own headers along the way, and the protocols in use (for example, IPv4 versus IPv6). Because of this, slicing operations with a hard-coded offset will not typically provide consistent results.

To address this, the slicing application lets you configure packet slicing using protocols which allows you to start slicing from a particular number of bytes after a specific packet header (IPv4, IPv6, UDP, and so on). The slicing application parses through Layer 4 (TCP/UDP) to identify the headers in use, slicing based on the variable offset identified for a particular header instead of a hard-coded number of bytes.

To add a slicing application:

1. Drag and drop **Slicing** from **APPLICATIONS** to the graphical workspace.
2. Click the Slicing application and select **Details**. The Application quick view appears.
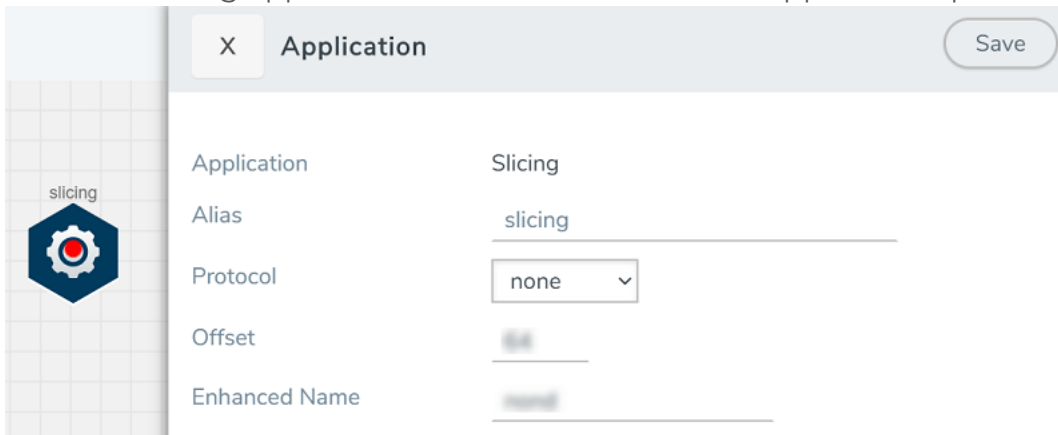
3. In the Application quick view, enter the information as follows:

Feature	Description
Alias	Enter a name for the application.
Protocol	The following are the protocols that you can select for from the protocol drop-down list: ○ **None** –Slice starting a specific number of bytes from the start of the packet. ○ **IPV4** – Slice starting a specified number of bytes after the IPv4 header. ○ **IPV6** – Slice starting a specified number of bytes after the IPv6 header. ○ **UDP** – Slice starting a specified number of bytes after the UDP header. ○ **TCP** – Slice starting a specified number of bytes after the TCP header. ○ **FTP** – Identify using TCP port 20 and slice payloads using offset from the TCP header. ○ **HTTPS** – Identify using TCP port 443. Slice encrypted payloads using offset from the TCP header. ○ **SSH** – Identify using TCP port 22. Slice encrypted payloads using offset from the TCP header. The slicing application can provide slicing for GTP tunnels, provided the user payloads are unencrypted. Both GTPv1 and GTPv2 are supported – GTP' (GTP prime) is not supported. Keep in mind that only GTP-u (user plane packets) are sliced. Control plane packets (GTP-c) are left unmodified because of their importance for analysis. ○ **GTP** – Slice starting a specified number of bytes after the outer GTP header. ○ **GTP-IPV4** – Slice starting a specified number of bytes after the IPv4 header inside the encapsulating GTP packet. ○ **GTP-UDP** – Slice starting a specified number of bytes after the UDP header inside the encapsulating GTP packet. ○ **GTP-TCP** – Slice starting a specified number of bytes after the TCP header inside the encapsulating GTP packet.
Offset	Specify the length of the packet that must be sliced.

4. Click **Save**.

Additional Sources of Information

This appendix provides additional sources of information. Refer to the following sections for details:

- Documentation
- Documentation Feedback
- Contact Technical Support
- Contact Sales
- The VÜE Community

Documentation

This table lists all the guides provided for GigaVUE Cloud Suite software and hardware. The first row provides an All-Documents Zip file that contains all the guides in the set for the release.

> **NOTE:** In the online documentation, view What's New to access quick links to topics for each of the new features in this Release; view Documentation Downloads to download all PDFs.

Table 1: Documentation Set for Gigamon Products

GigaVUE Cloud Suite 6.2 Hardware and Software Guides
DID YOU KNOW? If you keep all PDFs for a release in common folder, you can easily search across the doc set by opening one of the files in Acrobat and choosing **Edit > Advanced Search** from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.
Hardware   how to unpack, assemble, rack-mount, connect, and initially configure ports the respective GigaVUE Cloud Suite devices; reference information and specifications for the respective GigaVUE Cloud Suite devices
GigaVUE-HC1 Hardware Installation Guide
GigaVUE-HC2 Hardware Installation Guide
GigaVUE-HC3 Hardware Installation Guide
GigaVUE-HC1-Plus Hardware Installation Guide
GigaVUE-TA25E Hardware Installation Guide
GigaVUE-TA200E Hardware Installation Guide
GigaVUE-TA25 Hardware Installation Guide

GigaVUE Cloud Suite 6.2 Hardware and Software Guides
GigaVUE-TA200 Hardware Installation Guide
GigaVUE-TA400 Hardware Installation Guide
GigaVUE-TA10 Hardware Installation Guide
GigaVUE-TA40 Hardware Installation Guide
GigaVUE-TA100 Hardware Installation Guide
GigaVUE-TA100-CXP Hardware Installation Guide
GigaVUE-OS Installation Guide for DELL S4112F-ON
G-TAP A Series 2 Installation Guide
GigaVUE M Series Hardware Installation Guide
GigaVUE-FM Hardware Appliance Guide for GFM-HW1-FM010 and and GFM-HW1-FM001-HW
Software Installation and Upgrade Guides
GigaVUE-FM Installation, Migration, and Upgrade Guide
GigaVUE-OS Upgrade Guide
GigaVUE V Series Migration Guide
Fabric Management and Administration Guides
GigaVUE Administration Guide covers both GigaVUE-OS and GigaVUE-FM
GigaVUE Fabric Management Guide how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features
Cloud Guides how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms
*GigaVUE V Series Applications Guide
GigaVUE V Series Quick Start Guide
GigaVUE Cloud Suite for AWS–GigaVUE V Series 2 Guide
GigaVUE Cloud Suite for Azure–GigaVUE V Series 2 Guide
GigaVUE Cloud Suite for OpenStack–GigaVUE V Series 2 Guide
*GigaVUE Cloud Suite for Nutanix Guide—GigaVUE V Series 2 Guide
GigaVUE Cloud Suite for VMware—GigaVUE V Series Guide

GigaVUE Cloud Suite 6.2 Hardware and Software Guides
*GigaVUE Cloud Suite for Third Party Orchestration
GigaVUE Cloud Suite for AnyCloud Guide
Universal Container Tap Guide
Gigamon Containerized Broker Guide
GigaVUE Cloud Suite for AWS–GigaVUE V Series 1 Guide
GigaVUE Cloud Suite for Azure–GigaVUE V Series 1 Guide
GigaVUE Cloud Suite for OpenStack–GigaVUE V Series 1 Guide
GigaVUE Cloud Suite for Nutanix Guide—GigaVUE-VM Guide
GigaVUE Cloud Suite for VMware—GigaVUE-VM Guide
Reference Guides
GigaVUE-OS CLI Reference Guide library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE HC Series and TA Series devices
GigaVUE-OS Cabling Quick Reference Guide guidelines for the different types of cables used to connect Gigamon devices
GigaVUE-OS Compatibility and Interoperability Matrix compatibility information and interoperability requirements for Gigamon devices
GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide samples uses of the GigaVUE-FM Application Program Interfaces (APIs)
Release Notes
GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, G-TAP A Series, and GigaVUE Cloud Suite Release Notes new features, resolved issues, and known issues in this release ; important notes regarding installing and upgrading to this release NOTE: Release Notes are not included in the online documentation. NOTE: Registered Customers can log in to My Gigamon to download the Software and Release Notes from the Software & Docs page on to My Gigamon. Refer to How to Download Software and Release Notes from My Gigamon.
In-Product Help
GigaVUE-FM Online Help how to install, deploy, and operate GigaVUE-FM.

How to Download Software and Release Notes from My Gigamon

Registered Customers can download software and corresponding Release Notes documents from the **Software & Release Notes** page on to My Gigamon. Use the My Gigamon Software & Docs page to download:

- Gigamon Software installation and upgrade images,
- Release Notes for Gigamon Software, or
- Older versions of PDFs (pre-v5.7).

To download release-specific software, release notes, or older PDFs:

1. Log in to My Gigamon
2. Click on the **Software & Release Notes** link.
3. Use the **Product** and **Release** filters to find documentation for the current release. For example, select Product: "GigaVUE-FM" and Release: "5.6," enter "pdf" in the search box, and then click **GO** to view all PDF documentation for GigaVUE-FM 5.6.xx.

> **NOTE:** My Gigamon is available to registered customers only. Newer documentation PDFs, with the exception of release notes, are all available through the publicly available online documentation.

Documentation Feedback

We are continuously improving our documentation to make it more accessible while maintaining accuracy and ease of use. Your feedback helps us to improve. To provide feedback and report issues in our documentation, send an email to: documentationfeedback@gigamon.com

Please provide the following information in the email to help us identify and resolve the issue. Copy and paste this form into your email, complete it as able, and send. We will respond as soon as possible.

Documentation Feedback Form		
About You	**Your Name**	
	Your Role	
	Your Company	

For Online Topics	Online doc link	*(URL for where the issue is)*
	Topic Heading	*(if it's a long topic, please provide the heading of the section where the issue is)*
For PDF Topics	Document Title	*(shown on the cover page or in page header)*
	Product Version	*(shown on the cover page)*
	Document Version	*(shown on the cover page)*
	Chapter Heading	*(shown in footer)*
	PDF page #	*(shown in footer)*
How can we improve?	Describe the issue	*Describe the error or issue in the documentation.* *(If it helps, attach an image to show the issue.)*
	How can we improve the content? Be as specific as possible.	
	Any other comments?	

Contact Technical Support

For information about Technical Support: Go to **Settings** ⚙ **> Support > Contact Support** in GigaVUE-FM.

You can also refer to https://www.gigamon.com/support-and-services/contact-support for Technical Support hours and contact information.

Email Technical Support at support@gigamon.com.

Contact Sales

Use the following information to Gigamon channel partner or Gigamon sales representatives.

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

Partners: www.gigamon.com/partners.html

Premium Support

Email Gigamon at inside.sales@gigamon.com for information on purchasing 24x7 Premium Support. Premium Support entitles you to round-the-clock phone support with a dedicated Support Engineer every day of the week.

The VÜE Community

The VÜE Community is a technical site where Gigamon users, partners, security and network professionals and Gigamon employees come together to share knowledge and expertise, ask questions, build their network and learn about best practices for Gigamon products.

Visit the VÜE site to:

- Find knowledge base articles and documentation
- Ask and answer questions and learn best practices from other members.
- Join special-interest groups to have focused collaboration around a technology, use-case, vertical market or beta release
- Take online learning lessons and tutorials to broaden your knowledge of Gigamon products.
- Open support tickets (Customers only)
- Download the latest product updates and documentation (Customers only)

The VÜE Community is a great way to get answers fast, learn from experts and collaborate directly with other members around your areas of interest.

Register today at community.gigamon.com

Questions? Contact our Community team at community@gigamon.com.

Glossary

D

decrypt list

need to decrypt (formerly blacklist)

decryptlist

need to decrypt - CLI Command (formerly blacklist)

drop list

selective forwarding - drop (formerly blacklist)

F

forward list

selective forwarding - forward (formerly whitelist)

L

leader

leader in clustering node relationship (formerly master)

M

member node

follower in clustering node relationship (formerly slave or non-master)

N

no-decrypt list

no need to decrypt (formerly whitelist)

nodecryptlist

no need to decrypt- CLI Command (formerly whitelist)

P

primary source

root timing; transmits sync info to clocks in its network segment (formerly grandmaster)

R

receiver

follower in a bidirectional clock relationship (formerly slave)

S

source

leader in a bidirectional clock relationship (formerly master)