10.6.3 Firmware Release Notes

Release: 2015.09.21
Revision 2.0: 2015.10.09

Improvements

VPN

- **Security update of IPSec VPN**
  Description
  IPSec VPN uses the strongswan package. This addresses the following vulnerabilities:
  CVE-2014-2338
  CVE-2014-2891

Security

- **Security update to fix vulnerabilities in IPSec VPN and WAN Virtualization features**
  Description
  Update of curl package to fix the following vulnerabilities:
  CVE-2013-0249
  CVE-2013-1944
  CVE-2013-2174
  CVE-2013-6422
- **Security update to fix vulnerabilities in the DNS feature and internal system packages**
  Description
  Update dev-libs/libxslt to fix the following vulnerabilities:
  CVE-2012-2870
  CVE-2012-2893
  CVE-2012-6139
  CVE-2013-4520
- **The DHCP helper program was updated to address a security vulnerability**
  Description
  The following vulnerability was addressed: CVE-2013-2494
- **Security Issues addressed for DHCP WANs**
  Description
  DHCP WANs use a utility called dhcpcd which had a security vulnerability. The vulnerability that was addressed:
  CVE-2013-2494
- **Security Issues addressed for the traffic dump utility**
  Description
  The traffic dump utility uses a program called tcpdump which had a number of security vulnerabilities. The vulnerabilities that were addressed:
  CVE-2014-8767
  CVE-2014-8768
  CVE-2014-8769
  CVE-2014-9140
- **OpenSSL security issues addressed**
  Description
  OpenSSL security vulnerabilities addressed:
  CVE-2013-6449, CVE-2013-6450, CVE-2014-3505, CVE-2014-3506, CVE-2014-3507, CVE-2014-3509, CVE-2014-3510, CVE-2014-3511, CVE-2014-3512, CVE-2014-3513, CVE-2014-3567, CVE-2014-3568, CVE-2014-5139
- **Security Issues addressed for bash which is used on the device**
  Description

The following security vulnerabilities in bash were addressed:
CVE-2014-6277, CVE-2014-6278, CVE-2014-7186, CVE-2014-7187

- **Security vulnerabilities addressed for the SNMP monitoring utility**

Description
The SNMP utility uses a package called net-snmp, which has several security vulnerabilities. The following were addressed with this update:
CVE-2014-8767
CVE-2014-8768
CVE-2014-8769
CVE-2014-9140

- **Update of cryptographic libraries to fix security vulnerabilities**

Description
Update of dev-libs/libgcrypt to fix the following vulnerabilities:
CVE-2012-6085
CVE-2013-4242
CVE-2013-4351
CVE-2013-4402

- **Security update to fix vulnerabilities in the Software Update and Email Alert features**

Description
Update of libtasn package to fix the following vulnerabilities:
CVE-2012-1569

Update of gnutls package to fix the following vulnerabilities:
CVE-2009-2730
CVE-2009-3555
CVE-2011-4128
CVE-2012-1573

Update of libxml2 package to fix CVE-2011-3102.

- **Security update of SSL VPN feature**

Description
SSL VPN uses the openvpn package which has some security vulnerabilities. This updates that package to address CVE-2005-3555 and CVE-2013-2061

Static Routes

- **Static Route source and destination address field order reversed**

Description
Static Routes source and destination address fields were in a different order than the static route ports which could be confusing. The rest of the interface has the source addresses first followed by the destination addresses. This applied the same order for the static route address fields.

Fixes

System

- **System can become unresponsive when loading a configuration**

Description
When a configuration is being loaded and there are static route status changes occurring the system can become unresponsive.

WAN Virtualization

- **WAN Virtualization with configuration loading could cause the system to become unresponsive**

Description
When the WAN Virtualization monitoring service would re-establish a connection during a configuration load could cause the system to become unresponsive.

- **Fixed an issue where the WAN Virtualization device MTU was too high, causing**

fragmentation and reduced TCP performance

Description

TCP throughput performance through WAN Virtualization may be worse than expected when compared to performance outside of WAN Virtualization from WAN to WAN. This is due to an MTU on the WAN Virtualization device that is too high and doesn't account for additional headers required for encapsulation.

- **Do not allow packets to PPTP port 1723 from unknown sources, with or without the firewall enabled**

Description

With the firewall disabled, and WAN Virtualization enabled, the server side was allowing packets from anywhere to port 1723. Fixed to only allow packets from known sources

VPN

- **The authentication necessary for an IPSec Security Association would not be setup properly when it was enabled**

Description

The authentication settings for VPN users that are used with IPSec security associations would not be updated when a L2TP security association was enabled or modified. This issue has been fixed.

- **Fixed VPN Statistics in the GUI to show correct byte counts**

Description

Fixed VPN statistics for IPSec VPN Security Associations with multiple connections to show total byte counts for all connections.

- **Fixed a problem with IPSec VPN Active fail-over**

Description

Fix a problem where IPSec VPN Active fail-over would work once but then not fail-over again after that.

- **Making an IPSec VPN change while an SNMP request is received can cause the system to reinitialize**

Description

When making a configuration change to an IPSec VPN security association while there is an SNMP request made to the device can cause the system to reinitialize.

Workaround

1. Disable SNMP
2. Make the VPN changes
3. Re-enable SNMP

- **Network VPN Statistics will now show correctly for translucent WANs**

Description

The View VPN Statistics within the Network Statistics tab on the View Statistics could potentially show 0 instead of the correct value.

- **The device can become unresponsive when using a PPPoE WAN with VPN**

Description

The device can become unresponsive when using a PPPoE WAN with an IPSec VPN Security Association.

Workaround

Remove the PPPoE WAN from the VPN Security Association

QoS

- **Rapid QoS changes can cause the system to reinitialize**

Description

When scripting QoS changes via the CLI, where each QoS change has an associate commit command can cause the system to reinitialize. For scripting purposes it is recommended to make all the changes then do a commit at the end.

Workaround

Change the scripts so that a commit is done after all the changes have been done.

Static Routes

- **Fixed deadlock which could occur during a configuration load if a WAN line changed status**

  Description

  Fixed deadlock issue between configuration loading and WAN or WAN Virtualization status changes.

DNS

- **Fix the GUI DNS SOA Records entry fields so that they accept the proper ranges of inputs**

  Description

  Hovering the mouse over the DNS SOA Records entry fields generate tooltips that do not accurately reflect the proper range of valid inputs. When validating, the proper values were not used. Fix pulls the proper values in for validation, such that the GUI and CLI both use the same values.

- **Fix CLI so that DNS SOA records are validated before they are input**

  Description

  Ensure that all parameters related to DNS SOA records are validated. Previously, unwanted values could be passed in, giving undesired/unexpected behavior. An email without the '@' character would previously cause a segmentation fault.

Diagnostics

- **Fix the validation for the diagnostics Iperf utility**

  Description

  The validation for the diagnostics iperf utility was incorrect

Cloud View

- **Fixed the cloud view display not working for retrieving the remote status of the sites**

  Description

  On the cloud portal a user can look at a virtual version of their site. The problem was when a user would look at the virtual version the status images would remain N/A instead of showing the proper status. This issue has been addressed.

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.

WAN Virtualization

- **WAN Virtualization uses a lower default MTU and can cause remote sites to not be able to access some Internet sites via the main site**

  Description

  The default MTU used for the WAN Virtualization device is too low for remote sites that access the Internet via the main site. This is because some sites set 'Don't Fragment' in the IP header but don't adjust their TCP MSS based on Path MTU Discovery.

Workaround

In the CLI do: "wanvirt site modify alias SITE-NAME mtu 1500; commit save"

VPN

- **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 the 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.

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 get applied.

Workaround

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