Cisco ASA Password Recovery

By Don R. Crawley, CCNA Security

In this article, I'll explain how to perform a password "reset" on your Cisco ASA security appliance. The more commonly used term for this procedure is "password recovery" which is left over from the days when you could actually view passwords in configuration files in plain text. Today, such passwords are encrypted and not actually recoverable. Instead, you will gain access to the appliance via the console port and reset the password(s) to known values.

This procedure requires physical access to the device. You will power-cycle your appliance. You will then interrupt the boot process and change the configuration register value to prevent the appliance from reading its stored configuration at boot. Since the device ignores its saved configuration on boot, you are able to access its configuration modes without passwords. Once you're in configuration mode, you will load the saved configuration from flash memory, change the passwords to a known value, change the configuration register value to tell the device to load its saved configuration on boot, and reload the device.

Caution: As with all configuration procedures, these procedures should be tested in a laboratory environment prior to usage in a production environment to ensure suitability for your situation.

The following steps were designed using a Cisco ASA 5505 Security Appliance. They are not appropriate for a Cisco PIX Firewall appliance.

Power-cycle your security appliance.

When prompted, press Esc to interrupt the boot process and enter ROM Monitor mode.You should immediately see a rommon prompt (rommon #0>).

At the rommon prompt, enter the confreg command to view the current configuration register setting:

```
rommon #0>confreg
```

The current configuration register should be the default of 0×01 (it will actually display as 0x00000001). The security appliance will ask if you want to make changes to the configuration register. Answer no when prompted.

You must change the configuration register to 0×41, which tells the appliance to ignore its saved (startup) configuration upon boot:

```
rommon #1>confreg 0×41
```

Reset the appliance with the boot command:

```
rommon #2>boot
```

Notice that the security appliance ignores its startup configuration during the boot process. When it finishes booting, you should see a generic User Mode prompt:

```
ciscoasa>
```

Enter the enable command to enter Privileged Mode. When the appliance prompts you for a password, simply press (at this point, the password is blank):

```
ciscoasa>enable
Password:
ciscoasa#
```

Copy the startup configuration file into the running configuration with the following command:

```
ciscoasa#copy startup-config running-config
Destination filename [running-config]?
```

The previously saved configuration is now the active configuration, but since the security appliance is already in Privileged Mode, privileged access is not disabled. Next, in configuration mode, enter the following command to change the Privileged Mode password to a known value (in this case, we’ll use the password system):

```
asa#conf t
asa(config)#enable password system
```

While still in Configuration Mode, reset the configuration register to the default of 0×01 to force the security appliance to read its startup configuration on boot:

```
asa(config)#config-register 0×01
```

Use the following commands to view the configuration register setting:

```
asa(config)#show version
```

At bottom of the output of the show version command, you should see the following statement:

```
Configuration register is 0×41 (will be 0×1 at next reload)
```

Save the current configuration with the copy run start command to make the above changes persistent:

```
asa#copy run start
Source filename [running-config]
```

Reload the security appliance:

```
asa# reload
System config has been modified. Save? [Y]es/[N]o:yes

Cryptochecksum: e87f1433 54896e6b 4e21d072 d71a9cbf2149
bytes copied in 1.480 secs (2149 bytes/sec)Proceed with
reload? [confirm]
```

When your security appliance reloads, you should be able to use your newly reset password to enter privileged mode.

Learn more about working with Cisco ASA Security Appliances in our two-day Cisco ASA Training Seminar. Click here for details

soundtraining.net
Accelerated, task-based training for IT pros
On the web: www.soundtraining.net
On the phone: (206) 988-5858