Ecessa Firmware Release Notes

Version: 10.6.8
Release: 2017.05.19
Revision 1.0: 2017.05.19

Improvements

DNS

- **An SRV record which is entered with an underscore in the protocol or service will cause duplicate underscores in the zone file**
  Additional Information
  This causes DNS to function improperly on the device.

Fixes

WAN

- **Old DHCP addresses may silently remain on the device after a new one is received**
  Additional Information
  This can happen in two cases. One is Hardware Failover is disabled from an enabled state. The other is a cable is unplugged and the DHCP lease is allowed to expire.

WAN Virtualization

- **When loading a configuration, Uplink and Downlink speeds for a WAN Virtualization site may not load properly**
  Additional Information
  This occurs when the remote site has a higher maximum WAN speed than is allowable on the device.
- **Activating the WAN Virtualization advanced site Web UI page can display the wrong tunnel encryption selections**
  Additional Information
  The tunnel encryption selections are correct but are initially displayed incorrectly. Navigating again to the page will display the correct selections.

VPN

- **WAN graphs will report double the expected throughput for encrypted WAN Virtualization receive traffic**
  Additional Information
  For transport type VPN connections, like WAN Virtualization uses, the traffic gets counted both encrypted and again after decryption.

ACL

- **If the option 'Enable accessing Idle Service via Active Device (WAN Only)' is enabled for the Hardware Failover feature then traffic destined to the LAN which uses the same ports as management services for the Ecessa device will be rejected**
  Workaround
  Disable the following option on the Hardware Failover page:
  Hardware Failover -> Advanced -> Enable accessing Idle Service via Active Device (WAN Only). If you need to access the IDLE device then fill in an idle IP address instead of using this feature

Configuration

- **Adding a site to the Ecessa Insight may report as successful while the site will show DOWN in the dashboard even though the live site is UP**
  Additional Information
  This can also cause new configurations to not be sent to Ecessa Insight for sites that were configured in the past.

Diagnostics

- **Web Diagnostics ping timeout not working as expected**
  Additional Information
  The diagnostics ping utility sends multiple ICMP Requests until it receives a reply within the timeout specified. The expected behavior is to only send 1 ICMP echo request per test.
- **Diagnostics speed-test upload can fail if an aspx server is chosen**

DNS

- **Using CLI to modify DNS records does not update zones properly**
  Additional Information
  This bug does not effect modifying DNS Records via the web interface.
- **Within DNS domain configuration, Simple Host Records and Load Balanced Host Records mail entry should not be a dropdown menu**
  Additional Information
  The 'Mail Entry' drop-down is changed to a checkbox and renamed 'MX Record."
- **SRV record hostname error message is unclear**

Certificates

- **Email alerts are not sent for expiring Self CA certificates after a certificate is renewed**

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

- **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 paramenters**

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. Or add the site using the Web Interface.

- **Enabling WAN Virtualization encryption using the CLI without specifying a VPN name will create an IPSec VPN security association entry which has no name**

Additional Information

Modifying an unencrypted WAN Virtualization site by using the CLI to enable encryption, without specifying a vpn-name, will create an IPSec VPN Security Association entry which has no name. 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 GUI 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.

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

Additional Information

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

- **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.

LCD

- **The LCD display can become stuck and not display new information when keys are pressed**

  Workaround

  Reboot the device.

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 since it reorders them and deletes duplicates.

  Workaround

  Use the Web GUI to create aliases where the order of the addresses, and preservation of duplicates is important.