Ecessa Firmware Release Notes

Version: 10.6.9
Release: 2018.02.12
Revision 1.0: 2018.02.12

Improvements

Static Routes

● **Add validation to not allow aliases with FQDNs to be used for static routes**

Diagnostics

● **Diagnostics iperf now has the ability to set UDP bandwidth**

Users

● **The web interface now informs the user that user account information is not sent to the idle hardware failover device during replication**

Fixes

Hardware Failover

● **The idle hardware failover unit can get in a state where it can't communicate with the active unit**
<u>Additional Information</u>
Idle unit may not get fully configured if hardware failover is disabled and then re-enabled, resulting in the idle unit appearing down from the perspective of the active unit.
<u>Workaround</u>
Once in this state, disable then re-enable hardware failover on the idle unit

QoS

● **QoS applied to WAN Virtualization sites may cause packet loss when packet throughput rates are high**
<u>Additional Information</u>
QoS classes using fifo type queues, when applied to WAN Virtualization sites, create queues that have a very small size limit. Under moderate to heavy packet rates these queues can be overrun and result in packets being dropped.
<u>Workaround</u>
Use 'fair' type queues for QoS classes on virtual devices (WAN Virtualization and VLAN's) when traffic associated with those classes may be small packets or flow at a high packet rate.

DNS

● **The GUI "IP Address or Hostname" field for simple host records in a DNS domain will handle only up to 63 characters**
● **DNS simple host records do not accept underscores where an FQDN is accepted**

Monitoring

● **Devices connected to Ecessa Insight can create duplicate monitoring alerts**

Known Issues

System

● Ports can become disabled on legacy 600 product (7568c) when pulling a cable during traffic flow
Additional Information
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.

WAN

● The DHCP service can stop unexpectedly
Additional Information
The DHCP service stopping will cause DHCP WAN lines to miss IP Address updates.

Workaround
If a DHCP WAN does not properly update its IP Address then reboot the device.

● When a DHCP WAN is given a very short lease time by the modem the Ecessa device can become unresponsive
Additional Information
The duration of a lease is typically at least several hours. When the duration of the lease is less than a minute this problem can occur.

Workaround
Verify that the ISP modem is providing the DHCP WAN with a proper lease time.

WAN Virtualization

● When a device is running a configuration which has WAN Virtualization sites and loads a configuration which does not have WAN Virtualization sites configured the device software may restart
Additional Information
This is only a factor if the device has a product key which supports less WAN Virtualization sites then the configuration that is currently running

● WAN Virtualization configurations where tunnels have high packet loss and the tunnel testing parameters are set high can cause the tunnel to bounce more often then the testing parameters
Workaround
Make sure that the testing parameters for a tunnel have a lower timeout (less than 5 seconds) and instead increase the number of tests to match your requirements.

● Adding an encrypted WAN Virtualization site using the CLI may not work as expected
Additional Information
Using the CLI to add an encrypted WAN Virtualization site, and setting global WAN Virtualization options at the same time, will result in no VPN entry being created for the site.

Workaround
Using the CLI, commit global WAN Virtualization changes separately from committing the added site. Alternatively, add the site using the web interface.

● Enabling WAN Virtualization encryption using the CLI without specifying a VPN name will create an IPSec VPN entry with no name
Additional Information
Once an entry with no name is created, the user will then have no way to delete the entry.

Workaround
Make sure to specify the 'vpn-name' in the CLI command, or use the web interface to enable encryption for WAN Virtualization sites.

● 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
Additional Information
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.

● **WAN Virtualization hub location cannot have a site number that is greater than 127**
Additional Information
When a WAN Virtualization site is created, the hub site (which is defined as the site with the lower site ID number) must be 127 or lower. If the value is greater than 127 then the associated site will be unable to connect. This does not affect the remote site IDs, which can be greater than 127. This does not affect the total number of sites allowed.
Workaround
Set the associated hub site to have a lower site number.

VPN

● **Site-to-site VPN may attempt to use a WAN that is down**
Additional Information
This VPN will not try to recover even if failover testing is enabled, and will not connect until the WAN comes back up.

● **IPSec VPN failover test point type 'Manual IP Configuration' does not work as expected**
Additional Information
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.

● **A VTI VPN on an Ecessa device which is behind NAT will not be able to connect**
Additional Information
A VTI VPN 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.

Hardware Failover

● **Using Hardware Failover with high traffic throughput can cause excessive loading of the device**
Additional Information
Hardware Failover is by default stateful, and a very high number of TCP sessions can cause excessive loading of the device.
Workaround
If a Hardware Failover device becomes slow to respond, turn off the stateful option in Hardware Failover using the following CLI command: 'hwfo set stateful disable; commit save'

Virtual Product

● **Virtual Product may boot slowly**
Additional Information
Slow boot sequence has been observed. Infrequently the Virtual Product will take around four minutes to boot. Upon boot everything functions normally.
Workaround
Force reset the device.

SIP Proxy

● **Phone calls made within a short time after enabling the VoIP feature may not choose the Primary WAN**
Workaround
Wait at least 10 seconds after initially enabling the VoIP feature before making phone calls.

DNS

● **DNS Reverse Zone may not work correctly for load-balanced hosts**
Additional Information
DNS Reverse Zone information for load-balanced hosts may be set up incorrectly with PTR option.
Workaround
Remove the load-balanced host, activate changes, then add the load-

balanced host again.

Aliases

● **Using the CLI to create an alias with multiple addresses will reorder the addresses and remove duplicates, making the alias unusable for firewall forwarding rules**
Additional Information
If creating aliases to use for firewall WAN to LAN one-to-one forwarding rules, the CLI will not create them properly.
Workaround
Use the web interface to create aliases where the order of the addresses, and preservation of duplicates is important.

Static Routes

● **Failback static route over WAN Virtualization doesn't fail back after failing over to a WAN**

LCD

● **The LCD display can become stuck and not display new information when keys are pressed**
Workaround
Reboot the device.