Wie automatisieren Sie Protokollübertragungen?

Inhalt

Frage

Wie automatisieren Sie Protokollübertragungen?

Umgebung

Cisco Email Security Appliance (ESA), Web Security Appliance (WSA), Security Management Appliance (SMA) und alle Versionen von AsyncOS.

Auf der Sicherheits-Appliance werden viele verschiedene Protokolltypen erstellt. Möglicherweise möchten Sie, dass die Appliance bestimmte Protokolle automatisch auf einen anderen Server überträgt.

Diese Konfiguration kann über die GUI oder CLI mithilfe der FTP- oder SCP-Protokolle erfolgen. Bitte lesen Sie die folgenden Einzelheiten:

Benutzeroberfläche

1. Gehen Sie zu **Systemverwaltung -> Protokollabonnements**.
2. Klicken Sie im Feld 'Protokollname' auf den Protokollnamen des Protokolls, das Sie ändern möchten.
3. Unter 'Retrieval Method' können Sie 'FTP auf Remote-Server' oder 'SCP auf Remote-Server' auswählen.
4. Geben Sie die korrekten Werte in das gewünschte Szenario ein. Wenn Sie mit den richtigen Werten nicht vertraut sind, wenden Sie sich an Ihren System-/Netzwerkadministrator, da dieser Ihnen helfen kann, festzustellen, welche Server in Ihrem Netzwerk verfügbar sind.

CLI (Command Line Interface)

Siehe folgende CLI-Sequenz:

```
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
```

Wählen Sie die Methode aus, die Sie einrichten möchten. Ab diesem Punkt führt die CLI Sie durch die gleichen Verbindungseinstellungen, die in der GUI verfügbar sind.

Diese sind wie folgt:

FTP

- Maximales Zeitintervall zwischen der Übertragung: 3600 Sekunden
- FTP-Host: Hostname/IP-Adresse des FTP-Servers
- Verzeichnis: Remote Directory auf FTP-Server (relativ zur FTP-Anmeldung). Typischerweise '/')
- Benutzername: FTP-Benutzername
- Kennwort: FTP-Kennwort

SCP

- Maximales Zeitintervall zwischen der Übertragung: 3600 Sekunden
- Protokoll: SSH1 oder SSH2
- SCP-Host: Hostname/IP-Adresse des SCP-Servers
- Verzeichnis: Remote Directory auf SCP-Server (relativ zur SCP-Anmeldung). Typischerweise '/')
- Benutzername: SCP-Benutzername
- Host Key Checks aktivieren
- Automatisches Scannen
- Manuell eingeben

HINWEIS: FTP ist ein Nur-Text-Protokoll, d. h., vertrauliche Daten können von einem lesbar sein, der Netzwerkverkehr ausspuckt. SCP ist ein verschlüsseltes Protokoll, wodurch Sniffing beim Snooping von Daten unwirksam wird. Wenn die Daten vertraulich sind und die Sicherheit ein Problem darstellt, wird empfohlen, SCP anstelle von FTP zu verwenden.