Ecessa Firmware Release Notes

Version: 10.7.1
Release: 2017.01.16
Revision 1.0: 2017.01.16

New Features

OSPF

- **Open Shortest Path First (OSPF) dynamic routing protocol is now supported**

Changes

OSPF

- **Add ability to configure OSPF dynamic routing using the CLI**
- **Add ability to configure OSPF dynamic routing using the graphical user interface**
  Description
  This is located under the "Dynamic Routing" link on the main navigational pane.

Fixes

WAN

- **After deleting a WAN, or moving a WAN to a different port, any non-base IP addresses used by other features within the WAN subnet will not be removed from the old port**

WAN Virtualization

- **When dynamic local endpoint for WAN Virtualization/Channel Bonding site is entered as an IP, the site will not function correctly**
  Description
  If an IP is entered when a new IP is assigned, the site will no longer be able to connect properly.
- **WAN Virtualization email alerts can cause delays in processing Site and Tunnel status changes**
  Description
  When, for some reason, email alerts can not be sent it can cause delays in handling Site and tunnel status changes.
  Workaround
  If your site runs into this issue either address why the e-mail alerts are failing to be sent or disable WAN Virtualization e-mail alerts. This can be done via the WAN Virtualization main page.
- **WAN Virtualization status is not correct when viewing the live site from the cloud**

Static Route Path Testing

- **Hardware Failover Idle device performs static route path testing**

Next Hop Routes

- **Next Hop Routes feature allows user to enter total number of Sources that exceeds the maximum number allowed**

Description

The Sources entered beyond the maximum are ignored, and routing rules are not created for them.

Static Routes

- **Static Routes with a destination of 0.0.0.0/0 do not get applied**

Description

This does not affect entries where the destination is blank

Workaround

Change the destination to be blank instead of 0.0.0.0/0

- **Remote Syslog may get critical error messages when running static route path testing**
- **Loading configurations that use Static Route Path testing can cause the software to restart**
- **Static routes with a WAN IP entered as the route will not fail over correctly**
- **When using aliases in a static route, and path testing fails for a WAN, traffic for the static route may still be sent over that WAN**
- **Static Route Path testing can get in a state where it does not work as expected**

Services

- **Port Link Speed and Duplex Settings can get stuck displaying 'Auto Negotiate' when there are manual settings selected**

Description

This is known to occur with some settings on devices with 4 ports.

- **Making changes to services email-alert via command line interface may cause a services reset**

Description

This can cause a remote session to terminate due to setting SSH port to 0. Other parameters will be reset as well.

Workaround

Issue a 'services show' before making any services email-alert changes via CLI.

DNS

- **DNS SOA e-mail entry is too strict which does not allow valid SOA e-mail addresses**

Description

It is now possible to enter an SOA email entry without a full email address. It is possible to enter 'user@domain.com', 'user.domain.com', or simply 'user'.

Firewall

- **Traffic pulled from a bridge on a LAN to be forwarded will be dropped if the firewall is enabled**

Description

For example, a static route that specifies a WAN Virtualization route and the 'bridged' keyword will not send the specified traffic over WAN Virtualization if the firewall is enabled.

Update

- **The serial console can get into a state where it is not accessible after the device has been powered on**

One-to-One NAT

- **One to one NAT rule may not be fully removed when a matching LAN address exists in the disabled state**

Description

If a LAN exists with the same address/netmask of a WAN, such as in a translucent scenario, One to One NAT rules will not delete properly from that WAN.

Workaround

Rebooting the device will ensure all One to One NAT rules are removed properly. Additionally, deleting the disabled LAN will solve the problem.

- **One-to-one NAT rule will not be applied to a WAN in special circumstances**

Description

Adding a one-to-one NAT rule to a WAN that has the same IP as a disabled LAN will not function as expected.

Workaround

Make sure to delete any LAN with the same IP as the WAN instead of just disabling it.

ACL

- **Management ACL which uses hostnames can get into a state where those hostnames are not added to the ACL**

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.

WAN

- **The DHCP service can stop unexpectedly**

Description

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**

Description

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.

- **When changing static routes that use aliases it is possibie 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

- **Adding an encrypted WAN Virtualization site using the CLI may not work as expected**

Description

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**

Description

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**

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.

- **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 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

- **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.

- **A VTI VPN on an Ecessa device which is behind NAT will not be able to connect**

Description

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**

Description

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**

  Description

  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.

DNS

- **DNS Reverse Zone may not work correctly for load-balanced hosts**

  Description

  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

VoIP

- **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.

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**

  Description

  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.

Port Forwarding

- **Activating Port Forwarding configuration changes can cause the device software to restart**

  Description

  This has occurred rarely. If activating Port Forwarding changes causes an unexpected restart of the device software, the changes may not have been applied. In that case retry the changes or contact Ecessa Technical Support.