Support of Outdated Encryption Algorithms

SafeUTM is based on Fedora operating system. In Fedora 33, which was used in the previous SafeUTM version, the current system-wide encryption policy has been updated to further disable outdated cryptographic protocols (TLS 1.0 and TLS 1.1), weak Diffie-Hellman key exchange sizes (1024 bits), and the use of SHA-1 hash in signatures. You can read more about changes in the algorithm policy in the **article**.

Outdated algorithms, like (cryptographic) hashing and encryption, usually have a lifetime after which they are considered either too risky or even unsafe to use.

You may have problems related to HTTPS, for example, when running OWA (web interface for accessing Microsoft Exchange). If you encounter this, follow these steps to switch to the encryption policy levels compatibility mode:

1. Log in to the SafeUTM console. This can be done from the local menu, SSH, or SafeUTM web interface.
2. Enter `update-crypto-policies --set DEFAULT:FEDORA32` the command in the terminal.
3. Reboot SafeUTM.

> We strongly do not recommend using this setting, since after the next update of SafeUTM compatibility mode settings will be reset. And in newer versions, this feature will be disabled.

Revision #3
Created 27 August 2022 22:35:11 by Val Redman
Updated 13 October 2022 16:21:21 by Val Redman