ログの転送を自動化するには？

目次

質問

ログの転送を自動化するには？

環境

Cisco E メール セキュリティ アプライアンス (ESA)、Web セキュリティ アプライアンス (WSA)、セキュリティ管理アプライアンス (SMA)、および AsyncOS のすべてのバージョン

多くの異なる種類の口グがセキュリティ アプライアンスに作成されます。 アプライアンスが何らかの口グを別のサーバに自動転送するのがよい場合があります。

この設定は、FTP または SCP プロトコルを使用して、GUI または CLI で行うことができます。下記の詳細をお読みください。

GUI

1. [System Administration] > [Log Subsctiptions] に移動します。
2. [Log Name] フィールドで、変更するログのログ名をクリックします。
3. [Retrieval Method] で、[FTP on Remote Server] または [SCP on Remote server] を選択します。
4. 選択した該当するシナリオに正しい値を入力します。 正しい値がわからない場合は、システム管理者またはネットワーク管理者に連絡し、どのサーバがネットワークで使用可能かを確認してください。

CLI (コマンドライン インターフェイス)

次の CLI シーケンスを参照してください。

```
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
```

セットアップに使用する方式を選択します。 ここからは、CLI によって GUI で使用可能な接続設定と同じ設定の手順が示されます。

これらは次のとおりです。

FTP

- 転送最大間隔： 3600 秒
- FTP ホスト： FTP サーバのホスト名または IP アドレス
- ディレクトリ: FTP サーバのリモート ディレクトリ (FTP ログオンとの相対。 通常は「/」)
- ユーザ名： FTP ユーザ名
- パスワード： FTP パスワード

SCP

- 転送最大間隔： 3600 秒
- プロトコル： SSH1 もしくは SSH2
- SCP ホスト: SCP サーバのホスト名または IP アドレス
- ディレクトリ: SCP サーバのリモート ディレクトリ (SCP ログオンとの相対。 通常は「/」)
- ユーザ名： SCP ユーザ名
- ホストキーチェックを有効化
- 自動スキャン
- 手動設定

注： FTP はプレーン テキストのプロトコルなので、ネットワーク トラフィックを傍受している人がセンシティブ データを読み取る可能性があります。 SCP は暗号化プロトコルであるため、データのスヌーピングがされても傍受の効果はなくなります。 データが機密でセキュリティが問題となる場合、FTP ではなく SCP を使用することを推奨します。