Best Practices to Secure an ESA

Document ID: 118462

Contributed by Cisco TAC Engineers.

Oct 09, 2014

Contents

Introduction

The Cisco Email Security Appliance (ESA) is an extremely secure product "out−of−box" and needs minimal changes to create a secure system.

Procedure

The following are a combination of fundamental recommendations and next−level security practices to further secure the system and reduce the potential of the ESA becoming a security risk:

1. Re−name the default administrator password to a more secure variant.
2. Disable telnet, if possible. Telnet transmits data, including passwords, in clear text, which can be subject to numerous types of attacks.
3. Disable any network services not required; this includes HTTP and FTP. Please review the user guide for more information about specific service functionality.
4. Restrict access to the administrator account by creating user accounts based on necessary access requirements. Please refer to the user guide for "Adding Additional Users."
    − In addition, create operator accounts for all administrators.
5. Using SSL/TLS, obtain an SSL certificate from a CA or create a self−signed certificate. Since every ESA uses the same demo certificate, it is not secure and not recommended for general use.
6. Separate mail and management functionality onto separate network interfaces. This reduces the chance of unauthorized users from being able to access your internal 'Management' Network. Please refer to the user guide for "IP Interfaces."
7. Upgrade to the latest version of the AsyncOS.

Related Information

- ***Cisco Email Security Appliance − End−User Guides***
- ***Technical Support & Documentation − Cisco Systems***