10.5.3.2 Firmware Release Notes

Release: 2015.11.09
Revision 1.0: 2015.11.09

Fixes

WAN Virtualization

- **WAN Virtualization was using a lower default MTU which could cause remote sites to not be able to access some Internet sites via the main site**

Description

The default MTU (1400) used for encrypted WAN Virtualization may be too low for TCP traffic that may be routed through a device which clamps the MSS to a value greater than 1360, causing dropped packets if fragmentation is not allowed. Now uses 1500 by default.

- **Added WAN Virtualization CLI help for site MTU option**

Description

Added WAN Virtualization CLI help information about site MTU option and always shows MTU value in wanvirt display.

VPN

- **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.

Known Issues

System

- **Port becomes disabled on 7568C when pulling a cable during traffic flow**

Description

Ports can become disabled on 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.

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 IKEv2 security associations which connect with a Cisco ASA that contain multiple LAN networks can have an issue where not all the LAN networks have connectivity

Description

IPSec IKEv2 with multiple LANs creates one connection which all the networks available. The Cisco ASA with IKEv2 expects multiple connections to exist instead of one connection. This is not an issue when there is one LAN network defined at each side.

Workaround

Switch the security association to be a IKEv1 on both devices.

● 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.

● 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 that is behind the Ecessa that has 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.

● 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.

● Deleting and then re-adding a VPN via the command line interface can cause the VTI VPNs to not work correctly

Description

When there are multiple VPNs configured and one is deleted and re-added the VTI VPNs might not work correctly.

Workaround

In order to not run into this issue it is recommended to delete and re-add the VTI VPN using the GUI

QoS

● 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 Route comments with newline characters will cause static routes to not be applied

Description

When a static route comment contains a newline character then the static routes will not be applied.

Workaround

Change the static route comments to not have a newline character.