EncrypTight Release Notes, Version 3.4

This release note describes new features, requirements, known issues, and bug fixes in EncrypTight Manager Version 3.4.

What's New in EncrypTight Manager Version 3.4?

Network Addressing Mode Changes

ETM has enabled multiple configuration options for network addressing mode for encryption over the internet [ETM-905].

ETEP5-LC Support

- ET0005A enables NTP and specifies a ETM server as the time source by default [ETM-896].
- ETM does not support a throughput speed for ET0005A. Throughput speed is empty [ETM-875].
- ETM port configuration requirements for ET0005A [ETM-873].

vETEP Support

- ETVEP data transfer report [ETM-882].
- ETVEP Licensing interactions with Policy Mgmt in ETM [ETM-879].
- UI changes to support CPU licensing for ETVEPs [ETM-872].
- ETM supports a ETM license that includes CPU counts for ETVEPs as well as bandwidth licenses [ETM-871].

MPLS Encryption Option

- ETM has added an MPLS encryption option to the L2 Mesh Policy UI and enforced its usage for 2.2+ only ETEPs [ETM-876].

ETM UI Changes

- ETM has added a Security tab in the PEP edit form [ETM-864].
- ETM has added a Time Settings Tab [ETM-883].

Remote in-band management

ETM has added an in-band-management configuration attribute to the management interface [ETM-863].

RIBM allows devices to be managed remotely without using external switch ports to connect to the management port. The ETEP has a single management interface and single management IP address.

- Either out-of-band management or RIBM must be enabled, and both cannot be enabled at the same time
- If RIBM is enabled, then the management IP interface of the ETEP is reachable only via the remote port.
- If RIBM is enabled, then the local port cannot be used to manage the device

RIBM traffic passes through the data plane, so the administrator must set “pass TLS in the clear” or configure a policy to allow it to pass through the data plane

Transparent or non-transparent mode

All policies supported (L2, L3, L4) (except L2 IKE is **not** supported)

Remote IP and Management IP can use the same address

No IPv6 for RIBM

How RIBM affects ETM

With the release of 2.2 PEP software special policy design considerations must be taken into account for ETM access to ETEP devices for protocols such as FTP and SSH. Before the release of 2.2, all ETEPs were managed Out of Band. The management port was typically connected to the Local port LAN segment and followed the rules defined by the policy for that LAN segment. In most cases, TLS traffic was always passed in the clear and other management protocols such as FTP were encrypted and decrypted using the configured policy.

With the release of 2.2 ETEP code and the ET0005A, RIBM may change behavior depending on the addressing scheme used for the management IP addresses of the ETEP. If the management network is configured for a different IP subnet than that of the Customers LAN segments, protocols such as FTP and SSH will be blocked since the RIBM IP address does not match the configured policy. In this scenario, protocols such as FTP and SSH will be dropped by the remote ETEP and prevent upgrades, appliance log file retrieval and SSH access to the remote device.

NOTE

Although this may be a corner case in transparent mode, it will always be the case when the ETEP is in Non Transparent mode where the Management IP address will in most cases be the same IP address as the Remote port and not match the customers encryption policy.

Any operation that only requires TLS and XMLRPC will not be affected. For example, refresh status, policy deployments, statistic gathering etc..,

To prevent the potential problem defined above, an EZMesh Policy MUST be configured as the highest priority policy or before any encrypt policy using the wildcard address of 0.0.0.0 and the IP address of the ETM server. If ETM is configured as a cluster, include all /32 addresses of each node in the cluster.

Below is a screen shot of an example Easy Mesh policy that prevents the issue noted above. Also below is a diagram depicting the topology or addressing scheme that would require the Easy Mesh policy.

Figure 1 Add Easy Mesh Policy Menu

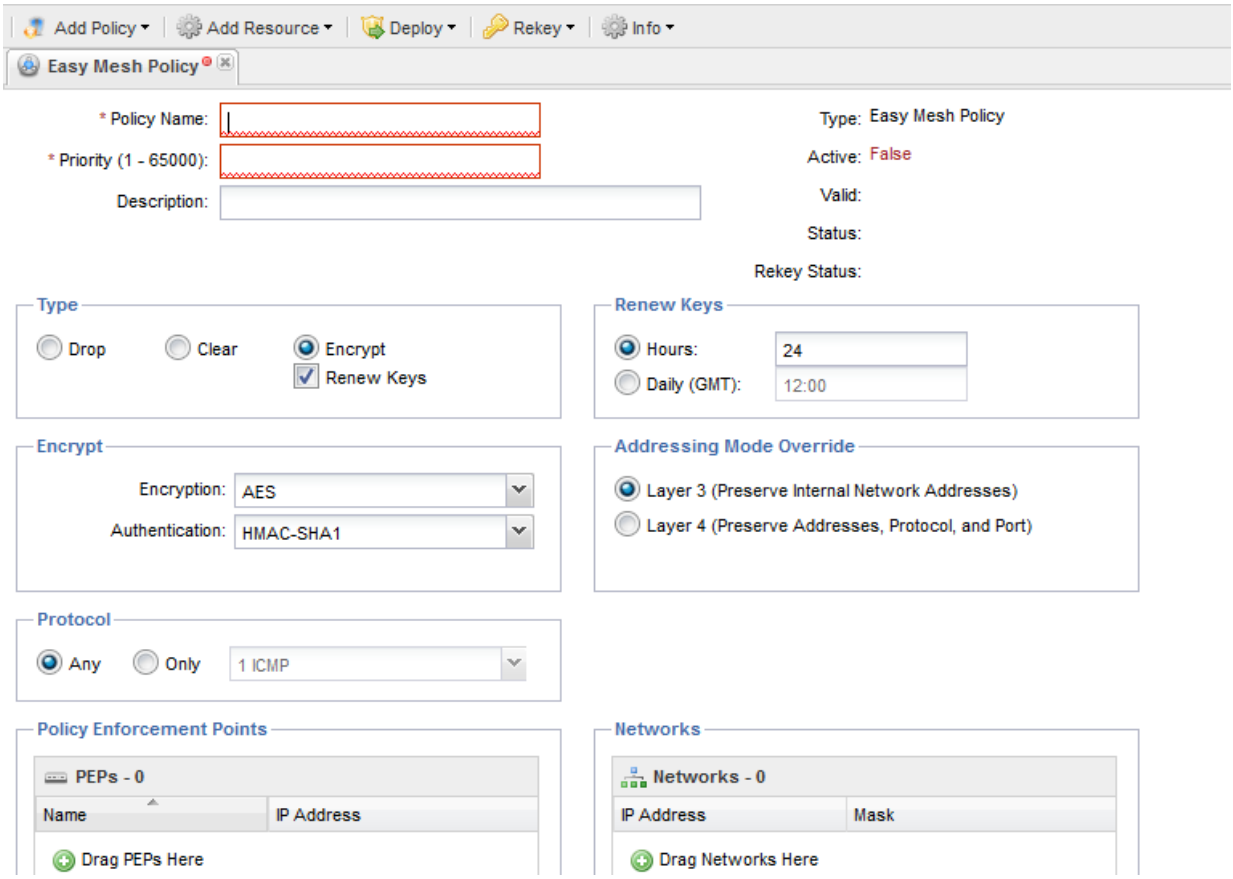

Figure 2 Topology Requiring Easy Mesh Policy

System Requirements

Software Requirements

The minimum version of VMWare supported is ESX 4.0 update 1 (or higher), released in June 2010.

Browser Requirements

For optimal security, stability and performance, the latest major release of the following browsers are fully supported and tested on a rolling basis*:

- Microsoft Internet Explorer®
- Mozilla Firefox®
- Google Chrome™

* Earlier versions and unlisted browsers may be fully or partially supported.

Known Issues

There are no known issues to exist in EncrypTight Manager, Version 3.4 at the time of release.

Resolved Issues, Additions, and Modifications

Issues noted below have been resolved, added, and/or modified in EncrypTight Manager, Version 3.4.

[Issue 592] - Implemented a new upgrade (updateSoftware) task for 2.0 appliances - poll for progress.

[Issue 827] - Replaced the use of companyName with oemKey or companyKey.

[Issue 856] - Allows ssh terminal access to the policy server and PEPs directly through ETM.

[Issue 865] - Does not restart server when upgrading/downgrading cluster.

[Issue 866] - Filters the PEP Edit form device type and software version stores according to the device type's minSoftwareVersion.

[Issue 867] - SSH command line access through ETM.

[Issue 883] - Moves NTP settings to a (new) Time Settings tab in the PEP Editor.

[Issue 887] - Only allows PEP deviceType or softwareVersion to be edited in dev mode, unless pre-provisioned or template.

[Issue 912] - Provides support in ETM for calling ntpdate with 2.2. appliances.

[Issue 926] - Copy PEP command does not include all critical fields that would need to be modified for the copy to succeed.

[Issue 931] - PEP configuration state is set to NOTEQUAL if PepOpInterceptor modifies any values in preCreate.

[Issue 933] - The ET0005A max MTU is 1500.

[**Issue 973] -** Treat TLS communication to PEP in FIPS mode the same as if ETM (overall) were using a FIPS provider.

[Issue 1098] - ET0010A and ET0100A interfaces (local and remote) have been made configurable for 1G speed. An additional drop down option for local and remote interfaces has been added. GigabitFullDuplex is now an available option.

Related Documentation

EncrypTight Manager

- EncrypTight Manager Installation Guide
- EncrypTight Manager User Guide

Encryption Appliances (PEPs)

- ETEP Enforcement Point, Installation Guide
- ETEP Enforcement Point, CLI User Guide
- ETEP Enforcement Point, Release Notes

Contacting Black Box Technical Support

Contact our FREE technical support, 24 hours a day, 7 days a week:

- Phone: 724-746-5500
- Fax: 724-746-0746
- e-mail: info@blackbox.com
- Web site: www.blackbox.com