10.6.5.2 Firmware Release Notes

Release: 2016.08.01
Revision 1.0: 2016.08.01

New Features

System

- **Firmware supports the Edge Appliances**

Description

This applies to the EV75 and EV150 product lines.

- **The Edge products are able to control the system fan via a smart fan system**

Description

This applies to the EV75 and EV150 product lines.

Hardware

- **Add support for the L7571 Platform**

Description

This applies to the PL600, CL600, WVR30, and WVDC20 product lines.

Improvements

System

- **Ethernet port Interrupt Throttle Rate will be configurable for legacy hardware types**

Description

The Interrupt Throttle Rate can be configured using the CLI: To turn off throttling: 'system port set interrupt-throttle 0' To enable dynamic throttling: 'system port set interrupt-throttle 3'

Diagnostics

- **Added the ability to specify a source WAN when using diagnostics traceroute via the CLI**

Description

Example CLI command: 'diagnostics traceroute host www.google.com source WAN1 interval 2 tests 15'

Changes

WAN

- **The GUI will accept both CIDR and Dotted Decimal notations for IP Network Address fields**

Description

The GUI will support entering Network addresses with the mask in either CIDR or Dotted decimal notations.

- **Add configurable default WAN Test Points**

Description

Configurable default WAN Test Points will be supported. These can be used when adding new WAN's in the Web and CLI. This will make WAN creation more simple and straightforward.

VPN

- **All Powerlink devices will have access to the firewall and the VPN features**

Description

As of this firmware release the PowerLink products which previously did not support the VPN and the firewall features will now have access to them.

LAN

- **Remove maximum global limit of 64 LANs**

Description

LANs were previously limited to a total of 64 globally. This change does not affect the maximum number of channels (WAN+LAN) allowed per port (16).

Fixes

WAN

- **WAN entries can show incorrect status if an individual test takes more time than specified**
- **A WAN which is configured to be DHCP can show the mask as /0 instead of the correct mask when a DHCP address is received**

Description

This is only an issue for WANs that are configured to be DHCP. This is also only a display issue.

- **Adding or modifying a WAN in the GUI, and leaving Test IP addresses blank, results in incorrect WAN recovery testing**

Description

Adding or modifying a WAN in the GUI, and leaving Test IP addresses blank, causes the last Test Point to use an invalid IP address in recovery testing.

- **A configuration where a spare WAN is before another WAN can cause the other WAN to not change state when it goes down**

Description

This will affect the status of all the WANs starting with the spare WAN.

Workaround

Move the WAN that is a spare to be the last WAN in the configuration.

- **Deleting a wan peer from a bridged WAN deletes the peer-to-peer IP address from the WAN port**

Description

Create a bridge and the bridge port gets an IP with a peer of the gateway. Then add a wan peer for the gateway to the bridge then delete it and the IP with the peer is removed from the port. This causes the WAN to not function properly.

- **A WAN peer for the gateway added to a translucent WAN can cause WAN testing to fail and the WAN to go down**

Description

A WAN peer added to a WAN for the gateway IP can cause routes for the WAN to be removed and WAN testing to stop.

- **After creating a bridge in the CLI you can not use the bridge alias as a port when creating a WAN**

Description

In the CLI when creating a WAN it does not recognize a bridge alias used for the 'port' parameter.

WAN Virtualization

- **A WAN Virtualization site which has at least 1 dynamic site configured and a static site configured will not allow the dynamic tunnels to establish**

Description

This applies specifically if the WAN Virtualization site contains multiple remote sites where 1 of the sites has remote dynamic endpoints. If the site has at least 1 dynamic

WAN Virtualization site then all the local WANs that are used for WAN virtualization will be open for remote access.

● WAN Virtualization static routes may not work properly if dynamic WAN's are used and the dynamic IP address changes

● Encrypted WAN Virtualization sites that use dynamic WAN's can allow unencrypted traffic to flow if the VPN goes down after a dynamic WAN IP address changes

● An Encrypted WAN Virtualization site which contains dynamic tunnels can get into a state where the dynamic tunnels stop passing traffic. This can occur if the local dynamic WAN IP address changes. NOTE: If the dynamic site is experiencing this issue then both the sites using the WAN Virtualization feature should be on the newer version

Description

This only affects the 10.6.5 and 10.6.5.1 releases.
If one of the sites cannot be upgraded to the newer version for whatever reason then both sites should use identifiers in the associated VPN configurations.

● Compression option will be removed from the WAN Virtualization feature

Description

WAN Virtualization compression option can cause dropped traffic in certain situations. The compression option will be removed from the feature.

● WAN Virtualization will send email alerts for tunnel bounces only after a configurable number of bounces in a time period

● When a WAN Virtualization site comes up it is possible that the default route for the site does not contain all the tunnels that it should contain

● WAN Virtualization can incorrectly determine the health of a site and attempt to recover the site which causes all tunnels to be bounced

Description

This can happen when the other tunnels that are used in a site are experiencing issues.

● Encrypted WAN Virtualization VPN connections can lose their ability to properly route traffic

VPN

● Making VPN configuration changes can cause device software to restart

Aliases

● Making alias changes may cause the device software to restart

DNS

● Attempting to activate on a DNS domain page can fail when it is associated to a reverse zone

Description

This only affects DNS domain names that end with .in-addr.arpa.

VoIP

● The VoIP feature may not become enabled after disabling then re-enabling it

● Ecessa VoIP authentication configuration with user names that contain special characters can cause the configuration to not load

Description

This only applies to the VoIP Authentication sections. The VoIP Authentication is only used when the provider authenticates during a call fail-over.

● Importing a VoIP Authentication domain can fail when the entries contain comma characters

Description

When importing an authentication domain that is formatted with a comma delimiter the username and password should not contain commas. If the import data contains extra commas then the import process will fail.

- **VoIP authentication domains that are configured with the line name or the password containing an apostrophe can cause the domain page to not show all the entries after activation**

  Description

  This issue will happen only if the line name or the password fields contain a single apostrophe.

- **VoIP call failover can take a long time due to support for silence suppression**

  Description

  Support for handling silence suppression results in a long failover delay because failover will not occur until the WAN line actually is detected as down.

Alerts

- **Modify memory parameters used to trigger alerts to avoid false alerting**

Services

- **Telnet option removed from user interface since it is no longer supported**

Firewall

- **The CLI 'firewall show' command prints out an empty source if not set**

  Description

  This can be troublesome if the show command output is used to copy and paste commands.

Port Forwarding

- **Port forwarding feature in the Web GUI does not accept the keyword "Any" for a port range**

  Description

  After activating a Port Forwarding entry with an empty Port Range value, it is automatically filled in with the word 'Any'. Activating again on the page results in an error indicating 'Any' is not a valid Port Range.

Security

- **Add an option to prevent clickjacking attacks on the web interface**

  Description

  X-Frame deny option (located in web options) allows for prevention of clickjacking attacks.

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

- **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

● 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.

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'

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.

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.

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.

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.