Software
Release Notes

Version 1

P/N D211051

NetEnforcer E8.1.1

AC-400/800 Series

This document details new features, known issues and clarifications concerning NetEnforcer software version E8.1.1. This release pertains only to the AC-400 and the AC-800 Series.

Please check http://www.allot.com/support/support_tech_info.asp for any updates to this document.

New Features

Allot Protocol Updates (APU) Support

Allot NetEnforcer version E8.1.1 supports Allot Protocol Updates (APU) mechanism which is activated through the NetXplorer.

This mechanism enables the user to update supported applications and protocols easily, frequently and without any interference to system and network operation. Through this mechanism the efficiency of DPI is greatly improved as well as its resiliency over time, since Internet applications tend to change regularly. Since software upgrades are no longer needed in order to upgrade identification facilities, no service downtime occurs during protocol updates.

The NetXplorer notifies the user when new updates are available, and then the user can easily install them by using the NetXplorer APU user interface.

Additionally, the APU protocol packages are posted on Allot's website periodically, and can be easily downloaded and installed by users whose NetXplorer is not connected to the Internet.

Allot Protocol Updates will be available only for products with valid support contracts. This means only NetXplorers and NetEnforcers under a valid support contract will allow the protocol pack upgrades to take place.

Please see the NetXplorer operations guide for more details on APU.

Enhanced protocols and applications support

Allot NetEnforcer version E8.1.1 comes with new and improved protocols support.

The new protocols support offers major capabilities in several application domains:

- **P2P Applications** – enhanced support for existing P2P software which includes the latest encrypted P2P support (Gnutella, eDonkey, Bittorrent), minimizing misidentifications and improved identification efficiency. Additionally, support for new P2P software is introduced with this version such as Thunder, NNTP, BitTorrent DNA, Pando, HTTP Download Manager & HTTP File Transfer.
- **Instant Messaging with Multimedia Support** – beyond the enhanced ability to classify the most popular versions of instant messaging applications (GoogleTalk, ICQ, MSN, Yahoo, QQ, Skype & Gadu Gadu), it is now possible to classify according to additional types of the application used (chat/voice/data/video). Support was added for IM+ (a mobile instant messaging application), MySpace instant messaging application and PalTalk instant messaging application.
- **New Streaming Applications** – among the newly supported applications are Joost, SlingBox, RTMP, IPTV, AOL streaming, CNN streaming, DivX WebPlayer, Gyao, QVOD, HTTP Streaming, iPlayer, iView, Veoh and more.
- **Gaming** – support for popular online games is included: XBOX and other gaming consoles, World of Warcraft, LineAge II, Yahoo games, GuildWars, RuneScape, Second Life, Counter Strike, Ragnarok, Knight Online, GTA4 (Grand Theft Auto IV for PlayStation 3), Tibia , Entropia, GaiaOnline, XFire, Chinese games and more.

In addition, GRE (Generic Routing Encapsulation) encapsulation is now supported. This means it is possible to identify applications tunneled over GRE.

A new protocols identification engine is introduced with this version, which both improves current protocol support and will enhance future protocol support. This new engine brings flexibility and modularity to the protocol identification realm and extends the platform's identification abilities. The high-end NetEnforcer devices use the same engine for protocols identification.

New Protocols and Applications

This version supports Allot Protocol Updates package version 2.7 and above.

For a complete list of the supported protocols and applications and for details on upgrading your protocols identification with the recent protocol pack go to http://www.allot.com/protocol-updates/ .

Resolved Issues

The following issues were solved or improved in E8.1.1:

- A VC/Pipe set to Ignore QoS no longer shows any bandwidth in the LCD or CLI.
- There are no longer any system failures when changing IP via the LCD.
- The Primary Domain Name Server (DNS) can be changed via the GUI.
- When adding a pipe or a VC via CLI, both group entries and non-group entries can be now used.
- Acstat command now shows Host ID instead of host name when using template with host group.
- “Parse by Port” is enabled by default for services which typically use UDP with fixed ports (e.g. TFTP and IKE).
- Changing the NetEnforcer device key will not automatically initiate a reboot, only in cases where it is essential (such as bandwidth control level changes)
- The following misclassification issues were resolved in version E8.1.1:
  - RTP is now handled efficiently and without errors
  - CamFrog is now properly identified
  - EyeBall is now properly identified over UDP
  - Hopster chat is now classified correctly
  - PCAnywhere is now properly identified
  - Identification of many SSL-encrypted applications was improved
  - GoogleTalk is now properly identified
  - MS-Exchange is properly identified (enabled by defining it as "parse by port")

Known Issues

- As stated above, E8.1.1 is aligned with protocol pack 2.7. As of protocol pack 2.7 the HTTP service catalog categories (HTTP Streaming, HTTP Audio, HTTP file transfer, HTTP browsing & HTTP Download Manager) are not supported for the AC-400/800 products and should not be used in the policy (please note a policy with HTTP categories defined can be saved but it has no meaning). HTTP content service catalog entries can be used instead where applicable. All HTTP traffic will be classified as HTTP unless HTTP content service entries have been defined.
- It takes about 2-3 minutes for the NetEnforcer to boot up if the NTP Server on the NetXplorer is not available.
- Setting line policy action access to reject isn't allowed.
- The upper interfaces of the AC-404 (Internal 2 and External 2) support speeds of up to 100Mbit/sec and do not support 1GBE speed.
- In the AC-400 series, parallel redundancy is not supported between devices with different backplane versions.
  In order to check backplane version use: acdc –i command. The output is either “CPLD Version” or “Logic Version”.
- After the first upgrade or following an improper shutdown, it might take up to 30 minutes for the device to load in extreme cases.
- It is advisable to use drop action instead of reject on policy elements defined by HTTP content rules due to some system limitations.
- When changing the bandwidth capacity limits (Inbound & Outbound defined the same) only the Outbound bandwidth limit is updated. The Inbound bandwidth remains the same (max allowed). Allot suggest to use "Inbound & Outbound defined separately" once in order to enable saving the changes which were made.
- No host classification by MAC address in an environment that uses ISL, VLAN and MPLS in combination.
- If the clocks of the NetEnforcer and the NetXplorer server are not synchronized and the time difference exceeds 1,024 seconds (approximately 17 minutes), the NetEnforcer unit will reboot itself.
- The device might malfunction when multiple lines are configured on a device which obtained a license key with single line support.
- An Active Redundancy configuration set via NetXplorer will take effect only after the NetEnforcer is rebooted.
- When using AC-40X versions in redundancy mode, one should disconnect the bypass beforehand. This can be done using the following CLI command: go config network –bypass_unit disable.
- It is only possible to exit bypass mode by rebooting the unit, not via the LCD.
- In some cases when changing parameters on the LCD while the management port is disconnected might cause the unit to fail. A reset is required for recovering the unit.
- In some cases misclassification of traffic occurs when the host entry assigned to Pipe/VC includes hostnames.
- After adding a new pipe through the GUI or CLI, the new pipe will be presented below the Fallback Pipe when viewing the list of Pipes in the CLI (go list pipes command). In the GUI however the new Pipe will be presented correctly. Note that although the Pipe presentation in the CLI is incorrect the traffic will be classified correctly to the Pipes.

- This version does not work in NetXplorer One mode (standalone).
- The following application misidentifications might still occur in E8.1.1:
  - In some cases eDonkey UDP connections might not be detected by the NetEnforcer.
  - Some of the ICQ traffic might not be detected by the NetEnforcer.
  - Yahoo messenger is occasionally misidentified in a proxy environment.
  - Napster web site traffic might be occasionally misidentified as P2P.

NetEnforcer Software Upgrade Procedure

For use with NetXplorer Server

If the NetEnforcer being upgraded will be managed by the full NetXplorer Server along with one or more other NetEnforcers, follow this procedure:

NOTE Users must receive a new key in order to upgrade to version E8.1.1 if upgrading from E7.4.X or previous versions (no need for a new key if upgrading from E8.1.0)

NOTE The Software Upgrade Procedure may fail if your NetEnforcer database is corrupted. In such cases, please consult Allot Customer Support at support@allot.com.

NOTE From this version, HTTP categories are no longer supported for AC-400/800 platforms (see known issues). Therefore, when upgrading from E8.1.0 with protocol packs 2.4, 2.5 or 2.6, please make sure your policy is adjusted accordingly after upgrading to E8.1.1 (does not contain HTTP categories).

1. Download the software version from the Allot ftp site by completing the following steps:

   - Open Telnet and log in to the NetEnforcer as User Name: **root** Password: **bagabu** (default).
   - Type **mkdir E811**.
   - Type **cd E811**.
   - Type **ftp ftp.allot.com** (the IP address is **69.56.134.142**)
   - Log into the ftp site with username: **Anonymous** and password: **<YOUR EMAIL ADDRESS>**.
   - Type **cd** /AC-Releases/Current_Versions/NetXplorer/NetEnforcer/AC-X0X/E811
   - Type **hash**.
   - Type **bin**.
   - Type **prompt.**
   - Type **mget ***

   All required files will be downloaded automatically.

   These include the following:

   - ne-instl.sh
   - ne-E8.1.1-7.tgz
   - packages-ne10.tgz

   When the download finishes, type **bye**. This will close the ftp site but leave Telnet open.

2. If upgrading from a basic management version (E5.x or before), please consult the Allot Database Conversion Guide for instructions regarding your database (Link to KB article: http://www.allot.com/support/KBItemDetails.aspx?ItemID=5537852).

   In addition, in case you are using QoS with burst definitions, make sure that the maximum burst is not higher than the maximum of the rule you are using it in.

   If you are upgrading from version E7.x.x or later, continue with the installation.

3. Type **chmod u+x ne-instl.sh**
4. Type **./ne-instl.sh**
5. The upgrade procedure could take as long as 10 minutes and then the unit will reboot.
6. **You will be prompted to enter a new key and to replace your password**.

NOTE Upon reboot an automated file system repair is performed. This can cause the reboot to take longer than usually (In rare cases, it can take more than 10 minutes), please wait patiently for the system to come up. Note: the first time this will be performed is at the reboot that follows the upgrade.

Changing Passwords

Notes The device's root password **must** be changed during upgrade/install. This is done in order to restrict the access to the device's CLI only to authorized users.

You should change the default passwords to ensure a minimum level of security.

You can change the login password for the Admin user, which has access to all NetEnforcer functions. It is **strongly** recommended to change the default password. NetEnforcer might enable access from anywhere on the Internet, and should therefore be protected with a unique password.

1. In the NetEnforcer Setup Menu, enter **3** (Change password) and press <**Enter**>.
2. Enter **1** to initiate the password change for the Admin user and press <**Enter**>.
3. Enter a new password and press <**Enter**>. The password must be between 5 and 8 characters. You can use a combination of upper and lower case letters and numbers.
4. Re-enter the password and press <**Enter**>. If NetEnforcer detects a simple password, a warning is displayed on the screen.