Copy Files Securely from Routers and Switches to Local PC

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Problem

Solution

Related Information

Introduction

This document describes how to securely copy files from Cisco routers and switches to the local Windows/Linux/macOS PC.

Prerequisites

Requirements

Cisco recommends that you have knowledge of Secure Shell (SSH) reachability to the device with privilege level 15 access.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco C9300-24P switch with Cisco IOS® 17.3.5
- Windows 10 OS
- RedHat Linux OS

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The process for how to securely copy the files from Cisco routers/switches to local Windows/Linux/macOS PC without the need for any external server or software like Trivial File Transfer Protocol (TFTP), File Transfer Protocol (FTP), Secure File Transfer Protocol (SFTP), or Secure Copy Protocol (SCP) is described in this document.

Problem

Sometimes in a secure environment, it is difficult to get to a TFTP/FTP/SFTP/SCP server to copy files like pcap, crash files, and Cisco IOS images from routers and switches to external sources. There is a chance the firewall blocks the ports used by any of these previously mentioned protocols between source and destination devices.

Solution

With SCP enabled on the Cisco device, you can copy the file from devices without any server or application to your local PC.

Here is the minimum configuration required on the device.

<#root>

```
hostname Switch
!
interface GigabitEthernet0/0
 ip address
```

10.197.249.101

```
 255.255.255.0
 no shut
!
ip route 0.0.0.0 0.0.0.0
```

10.197.249.1

```
!
aaa new-model
!
aaa authentication login default local
aaa authorization exec default local
!
ip domain name cisco.com
!
```

!--- key used in this example is 1024

```
!
crypto key generate rsa
!
username cisco privilege 15 secret 5 <redacted>
!
line vty 0 x
 transport input ssh
 login local
```

!

ip scp server enable

!--- you can disable the above command after copy is completed

```
!

end

!--- optional

!
ip ssh time-out 60
ip ssh authentication-retries 5
ip ssh version 2
!
```

Copy the files from Cisco router/switch with the use of this command on local Windows/Mac/Linux:

```
scp -O username@<ip_address_of_the_device>:flash:/filename
```

Windows 10:


```
C:\Users\mmehtabu.CISCO>
cd /

C:\>
cd ios

C:\ios>dir

Volume in drive C has no label.

Volume Serial Number is xxxx-yyyy

Directory of C:\ios
05-01-2023 09.32 AM <DIR> .
05-01-2023 09.32 AM <DIR> ..
 0 File(s) 0 bytes
 2 Dir(s) 163,191,525,376 bytes free

C:\ios>
scp -O cisco@10.197.249.101:flash:/mycap.pcap .

Password:

mycap.pcap                                                    100%   33MB 105.8KB/s   05:19
```

```
Connection to 10.197.249.101 closed by remote host.

C:\ios>
dir


Volume in drive C has no label.
Volume Serial Number is xxxx-yyyy

 Directory of C:\ios
05-01-2023 09.39 AM <DIR> .
05-01-2023 09.39 AM <DIR> ..
05-01-2023 09.40 AM 1,606,582
mycap.pcap


 1 File(s) 1,606,582 bytes
 2 Dir(s) 163,182,600,192 bytes free
```

Linux:

```
<#root>
 [root@root0 ~]#
pwd


/root

[root@root ~]#
ls -l

total 1


drwxr-xr-x. 2 root root 6 Apr 6 2022 Pictures

[root@root ~]#
scp -O cisco@10.197.249.101:flash:/mycap.pcap  .


Password:

flash:/mycap.pcap                                             100%   45MB   2.9MB/s   00:15

[root@cpnr000 ~]#
ls -l

total 1580
-rw-r--r--. 1 root root 1606582 Jan 5 09:47
mycap.pcap

drwxr-xr-x. 2 root root 6 Apr 6 2022 Pictures
```

The macOS has a similar command:

```
scp -O username@<ip_address_of_the_device>:flash:/filename
```

Related Information

- Secure Shell Configuration Guide
- Copy Cisco IOS Images to Routers and Switches Securely
- Technical Support & Documentation - Cisco Systems