Downloads, Updates oder Upgrades der Content Security Appliance unter Verwendung eines statischen Hosts

Inhalt

Einführung

Dieses Dokument beschreibt die IP-Adresse(n) und die Hosts, die für die Konfiguration der Cisco Content Security Appliance zur Verwendung mit einem statischen Host für Downloads, Updates und Upgrades erforderlich sind. Diese Konfigurationen werden entweder für Hardware oder virtuelle Cisco Email Security Appliance (ESA), Web Security Appliance (WSA) oder Security Management Appliance (SMA) verwendet.

Downloads, Updates oder Upgrades der Content Security Appliance unter Verwendung eines statischen Hosts

Cisco bietet statische Hosts für Kunden mit strengen Firewall- oder Proxy-Anforderungen. Wenn Sie Ihre Appliance so konfigurieren, dass sie die statischen Hosts für Downloads und Updates verwendet, müssen die gleichen statischen Hosts für Downloads und Updates auch in der Firewall und im Proxy im Netzwerk zugelassen sein.

Hier sind die statischen Hostnamen, IP-Adressen und Ports aufgeführt, die an den Download-, Aktualisierungs- und Aktualisierungsvorgängen beteiligt sind:

- downloads-static.ironport.com 208.90.58.105 (Port 80)
- updates-static.ironport.com 208.90.58.25 (Port 80)184.94.240.106 (Port 80)

Konfiguration der Service-Aktualisierung über GUI

Gehen Sie wie folgt vor, um die Konfiguration für den Download, die Aktualisierung oder das

Upgrade auf AsyncOS über die Benutzeroberfläche zu ändern:

1. Navigieren Sie zur Konfigurationsseite für Aktualisierungseinstellungen. WSA: **Systemverwaltung > Einstellungen für Upgrades und Aktualisierungen**ESA: **Sicherheitsdienste > Service-Updates**SMA: **Systemverwaltung > Einstellungen aktualisieren**
2. Klicken Sie auf **Aktualisierungseinstellungen bearbeiten...**.
3. Wählen Sie im Abschnitt *Update Servers (Images)* die Option Local Update Servers (location of update image files) aus.
4. Geben Sie im Feld *Basis-URL* in http://downloads-static.ironport.com und im Feld *Port* für Port **80 ein**.
5. Lassen Sie die Felder *Authentifizierung (optional)* leer.
6. (*) Nur ESA - Geben Sie im *Feld Host (McAfee Anti-Virus-Definitionen, PXE Engine-Updates, Sophos Anti-Virus-Definitionen, IronPort Anti-Spam-Regeln, Outbreak-Filterregeln, DLP-Aktualisierungen, Zeitzonenregeln und Anmeldungs-Client (zum Abrufen von Zertifikaten für URL-Filterung verwendet)* **"updates-static.ironport.com" ein**. (Port 80 ist optional.)
7. Lassen Sie den Bereich *Update Servers (Liste)* und die Felder, die alle auf die Cisco IronPort-Standardaktualisierungsserver eingestellt sind, unverändert.
8. Stellen Sie sicher, dass die Schnittstelle für die externe Kommunikation ausgewählt ist, wenn dies für die Kommunikation über eine bestimmte Schnittstelle erforderlich ist. Die Standardkonfiguration wird auf **Auto Select (Automatisch auswählen)** festgelegt.
9. Überprüfen und aktualisieren Sie ggf. die konfigurierten Proxyserver.
10. Klicken Sie auf **Senden**.
11. Klicken Sie in der rechten oberen Ecke auf **Änderungen bestätigen**.
12. Klicken Sie abschließend erneut auf **Änderungen bestätigen**, um alle Konfigurationsänderungen zu bestätigen.

Fahren Sie in diesem Dokument mit dem Abschnitt Überprüfung fort.

Konfiguration der Aktualisierungskonfiguration über die CLI

Dieselben Änderungen können über die CLI auf die Appliance angewendet werden. Gehen Sie wie folgt vor, um die Konfiguration für den Download, die Aktualisierung oder das Upgrade von AsyncOS über die CLI zu ändern:

1. Führen Sie den CLI-Befehl **updateconfig aus**.
2. Geben Sie den Befehl **SETUP ein**.
3. Der erste Abschnitt zur Konfiguration lautet "Feature Key Updates". Verwenden Sie **"2. Eigene Server verwenden'** und http://downloads-static.ironport.com:80/ eingeben.
4. (*) Nur ESA - Der zweite Abschnitt zur Konfiguration lautet "Service (Images)" (Service (Images)). Verwenden Sie **"2. Verwenden Sie einen eigenen Server'** und geben Sie **updates-static.ironport.com ein**.
5. Für alle anderen Konfigurationsaufforderungen kann die Standardeinstellung beibehalten werden.
6. Stellen Sie sicher, dass die Schnittstelle für die externe Kommunikation ausgewählt ist, wenn dies für die Kommunikation über eine bestimmte Schnittstelle erforderlich ist. Die Standardkonfiguration wird auf **Auto** eingestellt.
7. Überprüfen und aktualisieren Sie ggf. den konfigurierten Proxy-Server.
8. Kehren Sie zurück, um zur Haupt-CLI-Eingabeaufforderung zurückzukehren.
9. Führen Sie den CLI-Befehl **COMMIT** aus, um alle Konfigurationsänderungen zu speichern.

Fahren Sie in diesem Dokument mit dem Abschnitt Überprüfung fort.

Überprüfung

Aktualisierungen

Zur Überprüfung von Updates der Appliance empfiehlt es sich, diese über die CLI zu validieren.

Über die CLI:

1. Führen Sie **updatenow aus**. (*) Nur ESA - Sie können **updatenow force** ausführen, um alle Dienste und Regelsätze zu aktualisieren.
2. Führen Sie **tail updater_logs aus**.

Beachten Sie dabei die folgenden Zeilen: "http://updates-static.ironport.com/..." Dies sollte die Kommunikation signalisieren und mit dem statischen Aktualisierungsserver herunterladen.

Beispiel: Eine ESA aktualisiert die Cisco Antispam Engine (CASE) und die zugehörigen Regeln:

```
Wed Aug 2 09:22:05 2017 Info: case was signalled to start a new update
Wed Aug 2 09:22:05 2017 Info: case processing files from the server manifest
Wed Aug 2 09:22:05 2017 Info: case started downloading files
Wed Aug 2 09:22:05 2017 Info: case waiting on download lock
Wed Aug 2 09:22:05 2017 Info: case acquired download lock
Wed Aug 2 09:22:05 2017 Info: case beginning download of remote file "http://updates-
static.ironport.com/case/2.0/case/default/1480513074538790"
Wed Aug 2 09:22:07 2017 Info: case released download lock
Wed Aug 2 09:22:07 2017 Info: case successfully downloaded file
"case/2.0/case/default/1480513074538790"
Wed Aug 2 09:22:07 2017 Info: case waiting on download lock
Wed Aug 2 09:22:07 2017 Info: case acquired download lock
Wed Aug 2 09:22:07 2017 Info: case beginning download of remote file "http://updates-
static.ironport.com/case/2.0/case_rules/default/1501673364679194"
Wed Aug 2 09:22:10 2017 Info: case released download lock
<<<SNIP FOR BREVITY>>>
```

Solange der Dienst kommuniziert, heruntergeladen und dann erfolgreich aktualisiert wird, sind Sie festgelegt.

Nach Abschluss des Service-Updates werden in updater_logs folgende Werte angezeigt:

```
Wed Aug 2 09:22:50 2017 Info: case started applying files
Wed Aug 2 09:23:04 2017 Info: case cleaning up base dir [bindir]
Wed Aug 2 09:23:04 2017 Info: case verifying applied files
Wed Aug 2 09:23:04 2017 Info: case updating the client manifest
Wed Aug 2 09:23:04 2017 Info: case update completed
Wed Aug 2 09:23:04 2017 Info: case waiting for new updates
```

Upgrades

Um zu überprüfen, ob die Aktualisierungskommunikation erfolgreich war und abgeschlossen ist, navigieren Sie zur Seite **System Upgrade** und klicken Sie auf **Available Upgrades (Verfügbare Upgrades)**. Wenn die Liste der verfügbaren Versionen angezeigt wird, ist Ihr Setup abgeschlossen.

Über die CLI können Sie einfach den Befehl **upgrade** ausführen. Wählen Sie die **Download-**Option aus, um das Aktualisierungsmanifest anzuzeigen, wenn Upgrades verfügbar sind.

```
myesa.local> upgrade


Choose the operation you want to perform:
- DOWNLOADINSTALL - Downloads and installs the upgrade image (needs reboot).
- DOWNLOAD - Downloads the upgrade image.
[]> download

Upgrades available.
1. AsyncOS 9.6.0 build 051 upgrade For Email, 2015-09-02 this release is for General Deployment
2. AsyncOS 9.7.0 build 125 upgrade For Email, 2015-10-15. This release is for General Deployment
3. AsyncOS 9.7.1 build 066 upgrade For Email, 2016-02-16. This release is for General
Deployment.
4. cisco-sa-20150625-ironport SSH Keys Vulnerability Fix
[4]>
```

Fehlerbehebung

Aktualisierungen

Die Appliance sendet Benachrichtigungen, wenn die Updates fehlschlagen. Im Folgenden finden Sie ein Beispiel für die am häufigsten gesendete E-Mail-Benachrichtigung:

```
The updater has been unable to communicate with the update server for at least 1h.

Last message occurred 4 times between Tue Mar 1 18:02:01 2016 and Tue Mar 1 18:32:03 2016.

Version: 9.7.1-066
Serial Number: 888869DFCCCC-3##CV##
Timestamp: 01 Mar 2016 18:52:01 -0500
```

Sie möchten die Kommunikation von der Appliance zum angegebenen Aktualisierungsserver testen. In diesem Fall beschäftigen wir uns mit downloads-static.ironport.com. Bei Verwendung von Telnet sollte die Appliance über Port 80 eine offene Kommunikation aufweisen:

```
myesa.local> telnet downloads-static.ironport.com 80

Trying 208.90.58.105...
Connected to downloads-static.ironport.com.
Escape character is '^]'.
```

Genauso sollte dasselbe für updates-static.ironport.com gesehen werden:

```
> telnet updates-static.ironport.com 80

Trying 208.90.58.25...
Connected to origin-updates.ironport.com.
Escape character is '^]'.
```

Wenn Ihre Appliance über mehrere Schnittstellen verfügt, können Sie **Telnet** über die CLI ausführen und die Schnittstelle angeben, um zu überprüfen, ob die richtige Schnittstelle ausgewählt ist:

```
> telnet

Please select which interface you want to telnet from.
1. Auto
2. Management (172.18.249.120/24: myesa.local)
[1]>

Enter the remote hostname or IP address.
[]> downloads-static.ironport.com

Enter the remote port.
[25]> 80

Trying 208.90.58.105...
Connected to downloads-static.ironport.com.
Escape character is '^]'.
```

Upgrades

Beim Upgrade sehen Sie möglicherweise die folgende Antwort:

```
No available upgrades. If the image has already been downloaded it has been de-provisioned from
the upgrade server. Delete the downloaded image, if any and run upgrade.
```

Sie möchten die auf der Appliance ausgeführte Version von AsyncOS überprüfen und auch die Versionshinweise der Version von AsyncOS überprüfen, auf die Sie aktualisieren. Möglicherweise gibt es keinen Aktualisierungspfad von der aktuellen Version zur Version, auf die Sie ein Upgrade durchführen möchten.

Wenn Sie ein Upgrade auf eine Hot Patch (HP)-, Early Deployment (ED)- oder Limited Deployment (LD) AsyncOS-Version durchführen möchten, müssen Sie möglicherweise ein Support-Ticket öffnen, um eine ordnungsgemäße Bereitstellung anzufordern, damit die Appliance den Upgrade-Pfad bei Bedarf anzeigt.

Zugehörige Informationen

- Cisco Email Security Appliance - Versionshinweise
- Cisco Web Security Appliance - Versionshinweise
- Cisco Security Management Appliance - Versionshinweise
- Technischer Support und Dokumentation - Cisco Systems