Fehler beim automatischen Herunterladen von Updates in einem FirePOWER Management Center

Inhalt

Einleitung

In diesem Dokument wird erläutert, warum ein geplanter Task zur Aktualisierung eines Cisco FirePOWER Management Center fehlschlagen kann. Sie können ein Cisco FirePOWER Management Center manuell oder automatisch aktualisieren. Um ein automatisches Software-Update auszuführen, können Sie eine geplante Aufgabe in Ihrem Management Center erstellen, die zu einem späteren Zeitpunkt ausgeführt werden soll.

Mögliche Fehlerursachen

Ein FirePOWER Management Center kann möglicherweise keine Update-Datei von der Cisco Download Update Infrastructure herunterladen, wenn eine der folgenden Aktionen in Ihrem Netzwerk auftritt:

- Die Sicherheitsrichtlinie Ihres Unternehmens blockiert den DNS-Datenverkehr (Domain Name System).
- Die Konfiguration außerhalb des Management Centers wirkt sich auf den Download aus. Beispielsweise kann eine Firewall-Regel nur eine IP-Adresse für support.sourcefire.com zulassen.

Vorsicht: Cisco verwendet Round-Robin-DNS für Lastenausgleich, Fehlertoleranz und Betriebszeit. Daher können sich die IP-Adressen von DNS-Servern ändern.

Auswirkungen

Wenn Sie diese Methode verwenden...	Aktionselemer
Systemstandardkonfiguration für automatischen Download	Keine Aktion erforderlich
Laden Sie die Update-Datei manuell herunter und laden Sie sie in das Firepower	Keine Aktion

Management Center hoch.	erforderlich
Firewall-Regeln zur Filterung des Zugriffs auf die von Cisco verwaltete Download-Update-Infrastruktur	Folgen Sie der Lösung

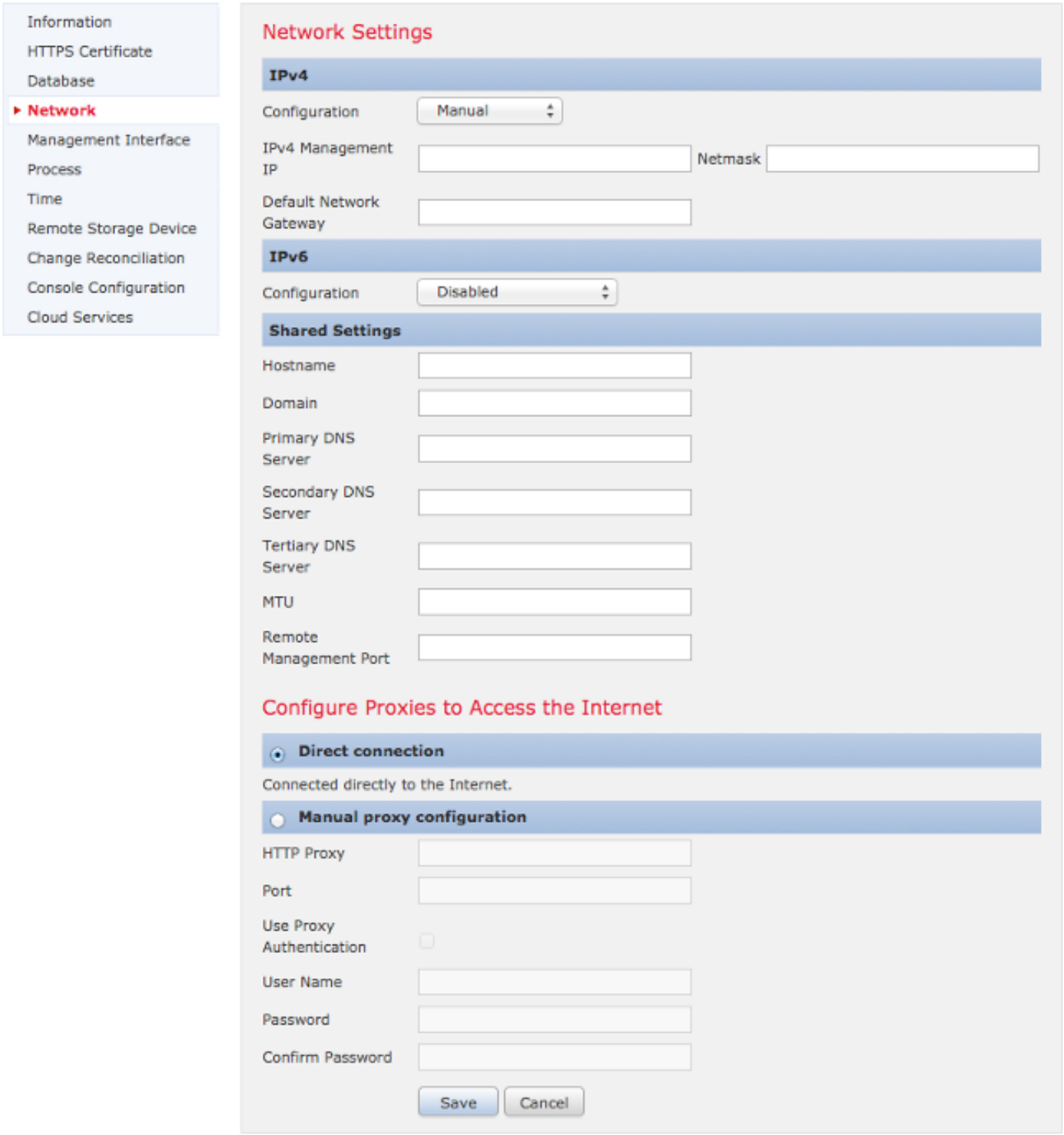
- Fehler werden durch die drei Wiederholungsversuche und den nächsten geplanten Durchlauf teilweise gemindert. Wiederholte Ausfälle sind wahrscheinlich ein Hinweis auf externe Faktoren wie Firewalls oder einen Ausfall der Infrastruktur.
- Da sich der Round-Robin-DNS auf dem Domänennamen befindet, müssen Sie Maßnahmen ergreifen, um sicherzustellen, dass es keine zeitweiligen Downloadfehler gibt.

Verifizierung

Überprüfen der DNS-Einstellungen

Stellen Sie sicher, dass Ihr FirePOWER Management Center für die Verwendung Ihres DNS-Servers konfiguriert ist.

> **Vorsicht:** Cisco empfiehlt nachdrücklich, die Standardeinstellungen beizubehalten.



Sie können die DNS-Einstellungen im Abschnitt **"Netzwerk" unter System > Local > Configuration** konfigurieren. Im Abschnitt **Shared Settings** können Sie bis zu drei DNS-Server angeben.

> **Anmerkung:** Wenn Sie in der **Konfigurations**-Dropdown-Liste **DHCP** ausgewählt haben, können Sie die **freigegebenen Einstellungen** nicht manuell festlegen.

Überprüfen der Verbindung

Sie können verschiedene Befehle wie telnet, nslookup oder dig verwenden, um den Status des DNS-Servers und die DNS-Einstellungen in Ihrem Firepower Management Center zu bestimmen. Beispiele:

```
telnet support.sourcefire.com 443

nslookup support.sourcefire.com

dig support.sourcefire.com
```

> **Anmerkung:** Ping an support.sourcefire.com funktioniert nicht. Daher sollte er nicht als Verbindungstest verwendet werden.

Um die Verbindung mit der Support-Site von einer Appliance aus zu testen (um Updates herunterzuladen usw.), können Sie sich über SSH oder direkten Konsolenzugriff bei Ihrer Appliance anmelden und den folgenden Befehl verwenden:

```
admin@Firepower:~# sudo openssl s_client -connect support.sourcefire.com:443
```

Dieser Befehl zeigt die Zertifikataushandlung an und bietet Ihnen eine Entsprechung zu einer Telnet-Sitzung mit einem Port 80-Webserver. Hier ist ein Beispiel für die Befehlsausgabe:

```
New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
Protocol : TLSv1
Cipher : AES256-SHA
Session-ID: 44A18130176C9171F50F33A367B55F5CFD10AA0FE87F9C5C1D8A7A7E519C695B
Session-ID-ctx:
Master-Key:
D406C5944B9462F1D6CB15D370E884B96B82049300D50E74F9B8332F84786F05C35BF3FD806672630BE26C2218AE5BDE
Key-Arg : None
Start Time: 1398171146
Timeout : 300 (sec)
Verify return code: 0 (ok)
---
```

An dieser Stelle sollte es keine Eingabeaufforderung geben. Da die Sitzung jedoch auf eine Eingabe wartet, können Sie den folgenden Befehl eingeben:

```
GET /
```

Sie sollten rohen HTML-Code erhalten, der die Anmeldeseite der Support-Website darstellt.

Fehlerbehebung

Option 1: Ersetzen Sie die statische IP-Adresse durch den Domänennamen support.sourcefire.com auf Firewalls. Wenn Sie eine statische IP-Adresse verwenden müssen, stellen Sie sicher, dass dies richtig ist. Hier sind die detaillierten Informationen zum Download-Server, der von einem FirePOWER-System verwendet wird:

- **Domäne**: support.sourcefire.com
- **Anschluss:** 443/tcp (bidirektional)
- **IP-Adresse:** 50.19.123.95, 50.16.210.129

Zusätzliche IP-Adressen, die ebenfalls von support.sourcefire.com verwendet werden (im Round-Robin-Verfahren):

```
54.221.210.248
54.221.211.1
54.221.212.60
54.221.212.170
54.221.212.241
54.221.213.96
54.221.213.209
54.221.214.25
54.221.214.81
```

Option 2: Sie können Updates manuell über einen Webbrowser herunterladen und dann während des Wartungsfensters manuell installieren.

Option 3: Fügen Sie einen A-Eintrag für support.sourcefire.com auf Ihrem DNS-Server hinzu.

Verwandte Dokumente

- Arten von Updates, die auf einem FirePOWER-System installiert werden können
- Erforderliche Serveradressen für AMP-Vorgänge (Advanced Malware Protection)
- Erforderliche Kommunikations-Ports für den Betrieb des FirePOWER-Systems
- Technischer Support und Dokumentation für Cisco Systeme