Ecessa Firmware Release Notes

Version: 12.0.0
Release: 2021.03.16
Revision 1.0: 2021.03.16

New Features

VPN

● **SSL VPN with username/password and optional multi-factor authentication login**
Additional Information
* Username/password authentication through RADIUS or Azure Active Directory integration
* Multi-factor authentication through Duo integration

Geoblocking

● **Geoblocking - block traffic passing through the device based on geographic location**
Additional Information
* Supports blocking traffic passing through the device associated with particular countries
* Supports whitelisting of addresses to exclude from being blocked by the feature
* Requires third-party integration with MaxMind GeoLite2 Country database
* Configurable automatic scheduled updating of third-party database
* This product includes GeoLite2 data created by MaxMind, available from http://www.maxmind.com

Improvements

System

● **The system smart fan can be enabled on any L7551 hardware model**
Additional Information
When the fan is not enabled it will go at full speed. If the software control fan is enabled, then it will only run depending on the temperature of the CPU. The minimum temperature is 50 C before it turns on.

VPN

● **SSL VPN client configurations now notify the server when they exit**
Additional Information
In previous versions, if a client disconnected, the session would remain open until the inactivity timeout was reached

● **SSL VPN connections were allowing VPN traffic to all LAN networks regardless of the local LANs configured for the connection**
Additional Information
With this fix, SSL VPN client access to LAN and Next Hop Route networks will be limited to just the networks configured in the Local LAN section of the SSL VPN Security Association.

Arbitrary networks can now be entered in the Local LAN section of the SSL VPN Security Association.

In order for VPN client traffic which will be routed out a WAN to return to the client, “SNAT Unmatched Traffic” must be enabled on the WAN page.

● **VPN User limit removed**
Additional Information

VPN users in prior versions were limited to 256 entries

IDS/IPS

● **IDS/IPS configuration improvements**
Additional Information
* Support for configuring a new category type, filename
* Configuring a filename category will apply to all rules present in the associated file
* Emerging Threats et/open files and descriptions have been added to the web interface and help pages
* Default configuration contains all categories from Emerging Threats et/open
* Changing the action for a category can now be done inline

Fixes

VPN

● **Loading a configuration will not stop running SSL VPNs in some cases**

● **L2TP VPN connections could leave old rules in place that would cause the static route page to hang**

● **SSL VPN server allows clients to access all LAN networks regardless of configuration**

● **IPSec L2TP VPN connections allow VPN traffic to all LAN networks regardless of the local LANs configured for the connection**
Additional Information
With this fix, VPN client access to LAN and Next Hop Route networks will be limited to just the networks configured in the Local LAN section of the IPSec VPN Security Association.

IDS/IPS

● **IDS/IPS log files are not included when downloading logs in graphical user interface**

● **IDS/IPS rules imported from external rulesets have their action overwritten to "alert"**

L2TP

● **L2TP VPN clients can fail to connect due to lock files already existing**

Certificates

● **Self-CA certificate extensions are lost after renewing the certificate**

Date

● **Timezones are not loaded from configurations**
Additional Information
Prior versions did not load timezones from configurations in most cases. Timezone values in configurations are now loaded when a configuration is loaded. If the timezone value in the configuration is malformed, the system time will be set to UTC.
It is recommended that you verify that your system timezone is correct after updating to this version. If it is not correct, change the system timezone and save your configuration.

Update

● **Firmware updates on devices that support multiple firmware versions appear to not finish**
Additional Information
The following conditions need to exist to see this issue:

* The device supports multiple firmware
* A reboot is disabled during the update

LAN

- **IPS firewall web site blocking rules will not work when a DHCP LAN has recursive resolver enabled**

HTTP Redirect

- **HTTP Redirect security settings are different than the main web service**

Additional Information

* TLS 1.2 and 1.3 are allowed
* The same cipher list is allowed as the main web service

Firewall

- **The firewall feature of the CLI does not support adding or viewing comments for firewall rules**
- **Firewall packet counters do not work**

Monitoring

- **An invalid cloud api_key on the device does not get re-pulled from the cloud**

Security

- **HTTPS TLS support versions changed. TLS supports only 1.2 and 1.3**

One-to-One NAT

- **Configuring One-to-one NAT for LAN networks larger than class C can fail to work correctly**