NetWitness® Platform XDR

GigamonGigaVUE FM Integration Guide

NETWITNESS
Platform XDR

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on NetWitness Community. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

November, 2022

Contents

NetWitness Platform XDR Integration with GigamonGigaVUE FM Series

GigaVUE Cloud Suite

The Gigamon Visibility Platform is the first pervasive visibility solution for the cloud that provides full and deep traffic visibility into your workloads in AWS. The GigaSECURE platform consists of distributed physical (GigaVUE H Series platforms) and virtual (GigaVUE-VM) nodes that provide an advanced level of filtering intelligence, managed as a single fabric. This platform is made up of three main elements:

- GigaVUE-FM Fabric Manager: Orchestration component that ensures scale, automation and elasticity across your Azure or AWS deployments.
- GigaVUE V Series: Virtual visibility nodes deployed in Azure or AWS aggregate traffic across multiple Azure or EC2 instances and send customized traffic to multiple security tools as needed.
- G-vTAP agents: Used to gain access to the traffic from the Azure or EC2 instances to the GigaVUE V Series nodes.

The Gigamon Visibility Platform can be deployed in either on-premises, Azure, or AWS. That means organizations do not need to duplicate the tools running in the on-premises and cloud. For example, if you are running tools on-premises, you do not need to be forced to deploy additional tools in the cloud because this will drive up cost and the need for resources. Instead, deploy the Gigamon Visibility Platform on-premises and backhaul network traffic of interest to your on-premises tools.

Integration Steps

Microsoft Azure

You can access Gigamon Visibility Platform through the Azure Marketplace on the Azure portal. It is activated by a BYOL license. A thirty-day free trial is also available. For more information on the Gigamon solution, see GigaVUE Cloud Suite for Azure.

For more information regarding GigaVUE Deployment, see https://docs.gigamon.com/doclib515/Content/GV-Cloud-Azure/preface-Azure.html?tocpath=GigaVUE%20Cloud%20Suites%7CAzure%7C_____0.

You will see the traffic incoming on NW Decoder Host once the Monitoring Session is deployed within the Gigamon GigaVUE-FM with Decoder receiver NIC as tunnel.

AWS

Gigamon® Visibility Platform on AWS will be available through the AWS Marketplace and activated by a BYOL license. A thirty-day free trial is also available.

For more information on the Gigamon® solution, see "Gigamon® Visibility Platform for AWS Data Sheet", https://www.gigamon.com/content/dam/resource-library/english/data-sheet/DS-GigaVUE-Cloud-Suite-for-AWS.pdf.

For more information on the deployment details, see "Gigamon® Visibility Platform for AWS Getting Started Guide", https://docs.gigamon.com/pdfs/Content/Resources/PDF%20Library/GV-6000-Doc/GigaVUE-Cloud-Suite-AWS-GigaVUE-V-Series-2-Guide-v60.pdf.

After the “Monitoring Session” is deployed within the Gigamon GigaVUE-FM, you can configure the Network Decoder Tunnel.

Configure Tunnel on the Network Decoder

1. SSH to the Decoder.
2. Submit the following command strings.

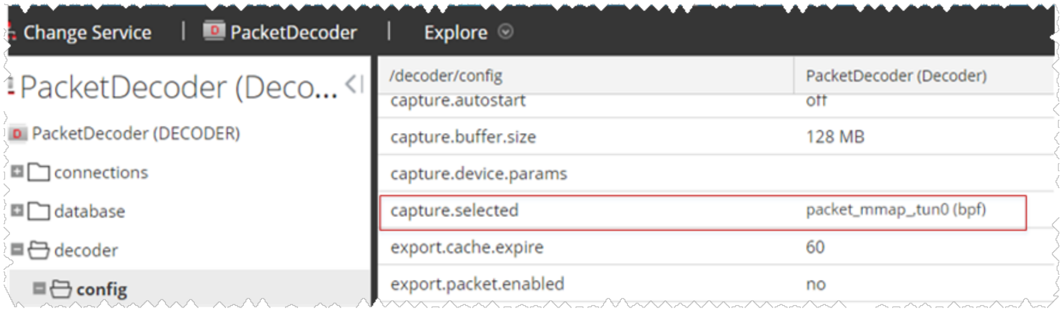
```
$ sudo ip link add tun0 type gretap local any remote <ip_address_of_
VSERIES_NODE_TUNNEL_INTERFACE> ttl 255 key 0

$ sudo ip link set tun0 up mtu <MTU-SIZE>

$ sudo ifconfig (to verify if the tunnel tun0 is being listed in the list
of interfaces)

$ sudo lsmod | grep gre ( to make sure if the below kernel modules are
running:

ip_gre 18245 0

ip_tunnel 25216 1)
```

```
If they are not running then execute the below commands to enable the
modules
```

```
$ sudo modprobe act_mirred
```

```
$ sudo modprobe ip_gre
```

3. Create a firewall rule in the Network Decoder to allow traffic through the tunnel.
   a. Open the `iptables` file.
   `vi /etc/sysconfig/iptables`
   b. Append the line `-A INPUT -p gre -j ACCEPT` before the `commit` statement
   c. Restart `iptables` by executing the following commands.
   `service iptables restart`
4. Set the interface in the Network Decoder.
   a. Log in to NetWitness Platform XDR, select the `decoder/config` node in Explorer view for the Network Decoder service.
   b. Set the `capture.selected` = `packet_mmap_,tun0`.

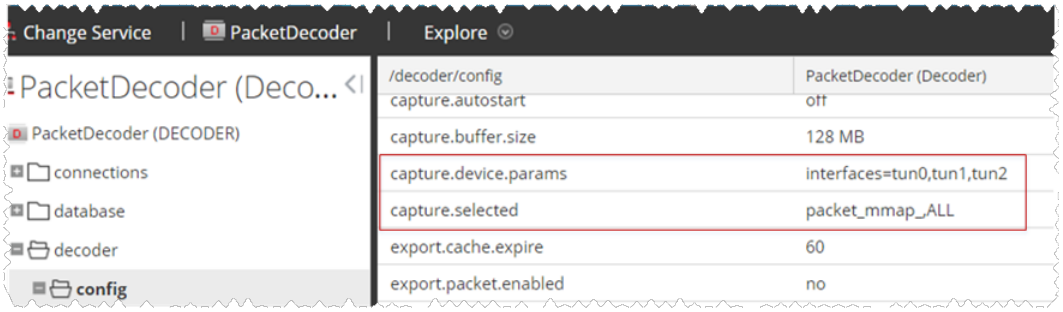


/decoder/config	PacketDecoder (Decoder)
capture.autostart	off
capture.buffer.size	128 MB
capture.device.params	
capture.selected	packet_mmap_tun0 (bpf)
export.cache.expire	60
export.packet.enabled	no

5. (Conditional) - If you have multiple tunnels on the Network Decoder.
   a. Restart Decoder service after you create the tunnel in Network Decoder.
   b. Log in to NetWitness Platform XDR, select the `decoder/config` node in Explorer view for the Network Decoder service, and set the following parameters.

```
capture.device.params = interfaces=tun0,tun1,tun2
```

```
capture.selected = packet_mmap_,All
```



/decoder/config	PacketDecoder (Decoder)
capture.autostart	off
capture.buffer.size	128 MB
capture.device.params	interfaces=tun0,tun1,tun2
capture.selected	packet_mmap_ALL
export.cache.expire	60
export.packet.enabled	no

6. Restart decoder service.

```
$ sudo restart nwdecoder
```

The user should be all set to capture the network traffic in Decoder.

Getting Help with NetWitness Platform XDR

Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness:

- See the documentation for all aspects of NetWitness here: https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation.
- Use the **Search** and **Create a Post** fields in NetWitness Community portal to find specific information here: https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions.
- See the NetWitness Knowledge Base: https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base.
- See Troubleshooting section in the guides.
- See also NetWitness® Platform Blog Posts.
- If you need further assistance, Contact NetWitness Support.

Contact NetWitness Support

When you contact NetWitness Support, please provide the following information:

- The version number of the NetWitness Platform XDR or application you are using.
- Logs information, even source version, and collection method.
- If you have problem with an event source, enable **Debug** parameter (set this parameter to **On** or **Verbose**) and collect the debug logs to share with the NetWitness Support team.

Use the following contact information if you have any questions or need assistance.

NetWitness Community Portal	https://community.netwitness.com In the main menu, click **Support > Case Portal > View My Cases**.
International Contacts (How to Contact NetWitness Support)	https://community.netwitness.com/t5/support/ct-p/support
Community	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions

Feedback on Product Documentation

You can send an email to nwdocsfeedback@netwitness.com to provide feedback on NetWitness Platform documentation.