Contents

Introduction

It is software based IPS which helps in mitigating various attacks based on signature definitions. This feature was introduced in 12.4(pi6)T and 5.x version of IOS-IPS came from 12.4(11)t and only this version is supported by us. It can be verified using the below command:

- sh subsys name ips

output: 2.xx.xx indicates 4.x and 3.xxx indicates 5.x

Configuration

1) Copy the required crypto key for IOS-IPS:

```
crypto key pubkey-chain rsa
named-key realm-cisco.pub signature
 key-string
  30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
  00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
  17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
  B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
  5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
  FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
  50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
  006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
  2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
  F3020301 0001
quit
exit
exit
```

2) Create a directory on flash to store compiled signature:

```
   mkdir ipsstore
   ip ips name myips
   ip ips config location flash:ipsstore
```

3) Enable the required category based on free memory.

```
 ip ips signature-category
```

```
   category all
    retired true
    exit
   category ios_ips basic
    retired false
    exit
    exit
```

ip ips signature-category

```
category all
retired true
exit
category ios_ips advanced
 retired false
 exit
 exit
```

4) Apply IOS-IPS to desired interfaces:

int fa 1

```
ip ips myips in
```

Note: It's always recommended to apply IOS-IPS on WAN interface in in direction.

5) Download the latest Advanced Signature file from cisco.com from following path: Security > Cisco IOS Intrusion Prevention System Feature Software > IOS IPS Signature Data File

For e.g; IOS-S473-CLI.pkg

6) Now copy and compile the downloaded signature file. Save the downloaded file on the desktop in the tftp folder and point the directory of the tftp server towards that folder:

1. copy tftp://10.10.10.100/IOS-S473-CLI.pkg idconf

Note: While running this commnads due to compilation of signatures CPU of router reaches 100% causing interruption in production so it is always recommended to run this during Off-hours.

Related show Commands

Router2800#sh ip ips ?

```
 all                 IPS all available information
 auto-update         IPS auto-update configuration
 category            Category
 configuration       IPS configuration
 event-action-rules  Event Action Rules (SEAP)
 interfaces          IPS interfaces
 name                IPS name
 sessions            IPS sessions
 signature-category  Signature Category
 signatures          IPS signatures
 statistics          IPS statistics
```

Related Information

==

Disabling a sig:

(config)#ip ips signature-definition

(config-sigdef)#signature 3124 0

(config-sigdef-sig)#status

(config-sigdef-sig-status)#retired true

(config-sigdef-sig-status)#end

===

ip ips deny-action ips-interface

```
Command to support load balancing configuration on IOS routers with IOS-IPS enabled.
```

===

Command Reference: http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html

Configuring Cisco IOS Intrusion Prevention System (IPS):
https://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_cfg_ips.html#wp1146846

Configuring IOS-IPS using SDM:
http://www.cisco.com/en/US/products/ps8775/products_configuration_example09186a008097dc4a.shtml

Configuring IOS-IPS using CCP:
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/prod_white_paper0900aecd8066d265.html

Cisco IOS Intrusion Prevention System (IPS)Configuration Examples and TechNotes
http://www.cisco.com/en/US/products/ps6634/prod_configuration_examples_list.html