Automatic Download Update Failure on a Firepower Management Center

Contents

Introduction

This document discusses reasons a scheduled task to update a Cisco Firepower Management Center might fail. You can update a Cisco Firepower Management Center manually or automatically. In order to perform an automatic software update, you can create a schedule task on your Management Center to run at a future time.

Possible Reasons for Failure

A Firepower Management Center might fail to download an update file from the Cisco Download Update Infrastructure when one of these actions occurs in your network:

- Security policy of your company blocks Domain Name System (DNS) traffic.
- Configuration outside of your Management Center impacts download. For example, a firewall rule might allow only one IP address for `support.sourcefire.com`.

  Caution: Cisco utilizes round robin DNS for load balancing, fault-tolerance, and uptime. Therefore, the IP Addresses of DNS servers might change.

Impact

If You Use This Method...	Action Item
System default configuration for automatic download	No action required
Download the update file manually and upload it to Firepower Management Center	No action required
Firewall rules to filter access to the Cisco managed Download Update Infrastructure	Follow the solution

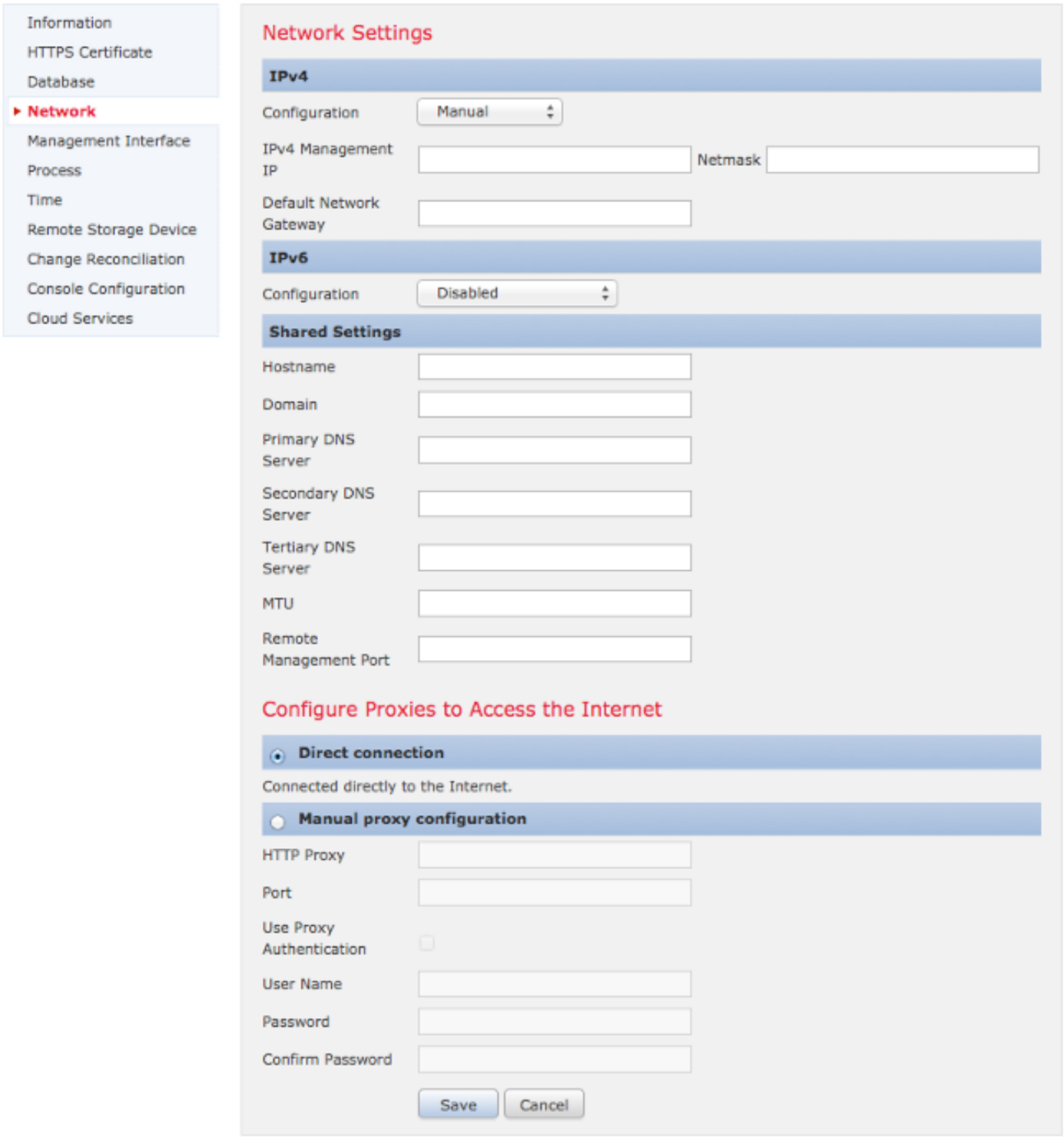
- Failures are partially mitigated by the three retries and the next scheduled run. Repeated failures are likely an indication of an external factor such as firewalls or an outage with the Infrastructure.
- As the round robin DNS is on the domain name, you need to take steps in order to ensure that there is no intermittent download failures.

Verification

Verify the DNS Settings

Ensure that your Firepower Management Center is configured to use your DNS server.

> **Caution**: Cisco strongly recommends that you keep the default settings.



You can configure the DNS settings in **System > Local > Configuration**, under the **Network** Section. Under the **Shared Settings** section, you can specify up to three DNS servers.

Note: If you selected **DHCP** in the **Configuration** drop-down list, you cannot manually specify the **Shared Settings**.

Verify the Connection

You can use various commands, such as `telnet`, `nslookup`, or `dig` in order to determine the state of the DNS server, and the DNS settings on your Firepower Management Center. For example:

```
telnet support.sourcefire.com 443
```

```
nslookup support.sourcefire.com
```

```
dig support.sourcefire.com
```

Note: Ping to `support.sourcefire.com` does not work. Hence it should not be used as a connectivity test.

In order to test connection to the support site from an appliance (to download updates, and so on), you can log into your appliance via SSH or direct-console access, and use this command:

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

This command shows the certificate negotiation, as well as provides you with an equivalent of a telnet session to a port 80 webserver. Here is an example of the command output:

```
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)
---
```

There should be no prompt at this point. However, as the session is waiting for input, you can then enter the command:

```
GET /
```

You should receive raw HTML that is the support site login page.

Troubleshoot

Option 1: Replace the static IP address with the Domain Name `support.sourcefire.com` on firewalls. If you have to use a static IP address, make sure that this is correct. Here is the detailed information of the download server used by a Firepower system:

- **Domain**: `support.sourcefire.com`
- **Port**: `443/tcp` (bidirectional)
- **IP Address**: `50.19.123.95, 50.16.210.129`

Additional IP addresses that are also used by the `support.sourcefire.com` (in round robin method) are:

```
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: You can download updates manually with a web browser, and then install it manually during your maintenance window.

Option 3: Add an `A` record for `support.sourcefire.com` on your DNS server.

Related Documents

- **Types of Updates That May Be Installed on a Firepower System**
- **Required Server Addresses for Advanced Malware Protection (AMP) Operations**
- **Required Communication Ports for Firepower System Operation**
- **Technical Support & Documentation - Cisco Systems**