6480 Via Del Oro
San Jose, CA 95119
+1 888-257-3000

Customer Release Notes

VSP Operating System Software

Software Release 8.3.1.0
June, 2021

INTRODUCTION:

This document provides specific information for version 8.3.1.0 of agent software for the VSP Operating System Software.

The purpose of this version is to address customer and internally found software issues. This release also includes a few feature enhancements for the Fabric Connect branch solution as indicated in the New in this Release section of this document.

Newly Purchased Switches Require Software Upgrade. You should promptly upgrade the VOSS software to the latest version available by visiting the Extreme Portal.

Extreme Networks recommends that you thoroughly review this document prior to installing or upgrading this product.

For the latest firmware versions, visit the download site at:
www.extremenetworks.com/support/

NEW IN THIS RELEASE:

Please see “New Features in this release” section below for more information.

IMPORTANT NOTES BEFORE UPGRADING TO THIS RELEASE:

If upgrading systems from either release 4.2.1.0 or release 4.2.1.1 that have ISIS enabled link(s) configured with HMAC-MD5 authentication, then you need to perform the procedure described in the section ***SPECIAL INSTRUCTIONS FOR UPGRADING FROM PREVIOUS RELEASES*** in order to avoid potential network connectivity loss.

If upgrading systems running 4.1.X releases which also have TACACS+ enabled, refer to the section ***SPECIAL INSTRUCTIONS FOR UPGRADING FROM PREVIOUS RELEASES*** for upgrade instructions.
If upgrading systems running 6.0.x releases or older, refer to the section ***SPECIAL INSTRUCTIONS FOR UPGRADING FROM PREVIOUS RELEASES*** for instructions about the need to step-through a 6.1.x release prior to going to 7.1.x release.

If upgrading systems running versions prior than 8.2.8.0, refer to the section ***SPECIAL INSTRUCTIONS FOR UPGRADING FROM PREVIOUS RELEASES*** for instructions about the possible need to renumber VRRP instances.

UPGRADE CONSIDERATIONS WHEN UPGRADING TO 8.3.1.0 FROM PREVIOUS RELEASES:

- VOSS 8.3.1 is not compatible with Fabric IPsec Gateway (FIGW) versions less than 4.0.0.0. To use the new features introduced in this release the FIGW image must be upgraded to at least 4.0.0.0. Also the FIGW 4.0.0.0 image is not compatible with VOSS versions prior to this release.
- When upgrading to 8.3.1.0, the VOSS image needs to be installed *first*, and after that the FIGW version must be upgraded to 4.0.0.0 if installed.
- The FIGW qcow2 image is no longer supported with this release, install the FIGW OVA image when upgrading.
- Supported ciphers are aes128gcm16-sha256 or aes256gcm16-sha256 (default is aes128gcm16-sha256). Others can be selected but are not supported in this release.
- The FIGW installation file has no integrity check enabled. Use SCP (not SFTP) to copy the file to the switch and make sure the file size is correct before installation. If the file is corrupted, it may not install or you may not be able to login. Re-transfer the file and re-install the VM in this case.
- After installing a FIGW VM the default password for user rwa must be changed to ensure security.
- VOSS 8.3.1 cannot be directly upgraded to 8.4 as it has only a subset of the feature set of VOSS 8.3.1
- The released TPVM images included with this release for the VSP4900 and VSP7400 are unchanged from the 8.3.0.0 release.
- For DVR deployments refer also to Outstanding Issues Section before upgrading.
- If you have a VLAN with VRRP instance of 37 provisioned and functional on a node running with several other VLANs with DvR enabled, upon upgrade to 8.3.1.0, VRRP configuration for instance 37 is removed from that VLAN. This would result in traffic loss for members of that VLAN. Recommend renumbering the VRRP instance IDs to values other than 37 and 38 on that VLAN before upgrading. DvR uses the same multicast addresses as VRRP ID 37 and 38 for its DvR controller and leaf implementation.

Example steps to configure the FIGW

1. `virtual-service figw install package FabricIPSecIPsecGW_VM_4.0.0.0`
2. Wait for 2 mins or so
3. `Configure terminal`
4. `show virtual-service install figw`

   Example:

```
FE_VSP4900_B2:1#show virtual-service install figw
**********************************************************************
                 Command Execution Time: Wed Jun 09 14:53:25 2021 EDT
**********************************************************************
    Stage : DONE
    Status: SUCCESS
```

5. `virtual-service figw num-cores 6` (for VSP4900 use `2`)

   `virtual-service figw mem-size 12288` (for VSP4900 use `4096`)

   `virtual-service figw vport eth0`

   Only on VSP7432CQ,VSP4900. Not needed for VSP7400-48Y-8C:

   `virtual-service figw vport eth0 port 1/s1`

   `virtual-service figw enable`
6. Wait 1 or 2 mins for the side band port to initialize.
7. `Virtual-service figw console`
8. At the prompt enter `rwa` password: `rwa` , change the password and confirm the password
9. Example config:

```
set global ipsec-tunnel-src-vlan 2012
set global ipsec-tunnel-src-ip 10.180.3.3/28
set global lan-intf-vlan 2001
set global lan-intf-ip 10.172.13.3/24
set global lan-intf-gw-ip 10.172.13.1
set global fe-tunnel-src-ip 10.180.1.1
set global wan-intf-gw-ip 10.180.3.1
set global mtu 1950
set ipsec 1 ipsec-dest-ip 10.172.60.27
set ipsec 1 mtu 1500
set ipsec 1 auth-key IPSECFE
set ipsec 1 tunnel-name toVSP7400n93
set ipsec 1 fe-tunnel-dest-ip 10.172.61.2
set ipsec 1 fragment-before-encrypt enable
set ipsec 1 esp aes256gcm16-sha256
set ipsec 1 admin-state enable
```

PLATFORMS SUPPORTED:

Virtual Services Platform 4400 Series
- Virtual Services Platform VSP 4450GSX-PWR+
- Virtual Services Platform VSP 4450GSX-DC
- Virtual Services Platform VSP 4450GTS-DC
- Virtual Services Platform VSP 4450GTX-HT-PWR+

Virtual Services Platform 4900 Series
- Virtual Services Platform VSP 4900-48P
- Virtual Services Platform VSP 4900-12MXU-12XE
- Virtual Services Platform VSP 4900-24S
- Virtual Services Platform VSP 4900-24XE

Virtual Services Platform 7200 Series
- Virtual Services Platform VSP 7254XSQ
- Virtual Services Platform VSP 7254XTQ

Virtual Services Platform 7400 Series
- Virtual Services Platform VSP 7432CQ
- Virtual Services Platform VSP 7400-48Y-8C

Virtual Services Platform 8200 Series
- Virtual Services Platform 8284XSQ

Virtual Services Platform 8400 Series
- Virtual Services Platform 8404
- Virtual Services Platform 8404C

ExtremeAccess Platform XA1400 Series
- ExtremeAccess Platform 1440
- ExtremeAccess Platform 1480

Extreme Switching 5520 Series
- 5520-24T

5520-24W
5520-48T
5520-48W
5520-12MW-36W
5520-24X
5520-48SE

SPECIAL INSTRUCTIONS FOR UPGRADING FROM PREVIOUS RELEASES:

I. The following procedure should be followed when upgrading systems running one of the following two releases, 4.2.1.0 or 4.2.1.1 which also have ISIS enabled links with HMAC-MD5 authentication on:

Disable ISIS authentication throughout the network a system at a time, a link at a time by disabling it on either side of each link, ensuring the link is stable before moving to the next. When a system has been reconfigured free of ISIS HMAC-MD5 authentication in all of its links, save the configuration file and perform the upgrade to release 4.2.3.0 or greater. After all these systems have been upgraded to release 4.2.3.0 or greater, you may re-enable authentication a system at a time, a link at a time and save the configuration file in each of the involved systems.

Example:

```
VSP:1(config)#interface gigabitethernet x/y
VSP:1(config-if)#no isis hello-auth
VSP:1(config-if)#save config
VSP:1(config-if)# PERFORM THE UPGRADE
VSP:1(config)#interface gigabitethernet x/y
VSP:1(config-if)# isis hello-auth type hmac-md5 key <keyname> [key-id
<keyed>]
VSP:1(config-if)#save config
```

II. The following procedure should be followed when upgrading systems running 4.1.X releases which also have TACACS+ enabled on:

When you upgrade from VOSS 4.1.X to VOSS 4.2 or a higher release, the TACACS+ host configurations will be lost. After the upgrade, the TACACS+ host configurations will not take effect so you must reconfigure them. After you make the configurations, you must save the changes on the device. You should also save the configuration to a file to retain the configuration settings.

III. Upgrading DvR configurations from releases 6.0.1.1 and earlier to 6.0.1.2 and beyond.
   a. All DvR nodes must be upgraded to the same release.
   b. All DvR leaves should be upgraded first.

IV. Upgrading from releases 6.0.x and earlier
   a. Direct upgrade from 6.0.x or earlier releases to 7.x+ releases is not supported.
   b. Please upgrade to a 6.1.x release first (Release 6.1.6.0 or higher is recommended). Then upgrade to the desired 7.x+ release (Release 7.1.1.0 or higher recommended).

Review items 5, 6, and 7 if the ISIS L1 area is **`00.1515.fee1.900d.1515.fee1.900d`**, 00.0000.0000 or all zero's.

V. Legacy ZTF Procedures for Releases 7.0.0.0 - 7.1.2.0, 8.0.0.0, 8.0.1.0, and 8.0.5.0
   a. Boot with factory-defaults fabric.
   b. ISIS manual-area set to 00.0000.0000, Dynamically Learned Area (DLA) displayed as 00.0000.0000 and ISIS enabled with other parameters.

c. HELLO PDUs not sent.
d. Listen on active ISIS interfaces for ISIS HELLO with non-zero Area ID. Zeros of any length up to 13 bytes are considered a zero value.
e. When an ISIS HELLO with a non-zero Area ID is received, use that area ID as the DLA and start sending HELLO with DLA on all ISIS interfaces.
f. DLA set and displayed as learned in the previous step.
g. Saving the configuration will save into the configuration file `manual-area 00.0000.0000`.
h. Boot with the saved configuration. The ZTF procedures are triggered. ISIS interfaces in passive mode not sending ISIS HELLOs. Only process incoming ISIS HELLO with non-zero Area ID.

Note: You can reach the fourth step by manually configuring the ISIS/SPBM with a manual-area equal to 0 (all values of 0, regardless of the length of zeros, are considered the same) and enabling ISIS.

VI. Modified ZTF Procedures for Releases 7.1.3.0+ and 8.0.6.0+

a. Boot with factory-defaults fabric
b. ISIS manual-area set to 00.1515.fee1.900d.1515.fee1.900d, Dynamically Learned Area (DLA) is blank and ISIS enabled with other parameters.
c. HELLO PDUs not sent
d. Listen on active ISIS interfaces for ISIS HELLO with and Area ID not equal to **`00.1515.fee1.900d.1515.fee1.900d`**.
e. When an ISIS HELLO with an Area ID not equal to **`00.1515.fee1.900d.1515.fee1.900d`** is received, use that Area ID as the DLA and start sending HELLO with DLA on all ISIS interfaces.
f. DLA set and displayed as learned in the previous step.
g. Saving the configuration file will save into the configuration file `manual-area 00.1515.fee1.900d.1515.fee1.900d`.
h. Boot with the saved configuration. ZTF procedures are triggered. ISIS interfaces in passive mode not sending ISIS HELLO's, only processing incoming ISIS HELLO with an Area ID note equal to **`00.1515.fee1.900d.1515.fee1.900d`**.

Note: You can reach the fourth step by manually configuring the ISIS/SPBM with a manual-area equal to 00.1515.fee1.900d.1515.fee1.900d and enabling ISIS.

VII. Migration to a Release supporting Modified ZTF such as 7.1.3.0+ or 8.0.6.0+

a. From Pre-ZTF feature Release such as 6.1.6.0

The following considerations should be taken into account when upgrading to this release from a pre-ZTF release:

i. Check the ISIS manual area (show isis manual-area).
ii. Determine if the manual area equals 00.1515.fee1.900d.1515.fee1.900d.
iii. This is a normal Area ID before the upgrade. After the upgrade, ZTF procedures, as previously described, will be triggered.

- If the existing behavior is desired, the ISIS manual area used in the network needs to be changed to a different value. Note, if ISIS is the management network used to get to the node, it will not form an ISIS adjacency after the upgrade and not join the network. This will isolate the node. The changes to the manual area within the topology should be made before any upgrades are performed.

b. From a Release Running Legacy ZTF such as 7.1.2.0

The following considerations should be taken into account when upgrading to a release supporting Modified ZTF from a Legacy ZTF release.

- Check the ISIS manual area (show isis manual-area).
- Determine if the manual area equals 00.0000.0000 or is a 00 of any length.
- This Area ID triggered the ZTF procedures before the upgrade. After the upgrade, ZTF procedures, as previously described, will NOT be triggered.
- If the existing behavior is desired, replace the value of ISIS manual area with 00.1515.fee1.900d.1515.fee1.900d. Note, if ISIS is the management network used to get to the node, it will not form an ISIS adjacency after the upgrade and not join the network. This will isolate the node. The change should be made before the upgrade.
- Determine if the manual area equals 00.1515.fee1.900d.1515.fee1.900d.
    - This is a normal Area ID before the upgrade. After the upgrade to a release implementing
- Modified ZTF, the ZTF procedures, as previously described, will be triggered.
- If this is not desired, replace the value of ISIS manual area with a different value. Note, if ISIS is the management network used to get to the node, it will not form an ISIS adjacency after the upgrade and not join the network. This will isolate the node. The change should be made before the upgrade.

NOTES FOR UPGRADE:

Please see “Release Notes for VSP Operating System Software (VOSS)” for software release 8.3.0 available at https://www.extremenetworks.com/support/release-notes for details regarding Known Limitations.

FILE NAMES FOR THIS RELEASE:

Virtual Services Platform 4400 Series

File Name	Module or File Type	File Size (bytes)
VOSS4400.8.3.1.0.sha512	SHA512 Checksums	1395
VOSS4400.8.3.1.0.md5	MD5 Checksums	476
VOSS4400.8.3.1.0.tgz	Release 8.3.1.0 archived software distribution	130245605
VOSS4400.8.3.1.0_mib.zip	Archive of all MIB files	1181027
VOSS4400.8.3.1.0_mib.txt	MIB file	7845607
VOSS4400.8.3.1.0_mib_sup.txt	MIB file	1419117
VOSSv830_HELP_EDM_gzip.zip	EDM Help file	4880897
restconf_yang.tgz	YANG model	506020

Virtual Services Platform 4900 Series

File Name	Module or File Type	File Size (bytes)
VOSS4900.8.3.1.0.sha512	SHA512 Checksums	1706

File Name	Module or File Type	File Size (bytes)
VOSS4900.8.3.1.0.md5	MD5 Checksums	595
VOSS4900.8.3.1.0.tgz	Release 8.3.1.0 archived software distribution	269625780
VOSS4900.8.3.1.0_mib.zip	Archive of all MIB files	1181027
VOSS4900.8.3.1.0_mib.txt	MIB file	7845607
VOSS4900.8.3.1.0_mib_sup.txt	MIB file	1444384
VOSSv830_HELP_EDM_gzip.zip	EDM Help file	4880897
restconf_yang.tgz	YANG model	506020
TPVM_4900_8.3.0.0.img	Third Party Virtual Machine (TPVM)	1677066240
FabricIPSecGW_VM_4.0.0.0.ova	Fabric Ipsec Gateway Virtual Machine	3876669440

Virtual Services Platform 7200 Series

File Name	Module or File Type	File Size (bytes)
VOSS7200.8.3.1.0.sha512	SHA512 Checksums	1395
VOSS7200.8.3.1.0.md5	MD5 Checksums	476
VOSS7200.8.3.1.0.tgz	Release 8.3.1.0 archived software distribution	144802627
VOSS7200.8.3.1.0_mib.zip	Archive of all MIB files	1181027
VOSS7200.8.3.1.0_mib.txt	MIB file	7845607
VOSS7200.8.3.1.0_mib_sup.txt	MIB file	1385356
VOSSv830_HELP_EDM_gzip.zip	EDM Help file	4880897
restconf_yang.tgz	YANG model	506020

Virtual Services Platform 7400 Series

File Name	Module or File Type	File Size (bytes)
VOSS7400.8.3.1.0.sha512	SHA512 Checksums	1706
VOSS7400.8.3.1.0.md5	MD5 Checksums	595
VOSS7400.8.3.1.0.tgz	Release 8.3.1.0 archived software distribution	269279125
VOSS7400.8.3.1.0_mib.zip	Archive of all MIB files	1181027
VOSS7400.8.3.1.0_mib.txt	MIB file	7845607
VOSS7400.8.3.1.0_mib_sup.txt	MIB file	1437804
VOSSv830_HELP_EDM_gzip.zip	EDM Help file	4880897
restconf_yang.tgz	YANG model	506020
TPVM_7400_8.3.0.0.img	Third Party Virtual Machine (TPVM)	1677066240
FabricIPSecGW_VM_4.0.0.0.ova	Fabric Ipsec Gateway Virtual Machine	3876669440

Virtual Services Platform 8200 Series

File Name	Module or File Type	File Size (bytes)
VOSS8200.8.3.1.0.sha512	SHA512 Checksums	1395

File Name	Module or File Type	File Size (bytes)
VOSS8200.8.3.1.0.md5	MD5 Checksums	476
VOSS8200.8.3.1.0.tgz	Release 8.3.1.0 archived software distribution	144803207
VOSS8200.8.3.1.0_mib.zip	Archive of all MIB files	1181027
VOSS8200.8.3.1.0_mib.txt	MIB file	7845607
VOSS8200.8.3.1.0_mib_sup.txt	MIB file	1385356
VOSSv830_HELP_EDM_gzip.zip	EDM Help file	4880897
restconf_yang.tgz	YANG model	506020

Virtual Services Platform 8400 Series

File Name	Module or File Type	File Size (bytes)
VOSS8400.8.3.1.0.sha512	SHA512 Checksums	1395
VOSS8400.8.3.1.0.md5	MD5 Checksums	476
VOSS8400.8.3.1.0.tgz	Release 8.3.1.0 archived software distribution	206657367
VOSS8400.8.3.1.0_mib.zip	Archive of all MIB files	1181027
VOSS8400.8.3.1.0_mib.txt	MIB file	7845607
VOSS8400.8.3.1.0_mib_sup.txt	MIB file	1385356
VOSSv830_HELP_EDM_gzip.zip	EDM Help file	4880897
restconf_yang.tgz	YANG model	506020

ExtremeAccess 1400 Series

File Name	Module or File Type	File Size (bytes)
VOSS1400.8.3.1.0.sha512	SHA512 Checksums	1247
VOSS1400.8.3.1.0.md5	MD5 Checksums	424
VOSS1400.8.3.1.0.tgz	Release 8.3.1.0 archived software distribution	343868622
VOSS1400.8.3.1.0_mib.zip	Archive of all MIB files	1181027
VOSS1400.8.3.1.0_mib.txt	MIB file	7845607
VOSS1400.8.3.1.0_mib_sup.txt	MIB file	1093633
VOSSv830_HELP_EDM_gzip.zip	EDM Help file	4880897

Extreme Switching 5520 Series

File Name	Module or File Type	File Size (bytes)
5520.8.3.1.0.sha512	SHA512 Checksums	1368
5520.8.3.1.0.md5	MD5 Checksums	453
5520.8.3.1.0.voss	Release 8.3.1.0 archived software distribution	103949989
5520.8.3.1.0_mib.zip	Archive of all MIB files	1181027
5520.8.3.1.0_mib.txt	MIB file	7845607
5520.8.3.1.0_mib_sup.txt	MIB file	1441349
VOSSv830_HELP_EDM_gzip.zip	EDM Help file	4880897

File Name	Module or File Type	File Size (bytes)
restconf_yang.tgz	YANG model	506020

Note about image download:

Ensure images are downloaded using the binary file transfer. Perform MD5 checksum check on downloaded files to ensure file integrity.

Check that the file type suffix is ".tgz" and the image names after download to device match those shown in the above table. Some download utilities have been observed to append ".tar" to the file name or change the filename extension from ".tgz" to ".tar". If file type suffix is ".tar" or file name does not exactly match the names shown in above table, rename the downloaded file to the name shown in the table above so that the activation procedures will operate properly.

Load activation procedures:

```
software add VOSS4400.8.3.1.0.tgz
software activate 8.3.1.0.GA
```

or

```
software add VOSS4900.8.3.1.0.tgz
software activate 8.3.1.0.GA
```

or

```
software add VOSS7200.8.3.1.0.tgz
software activate 8.3.1.0.GA
```

or

```
software add VOSS7400.8.3.1.0.tgz
software activate 8.3.1.0.GA
```

or

```
software add VOSS8200.8.3.1.0.tgz
software activate 8.3.1.0.GA
```

or

```
software add VOSS8400.8.3.1.0.tgz
software activate 8.3.1.0.GA
```

or

```
software add VOSS1400.8.3.1.0.tgz
software activate 8.3.1.0.GA
```

or

```
software add 5520.8.3.1.0.voss
software activate 8.3.1.0.GA
```

COMPATIBILITY:

This software release is managed with Enterprise Device Manager (EDM), which is integrated into the agent software.

CHANGES IN THIS RELEASE:

New Features in This Release

IPsec fragment-before-encrypt

When IPsec fragment-before-encrypt is enabled when using IPsec over Fabric-Extend (FE)IPsec, based on the tunnel MTU, packets are fragmented before encryption and IPsec encapsulation.

The IPsec fragment-before-encrypt is an option per logical interface and its default state is **disabled.** In the default (disabled) state, the packets are first encrypted & IPsec encapsulated and after that fragmented. The fragmentation is applied only if final packet (including IPsec header) is larger than the tunnel MTU. So, when there is a tunnel with fragment before encryption disabled, the packets egressing the specific NNI port will be ESP and fragmented IP packets (both packets are encrypted but they will have different headers).

When the IPsec fragment-before-encrypt is **enabled** on logical interface, the fragmentation of the packets will happen before encryption and IPsec encapsulation. In this case, the packets will be fragmented based on the tunnel MTU minus the IPsec header, so that the final packet will not exceed the tunnel MTU. For this tunnel the packets egressing the specific NNI port will be only ESP packets.

This feature is supported natively on XA1400and on the Fabric IPsec Gateway on VSP4900 and VSP7400.

XA1400 Series

Note:

It is recommended to use the fragment-before-encrypt option for traversing over the Internet, to avoid possible throughput “penalty” for sending fragmented packets over the Internet.

The IPsec fragment-before-encrypt can be enabled only if IPsec over FE is in IPsec decoupled mode (IPsec source and destination IPs are different than the FE ones). The configuration shown below must be completed prior to enabling IPsec fragment-before-encrypt on logical interface:

- IPsec tunnel source address needs to be configured globally (under *router isis*)
- Per logical interface: (under *logical-interface isis*)
    - IPsec need to be disabled
    - IPsec tunnel-destination-IP or IPsec remote-nat-ip or IPsec responder-only need to be configured

CLI commands:

Enable/Disable IPsec Fragment-before-encrypt:

```
Mode: isis logical interface configuration

      [no] ipsec fragment-before-encrypt
```

To display IPsec fragment-before-encrypt:

```
Mode: global

      show isis logical-interface ipsec

XA1480:1(config-isis-2-192.168.20.1)#ipsec ?
```

```
fragment-before-encrypt Enable IPsec fragment before encrypt on this logical
interface

XA1480:1(config-isis-2-192.168.20.1)#sho isis logical-interface ipsec
********************************************************************************
                Command Execution Time: Fri Jun 04 21:02:20 2021 UTC
********************************************************************************

================================================================================================================
                                    ISIS Logical Interface IPsec
================================================================================================================
ID       Auth-Key   Responder-Only   Remote NAT IP        Auth-Key-Len Compression Frag-before-encrypt
----------------------------------------------------------------------------------------------------------------
2        ******     False            -                    128          False       True

----------------------------------------------------------------------------------------------------------------
 1 out of 1 Total Num of Logical ISIS interfaces
----------------------------------------------------------------------------------------------------------------
```

CLI consistency check and corresponding error messages

In the following scenarios, error messages will be displayed:

- When you try to enable IPsec fragment-before-encrypt and IPsec is enabled on logical interface

  ```
  Error: IPsec is enabled on logical interface, please disable IPsec
  before configuring ipsec fragment-before-encrypt
  ```

- When you try to enable IPsec fragment-before-encrypt and IPsec tunnel source address is not configured globally

  ```
  Error: You need to configure ipsec tunnel-source-address before
  modifying fragment-before-encrypt
  ```

- When you try to enable IPsec fragment-before-encrypt and no IPsec tunnel destination IP or IPsec remote NAT IP or IPsec responder only is configured on the logical interface

  ```
  Error: You need to have ipsec tunnel-dst-ip or for NAT case
  ipsecRemoteNatIp or ipsec responder-only configured before modifying
  fragment-before-encrypt
  ```

- When you try to enable IPsec on a logical interface and IPsec fragment before encrypt is enabled but no IPsec tunnel destination IP or IPsec remote nat IP or IPsec responder only is configured

  ```
  Error: IPsec fragment-before-encrypt is enabled on logical interface.
  You need to have ipsec tunnel-dst-ip or ipsecRemoteNatIp or ipsec
  responder-only configured before enable ipsec
  ```

- When you try toremove IPsec tunnel source address from the router IS-IS global configuration and IPsec fragment-before-encrypt is enabled on at least one logical interface

Note: Before using a release without support for this enhancement, follow the next sequence:

- Default the IPsec fragment-before-encrypt on all logical interfaces:

```
        XA1480:1(config)#logical-intf isis 1
        XA1480:1(config-isis-1-1.1.1.1)#no ipsec
        XA1480:1(config-isis-1-1.1.1.1)#no ipsec fragment-before-encrypt
        XA1480:1(config-isis-1-1.1.1.1)#ipsec
        XA1480:1(config-isis-1-1.1.1.1)#exit
        XA1480:1(config)#
```

- Save config
- Load new image

Fabric IPsec Gateway (FIGW)

By default, this feature is **disabled**.

CLI Commands:

- To enable fragmentation before IPsec encryption:

```
set ipsec <ID> fragment-before-encrypt enable
```

Note: IPsec admin state must be disabled to enable fragmentation before encryption.

Fragmentation before encryption can be enabled if IPSEC destination IP is configured or responder mode is enabled.

- To disable fragmentation before IPSEC encryption

```
delete ipsec <ID> fragment-before-encrypt enable
```

Note: Ipsec admin state must be disabled to disable fragmentation before encryption.

- To display the configured option:

```
FIGW> show ipsec-config 2 (tunnel id)
ipsec {
    tunnel_id 2;
    encryption-key-length 256;
    fe-tunnel-dest-ip 192.168.31.212;
    ipsec-dest-ip 23.30.150.86;
    mtu 1400;
    responder-only false;
    auth-method psk;
    auth-key *****;
    egress-shaping-rate 0;
    fragment-before-encrypt enable;
    admin-state disable;
}
```

Egress Tunnel Shaping on Fabric IPsec Gateway (FIGW) VM

Egress shaping is used to limit the egress traffic rate on logical interfaces.

You can configure egress shaper per IPsec / Fragmentation & Reassembly (F&R) tunnel on the Fabric IPsec Gatewayto shape the egress traffic.

The configurable shaper range is from 1 Mbps to 1000 Mbps. Every tunnel will have its own shaper even if multiple tunnels have same shaper rate.

Default value: Disabled

CLI Commands

To configure egress shaper rate:

- Set on IPsec tunnel:

Egress shaper must be set before enabling the IPsec tunnel

```
set ipsec <tunnel id > egress-shaping-rate ?

<egress-shaping-rate> Shaping rate in Mbps [1 – 1000]
```

- Set on logical interface:

```
set logical-intf-tunnel <tunnel id> egress-shaping-rate ?

<egress-shaping-rate> Shaping rate in Mbps [1 - 1000]
```

- Delete shaper rate on IPsec tunnel:

Egress shaper can deleted only after disabling the IPsec tunnel.

```
del ipsec <tunnel id > egress-shaping-rate
```

- Delete shaper rate on logical interface:

```
del logical-intf-tunnel <tunnel id> egress-shaping-rate
```

- To show configure shaper rate

```
show ipsec-config <tunnel id>

show logical-intf-config <tunnel id>
```

Platform Specific Features and Limitations

- Ingress UNI traffic which should transmit via tunnel where egress shaper configured, should not have following DSCP or 802.1p value. It can cause IS-IS adjacency flapping.

DSCP value	802.1P value
0x28	6
0x2E	6
0x2F	6
0x30	7
0x38	7

- Tunnel shaping granularity may differ from the user configured values when packets are fragmented if the packet size if greater than the FE tunnel MTU. This is because when packet fragmentation happens there is a higher packet header overhead.

TCP Maximum Segment Size (MSS)

The TCP maximum segment size (MSS) clamping feature is used to avoid fragmentation by reducing the packet size used by end nodes when transmitting data over tunnels with FE and IPsec encapsulating headers. Prior to 8.3.1 the TCP MSS feature was only supported on the XA1400 Series. 8.3.1 adds support of this feature to the VSP 7400 and VSP 4900 Series switches.

XA1400 Series

- There are changes to CLI config and show commands as well as EDM screens (see below for more details).
- There are no changes to the TCP MSS functionality.
- TCP MSS is enabled automatically on this platform whenever a tunnel is configured with an MTU of 1500 or less.
- The auto-derived TCP MSS value will be the lowest tunnel MTU - 200 (e.g. if tunnel MTU is 1500, TCP MSS value is set to 1300). This value can be manually overridden via CLI or EDM config.
- TCP MSS adjustment will occur bidirectionally on packets flowing from UNI-NNI or NNI-UNI interfaces (not NNI-NNI).
- Since modification of the TCP MSS value happens in both directions, the feature is only needed on one side of the FE/IPsec tunnel.

VSP4900 & VSP 7400 Series

- With the introduction of this feature in this release, TCP MSS values can be configured for use in TCP SYN/SYN_ACK packets traversing the VSP 4900 and VSP7400.
- Unlike the XA, TCP MSS must be manually enabled. The default TCP MSS value is 1300 and can be modified as needed.
- On the 4900, TCP MSS modification will only occur unidirectionally when a packet is being forwarded from a UNI interface to any other interface (e.g. UNI-NNI, UNI-UNI, UNI-FE, etc). Packets coming in on NNI will not be modified. Because of this restriction, TCP MSS must be enabled at both the head-end and branch locations.
- On the 7400, tcp mss modification will only occur unidirectionally when a packet is being forwarded into an FE tunnel (e.g. UNI-FE, NNI-FE, etc). TCP SYN/SYN_ACK packets being forwarded to another NNI or UNI interface will not be adjusted.

- With TCP MSS enabled, untagged Switched UNIs MUST have Platform VLAN attached. If no Platform VLAN is attached the MSS adjustment would not work and TCP session start packets may get dropped.

CLI commands:

To enable:
```
   ip tcp adjust-mss enable                #Default is 1300
```

Set value:
```
   ip tcp adjust-mss <max-segment-size>    #Range is 500-1900
```
To Disable:
```
   no ip tcp adjust-mss enable
```

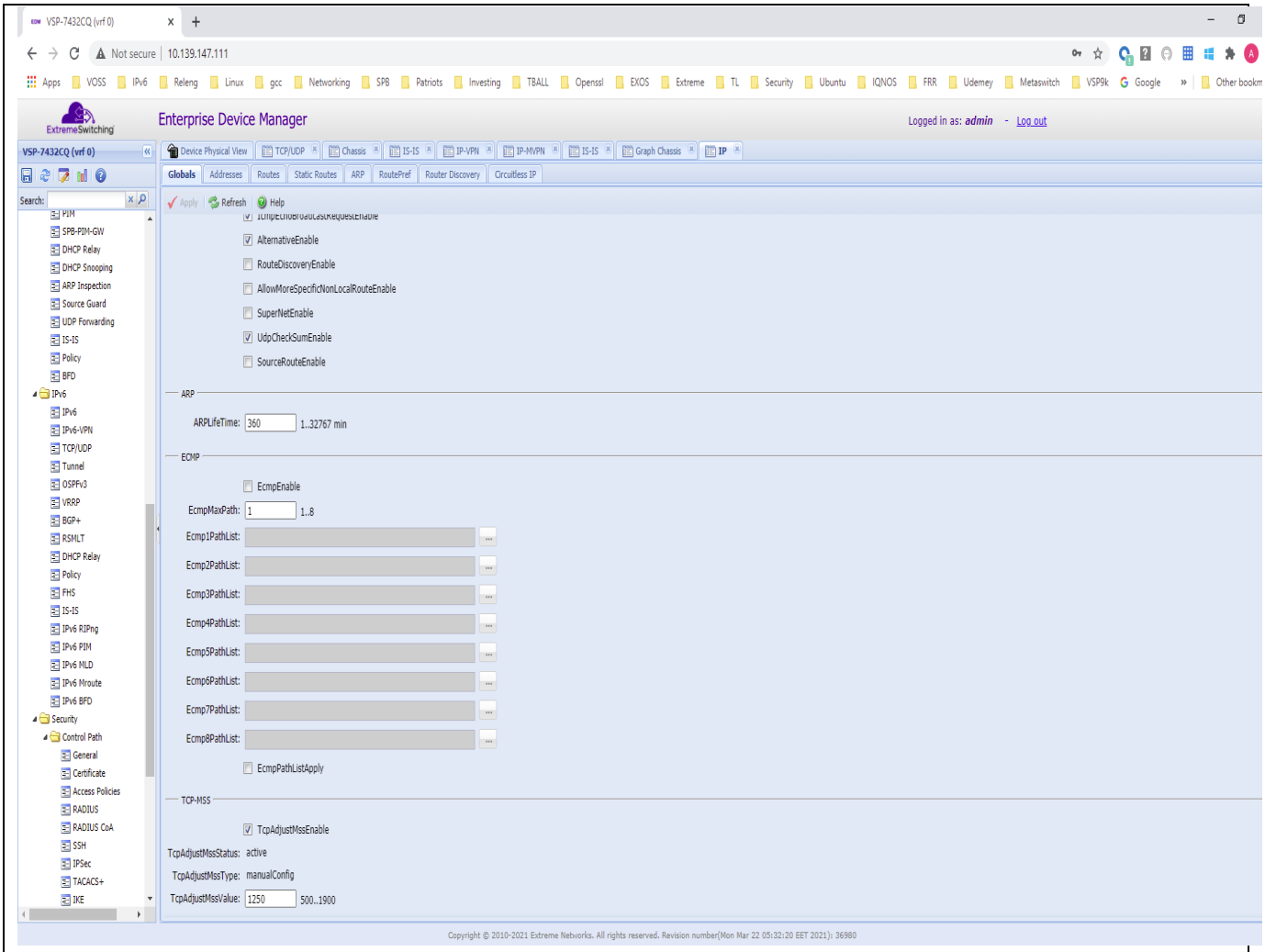
Default:
```
   default ip tcp adjust-mss         #Will set to auto-derive on XA,
                                     #to default value 1300 on 4900/7400
```

Config example (enable tcp-mss with value of 1150):
```
   ip tcp adjust-mss enable
   ip tcp adjust-mss 1150
```

Show command:
```
VSP-7432CQ:1#show ip tcp adjust-mss
********************************************************************************
            Command Execution Time: Fri Apr 16 14:26:04 2021 UTC
********************************************************************************

================================================================================
                                IP TCP Adjust MSS
================================================================================
ENABLE            STATUS            TCP MSS                   TCP MSS
                                    TYPE                      VALUE
--------------------------------------------------------------------------------
TRUE              ACTIVE            MANUAL-CONFIG             1300
```

EDM changes:

To show or edit tcp mss settings
```
IP -> IP -> Globals     (tcp-mss is at bottom)
```



IPsec tunnel source IP address per logical interface for XA1400

You can configure an IPsec tunnel source IP address per logical interface to allow IPsec tunnels through two different Internet Service Providers

Prior to 8.3.1 you could only configure a global IPsec source address which was used for all logical interfaces with IPsec enabled.
Starting with 8.3.1 you can configure IPsec source IP address per logical interface. The global IPsec source can still be used for all logical interfaces when no specific IPsec source IP is set.

The per tunnel IPsec source IP address can be defined in two ways:

Static: A user defined IPsec IP address. Note the following before configuring a Static IPsec IP address:

- A VLAN/brouter/CLIP IP address that will be used by the IPsec tunnel must be configured in the same VRF as used by the tunnel
- IPsec must be disabled on the logical interface
- The specified IP must be different than the Global IPsec IP source address

- The specified IP can be the same as the mgmt IP if do not have other logical IPsec interfaces with source IP type of DHCP
- Multiple logical interfaces can have the same statically configured IPsec source IP
- The VLAN/brouter/CLIP IP address cannot be deleted if it is used as static IPsec source IP

DHCP: The IPsec source IP is obtained from the mgmt IP assigned through DHCP

- To be able to set the type DHCP, the mgmt VLAN must have DHCP enabled
- The "co-existence" mode (the same mgmt IP and routing IP present on the same VLAN) needs to be present on the voss side in order to be able to configure dhcp type. If it is not present an error is displayed. To set the "co-existence" mode automatically propagate-to-routing command, from the mgmt_vlan level, can be used.
- After the *ipsec tunnel-source-address type dhcp* command is entered the IP & VRF used for the mgmt VLAN will be imported and used as IPsec source IP on logical interface.
- The VRF can be different than the Tunnel VRF
- The VLAN cannot be deleted and its IP address cannot be modified if the IP address is used as the IPsec source IP
- The IPsec source IP type DHCP cannot be same as the global IPsec source IP address or statically configured IP address. If a mgmt IP was already set as IPsec global/static IP an error will be reported.
- After the DHCP IP address is imported for use by IPsec, modifications to the mgmt vlan are permitted i.e. DHCP can be disabled on the mgmt VLAN or the mgmt VLAN ID can be changed or the mgmt VLAN can be deleted
- When saving the config, the IP & VRF imported for use byIPsec will be saved to the config file using *ipsec tunnel-source-ip type dhcp <IP_address> vrf <vrf_name>*. After a reboot, the information from the config file is used and the IPsec tunnel IP address is no longer imported from the mgmt VLAN.

CLI commands:

To set a specific IPsec source address with type static or dhcp:

```
(config-logical-interface)#ipsec tunnel-source-address type dhcp
(config-logical-interface)#ipsec tunnel-source-address type static {A.B.C.D}
```

In order to remove the specify address set on the logical interface, the next delete command need to be used:

```
(config-logical-interface)#no ipsec tunnel-source-address
```

Config example:

```
logical-intf isis 1 dest-ip 192.192.192.192 mtu 1300
isis
isis spbm 1
isis enable
auth-key ******
ipsec tunnel-source-address type dhcp
ipsec tunnel-dest-ip 10.3.1.55
ipsec


logical-intf isis 3 dest-ip 196.196.196.196 mtu 1500
```

```
isis
isis spbm 1
isis enable
auth-key ******
ipsec tunnel-source-address type static 20.20.20.20
ipsec tunnel-dest-ip 120.120.120.6
ipsec
```

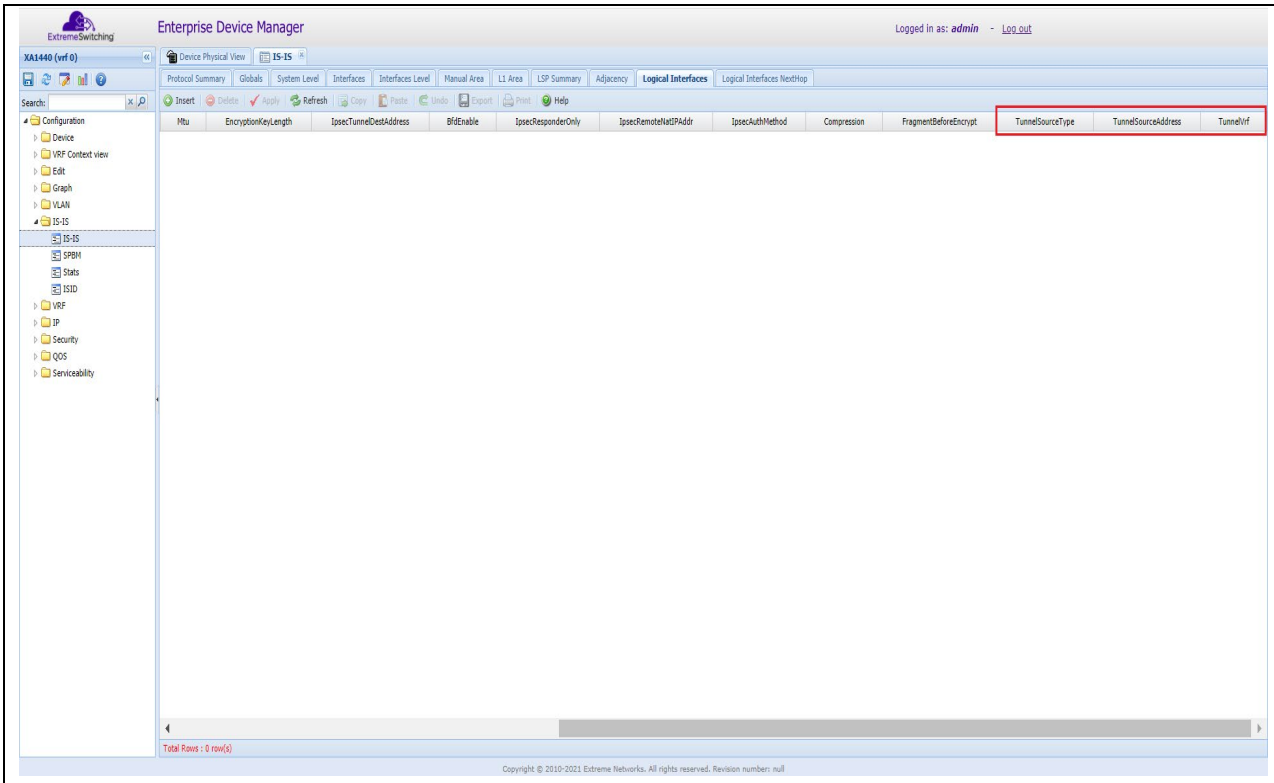
Show command:

```
XA1480:1(config-isis)#show isis logical-interface ipsec
================================================================================================================================
============
                                                ISIS Logical Interface IPsec
================================================================================================================================
============
ID  Status   Auth-Method    Auth-Key   Responder-Only   Remote NAT IP        Auth-Key-Len  Compression Frag-before-
encrypt
--------------------------------------------------------------------------------------------------------------------------------
------------
1   Enable     PSK            ******     False            -                    128             False       True
2   Enable     PSK            ******     False            -                    128             False       True
3   Enable     PSK            ******     False            -                    128             False       True
--------------------------------------------------------------------------------------------------------------------------------
------------

 1 out of 1 Total Num of Logical ISIS interfaces

--------------------------------------------------------------------------------------------------------------------------------
------------

================================================================================================

                               IPsec Tunnel General Info

================================================================================================

              IPsec tunnel global source-ip-address :10.101.21.141

================================================================================================

================================================================================================

                              ISIS IPsec Tunnels

================================================================================================

ID    IPsec source IP        IPsec Dst Ip        TUNNEL_NEXT_HOP

      type     address                           PORT/MLT   VLAN      VRF

------------------------------------------------------------------------------------------------

1     DHCP  10.192.168.20     10.3.1.5            Port1/8    4048     GlobalRouter

2    GLOBAL 10.101.21.141    100.100.100.6        Port 1/1    450     fe

3    STATIC 20.20.20.20      120.120.120.6        Port 1/1    20      fe
```

EDM changes:

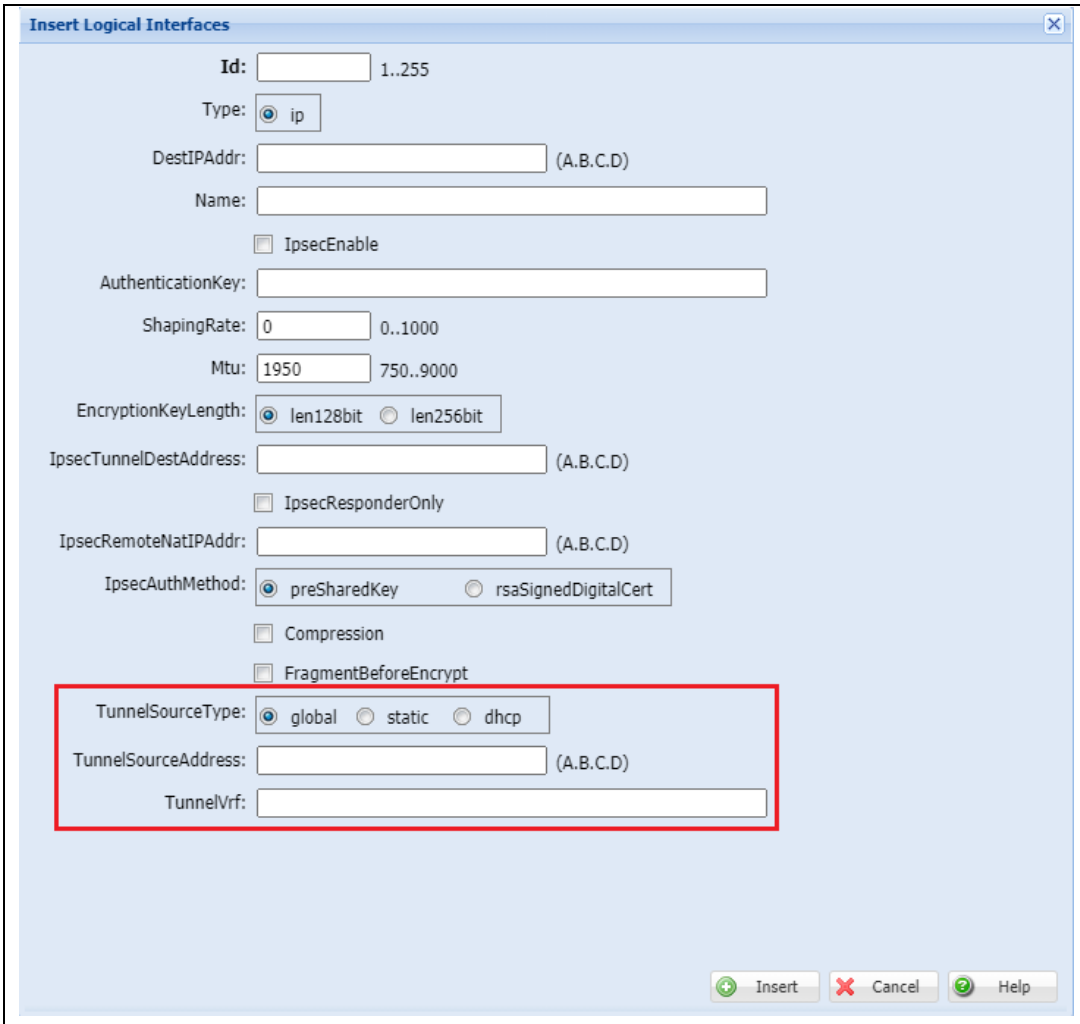
To show IPsec source IP per logical interface:

```
IS-IS -> IS-IS -> Logical Interfaces
```



Insert a logical interface:

```
IS-IS -> IS-IS -> Logical Interfaces -> Insert
```



Virtual Service CLI enhancments

The following new CLI commands apply to any virtual-service used on the box:

- copy a file from the VM to VOSS or vice versa.
- execute a CLI command on the VM and return the result to the VOSS CLI.
- change a user's password on the VM.
- view the Fabric IPsec Gateway package name and version

CLI Commands

1. Copying a file from the VM to VOSS

```
VSP7400# virtual-service copy-file source_vm_name:path_on_vm path_on_voss
```

where:

- source_vm_name is the name of the source VM from where the file will be copied.
- path_on_vm is the source path to the file on the VM (including the file name).
- path_on_voss is the destination path (including the file name) on the local box (on VOSS).

Note:

- The path should always contain the file name.

- The source_vm_name must exist and should already be enabled and running.
- path_on_voss is limited to /intflash, /extflash, /usb, /var/lib/insight/packages.

Example: *virtual-service copy-file ipsecgwn70:/home/rwa/configs/config.cfg /intflash/ipsecgwn70_06032021*

2. Copying a file from VOSS to the VM

```
VSP7400# virtual-service copy-file path_on_voss dest_vm_name:path_on_vm
```

where:

- path_on_voss is the source path (including the file name) on the local box (on VOSS);
- dest_vm_name is the name of the destination VM where the file will be copied to;
- path_on_vm is the destination path to the file on the VM (including the file name).

Remarks:

- The path should always contain the file name;
- The dest_vm_name must exist and should already be enabled and running;
- path_on_voss is limited to /intflash, /extflash, /usb, /var/lib/insight/packages.
- Example: *virtual-service copy-file /intflash/ipsecgwn70_cleartxt.cfg ipsecgwn70:/home/rwa/configs/config_clear.cfg*
-

3. Executing a CLI command on the VM

```
VSP7400(config)# virtual-service vm_name exec-command "command"
```

where:

- vm_name is the virtual-service name on which the command is executed;
- "command" is the actual command that will be executed on the VM.

Remarks:

- The vm_name must exist and should already be enabled and running;
- "command" must use quotes if the command contains spaces.
- Example: *virtual-service ipsecgwn70 exec-command "ls /home/rwa"*

4. Changing a user's password on the VM

```
VSP7400(config)# virtual-service vm_name change-user-pass user pass
```

where:

- vm_name is the virtual-service name on which the command is executed;
- user is the username local to the VM that will have it's password changed;
- pass is the new password for the selected user.

Remarks:

- The vm_name must exist and should already be enabled and running;
- The old password for the user is not required.
- Example: *virtual-service ipsecgwn70 change-user-pass rwa*

5. View the Fabric IPsec Gateway package name and version

```
VSP-7400-48Y-8C-70170:1#show virtual-service config
*********************************************************************************
                Command Execution Time: Wed Jun 16 15:15:35 2021 EDT
*********************************************************************************

================================================================================
==========
                                Installed Packages
================================================================================
==========

    Package:             figw4
    Package App Name:    FabricIPSecGW_VM_4.0.0.0
    Package Version:     4
    Package Name:        FabricIPSecGW_VM_4.0.0.0.ova
```

```
================================================================================
                          Virtual Services Config
================================================================================

Virtual Service :figw4
  Memory Assigned(M) : 8192
  Number of Cores    : 6
  Additional Disk Assigned:


  VPort Information:
  Name                  Vlan            Connect Type    Insight Port    NIC Type
  eth0                                  vtd             1/s1

Management Status :              Enabled
--------------------------------------------------------------------------------
```

New error messages

Any error messages encountered will depend on the VM command output and are printed to the console as they appear. In general, there is no indication of success. SNMP error messages are not available for commands (3) and (4):

1. If virtual-service name is not valid:
```
Error: Virtual service has not been installed
```

2. If VOSS file path does not start with /intflash, /extflash, /usb or /var/lib/insight/packages:
```
Error: invalid filename
```

3. If the file copy command cannot be executed:
```
An error occurred executing copy command!
```

4. If the file copy command fails:
```
An error occurred copying the file: <error_code>
```

5. If the exec-command cannot be executed or the password change command fails:
```
An error occurred executing the command!
```

6. If the user does not exist when changing the password:
```
The user does not exist!
```

ISIS Hello Padding

ISIS pads the Hello packets to the full interface Maximum Transmission Unit (MTU), in order to detect MTU mismatches.For FE NNI links, all hello packets are padded and on non-FE pt-to-pt NNI links the hello packets are padded, till a hello packet is received from the other side.

This release includes a mechanism (CLI Only) to disable the hello padding, to avoid hello packets fragmentation.

- The default state is hello padding enabled (therefore, no change after upgrade).
- After disabling padding, the config can be saved to a file. ***Note***, the new config file cannot be used in prior release.In order to downgrade, disable or use default keyword to enable padding and save config file.
- The config command to enable/disable padding is a global flag that will take effect on all ISIS NNI links. This flag can be used dynamically, that is, does not require disabling ISIS or any NNI link.

CLI Commands

Show mode:

```
6001:1#show isis
*******************************************************************************
            Command Execution Time: Thu Jan 28 22:11:29 2021 UTC
*******************************************************************************

================================================================================================================
                                  ISIS General Info
================================================================================================================
                            AdminState : enabled
                            RouterType : Level 1
                             System ID : 0001.0001.6001
                  Max LSP Gen Interval : 900
                                Metric : wide
                   Overload-on-startup : 20
                              Overload : false
                           Csnp Interval : 10
                           PSNP Interval : 2
                     Rxmt LSP Interval : 5
                              spf-delay : 100
                            Router Name : 6001
                     ip source-address :
                   ipv6 source-address :
               ip tunnel source-address :
                              Tunnel vrf :
                           ip tunnel mtu :
                     Num of Interfaces : 2
                  Num of Area Addresses : 1
                     Inband Mgmt Clip Ip :
                               backbone : disabled
               Dynamically Learned Area :
                              FAN Member : No
                          Hello Padding : enabled
```

Config mode:

```
6001:1#configure t
Enter configuration commands, one per line. End with CNTL/Z.
6001:1(config)#router isis
6001:1(config-isis)#no hello-padding
6001:1(config-isis)#show isis
*******************************************************************************
            Command Execution Time: Thu Jan 28 22:02:10 2021 UTC
*******************************************************************************

================================================================================================================
                                  ISIS General Info
================================================================================================================
                            AdminState : enabled
                            RouterType : Level 1
                             System ID : 0001.0001.6001
                  Max LSP Gen Interval : 900
                                Metric : wide
                   Overload-on-startup : 20
                              Overload : false
                           Csnp Interval : 10
                           PSNP Interval : 2
                     Rxmt LSP Interval : 5
                              spf-delay : 100
                            Router Name : 6001
                     ip source-address : ipv6
                        source-address :
               ip tunnel source-address :
                              Tunnel vrf :
                           ip tunnel mtu :
                     Num of Interfaces :
                 2 Num of Area Addresses : 1
                     Inband Mgmt Clip Ip :
```

```
                              backbone : disabled
                Dynamically Learned Area :
                             FAN Member : No
                          Hello Padding : disabled
```

To restore default behavior, use

```
6001:1(config-isis)#default hello-padding
```

or

```
6001:1(config-isis)#no hello-padding
```

Config File: When padding is disabled or in the verbose mode, “show running-config” will show the padding option

```
#
# ISIS CONFIGURATION#

router isis
sys-name  "6001" no
backbone enable
no hello-padding
is-type l1
system-id 0001.0001.6001

manual-area 49.0000
exit
router isis enable
```

FIGW version show command

A new FIGW CLI command is introduced which shows the version of the FIGW service.
Note: This command need to be executed from within the FIGW CLI service.

CLI Commands:

Show version

Example:

```
FIGW login: rwa
Password:

Welcome to Extreme Networks FabricIPSecGW (4.0.0.0)

Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-66-generic x86_64)

* Documentation:  https://help.ubuntu.com

  System information as of Wed 09 Jun 2021 04:34:44 PM EDT

  System load:  5.68              Processes:                135
  Usage of /:   43.1% of 8.78GB   Users logged in:          0
  Memory usage: 4%                IPv4 address for docker0: 172.17.0.1
  Swap usage:   0%

0 updates can be installed immediately.
0 of these updates are security updates.


The list of available updates is more than a week old.
```

```
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check
your Internet connection or proxy settings


Last login: Tue Jun  8 13:43:00 EDT 2021 on ttyS0

FIGW> show version
FabricIPSecGW_VM_4.0.0.0
```

Old Features Removed From This Release
None.

Problems Resolved in This Release	
VOSS-21228	IE 11 connects and displays switch/ports but none of menu items function
VOSS-20143	EDM: While placing the cursor on the port, the port label show up incorrect
VOSS-20214	LLDP med + Mitel IP phone not working
VOSS-20462	EDM: LldpAuthEnabled, DynamicMHSAEnabled and FlexUniStatus are not displayed right
VOSS-20696	DVR Leaf cannot delete mgmt clip; error message saying VLAN must be deleted first
VOSS-20648	XA1440 – could hit an exception when ipsec/FE tunnel is taken down
VOSS-20711	Endianness issue on VSP74xx/4900/XA with NTP server when specific DNS servers are used
VOSS-20793	Set ISIS sys-name to same system name pushed by XMC
VOSS-20642	After upgrading port names are not shown in EDM when configuring from CLI. The same issue happens when configuring with EDM
VOSS-20521	VSP4900 Ports 2+8n (2, 10, 18, 26....) frequently go down for no reason
VOSS-20449	VSP7400 IPFIX flows 'Timestamp/obseravation time' is not in sync with system time
VOSS-20802	VSP-4900-48P LLDP-MED not assigning ip phone to voice vlan

Fixes from Previous Releases
VOSS 8.3.1.0 incorporates all fixes from prior releases, up to and including VOSS 8.2.7.0, VOSS 7.1.7.0, VOSS 8.0.9.0 and VOSS 8.1.9.0.

OUTSTANDING ISSUES:

Please see “Release Notes for VSP Operating System Software (VOSS)” for software release 8.3.0.0 available at for details regarding Known Issues.

VOSS-21605	Per tunnel interface FIGW stats are unavailable in XMC
VOSS-21590	AES256GCM encryption throughput per FIGW core decreases significantly when ipsec tunnel configuration is scaled
VOSS-21478	Connection refused after running OpenVAS using SSH credentials

VOSS-21060	Transfers of files > 2GB will fail with SFTP; Use SCP or USB media
VOSS-21037	CPU usage statictics reports incorrectly that FIGW processor is at 100% after starting L2VSN traffic
VOSS-21705	VSP4900: Error message “Exceeds maximum allowed memory size” message is generated when enabling IPSEC VM without specifying the memory size
VOSS-20030	An interaction between DVR host learning and wireless solutions configured with proxy-ARP and bridging at the AP may create instability within the DVR domain due to specific combinations of roaming events and topology factors. This interaction is exposed when a client roams between AP’s connected to different BEB’s and both AP’s momentarily respond for the client IP on both BEB’s (host duplication). These interactions can be avoided by using VRRP instead of DVR for wireless segments.
VOSS-20258	XA1440: EDM: IP Compression is not editable from EDM; Workaround: use CLI to configure

KNOWN LIMITATIONS:

Please see “Release Notes for VSP Operating System Software (VOSS)” for software release 8.3.0 available at https://www.extremenetworks.com/support/release-notes for details regarding Known Limitations.

Regular cleanup of unneeded files on USB drives is recommended to minimize possibility of USB corruption when a system is reset, shut down, or power is lost.

DOCUMENTATION CORRECTIONS:

For other known issues, please refer to the product release notes and technical documentation available at: https://www.extremenetworks.com/support/documentation.

GLOBAL SUPPORT

By Phone: +1 800-998-2408 (toll-free in U.S. and Canada)

For the toll-free support number in your country:
www.extremenetworks.com/support/

By Email: support@extremenetworks.com

By Web: www.extremenetworks.com/support/

By Mail: Extreme Networks, Inc.
6480 Via Del Oro
San Jose, CA 95119

For information regarding the latest software available, recent release note revisions, or if you require additional assistance, please visit the Extreme Networks Support website.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks