Error de actualización de descarga automática en un FirePOWER Management Center

Contenido

Introducción

Este documento explica las razones por las que una tarea programada para actualizar un Cisco Firepower Management Center podría fallar. Puede actualizar un Cisco Firepower Management Center manual o automáticamente. Para realizar una actualización de software automática, puede crear una tarea de planificación en Management Center para que se ejecute en el futuro.

Posibles razones del fallo

Es posible que un Firepower Management Center no pueda descargar un archivo de actualización de la infraestructura de actualización de descarga de Cisco cuando se produzca una de estas acciones en la red:

- La directiva de seguridad de su empresa bloquea el tráfico del Sistema de nombres de dominio (DNS).
- La configuración fuera de Management Center afecta a la descarga. Por ejemplo, una regla de firewall podría permitir sólo una dirección IP para support.sourcefire.com.

Precaución: Cisco utiliza DNS de ordenamiento cíclico para el equilibrio de carga, la tolerancia a fallos y el tiempo de actividad. Por lo tanto, las direcciones IP de los servidores DNS pueden cambiar.

Impacto

Si Utiliza Este Método...	Elemento de acci
Configuración predeterminada del sistema para descarga automática	No se requiere nir acción
Descargue el archivo de actualización manualmente y cárguelo en Firepower Management Center	No se requiere nir acción
Reglas de firewall para filtrar el acceso a la infraestructura de actualización de descargas gestionada de Cisco	Siga la solución

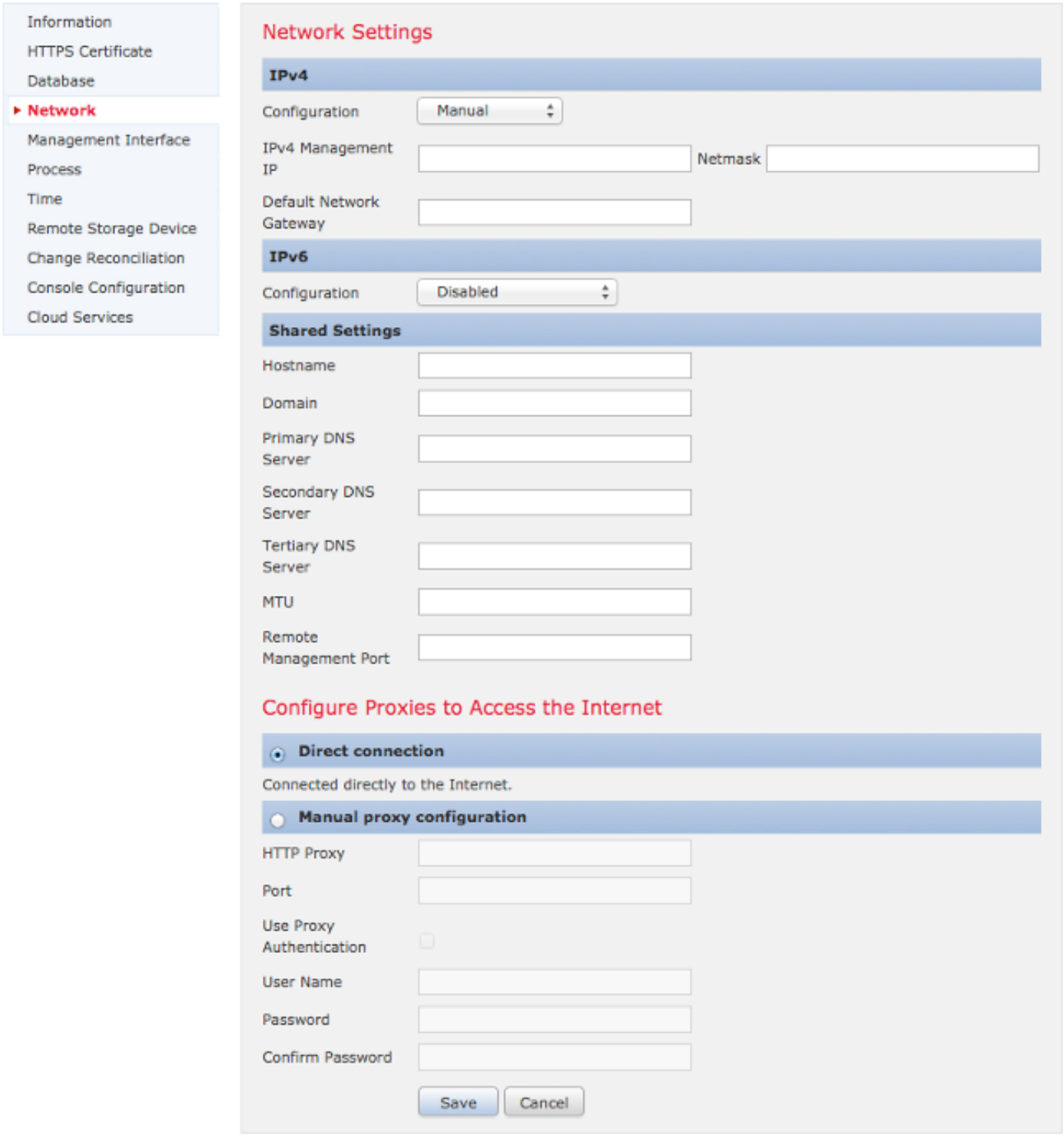
- Los errores se mitigan parcialmente con los tres reintentos y la siguiente ejecución programada. Los fallos repetidos son probablemente un indicio de un factor externo, como firewalls o una interrupción de la infraestructura.
- Como el DNS de ordenamiento cíclico está en el nombre de dominio, debe tomar medidas para asegurarse de que no haya fallas de descarga intermitentes.

Verificación

Compruebe la configuración de DNS

Asegúrese de que Firepower Management Center está configurado para utilizar el servidor DNS.

> **Precaución:** Cisco recomienda encarecidamente mantener los parámetros predeterminados.



Puede configurar los ajustes de DNS en **System > Local > Configuration**, en la sección **Network**. En la sección **Shared Settings**, puede especificar hasta tres servidores DNS.

> **Nota:** Si seleccionó **DHCP** en la lista desplegable **Configuration**, no puede especificar manualmente los **Shared Settings**.

Verifique la conexión

Puede utilizar varios comandos, como telnet, nslookup o dig para determinar el estado del servidor DNS y la configuración de DNS en Firepower Management Center. Por ejemplo:

```
telnet support.sourcefire.com 443

nslookup support.sourcefire.com

dig support.sourcefire.com
```

> **Nota:** El ping a support.sourcefire.com no funciona. Por lo tanto, no debe utilizarse como prueba de conectividad.

Para probar la conexión al sitio de soporte desde un dispositivo (para descargar actualizaciones, etc.), puede iniciar sesión en su dispositivo a través de SSH o acceso directo a la consola y utilizar este comando:

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

Este comando muestra la negociación de certificado, así como le proporciona un equivalente de una sesión telnet a un servidor web del puerto 80. Aquí hay un ejemplo del resultado del 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)
---
```

No debe haber ningún mensaje en este momento. Sin embargo, mientras la sesión espera una entrada, puede introducir el comando:

```
GET /
```

Debería recibir HTML sin procesar que es la página de inicio de sesión del sitio de soporte.

Troubleshoot

Opción 1: Reemplace la dirección IP estática con el nombre de dominio support.sourcefire.com en los firewalls. Si tiene que utilizar una dirección IP estática, asegúrese de que sea correcta. A continuación se muestra la información detallada del servidor de descarga utilizado por un sistema Firepower:

- **Dominio:** support.sourcefire.com
- **Puerto:** 443/tcp (bidireccional)
- **IP Address:** 50.19.123.95, 50.16.210.129

Las direcciones IP adicionales que también utiliza support.sourcefire.com (en el método de ordenamiento cíclico) son:

```
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
```

Opción 2: Puede descargar las actualizaciones manualmente con un explorador Web y, a continuación, instalarlas manualmente durante el período de mantenimiento.

Opción 3: Agregue un registro A para support.sourcefire.com en su servidor DNS.

Documentos Relacionados

- Tipos de actualizaciones que se pueden instalar en un sistema Firepower
- Direcciones de servidor necesarias para las operaciones de protección frente a malware avanzado (AMP)
- Puertos de comunicación necesarios para el funcionamiento del sistema Firepower
- Soporte Técnico y Documentación - Cisco Systems