

# Cisco Automated IOS Protection Configuration Guide

## Introduction

The Cisco Automated IOS® Protection capability uses a group of traffic filters that are updated as needed to protect the router against new exploits and vulnerabilities. These filters can be applied to protect the Cisco IOS Software control plane and (if desired) to filter traffic going through one or more interfaces on the router.

## Configuration for Automatic Download

The Cisco Automated IOS Protection capability can be configured to automatically download protection (filter) packages from a central server maintained on the customer premises or directly from Cisco.com (if the router has access to the Internet) at desired intervals using one of the supported protocols and providing a username and password if necessary.

Follow the steps shown here to configure periodic updates of Cisco Automated IOS Protection capability filter packages from a local or central server.

Note that “fpm” refers to the Flexible Packet Matching technology used by the Cisco Automated IOS Protection capability. Note also that “AIP” refers to the Cisco Automated IOS Protection Solution.

### Step 1

Configure a time range to periodically check for new updates of Cisco Automated IOS Protection Solution filter packages:

```
Router#conf t
Router(config)# time-range AIPTimer
Router(config-time-range)# periodic daily 23:30 to 23:59
Router(config-time-range)# exit
```

Here is another example of time range configuration:

```
Router#conf t
Router(config)# time-range AIPTimer
Router(config-time-range)# periodic Sunday 5:00 to 6:00
Router(config-time-range)# exit
```

### Step 2

Configure parameters for the remote or central server, username, password, etc. and associate the package information with the time range configured in step 1. Use the following sample configuration:

```
Router(config)#fpm package-info
Router(config-fpm-pak-info)# host ftp.cisco.com
Router(config-fpm-pak-info)# username Amy
Router(config-fpm-pak-info)# password xxxxxxxx
```

```

Router(config-fpm-pak-info)# local-path flash:

! one may use any other user-created local directory on the router

Router(config-fpm-pak-info)# time-range AIPtimer
Router(config-fpm-pak-info)# protocol ftp
Router(config-fpm-pak-info)# remote-path AIP/filters/
Router(config-fpm-pak-info)# exit

```

Note that the username and password are not required if TFTP is used. For servers supporting non-authentication-based HTTP, you can use any dummy username and password. Other supported protocols are HTTPS, FTP, and SCP.

### Step 3

Configure the Cisco Automated IOS Protection Solution filter package group to include the Cisco Automated IOS Protection Solution filter package that will be posted by Cisco with traffic filters for new vulnerabilities as needed. Although you can add other traffic filter packages to this filter package group, they are not needed for or relevant to the operation of the Cisco Automated IOS Protection Solution. Hence, this filter package group is created to contain only the Cisco Automated IOS Protection Solution filter package. If the traffic being monitored matches any of the filters in the package provided, it will be dropped and an event log will be generated.

```

Router# conf t
Router(config)# fpm package-group AIP_package_group
Router(config-fpm-pak-grp)# package Cisco_AIP_Filters

! Must use the exact filter package (base) file name which will be
! provided and announced by Cisco PSIRT Team soon.

Router(config-fpm-pak)# action log
Router(config-fpm-pak)# action drop
Router(config-fpm-pak)# end

```

### Step 4

Configure the Cisco Automated IOS Protection Solution filter package group so that it is auto-loaded from a remote, central, or Cisco® server; using the auto-load keyword.

```

Router(config)# fpm package-group AIP_package_group
Router(config-fpm-pak-grp)# auto-load
Router(config-fpm-pak-grp)# end

```

### Step 5

Apply the Cisco Automated IOS Protection Solution filter package group to the control plane internal interface to protect the router (as shown here) and (if desired) any combination of the physical (external) interfaces to monitor the traffic going through them in the inbound and outbound directions.

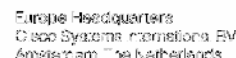
```

Router(config)# control-plane
Router(config-cp)# fpm package-group input AIP_package_group
Router(config-cp)# exit

```

Cisco Automated IOS Protection Solution filter package updates (downloads) can be also invoked immediately through the Cisco IOS Software executive mode command line.

```
router#fpm package-update server
```



CC BY-NC-SA  
Computing System, Cisco WebEx, iGlobe, Hip Channels, Hio for Good, Hio Mine, FlipShare (Design), Hip Utra, Hip Video, Hip Video (Design), Instant! Brandmark, and We come to the Human Network are trademarks.  
Changing the Way We Work, Live, Play and Learn, Cisco Capital, Cisco Capital (Stylized), Cisco Store, Hip GTR Card, and One Million Acts of Green are service marks, and Access Registered,  
Airmet, Allpush, AsyncOS, Bringing the Meeting To You, Catalyst, CDA, CCC, CGE, COIP, CGNA, CONE, COS, CGOV; Cisco, the Cisco Switched Internetwork Event logo, Cisco OS, Cisco Linux, Cisco Xrnx, Cisco Press,  
Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, Etherfast, Etherswitch, Event Center, SealStar, Flow Me Nowling, GenWave, LYNX, OS, iPhone,  
IronPort, the IronPort logo, Laser Link, LightStream, Linksys, Maching@Work, MeetingPlace Online Sound, MGX, Networks, Networking Academy, PCNow, PX, PowerKEY, PowerPac's, PowerTV, PowerTV (Design), PowerVu,  
Prisma, ProConnect, rOSA, Routerize.com, SNAI Thel, Spectrum Expert, StackWise, Wapix x, and the Webex logos are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Ciena and any other company. ©2012