Falha automática de atualização de download em um Firepower Management Center

Contents

Introduction

Este documento discute os motivos pelos quais uma tarefa programada para atualizar um Cisco Firepower Management Center pode falhar. Você pode atualizar um Cisco Firepower Management Center manual ou automaticamente. Para executar uma atualização automática de software, você pode criar uma tarefa de agendamento no Centro de Gerenciamento para execução futura.

Possíveis motivos para falha

Um Firepower Management Center pode falhar ao fazer o download de um arquivo de atualização da infraestrutura de atualização de download da Cisco quando uma destas ações ocorrer em sua rede:

- A política de segurança de sua empresa bloqueia o tráfego do Sistema de Nome de Domínio (DNS).
- A configuração fora do seu Management Center afeta o download. Por exemplo, uma regra de firewall pode permitir apenas um endereço IP para support.sourcefire.com.

  Caution: A Cisco utiliza DNS de rodízio para balanceamento de carga, tolerância a falhas e tempo de atividade. Portanto, os endereços IP dos servidores DNS podem mudar.

Impacto

Se Você Usar Este Método...	Item de Ação
Configuração padrão do sistema para download automático	Nenhuma ação é necessária
Baixe o arquivo de atualização manualmente e carregue-o no Firepower Management Center	Nenhuma ação é necessária
Regras de firewall para filtrar o acesso à infraestrutura de atualização de download gerenciada da Cisco	Siga a solução

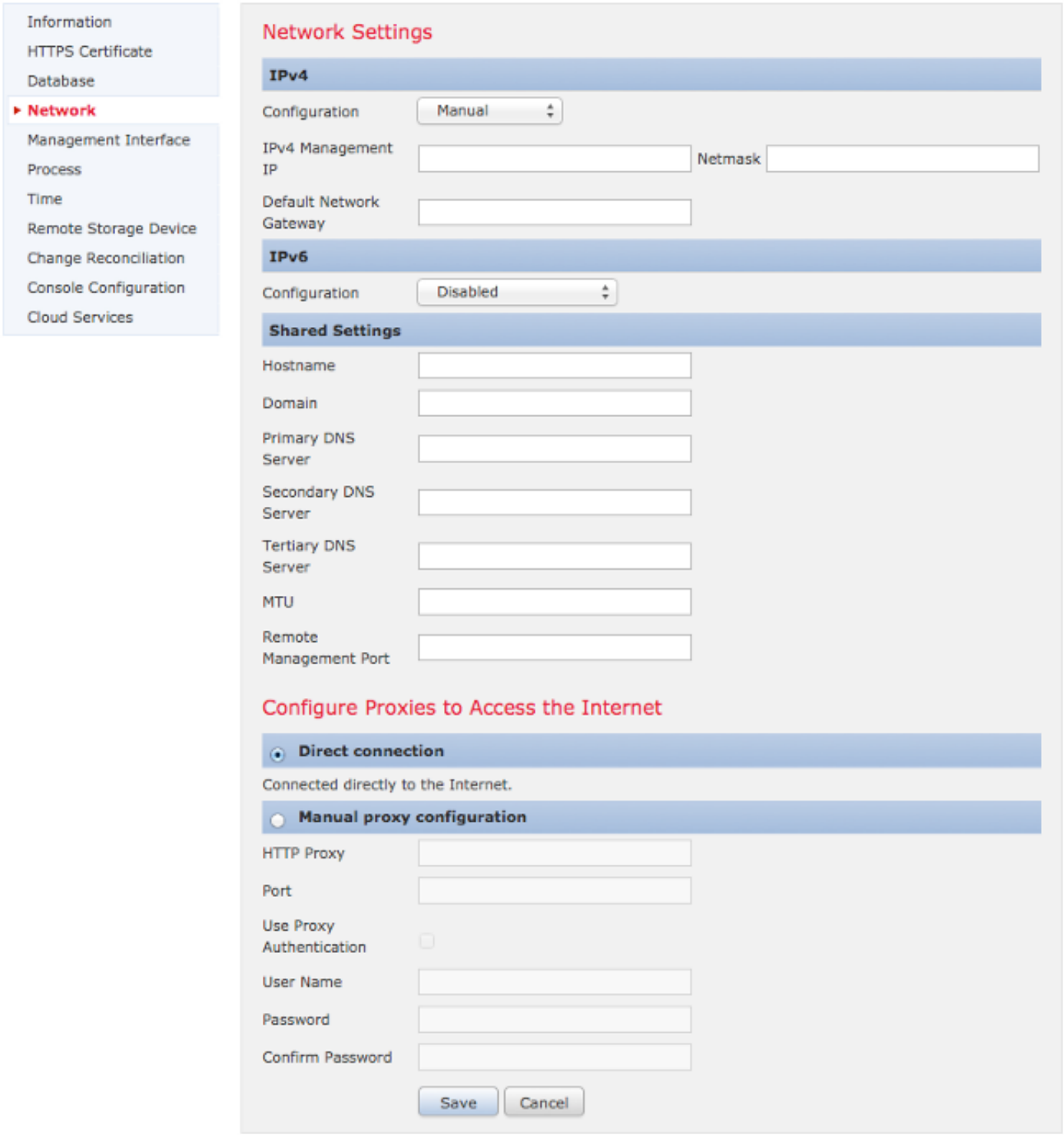
- As falhas são parcialmente atenuadas pelas três tentativas e pela próxima execução agendada. Falhas repetidas são provavelmente uma indicação de um fator externo, como firewalls, ou uma interrupção com a infraestrutura.
- Como o DNS de rodízio está no nome do domínio, você precisa tomar medidas para garantir que não haja falhas de download intermitentes.

Verificação

Verifique as configurações DNS

Verifique se o Firepower Management Center está configurado para usar o servidor DNS.

> **Caution**: A Cisco recomenda que você mantenha as configurações padrão.



Você pode definir as configurações DNS em **System > Local > Configuration**, na seção **Network**. Na seção **Configurações compartilhadas**, você pode especificar até três servidores DNS.

> **Note**: Se você selecionou **DHCP** na lista suspensa **Configuração**, não será possível especificar manualmente as **Configurações compartilhadas**.

Verificar a conexão

Você pode usar vários comandos, como telnet, nslookup ou dig para determinar o estado do servidor DNS e as configurações DNS no Firepower Management Center. Por exemplo:

```
telnet support.sourcefire.com 443

nslookup support.sourcefire.com

dig support.sourcefire.com
```

> **Note**: O ping para support.sourcefire.com não funciona. Portanto, não deve ser usado como um teste de conectividade.

Para testar a conexão com o site de suporte de um equipamento (para baixar atualizações, etc.), você pode fazer login no equipamento via SSH ou acesso direto ao console e usar este comando:

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

Esse comando mostra a negociação do certificado, bem como fornece um equivalente de uma sessão telnet para um servidor Web da porta 80. Aqui está um exemplo da saída do comando:

```
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)
---
```

Não deve haver nenhum prompt neste ponto. No entanto, como a sessão está aguardando entrada, você pode inserir o comando:

```
GET /
```

Você deve receber HTML bruto que é a página de login do site de suporte.

Troubleshoot

Opção 1: Substitua o endereço IP estático pelo nome de domínio support.sourcefire.com nos firewalls. Se precisar usar um endereço IP estático, verifique se está correto. Estas são as informações detalhadas do servidor de download usado por um sistema Firepower:

- **Domínio:** support.sourcefire.com
- **Porta:** 443/tcp (bidirecional)
- **Endereço IP:** 50.19.123.95, 50.16.210.129

Os endereços IP adicionais que também são usados pelo support.sourcefire.com (no método round robin) são:

```
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
```

Opção 2: Você pode fazer o download das atualizações manualmente com um navegador da Web e instalá-las manualmente durante a janela de manutenção.

Opção 3: Adicione um registro A para support.sourcefire.com em seu servidor DNS.

Documentos relacionados

- Tipos de atualizações que podem ser instaladas em um sistema Firepower
- Endereços de servidor necessários para operações de proteção avançada contra malware (AMP)
- Portas de comunicação necessárias para operação do sistema Firepower
- Suporte Técnico e Documentação - Cisco Systems