Automatische updates van downloads op een FireSIGHT Management Center

Inhoud

Inleiding

Dit document behandelt redenen waarom een geplande taak om een Cisco FireSIGHT Management Center bij te werken mogelijk mislukt. U kunt een Cisco FireSIGHT Management Center handmatig of automatisch bijwerken. U kunt een automatische softwareupdate uitvoeren door een planningtaak op uw beheercentrum te maken om op een later tijdstip te starten.

Mogelijke redenen voor falen

Een FireSIGHT Management Center kan geen update-bestand van de Cisco Download Update infrastructuur downloaden wanneer een van deze acties in uw netwerk plaatsvindt:

- Het veiligheidsbeleid van uw bedrijf blokkeert het verkeer van de Naam van het Systeem (DNS).
- Configuratie buiten uw beheercentrum beïnvloedt de download. Een firewallregel zou bijvoorbeeld slechts één IP-adres voor support.sourcefire.com kunnen toestaan.

  Voorzichtig: Cisco gebruikt ronde DNS-lijn voor taakverdeling, fouttolerantie en uptime. Daarom zouden de IP-adressen van DNS-servers kunnen veranderen.

Impact

Als u deze methode gebruikt...	Actiepost
Standaard systeemconfiguratie voor automatische download	Geen actie vereist
Download het update bestand handmatig en uploaden het naar FireSIGHT Management Center	Geen actie vereist
Firewallregels om toegang tot het Cisco-systeem voor beheerde downloadoptie te filteren	Volg de oplossing

- Fouten worden gedeeltelijk verzacht door de drie herhalingen en de volgende geplande reeks. Herhaalde storingen zijn waarschijnlijk een aanwijzing voor een externe factor zoals firewalls

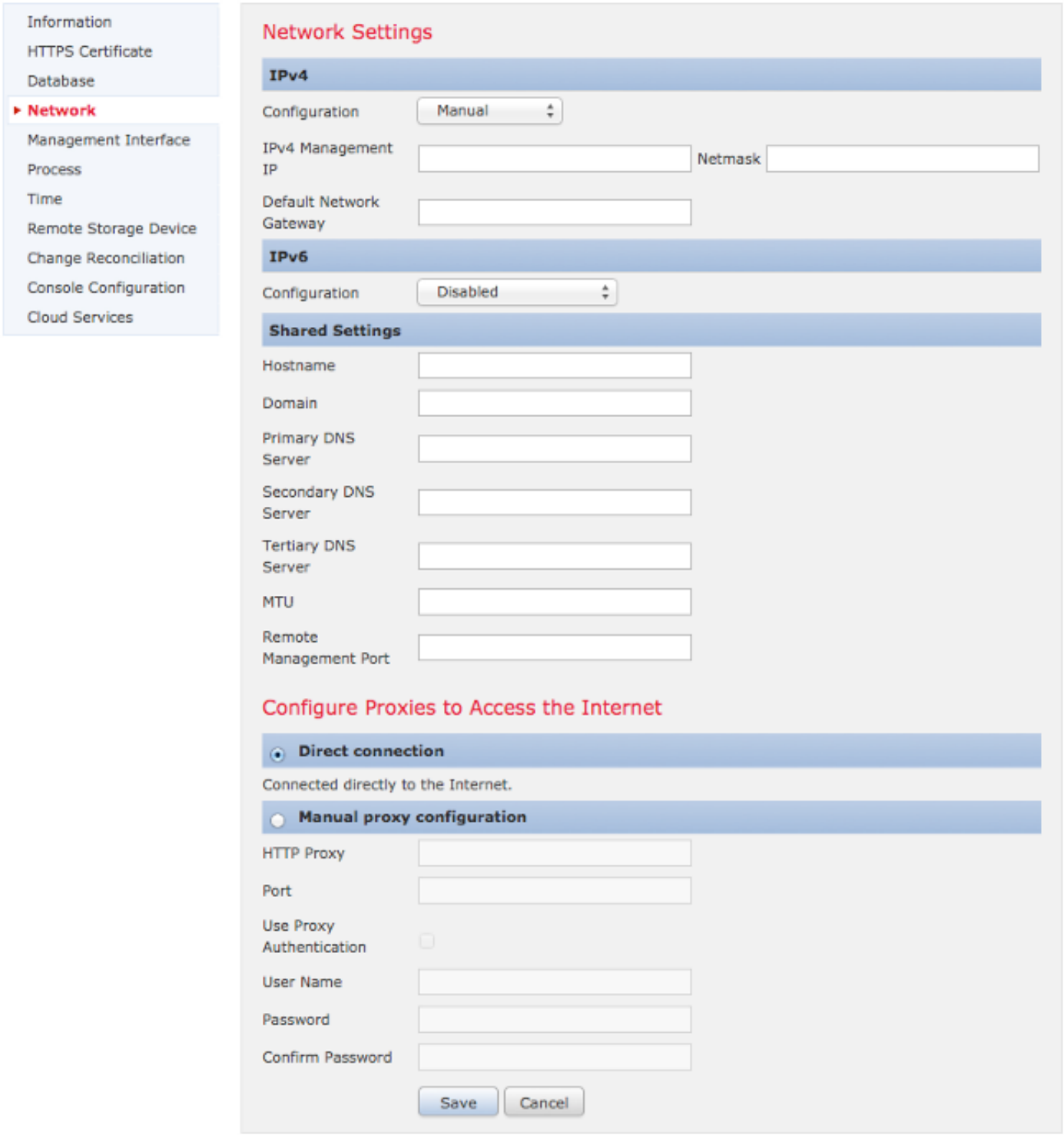
of een stroomstoring met de infrastructuur.
- Aangezien de round robin DNS op de domeinnaam staat, moet u stappen ondernemen om ervoor te zorgen dat er geen periodieke downloadfouten zijn.

Verificatie

Controleer de DNS-instellingen

Zorg ervoor dat uw FireSIGHT Management Center is ingesteld om uw DNS-server te gebruiken.

> **Voorzichtig:** Cisco raadt sterk aan de standaardinstellingen te houden.



U kunt de DNS-instellingen configureren in **systeem > Local > Configuration** onder het **Network** Section. Onder het gedeelte **Shared Settings** kunt u maximaal drie DNS-servers instellen.

> **Opmerking:** Als u **DHCP** in de vervolgkeuzelijst **Configuration** hebt geselecteerd, kunt u niet handmatig de **gedeelde instellingen** specificeren.

Controleer de verbinding

U kunt verschillende opdrachten gebruiken, zoals telnet, nslookup of opgraven om de status van de DNS-server en de DNS-instellingen in uw FireSIGHT Management Center te bepalen. Voorbeeld:

```
telnet support.sourcefire.com 443

nslookup support.sourcefire.com

dig support.sourcefire.com
```

> **Opmerking:** Ping naar support.sourcefire.com werkt niet. Daarom mag het niet worden gebruikt als een aansluitingstest.

Om de aansluiting op de ondersteuningswebsite van een apparaat te testen (om updates te downloaden, enzovoort), kunt u via SSH of directe console in uw apparaat loggen en deze opdracht gebruiken:

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

Deze opdracht toont de certificeringsonderhandeling en voorziet u van een equivalent van een telnet-sessie aan een poort 80 webserver. Hier is een voorbeeld van de opdrachtoutput:

```
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)
---
```

Op dit moment mag er geen reden zijn. Aangezien de sessie wacht op input, kunt u vervolgens de opdracht invoeren:

```
GET /
```

U dient ruwe HTML te ontvangen dat de logpagina van de ondersteuningswebsite is.

Problemen oplossen

Optie 1: Vervang het statische IP adres met de Domain Name support.sourcefire.com op firewalls. Als u een statisch IP-adres moet gebruiken, zorg er dan voor dat dit correct is. Hier vindt u gedetailleerde informatie over de downloadserver die gebruikt wordt door een FirePOWER-systeem:

- **Domain**: support.sourcefire.com
- **Port:** 443/tcp (bidirectioneel)
- **IP-adres:** 50.19.123.95, 50.16.210.129

Aanvullende IP-adressen die ook door support.sourcefire.com worden gebruikt (in round robin methode) zijn:

```
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
```

Optie 2: U kunt updates handmatig met een webbrowser downloaden en deze vervolgens handmatig tijdens uw onderhoudsvenster installeren.

Optie 3: Voeg een A-record voor support.sourcefire.com toe op uw DNS-server.

Verwante documenten

- Typen updates die op een energiesysteem kunnen worden geïnstalleerd
- Vereiste serveradressen voor Advanced Malware Protection (AMP)
- Vereiste communicatiepoorten voor FirePOWER System-werking
- Technische ondersteuning en documentatie – Cisco Systems