8.8 Release README
April 2017

New Features in this Release

- The NSE software now supports an updated version of the AG 5900 hardware that includes a plug-in module containing two SFP+ 10 Gigabit fiber interface ports. The module may be initially shipped with the unit, or can be inserted later as an add-on. There are several points to keep in mind regarding this feature:

    - The system **MUST** be powered down, and the power cord unplugged from the unit, prior to insertion or removal of the module. Severe damage to the module and/or the NSE could result if the module is inserted or removed while power is applied. (NOTE: Due to a minor change in power management required to support the module, when shutting down the system, it may be necessary to hold down the power button on the unit for a few seconds in order for the process to initiate.)

    - The requirement to power off the system does not apply to insertion and removal of transceivers from the SFP+ ports. This can be done with power either on or off.

    - The 10G SFP+ ports only support 10 Gigabit transceivers at this time. 1G standard SFP transceivers are not supported.

    - When the SFP+ ports are present and configured in the WAN role, they become the highest priority interfaces on the system. For example, if the SFP+0 slot is configured as WAN, system traffic will be routed through that interface.

- The NSE now supports a Fast Forwarding mode. When enabled, overall throughput for the total system is enhanced, offering significant improvement over the maximum rate that could previously be achieved on the specific NSE platform being used. Items to note about this feature:

    - On higher-end NSE platforms, the maximum rate the system can achieve may be limited by the line rate of the interfaces used. In order to benefit from the Fast Forwarding feature on these platforms, it will be necessary to use either the fiber interfaces, if present (discussed above), or to use multiple 1G standard ethernet interfaces (both on the network and subscriber sides) with the Load Balancing feature enabled.

    - Weighted Fair Queueing (WFQ) must be enabled for the Fast Forwarding feature to be used. If an attempt is made to enable Fast Forwarding while WFQ is disabled, a pop-up warning will be displayed.

  - Due to the mechanism used to achieve the greater data rate, events triggered from accounting statistics (bytes sent / received, for instance) could be delayed by up to 5 seconds. Thus, volume-based billing quotas could be overrun by approximately 5 seconds.

- The NSE now includes IPv6 configuration options for interfaces set to the WAN role, which allows administrative control and system traffic over IPv6. The global IPv6 enable selection has been removed, and replaced with a *per-interface* IPv6 enable/disable. (Please note, however, that ***subscriber*** traffic over IPv6 is not yet supported. This is expected in a future release).

- “Device Add” and “Device Delete” XML commands are now available to add/delete Devices to/from the NSE’s internal database (in the same manner as the User Add and Delete commands are used for regular subscribers).

- When multiple interfaces are configured in the WAN role and Load Balancing is enabled, DNS requests issued by VALID subscribers will now be forwarded from the WAN interface to which the subscriber is assigned, and thus to the DNS server address(es) specifically configured for that interface (previously, all DNS requests were considered system traffic, and were always sent from the highest priority WAN interface).

- Subscriber tracking (“Lawful Intercept”) is now supported for non-translated subscribers.

- A number of functional and aesthetic improvements have been made to the Web Management Interface.

- The RADIUS Acct-Terminate-Cause code sent in accounting stop packets triggered by zone migration is now customizable.

Hyatt Freebird Feature

The NSE Hyatt Freebird feature requires authorization from the Hyatt Corporation in order to be used. It is a licensed feature. Please contact Hyatt for inquiries regarding availability of the Freebird functionality.

Bug / Issue Fixes with this Release

- A situation with the NSE's DNSSEC feature which could potentially result in a lockup condition has been corrected.

- A link negotiation problem with certain Cisco switches has been corrected (this may also correct similar issues with other switches / interfaces if such symptoms are observed using earlier NSE builds).

- When using the NSE's Local Web Server feature, if a landing page was referenced by an "?OS=" parameter in a secure URL string (i.e., https), the redirect to that page was not handled properly. This has been corrected.

- Use of a colon character (':') in a RADIUS shared secret string now works correctly. Previously this could cause the string to be truncated.

- Use of the CLASS_NAME element in an XML Group Add command now works correctly.

- A condition existed where logging out of a serial CLI session immediately following a soft reboot of the NSE could result in a subsequent "silent" reboot. This has been corrected.

- The portal post RADIUS_LOGOUT_ADMIN_RESET message is now sent only for RADIUS subscribers when a current table entry is administratively deleted (there are certain other subscriber types that reside exclusively in NSE memory, such as Post-Paid PMS, and previously this message was being sent for those as well).

- Tables displayed in the Web Management Interface will now scroll properly on Apple iOS devices.

- A condition in which the NSE could stop sending XML Portal Post messages has been fixed.

- PPPoE authentication using PAP now works correctly.

- An interface set to PPPoE will now operate properly immediately after being changed to WAN from OOS (previously the system could require a reboot before the PPPoE connection could be successfully established).

- Command Line Interface settings for the Bandwidth Management feature are now located in their own sub-menu (under Configuration).

- Using the RADIUS "Remember Me" login option could result in an endless loop if no credentials were entered. This has been corrected.

- Routing for multiple WAN ports now works correctly when Load Balancing is disabled.

- The character limit for Facebook App IDs has been increased.

- On the Subscriber Administration / Statistics page, the "Subscriber Licenses in Use" field could give an incorrect count of the number of licenses used in the event that AAA was disabled (entries in the NSE database were included in the total even though they are not effective in this situation). Now if AAA is off, the database entries are omitted from the total.

Known Issues with this Release

- Subscribers with an IP address on the same subnet as a Remote IPSec subnet do not get redirected to the splash and login page correctly.

- On the AG 5900 only, power management changes in this release require that the power switch be depressed for at least five seconds to shut down the unit.

- There are certain addresses on the NSE that are considered “blacklisted” – that is, they are defined for specific purposes and are reserved, and therefore unavailable for use by subscribers (these include WAN interface addresses, DNS server entries, iNAT pool addresses, and some others). In previous builds, a defect existed in which it was possible to configure a DHCP pool such that the pool scope could overlap these addresses, and the conflict was not caught. This was corrected in the 8.5 release. However, if while on a build prior to 8.5 such a situation did exist, and the system is then upgraded to 8.5 or later, after the upgrade, the “offending” DHCP pool will be deleted, and a DHCP-related syslog will be sent. If this occurs, it will be necessary to re-create the pool (and if while creating the new definition the same conflict arises, the system will now catch this and not allow the pool to be created incorrectly as before).

- When configuring any of the physical Ethernet ports other than the labeled WAN interface to function in WAN mode, care should be taken by administrators to insure that a given port that has been functioning in the WAN role is *not* inadvertently changed to the Subscriber role while a physical connection to a WAN-side subnet is still in place. If that occurs, and the NSE’s subscriber-side DHCP service is running, hosts on the WAN subnet may begin to pick up addresses from the NSE’s subscriber pool(s), and find that web requests are being re-directed to the NSE’s login page.

- The support for multiple WAN ports provides the ability to balance subscriber traffic between two or more WAN ports. However, these features are not all available after a software upgrade without additional actions. Load balancing and failover of subscriber and administrative network traffic require upgrading the per-unit license to include the Load Balancing feature. Without this feature, support for multiple WAN interfaces is strictly limited. Subscriber traffic will be able to use only a single WAN port, and the system will have no ability to automatically direct traffic to alternate WAN ports in response to a network link outage. This behavior will also be seen if a license upgrade has been performed but Load Balancing is disabled, which in large part restricts the NSE’s WAN functionality to that of previous software releases. If you wish to use multiple network WAN links, Nomadix strongly recommends purchasing the Load Balancing upgrade, and for full functionality Load Balancing should be configured in either Failover or Load Balancing modes.

- If two or more NSE interfaces are set to the WAN role and are configured such that they are attached to the same local subnet, if there is a port failover event for one of those ports, packets will then be sent using a different source address. Therefore, any systems or devices on that subnet that invoke processing decisions based on packet *source* addresses (such as RADIUS servers) should be configured so that they will respond to any of the NSE interface addresses that are configured on that subnet. For example, if two NSE WAN ports having addresses of 205.5.6.10 and 205.5.6.20, respectively, are directly connected to the 205.5.6.0 subnet, and a RADIUS server is located directly on the 205.5.6.0 subnet, the server should have both 205.5.6.10 and 205.5.6.20 configured as valid RADIUS client addresses in order to guarantee that any RADIUS requests originating from the NSE for that server will be accepted.

- If two or more ethernet interfaces are configured in the WAN role, and both Load Balancing and Class-Based Queueing are enabled, when a subscriber logs in via RADIUS to an account that returns both the Preferred WAN and Class attributes, that subscriber will be assigned to the correct WAN port and class accordingly, and will be shown as such in the current table. However, if subsequently internet access becomes unavailable for the WAN interface to which the subscriber is assigned, the subscriber’s traffic should be routed out through a different available WAN interface, but the current table will not accurately indicate this (i.e., the preferred WAN port will still be shown as the active primary, and the class information will not display the asterisk that indicates that the class cannot currently be applied to the subscriber's traffic).

- When configuring two NSE's to operate in system failover mode, it is important to remember that the Ethernet Port settings are NOT transferred from the Primary to the Secondary. This includes not only the IP address information (including DNS), but the port role settings as well (i.e., WAN, SUB, or OOS). This can become an issue if the NSE is configured with multiple WAN or subscriber ports, or any other changes from the default port roles. Therefore, assuming that it is desired for both the Primary and Secondary to have the same logical port role setup, the port role configuration on the secondary NSE should be manually configured to match that of the primary prior to enabling the failover operation.

- The clustering feature provides a means to spread a large number of subscribers across multiple NSE's. However, there is a limitation with regard to the number of defined port locations that can be configured. A given NSE does not support more defined port locations than the number of licensed users on that unit, and the port location configuration will need to be common to all units in the cluster. Therefore, the maximum number of port locations that can be defined will be equal to the number of licensed users on a single NSE in the cluster. For example, if a cluster is set up using two AG5800's, each of which has a license key enabling 4000 users, the maximum user count will be 8000, but the maximum number of port locations that can be defined will be 4000.

- When initially configuring the clustering feature in an existing installation (which will normally involve adding one or more additional NSE's and then enabling the feature), if certain users appear to lose access, this can be corrected by having those users disconnect and then reconnect again.

- When configuring multiple WAN interfaces, please note that explicitly labeled ports (WAN and LAN) cannot be configured to the opposite role. Such ports may set to Out Of Service, but explicitly labeled WAN ports may not be configured to the SUB role, and vice versa. Ports labeled Eth(X) or Aux(X) may be configured to any role.

- When the NSE is placed in bridge mode, all packets that arrive at any interface will automatically be propagated to all other interfaces, unless those interfaces are currently set to OOS (Out of Service). Therefore, if the NSE is configured to use multiple WAN interfaces that connect to different subnets, entering bridge mode has the effect of creating direct connections between those subnets. This is usually an undesirable condition. It is recommended that only one WAN interface should be active before placing the NSE in bridge mode (either by placing all other WAN interfaces into the OOS role, or by physically disconnecting them).

- When using a routed subscriber configuration, if Cisco HSRP (Hot Standby Router Protocol) is being used for routers on the subscriber side of the NSE, there are some additional issues to consider. HSRP routers are normally configured to use virtual MAC and IP addresses, and these defined values must be entered into the NSE's ARP and routing tables as appropriate. However, for certain functions (such as ARP requests), the HSRP routers use the physical source MAC and source IP of its NSE-facing interface, instead of the virtual values. For this reason, it is necessary to configure the NSE to add persistent ARP entries for physical IP and MAC addresses of each NSE-facing router interface of all directly connected routers on the subscriber side.

- In 8.0 and later releases, SIP ALG processing has been removed. The NSE utilizes Endpoint-Independent Mapping for UDP traffic; thus, allowing SIP clients to successfully negotiate connections through the gateway without a need for the internal SIP ALG processing that the NSE previously provided.

- When using Micros Fidelio PMS, an option now exists to disable the need to enter the Registration Number (configured on the WMI PMS page). If this option is used, administrators will also want to modify the prompt string that appears on the page on which subscriber enter the PMS login credentials, so that it doesn't refer to the registration number field. This can be done by modifying the string in the “Micros Fidelio Login Message” field, located on the Subscriber Interface \ Login UI page.

- Certain features in this release (SSL, HTTPS Redirection, and HTTPS management connections to the Web Management Interface) require that a working set of certificate files (consisting of cakey.pem, cacert.pem, and server.pem) is installed on the flash. This release ships with a “dummy” set of these files that will allow these features to be enabled; however, if these dummy files are used, any systems that attempt to connect to the NSE using such connections will receive security warnings. Please see the section in the User Guide that covers the set up of the SSL feature for instructions on how to configure a properly working set of certificate files for your specific installation.

- The NSE’s IPSec feature now includes a NAT Traversal option. This can be used in cases where there are one or more NAT’s between the NSE and the IPSec tunnel endpoint that are unable to translate IPSec traffic. It should be noted that in such situations, if NAT Traversal is *not* used initially, the NSE may still report that tunnel(s) are up, but actual tunneled traffic will not get through (this is because the negotiation phase may not be able to directly detect the presence of the NAT’s in the path). If this occurs, it is recommended to enable NAT Traversal and see if this corrects the difficulty.

- Connections from mis-configured (i.e., translated) subscribers that run over UDP do not support UDP fragmentation. If transactions from such users (such as TFTP connections) are not successful, it may be necessary to adjust the endpoint configurations so that fragmentation is not invoked.

- If a user is entered via the XML User Payment Plan command and a defined X-over-Y plan is specified, then the Current Plan field in the authorization database will be set to -1 (simply denoting entry via XML), instead of flagging the XoverY plan properly. This prevents the logout / log-back-in feature from working. However, if the user is added via the XML Add User X-over-Y command and the same plan is specified, the user will be entered with the Current Plan field flagged correctly (as *n, where n is the plan number). The logout function will then work properly.

- When the NSE is configured to use GRE tunneling and GRE is enabled, any servers / hosts that provide essential network services (such as DNS, RADIUS, FTP, Portal Page / Post, or other services that need be accessed through connections originated by subscribers or by the NSE itself) SHOULD NOT be configured with non-tunneled local addresses (i.e. on the same subnet as the NSE WAN interface). Access to devices / hosts on the immediate non-tunneled local subnet is undefined for NSE-initiated connections when GRE is enabled. The NSE’s management interfaces will continue to be accessible from systems on the local subnet via the NSE’s WAN IP, *provided that those devices are initiating the transaction*, but it should be assumed that traffic originating from or “through” the NSE will be routed through the GRE tunnel.

- Changing the PMS payment mode (from pre-pay to post-pay, or vice versa) while PMS subscribers are currently in a valid state may result in erroneous charge and/or logout behavior for those subscribers. It is recommended that if a configuration change of the payment mode is required, the operation should be performed when no PMS subscribers are logged in.

- ICC does not support changing billing plans if subscribers purchased access with Post-Paid PMS.

- When the NSE is configured to use a dynamic address (whether via DHCP or PPPoE), but for some reason is unable to obtain one (such as a link-down condition on the network side) subscriber-side access to the unit will succeed only if the subscriber system is on the same subnet as the NSE's Administrative IP.

- The SNMP MIB contains SNMP objects for all major NSE features running on the Access Gateway. If your current license does not contain a particular feature, you will not be able to GET or SET the object for the feature.

- You cannot configure Auto-Configuration using SNMP.
- You cannot Delete All DAT Sessions using SNMP.
- You cannot configure PMS interface settings using SNMP.
- The Administrative interface that displays the DAT sessions for the Nomadix NSE shows both Active and Inactive sessions at the same time. While the DAT session cleanup routine is working, there will still be inactive sessions on a unit that are displayed in the management interface.

Contact Information

Corporate:

Nomadix, Inc
30851 Agoura Road
Suite 102
Agoura Hills, CA 91301
USA
++1.818.597.1500
http://www.nomadix.com/

Sales:

++1.800.NOMADIX
sales@nomadix.com

Technical Support:

++1.818.575.2590
support@nomadix.com