How do you automate log transfers?

Document ID: 118292

Contributed by Cisco TAC Engineers.
Aug 15, 2014

Contents

Question

How do you automate log transfers?

Environment

Cisco Email Security Appliance (ESA), Web Security Appliance (WSA), Security Management Appliance (SMA), and all versions of AsyncOS.

Many different types of logs are created on the Security Appliance. You may wish to have the appliance automatically transfer certain logs to another server.

This setup can be done via the GUI or CLI using the FTP or SCP protocols. Please read specifics below:

GUI

1. Go to ***System Administration -> Log Subscriptions***.
2. Click the log name of the log you wish to modify under the 'Log Name' Field.
3. Under 'Retrieval Method', you may select 'FTP on Remote Server' or 'SCP on Remote server'.
4. Enter the correct values in the appropriate scenario you choose. If you are not familiar with the correct values, please contact your systems / network administrator as they can help you determine which servers are available in your network.

CLI (Command Line Interface)

See the following CLI sequence:

```
S-Series> logconfig
[]> edit
[]> <appropriate number correlating to the log you wish to modify>

Please enter the name for the log:
[Log_name]> <enter for default>

Log level:
1. Critical
2. Warning
```

```
3. Information
4. Debug
5. Trace

[3]> <enter for the default>

Choose the method to retrieve the logs.
1. FTP Poll
2. FTP Push
3. SCP Push
```

Choose the method that you desire to set up. From this point, the CLI will walk you through the same connection settings that are available in the GUI.

These are as follows:

FTP

- Maximum Time Interval Between Transferring: 3600 seconds
- FTP Host: Host name / IP address of the FTP server
- Directory: Remote directory on FTP server (relative to the FTP logon. Typically '/')
- Username: FTP username
- Password: FTP password

SCP

- Maximum Time Interval Between Transferring: 3600 seconds
- Protocol: SSH1 or SSH2
- SCP Host: Host name / IP address of the SCP Server
- Directory: Remote directory on SCP server (relative to the SCP logon. Typically '/')
- Username: SCP username
- Enable Host Key Checking
- Automatically Scan
- Enter Manually

NOTE: FTP is a plain text protocol, meaning that sensitive data may be readable by some one who is sniffing network traffic. SCP is an encrypted protocol, thus making sniffing ineffective at snooping data. If the data is sensitive and security is a concern, it is recommended that SCP be used instead of FTP.

Updated: Aug 15, 2014 Document ID: 118292