10.6.4.1 Firmware Release Notes

Release: 2016.03.08
Revision 1.0: 2016.03.08

Improvements

System

● When the device sees that the available memory is getting low an e-mail alert will be sent

Description

The device will now send out a e-mail alert when the device notices that the memory is too low.

WAN Virtualization

● WAN Virtualization can send out e-mail alerts on status changes

Description

WAN Virtualization can send out e-mail alerts when there are site or tunnel status changes.

Hardware Failover

● Improve Hardware Failover to attempt recovery of Idle device when communication is lost

Description

Attempt Hardware Failover recovery of Idle device when communication to it is lost.

Alerts

● Automatic error reporting feature has been added to improve the quality of the software

Description

Automatic error reporting allows the device to send critical information back to Ecessa to assist in product quality improvement.

SNMP

● Added SerialNumber object to ECESSA-MIB

Description

Device serial number is readable via ECESSA-MIB::SerialNumber.0.

Fixes

System

● The network device driver can cause the device to become unresponsive

Description

The network device driver can cause the device to become unresponsive.

WAN

● Translucent mode WAN's with auto-created LAN's can use the wrong network mask for the WAN

Description

Translucent mode WAN's with auto-created LAN's can use the wrong network mask for the WAN. The actual network mask can be used when creating the WAN.

WAN Virtualization

● IPSec VPN connections can lose their ability to properly route traffic

Description

IPSec VPN connections can lose the ability to properly route traffic, resulting in traffic instead going out a WAN unencrypted.

● A translucent mode WAN and a NAT WAN on the same port can cause encrypted WAN Virtualization traffic problems

Description

Having a translucent WAN and a NAT WAN on the same port can cause source NAT rules that NAT traffic going out the translucent WAN to the IP of the NAT WAN. This can cause traffic problems such as WAN Virtualization tunnels not being able to connect.

VPN

● Loading a configuration while IPSec VPN is active may cause device to become inaccessible

Description

Loading a configuration while IPSec VPN is active and VPN Failover Testing is enabled can cause the device to become inaccessible.

● VPN IPSec security associations which have auto start enabled will attempt to start the connection twice

Description

When the VPN IPSec security association has auto start enabled, the device will attempt to start the connection twice. This can be an issue when connecting to certain third party hardware.

● IPSec VPN connections may connect with the wrong configured Security Association

Description

IPSec VPN connections may incorrectly connect with unrelated configured Security Associations, causing the connection to appear as down at one site while up at the other.

● IPSec IKEv2 security associations to Cisco devices not properly passing traffic on all subnets

Description

IKEv2 compatibility mode added to both the web interface and the command line. With this feature enabled, An Ecessa connecting to a Cisco device (or any other device where traffic does not pass properly) will properly pass traffic to all defined subnets.

● VPN IKEv2 connections can fail when connectivity to the remote device is lost, and continue to fail after connectivity is restored

Description

Loss of connectivity to the remote device after an IKEv2 VPN connection is established can cause the main VPN process to die if connectivity is restored after rekeying is attempted. This results in the process restarting but the connection is left in a down state.

● VPN entries with long names may crash the web server on disable

Description

VPN entries with names of length 23 or more characters in length cause a web server crash when said VPN is disabled via the GUI. This will not affect any user data, configuration, or traffic flow. The web server will restart properly on reloading.

Workaround

Ensure that VPN names are less than 23 characters long.

● IPSec VPNs might not work properly when adding security associations while disabled and then enabling the VPN

Description

When the VPN is disabled globally and a security association is added then when the VPN is enabled globally the associated security associations might not work.

Workaround

When this issue is seen it is recommended to disable the VPN feature globally and then to re-enable the feature.

● Loading a different configuration can cause problems when trying to create and connect IPSec VPN's

Description

Loading a different configuration while IPSec VPN Security Associations are active can leave IPSec files and devices behind that could prevent creating and connecting future IPSec VPN Security Associations.

Workaround

Delete IPSec VPN Security Associations before loading a configuration that doesn't have them.

● Configured IPSec VPN connections may not get activated

Description

Configured IPSec VPN connections may not get properly activated, even after activating or stopping and starting them.

● When creating an IPSec VPN with the CLI the number of tests default to zero, which can cause an unnecessary fail-over

Description

The default number-of-tests-performed for IPSec VPN in the CLI is zero, which can cause constant connection fail-overs.

● When connecting to a PPTP server behind the Ecessa with WAN Virtualization enabled the device can become unresponsive

Description

When connecting to a PPTP Windows 2008 R2 server through the Ecessa with WAN Virtualization feature enabled the device can become unresponsive. This only happens with certain mobile devices connecting to the PPTP server.

If a user experiences this issue we recommend contacting Ecessa Technical support.

● Loading configurations with IPSec VPN SA names that differ only by case from existing SA names can result in both connections running and incorrect behavior

Description

After loading a saved configuration containing an IPSec VPN named similarly (matches except for case) to a currently running SA can cause both of the connections to be running and behavior such as the connection appearing to be DOWN when it is actually UP.

● VPN between two Ecessa devices could get into a scenario where one side shows UP and the other shows DOWN

Description

When the VPN feature is setup between two Ecessa devices, in rare circumstances one Ecessa can show UP while the other shows DOWN.

● L2TP VPN connections can fail to establish after activating changes to another VPN connection

Description

L2TP VPN connections will work initially but after making changes new connections can fail to connect if another VPN Security Association uses the same local WAN IP as the L2TP.

Workaround

In order for the connections to re-establish the security association must be disabled and re-enabled on the Ecessa. We also would like to be informed when this issue is seen with specifics about the issue such as what clients were connected at the time and how long it took before users were not able to re-connect.

● Device can become unresponsive for a period of time when stopping and starting VPN connections from the CLI

Description

System can become unresponsive for a period of time while stopping and starting VPN connections using the CLI.

● When creating an IPSec Site to Site VPN in the GUI there is no validation to not allow the user to not enter any local or remote LANs, which will result in the connection not working

Description
The GUI does not validate that at least one local and remote LAN is configured when creating a Site to Site IPSec VPN. This will result in the connection not being started.

● Loading a configuration with IPSec VPNs can cause device to become unresponsive

Description
High CPU load and unresponsiveness can occur when loading a configuration that contained IPSec VPNs.

● Deleting and adding IPSec VPN security associations can cause some connections to not come up properly

Description
When adding and removing VPN IPSec security associations, the device can get into a state where not all the security associations come up properly.

● Deleting IPSec VPN Security Associations, then adding others, can result in some of them not connecting or not passing traffic properly

Description
Deleting IPSec VPN SA's and adding others can cause connections to not establish properly or the associated static routes to not be put in place.

Hardware Failover

● It should be recommended to the user that e-mail alerts are also enabled when Hardware Failover is enabled

Description
When a user enables hardware failover, and the e-mail alerts are disabled, it should be recommended that they also enable the e-mail alerts.

● Replacing a Hardware Failover unit with a different device, then replicating the configuration to the idle unit, can cause the pair to lose communication with each other

Description
Hardware Failover replication to idle after replacing one unit of the pair can cause the devices to use the same Keep-alive IP address and cause loss of communication between the devices.

QoS

● Multiple simultaneous QoS changes can cause the system to restart

Description
Doing multiple QoS changes at the same time can cause the software to restart.

● Deleting a QoS classifier from the GUI might not work properly

Description
When on the GUI and a QoS classifier is deleted the QoS classifier might show up in the list again.

Workaround
In order to delete the QoS classifier that is failing to be removed from the GUI log into the CLI for the Ecessa device and remove the QoS classifier from the qos menu.

Example:
qos classifier delete name CLASSIFIER
commit save

Static Routes

● Static Routes may not apply properly for bridges which had the same name as the WAN

Description
When a bridge and WAN have the same name, and used in a static route, rules are not correctly built on a WAN status change.

Workaround

Change the bridge alias to be named differently than the WAN and update the associated WAN to be on the updated bridge.

● All comment sections throughout command line and web interface should not allow invalid characters

Description

Comment sections for features in GUI and CLI accept newline and other invalid characters. This can cause functionality problems in those features.

Alerts

● Multiple email alerts triggered simultaneously are received as duplicates of the last alert created

Description

When multiple email alerts are triggered at or nearly at the same time, the last alert message created will overwrite all previous messages. From the perspective of the receiver it appears as though multiple duplicate copies of the same email arrived.

Statistics

● Top Services graph shows incorrect port numbers

Description

When viewing the top services graph in the web interface, service ports displayed do not match the actual traffic service ports.

SNMP

● SNMP Trap and Inform functionality plus WAN Virtualization tunnel information added to the ECESSA MIB

Description

Added WanOperStatusNotif, VpnSAStatusNotif, S2sStatusNotif, S2sTunStatusNotif, DnsStatusNotif, and testPointOperStatusNotif traps and informs to ECESSA-MIB. In addition, added the ability to toggle between v2c trap mode or v2c inform mode.

Services

● Web service can potentially not start during the boot up sequence

Description

During the device boot up sequence the web service may not start up properly.

Diagnostics

● When viewing current sessions in the GUI or the CLI ports show up incorrectly

Description

Both the GUI and the CLI allow the user to view current sessions. In both these views, incorrect ports are displayed.

● Diagnostics iperf not accepting time parameter

Description

Diagnostics iperf accepts a 'time' parameter, but is not applied properly.

DNS

● DNS domains that are queried for load balanced records always respond in the same order

Description

When querying the domain via the name server on the Ecessa device for load balanced records which contain multiple addresses the order of the results would always be the same.

● Dual Role DNS backup site could potentially not respond with the updated zone from the master site when a change was made

Description

When the dual role master makes a change to the zone the backup should respond with the updated master as long as the master is available. In certain cases the backup would respond with the previous zone of the master.

VoIP

- **VoIP CLI show command prints empty source port**

Description

VoIP CLI redirect 'show' command displays src-port parameter when no source port has been assigned.

Known Issues

System

- **Ports can become disabled on legacy 600 product (7568c) when pulling a cable during traffic flow**

Description

Ports can become disabled on legacy 600 family of products (7568c) when pulling cables during traffic flow. The device will have to be manually rebooted in order to get the port into a working state.

Workaround

Reboot the device.

- **Device can restart after a period of time when the sites tunnel configurations do not match**

Description

The device can run out of memory when 2 or more WAN Virtualization sites do not have matching tunnels.

Workaround

Make sure that WAN Virtualization sites are correctly configured and have corresponding tunnels setup.

WAN

- **When changing static routes that use aliases there is a small possibility that traffic could continue using the WAN over which it was previously routed**

Description

This issue can occur when modifying a static route which uses aliases to a different route.

Workaround

The workaround for this issue is to contact technical support at Ecessa when this issue occurs. To fix this issue without contacting support the device needs to be rebooted.

WAN Virtualization

- **WAN Virtualization which is using non base IP addresses can not route as expected when a static route is in place which applies to all traffic**

Description

WAN Virtualization feature which is setup to use non base IP addresses can have issues when there is a static route that is in place which is setup to apply to all traffic.

Workaround

There are several ways to address this issue:
1. If possible use the base IP addresses for WAN Virtualization.
2. Change the static route so that it only applies to the traffic that is necessary.

- **Encrypted WAN Virtualization traffic may not route as expected when the feature is not configured correctly**

Description

If Encrypted WAN Virtualization is not configured properly, the traffic associated to it might not route as expected.

Workaround

1. Make sure WAN Virtualization and VPN encryption configurations are correct and match on both sites.
2. Before making any changes to the VPN configuration, disable the associated WAN Virtualization site then re-enable it after activating VPN changes.
3. Enable and start all VPN connections before connecting WAN Virtualization sites.

- **WAN Virtualization hub location cannot have a site number that is greater than 127**

Description

When a WAN Virtualization site is created the hub site which in the feature is categorized as the lower site ID number must be 127 or lower. If the value is greater than 127 than the associated site will be unable to connect. This does not affect the remote site IDs which are categorized as the higher site id. The remote site IDs can be greater than 127. This does not affect the total number of sites.

Workaround

Set the associated hub site to have a lower site number.

VPN

- **IPSec VPN failover test point type 'Manual IP Configuration' does not work as expected**

Description

The IPSec VPN failover test point type 'Manual IP Configuration' does not work. The test pings to the far LAN should get source NAT'ed to the local LAN IP to get sent through the VPN. Instead, they get sent out a WAN.

- **IPSec VPN Failback option does not work as expected**

Description

With IPSec VPN Failback enabled it does not fail back to the preferred path when that path comes back up.

- **VTI VPN which is behind NAT will not be able to connect**

Description

VTI VPN which is configured on the Ecessa device will show as UP but the traffic will not pass through it. This is only a problem if one of the Ecessa devices is behind NAT.