Security – AutoSecure

Packet Lab

Router Hardening…Automagically

The process of turning off unnecessary services is called “hardening” a router to prevent attacks or exploits. The basic steps of router hardening are:

1) Administratively shut down any unused router interfaces
2) Disable any unused services.

Two methods of “automagically” hardening your router:

1) AutoSecure - The AutoSecure IOS feature is invoked by issuing the “auto secure” command from the CLI. This allows an administrator to lock down the device with a single CLI command.
2) Cisco SDM One-Step Lockdown - The Cisco SDM One-Step Lockdown method for securing a router uses a wizard in the Cisco SDM graphical interface.

AutoSecure

auto secure command

AutoSecure is valuable to customers without special Security Operations Applications because it allows them to quickly secure their network without thorough knowledge of all the Cisco IOS features.

This feature eliminates the complexity of securing a router by creating a new CLI that automates the configuration of security features and disables certain features enabled by default that could be exploited for security holes.

This command takes you through a semi-interactive session (also known as the AutoSecure dialogue) in which to secure the management and forwarding planes. This command gives you the option to secure just the management or forwarding plane; if neither option is selected, the dialogue will ask you to configure both planes.

Caution: If your device is managed by a network management (NM) application, securing the management plane could turn off vital services and disrupt the NM application support.

In Cisco IOS Release 12.3(8)T, support for roll-back of the AutoSecure configuration is introduced. Roll-back enables a router to revert back to its preautosecure configuration state if the AutoSecure configuration fails.

Prior to Cisco IOS Release 12.3(8)T, roll-back of the AutoSecure configuration is unavailable; thus, you should always save the running configuration before configuring AutoSecure.

Packet Lab

auto secure options

```
r2#auto secure ?
  firewall        AutoSecure Firewall
  forwarding      Secure Forwarding Plane
  full            Interactive full session of AutoSecure
  login           AutoSecure Login
  management      Secure Management Plane
  no-interact     Non-interactive session of AutoSecure
  ntp             AutoSecure NTP
  ssh             AutoSecure SSH
  tcp-intercept   AutoSecure TCP Intercept
  <cr>
```

Packet Lab

AutoSecure Dialogue

```
r2#auto secure
                --- AutoSecure Configuration ---
*** AutoSecure configuration enhances the security of
the router, but it will not make it absolutely resistant
to all security attacks ***

AutoSecure will modify the configuration of your device.
All configuration changes will be shown. For a detailed
explanation of how the configuration changes enhance security
and any possible side effects, please refer to Cisco.com for
Autosecure documentation.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure

Is this router connected to internet? [no]: y
Enter the number of interfaces facing the internet [1]: 1
<-output truncated->
```

AutoSecure Verification

```
r2# show auto secure config
no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
<-output truncated->

r1#show auto secure config
AutoSecure is not configured
```

Packet Lab

AutoSecure Rollback

Cisco AutoSecure Rollback enhances the Cisco AutoSecure, by providing a method to restore the system configuration back to its state prior to execution of the autosecure command. **This feature takes a snapshot of the current running configuration and stores that in the ATA Disk prior to execution of the autosecure command**. When rollback is initiated, the system will be restored to the snapshot configuration.

Rollback could occur in either automated or manual mode. Automated rollback will be initiated if Cisco AutoSecure experiences a failure during its operation. **In manual mode, the user simply issues the standard CLI rollback command and the rollback process will be initiated.**

Cisco AutoSecure Logging initiates a syslog message when the autosecure set of commands are executed.

Benefits

- Simplifies Device Lockdown - With Cisco AutoSecure Rollback & Logging, users will feel more confident using the Cisco AutoSecure. If the command was accidentally issued, one can easily restore the configuration back to its original state.
- Tracking of Cisco AutoSecure Execution - With the Cisco AutoSecure logging feature, a system administrator can track when autosecure has been executed.

Models:

- Cisco 2691 Router
- Cisco 1700 and 3700 Series Routers
- Cisco 7200 Series with ATA Disk

To AutoSecure or not to AutoSecure – that is the question

The biggest advantage of using AutoSecure is that you can harden a router with a single command. This is a blessing and a curse. The command is intended to assist those who don't know much about routers and and want to make sure their device is secure. The problem with this is that if you don't know much about routers then you're going to have a hell of a time troubleshooting any issues brought on by AutoSecure.

My suggestion is to configure AutoSecure, then issue the "show auto secure config" command and take a look at the commands that AutoSecure has configured. Cut and paste that output into a textfile. You can then rollback AutoSecure with a reload(make sure you don't write the config) or using the mystery rollback command on supported models. Now you can review the commands and delete any that you don't want to implement and paste the rest into your configuration.