Technote on FAQ for Remote Access on Cisco ESA/WSA/SMA

Contents

Introduction

This document provides answers to frequently asked questions about the use of remote access by Cisco Technical Support on Cisco Content Security appliances. This includes the Cisco Email Security Appliance (ESA), the Cisco Web Security Appliance (WSA), and the Cisco Security Management Appliance (SMA).

Prerequisites

Components Used

The information in this document is based on the Cisco Content Security appliances running any version of AsyncOS.

What is remote access?

Remote access is a Secure Shell (SSH) connection that is enabled from a Cisco Content Security appliance to a secure host at Cisco. Only Cisco Customer Assistance can access the appliance once a remote session is enabled. Remote access allows Cisco Customer Support to analyze an appliance. Support accesses the appliance through an SSH tunnel that this procedure creates

between the appliance and the upgrades.ironport.com server.

How remote access works

When a remote access connection initiates, the appliance opens a secure, random, high-source port via an SSH connection on the appliance to the configured/selected port one of the following Cisco Content Security servers:

IP Address	Hostname	Use
63.251.108.107	upgrades.ironport.com	All Content Security Appliances
63.251.108.107	c.tunnels.ironport.com	C-Series appliances (ESA)
63.251.108.107	x.tunnels.ironport.com	X-Series appliances (ESA)
63.251.108.107	m.tunnels.ironport.com	M-Series appliances (SMA)
63.251.108.107	s.tunnels.ironport.com	S-Series appliances (WSA)

It is important to note that a customer firewall may need to be configured to allow outbound connections to one of the above listed servers. If your firewall has SMTP protocol inspection enabled, the tunnel will not establish. Ports that Cisco will accept connections from the appliance for the remote access are:

- 22
- 25 (Default)
- 53
- 80
- 443
- 4766

The remote access connection is made to a host name and not to a hard-coded IP address. This does require Domain Name Server (DNS) to be configured on the appliance in order to establish the outbound connection.

On a customer network, some protocol-aware network devices may block this connection due to the protocol/port mismatch. Some Simple Mail Transport Protocol (SMTP)-aware devices may also interrupt the connection. In cases where there are protocol-aware devices or outbound connections that are blocked, the use of a port other than the default (25) may be required. Access to the remote end of the tunnel is restricted to only Cisco Customer Support. Please be sure that you review your firewall/network for outbound connections when trying to establish or troubleshoot remote access connections for your appliance.

> **Note**: When a Cisco Customer Support Engineer is connected to the appliance via remote access the system prompt on the appliance shows *(SERVICE)*.

How to enable remote access

> **Note**: Please be sure to review the User Guide of your appliance and version of AsyncOS for instructions on "Enabling Remote Access for Cisco Technical Support Personnel".

> **Note**: Attachments sent via email to attach@cisco.com may not be secure in transit. Support Case Manager is Cisco's preferred secure option to upload information to your case. To

learn more about the security and size limitations of other file upload options: Customer File Uploads to Cisco Technical Assistance Center

Identify a port that can be reached from the Internet. The default is port 25, which will work in most environments because the system also requires general access over that port in order to send email messages. Connections over this port are allowed in most firewall configurations.

CLI

In order to establish a remote access connection via the CLI, as an Admin user, complete these steps:

1. Enter the **techsupport** command
2. Choose **TUNNEL**
3. Choose to Generate or *Enter* a random seed string
4. Specify the port number for the connection
5. Reply "**Y**" to enable service access

Remote access wil be enabled at this time. The appliance now work to establish the secure connection to the secure bastion host at Cisco. Provide both the appliance serial number and the seed string that is generated to the TAC Engineer supporting your case.

GUI

In order to establish a remote access connection via the GUI, as an Admin user, complete these steps:

1. Navigate to **Help and Support > Remote Access** (for ESA, SMA), **Support and Help > Remote Access** (for WSA)
2. Click **Enable**
3. Choose the method for the seed string
4. Ensure that you check the *Initiate connection via secure tunnel* check box and specify the port number for connection
5. Click **Submit**

Remote access wil be enabled at this time. The appliance now work to establish the secure connection to the secure bastion host at Cisco. Provide both the appliance serial number and the seed string that is generated to the TAC Engineer supporting your case.

How to disable remote access

CLI

1. Enter the **techsupport** command
2. Choose **DISABLE**
3. Reply "**Y**" when prompted "Are you sure you want to disable service access?"

GUI

1. Navigate to **Help and Support > Remote Access** (for ESA, SMA), **Support and Help > Remote Access** (for WSA).
2. Click **Disable**
3. The GUI output will show "Success — Remote Access has been disabled"

How to test remote access connectivity

Use this example in order to perform an initial test for connectivity from your appliance to Cisco:

```
example.run> > telnet upgrades.ironport.com 25

Trying 63.251.108.107...
Connected to 63.251.108.107.
Escape character is '^]'.
SSH-2.0-OpenSSH_6.2 CiscoTunnels1
```

Connectivity can be tested for any of the ports listed above: 22, 25, 53, 80, 443, or 4766. If connectivity fails, you may need to run a packet capture to see where the connection is failing from your appliance/network.

Why does the remote access not work on the SMA?

Remote access may not enable on an SMA if the SMA is placed in the local network without direct access to the Internet. For this instance, remote access can be enabled on an ESA or WSA, and SSH access can be enabled on the SMA. This allows Cisco Support to first connect via remote access to the ESA/WSA, and then from the ESA/WSA to the SMA via SSH. This will require connectivity between the ESA/WSA and the SMA on port 22.

> **Note**: Please be sure to review the User Guide of your appliance and version of AsyncOS for instructions on "Enabling Remote Access to Appliances Without a Direct Internet Connection".

CLI

In order to establish a remote access connection via the CLI, as an Admin user, complete these steps:

1. Enter the **techsupport** command
2. Choose **SSHACCESS**
3. Choose to Generate or *Enter* a random seed string
4. Reply "**Y**" to enable service access

Remote access wil be enabled at this time. The CLI output will show the seed string. Please provide this to the Cisco Customer Support Engineer. The CLI output will also show the connection status and remote access details, including the appliance serial number. Please provide this serial number to the Customer Customer Support Engineer.

GUI

In order to establish a remote access connection via the GUI, as an Admin user, complete these steps:

1. Navigate to **Help and Support > Remote Access** (for ESA, SMA), **Support and Help > Remote Access** (for WSA)
2. Click **Enable**
3. Choose the method for the seed string
4. Do NOT check the *Initiate connection via secure tunnel* check box
5. Click **Submit**

Remote access wil be enabled at this time. The GUI output will show you a success message and the appliance's seed string. Please provide this to the Cisco Customer Support Engineer. The GUI output will also show the connection status and the remote access details, including the appliance serial number. Please provide this serial number to the Customer Customer Support Engineer.

How to disable remote access when enabled for SSHACCESS

Disabling remote access for SSHACCESS is the same steps as provided above.

Troubleshooting

If the appliance is not able to enabled remote access and connect to upgrades.ironport.com via one of the ports listed, you will need to run a packet capture directly from the appliance to review what is causing the outbound connection to fail.

> **Note**: Please be sure to review the User Guide of your appliance and version of AsyncOS for instructions on "Running a Packet Capture".

The Cisco Customer Support Engineer may request to have the .pcap file provided in order to review and assist with troubleshooting.

Related Information

- **ESA FAQ: What are the levels of administrative access available on the ESA?**
- **Cisco Email Security Appliance Product Support**
- **Cisco Web Security Product Support**
- **Cisco Content Security Management Appliance Product Support**
- **Technical Support & Documentation - Cisco Systems**