Cisco IOS Intrusion Prevention System Best Practices

Alex Yeung

Technical Marketing Engineer

October 2008

IOS IPS Best Practices

- Understanding of terms used for signature status
- Dealing with memory allocation errors when compiling signatures
- Total number of signatures can be compiled
- Dealing with signature failing to compile
- Configuration steps
- Dealing with IOS IPS policy applied at the wrong direction and/or interface
- Dealing with signature that do not fire with matching traffic
- Dealing with Packet/Connections dropped due to packets arriving out of order

Understanding of Terms Used for Signature Status

- Retire vs. unretire
- Enable vs. disable
- Compiled vs. loaded
- Cisco IOS IPS inherited these terms from IPS 4200 series appliance
- Due to memory constraints, most of the signatures on router are retired by default
- IOS IPS users need to worry about enable/disable as well as retire/unretire

Understanding of Terms Used for Signature Status (Cont.)

- Retire vs. unretire

  Select/de-select which signatures are being used by IOS IPS to scan traffic

  Retiring a signature means IOS IPS will NOT compile that signature into memory for scanning

  Unretiring a signature instructs IOS IPS to compile the signature into memory and use the signature to scan traffic

  You can use IOS command-line interface (CLI) or SDM/CCP to retire or unretire individual signatures or a signature category

Understanding of Terms Used for Signature Status (Cont.)

- Enable vs. disable

  Enable/disable is NOT used to select/de-select signatures to be used by IOS IPS

  Enabling a signature means that when triggered by a matching packet (or packet flow), the signature takes the appropriate action associated with it

  However, only unretired AND successfully compiled signatures will take the action when they are enabled. In other words, if a signature is retired, even though it is enabled, it will not be compiled (because it is retired) and it will not take the action associated with it

  Disabling a signature means that when triggered by a matching packet (or packet flow), the signature DOES NOT take the appropriate action associated with it

  In other words, when a signature is disabled, even though it is unretired and successfully compiled, it will not take the action associated with it

  You can use IOS command-line interface (CLI) or SDM/CCP to enable or disable individual signatures or a signature category

Understanding of Terms Used for Signature Status (Cont.)

- Compiled vs. loaded

Loading refers to the process where IOS IPS parse the signature files (XML files in the config location) and fill in the signature database

This happens when signatures are loaded via “copy <sig file> idconf” or the router reboots with IOS IPS already configured

Compiling refers to the process where the parameter values from unretired signatures are compiled into a regular expression table

This happens when signatures are unretired or when other parameters of signatures belonging to that regular expression table changes

Once signatures are compiled, traffic is scanned against the compiled signatures

Dealing with Memory Allocation Errors When Compiling Signatures

- The number of signatures that can be compiled depends on the free memory available on the router
- When router does not have enough memory to compile signatures, memory allocation failure messages are logged
- Already compiled signatures will still be used to scan traffic. No additional signatures will be compiled for that engine during the compiling process. IOS IPS will proceed with compiling signatures for the next engine

```
*Mar 18 07:09:36.887: %SYS-2-MALLOCFAIL: Memory allocation of 65536 bytes failed from 0x400C1024, alignment 0
Pool: Processor  Free: 673268  Cause: Memory fragmentation
Alternate Pool: None  Free: 0  Cause: No Alternate pool
 -Process= "Exec", ipl= 0, pid= 3,  -Traceback= 0x4164F41C 0x400AEF1C 0x400B4D58 0x400B52C4 0x400C102C
 0x400C0820 0x400C23EC 0x400C0484 0x424C1DEC 0x424C2A4C 0x424C2FF0 0x424C31A0 0x430D6ECC 0x430D7864
 0x430F0210 0x430FA0E8
*Mar 18 07:09:36.911: %SYS-2-CHUNKEXPANDFAIL: Could not expand chunk pool for regex. No memory available
-Process= "Chunk Manager", ipl= 3, pid= 1,  -Traceback= 0x4164F41C 0x400C06FC
*Mar 18 07:09:37.115: %IPS-4-SIGNATURE_COMPILE_FAILURE: service-http 12024:0 - compilation of regular
 expression failed
*Mar 18 07:09:41.535: %IPS-4-SIGNATURE_COMPILE_FAILURE: service-http 5280:0 - compilation of regular
 expression failed
*Mar 18 07:09:44.955: %IPS-4-SIGNATURE_COMPILE_FAILURE: service-http 5284:0 - compilation of regular
 expression failed
*Mar 18 07:09:44.979: %IPS-4-SIGNATURE_COMPILE_FAILURE: service-http 12023:0 - compiles discontinued for this
 engine
```

Dealing with Memory Allocation Errors When Compiling Signatures – Best Practice

- The pre-defined IOS IPS Basic and Advanced signature categories contain optimum combination of signatures for all standard memory configurations, providing a good starting point
- Never unretire the “all” category
- For routers with 128MB memory, start with the IOS IPS Basic category
- For routers with 256MB memory, start with the IOS IPS Advanced category
- Then customize the signature set by unretiring/retiring few signatures at a time according to your network needs
- Pay attention to the free memory every time after you unretiring/retiring signatures

Total Number of Signatures that Can Be Compiled

- There is no magic number!
- Many factors can have impact:

  Available free memory on router

  Type of signatures being unretired, e.g. signatures in the complex STRING.TCP engine

- When router free memory drops below 10% of the total installed memory, then stop unretiring signatures

Dealing with Signatures Failing to Compile

- There are mainly three reasons that could cause a signature fail to compile

  Memory constraint, running out of memory

  Signatures are not supported in IOS IPS: META signatures

  Regular Expression table for a particular engine exceeds 32MB entries

- Check the list of supported signatures in IOS IPS at:

  http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/prod_white_paper0900aecd8062ac75.html

- Retire signatures not supported by IOS IPS and signatures not applicable to your network to save memory

Configuration Steps

- Follow the steps in the following order for initial Cisco IOS IPS configuration:

  Step 1: Download IOS IPS signature package to PC

  Step 2: Create IOS IPS configuration directory

  Step 3: Configure IOS IPS crypto key

  Step 4: Create IOS IPS policy and apply to interface(s)

  Remember to FIRST retire the “all” category

  Step 5: Load IOS IPS signature package

- Next verify the configuration and signatures are compiled:

  show ip ips configuration

  show ip ips signatures count

Configuration Steps – Cont.

- Next you can start to tune the signature set with the following options:

  Retire/unretire signatures (i.e. add/remove signatures to/from the compiled list)

  Enable/disable signatures (i.e. enforce/disregard actions)

  Change actions associated with signatures

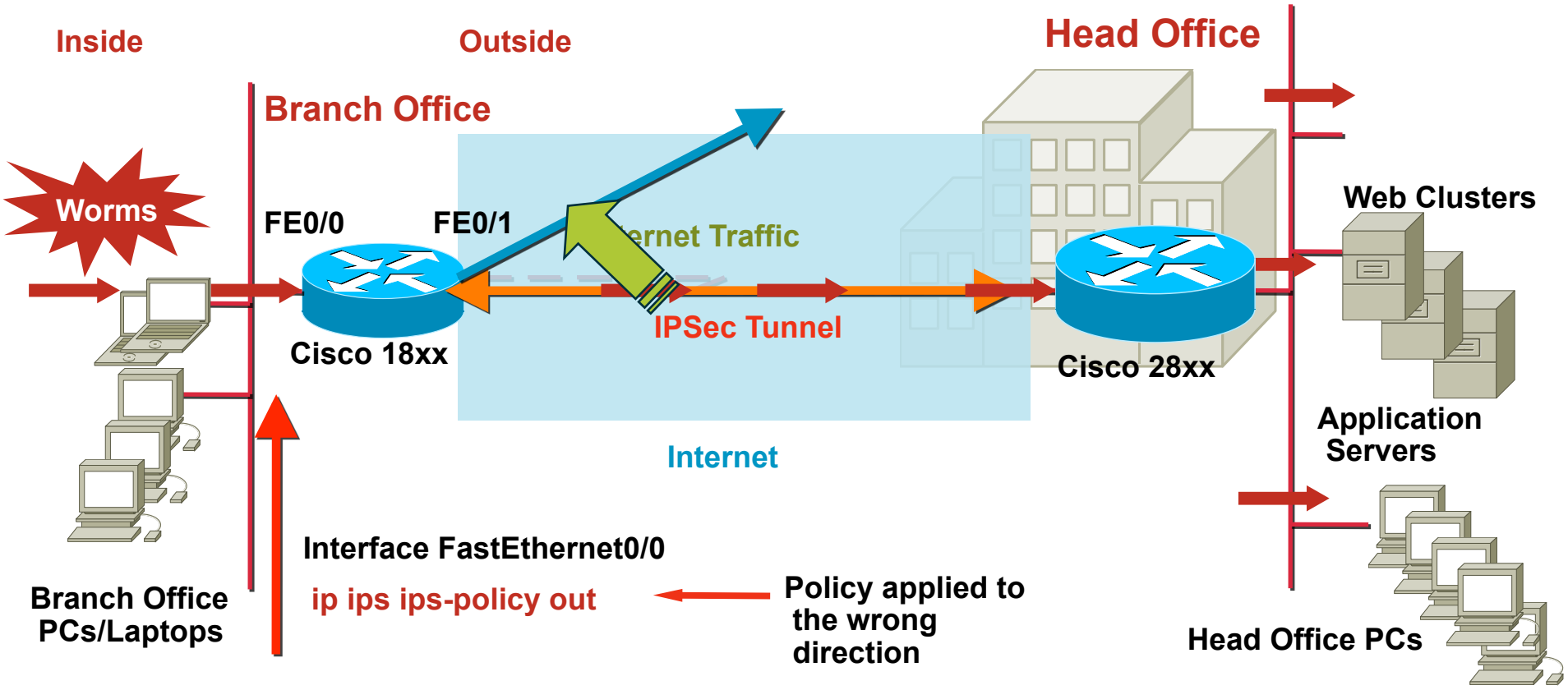
- Refer to Getting Started Guide at:

  http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/prod_white_paper0900aecd805c4ea8.html

Dealing with IOS IPS Policy Applied at the Wrong Direction/Interface—Incorrect Configuration

Case A: Issue

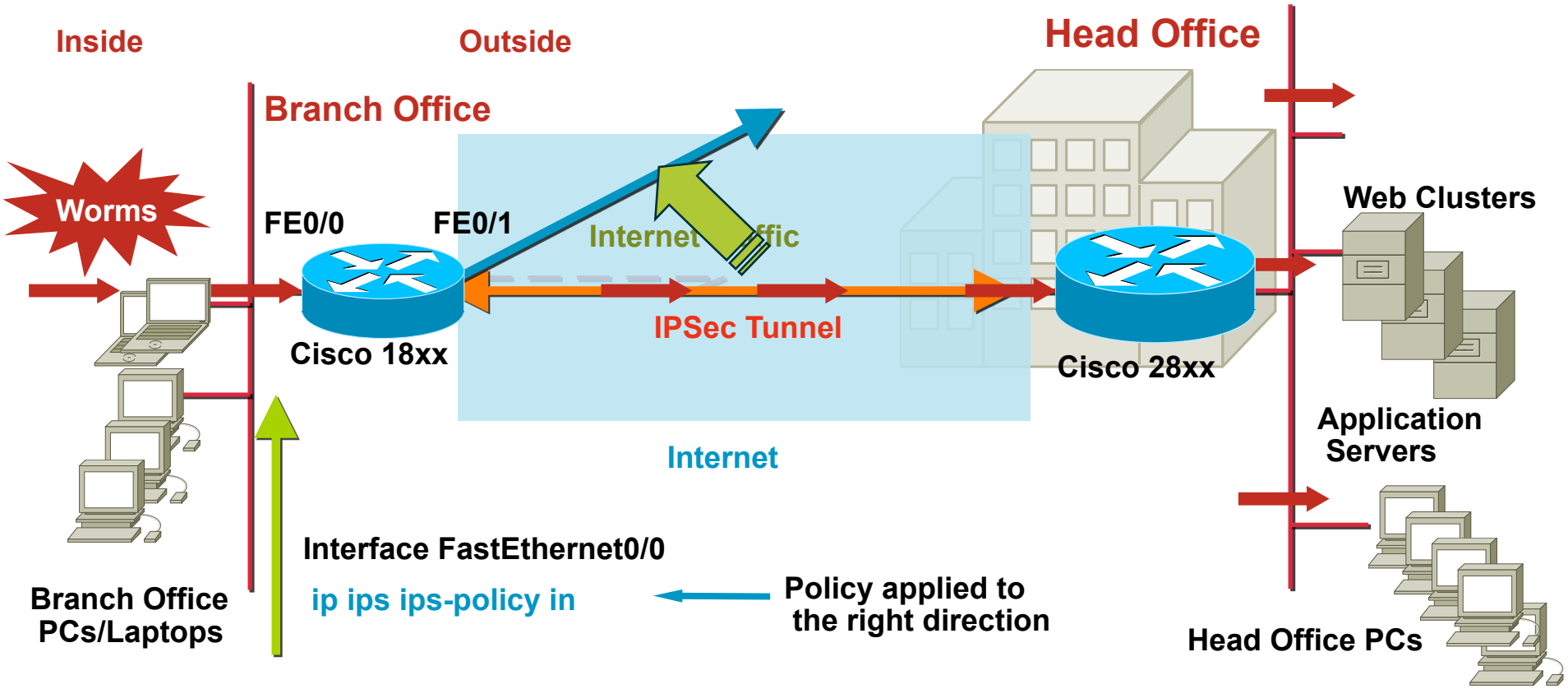
Protecting Attacks from Inside



Dealing with IOS IPS Policy Applied at the Wrong Direction/Interface—Resolution

Case A: Solution

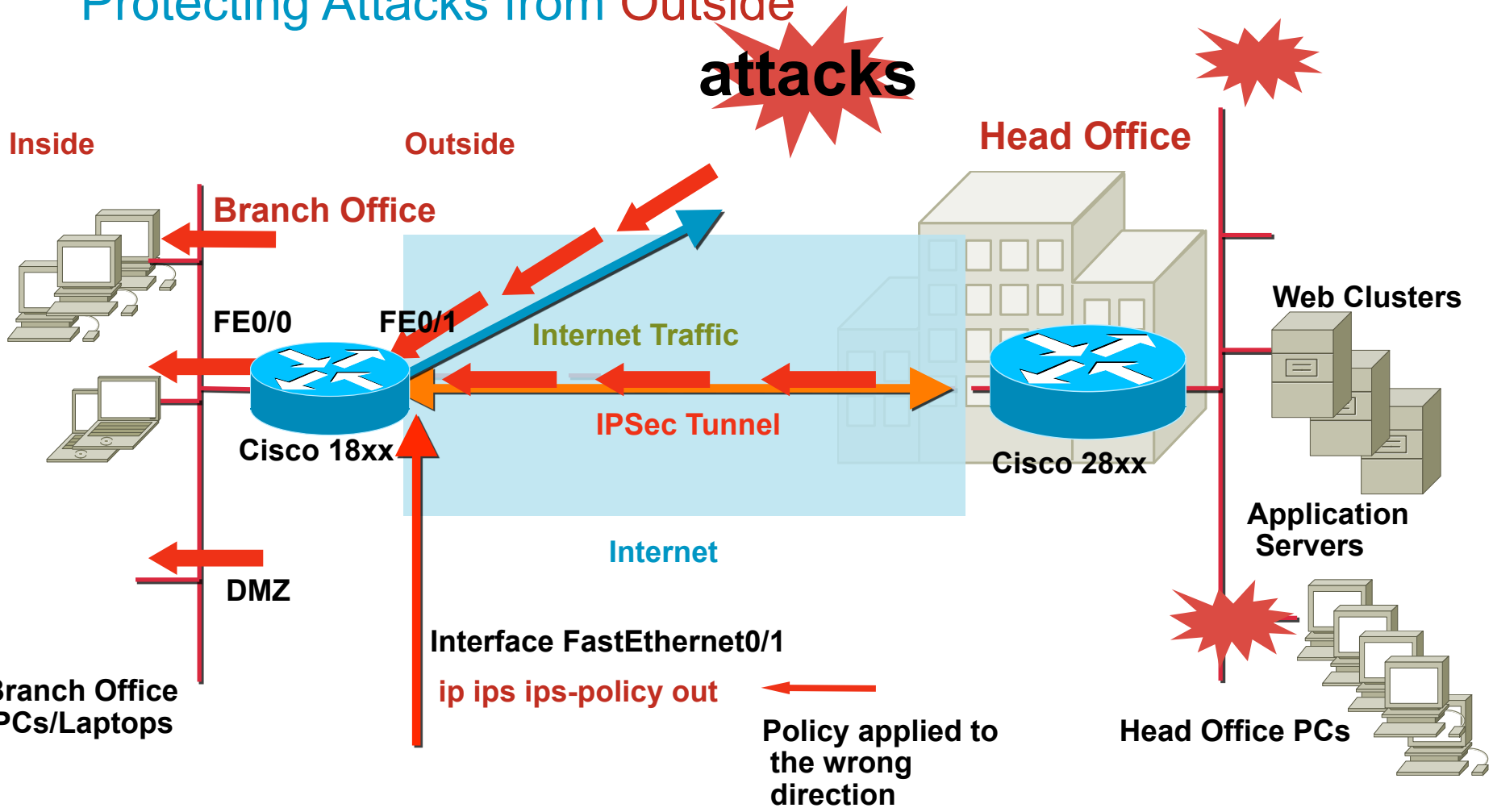
Protecting Attacks from Inside



Dealing with IOS IPS Policy Applied at the Wrong Direction/Interface—Incorrect Configuration

Case B: Issue

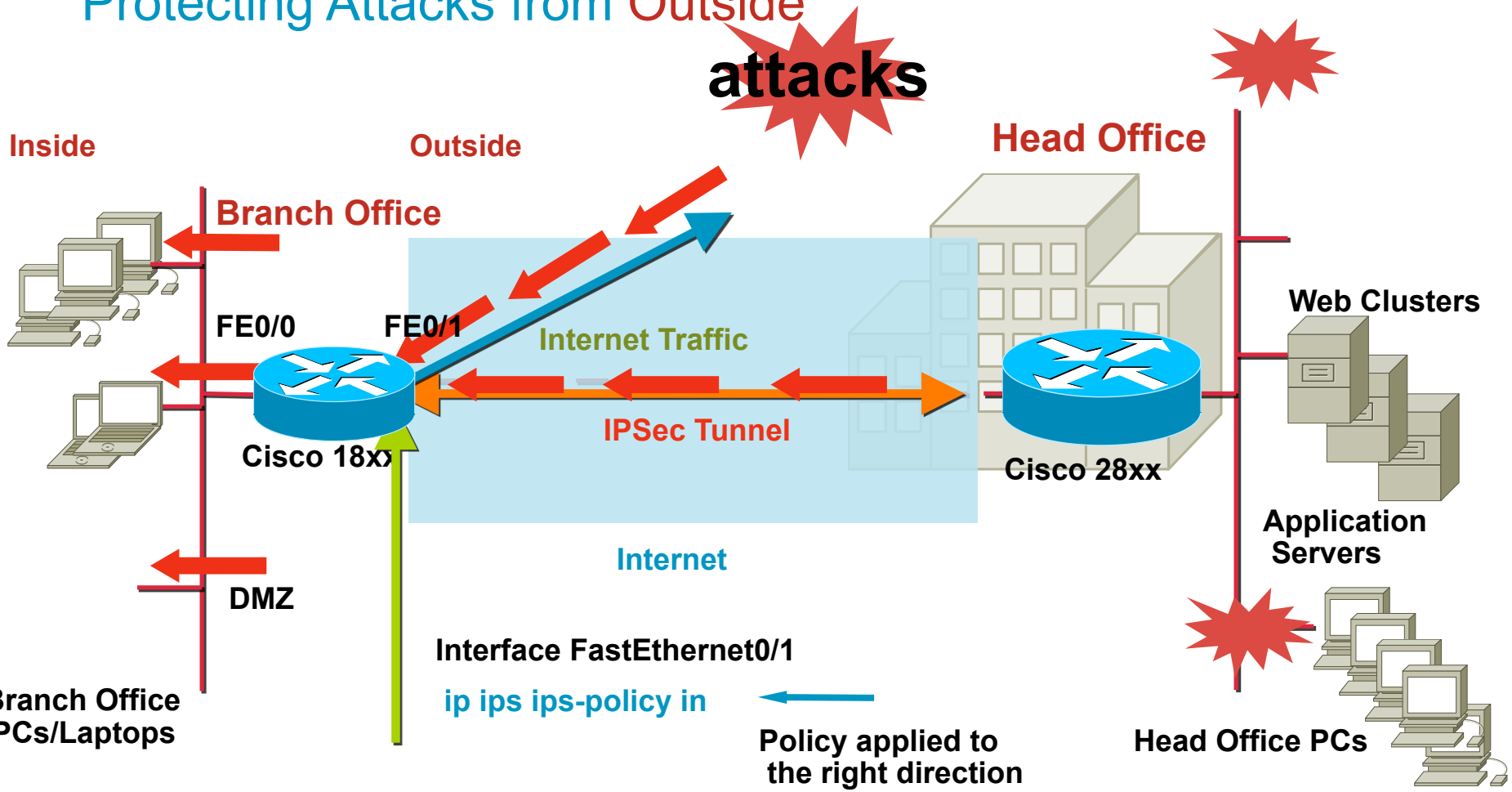
Protecting Attacks from Outside



Dealing with IOS IPS Policy Applied at the Wrong Direction/Interface—Resolution

Case B: Solution

Protecting Attacks from Outside



Dealing with Signature that Do Not Fire with Matching Traffic

1. Are all signatures not firing or only a specific signature not firing?
2. If a specific signature is not firing
   - i) Check signature status – enabled/disabled/deleted?
   - ii) Is IOS IPS event notification enabled? i.e. syslog/SDEE
3. If all signature are not firing
   - i) Check whether signature package is loaded or not
   - ii) Verify IOS IPS is applied in the right direction (inbound/outbound) and on the right interface
   - iii) Is IOS IPS event notification enabled? i.e. syslog/SDEE
   - iv) Do you see alarms/alerts showing signature matching?
   - v) Use “show ip ips sessions detail” make sure traffic is going through IOS IPS
   - vi) Use “show ip ips signatures statistics | i <sig id>” to see signature hits

Dealing with Packet/Connections dropped due to packets arriving out of order

FW Drops Out-of-Order Packet Slows Down Network Traffic

After turn on IPS, web traffic response time slows down. Go to the router and find out there are syslog messages dropping out of order packets.

```
*Jan  6 19:08:45.507: %FW-6-DROP_PKT: Dropping tcp pkt10.10.10.2:1090 => 199.200.9.1:443
*Jan  6 19:09:47.303: %FW-6-DROP_PKT: Dropping tcp pkt10.10.10.2:1091 => 199.200.9.1:443
*Jan  6 19:13:38.223: %FW-6-DROP_PKT: Dropping tcp pkt66.102.7.99:80 =>
 192.168.18.21:1100
```

debug ip inspect detail shows Out-Of-Order packet

```
*Jan  6 19:15:28.931: CBAC* sis 84062FEC L4 inspectresult: SKIP packet 83A6F83C (199.200.9.1:443)
 (192.168.18.21:1118) bytes 174 ErrStr = Out-Of-OrderSegment tcp
*Jan  6 19:15:28.931: CBAC* sis 84062FEC pak 83A6FF64SIS_OPEN/ESTAB TCP ACK 842755785 SEQ
 2748926608 LEN 0 (10.10.10.2:1118) => (199.200.9.1:443)
*Jan  6 19:15:28.931: CBAC* sis 84062FEC pak 83A6F83CSIS_OPEN/ESTAB TCP ACK 2748926608 SEQ
 842755785 LEN 1317 (199.200.9.1:443) <= (192.168.18.21:1118)
*Jan  6 19:15:28.931: CBAC* sis 84062FEC L4 inspectresult: SKIP packet 83A6F83C (199.200.9.1:443)
 (192.168.18.21:1118) bytes 1317 ErrStr = RetransmittedSegment tcp
*Jan  6 19:15:28.935: CBAC* sis 84062FEC pak 83A6F83CSIS_OPEN/ESTAB TCP PSH ACK 2748926608
 SEQ 842758636 LEN 137 (199.200.9.1:443) <=(192.168.18.21:1118)
*Jan  6 19:15:28.935: CBAC* sis 84062FEC L4 inspectresult: SKIP packet 83A6F83C (199.200.9.1:443)
 (192.168.18.21:1118) bytes 137 ErrStr = Out-Of-OrderSegment tcp
```

Dealing with Packet/Connections dropped due to packets arriving out of order – Resolution

FW Drops Out-of-Order Packet Slows Down Network Traffic

- IPS requires packets arrive in order to perform signature scanning, thus drops out -of-order packet; this is one of the reasons for slow response and longer latency in network traffic
- IOS IPS supports Out-of-Order packet starting from 12.4(9)T2 and later 12.4T releases
- Not fixed in 12.4 mainline releases
- Out-of-Order fix also applies to application firewall
- Out-of-order fix DOES NOT work when IOS IPS interface is included in a Zone -Based FW zone
- Out-of-order fix works between IOS IPS and Classic IOS FW (ip inspect)
- If using a release that does not have the fix, workaround is to use ACL to bypass IOS IPS inspection for the traffic flow in question

```
router(config)#access-list 120 deny ip any host 199.200.9.1
router(config)#access-list 120 deny ip host 199.200.9.1 any
router(config)#access-list 120 permit ip any any
router(config)#ip ips name myips list 120
```

- In the example, ACL 120 denies traffic and remove the traffic from IPS scanning; the network traffic between the two site do not experience slow response

IOS IPS Best Practices – Summary

- First time users, follow **Getting Started with Cisco IOS IPS Guide**

  http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/prod_white_paper0900aecd805c4ea8.html

- **Always remember to RETIRE ALL signatures first**

```
router(config)#ip ips signature-category
router(config-ips-category)#category all
router(config-ips-category-action)#retired true
router(config-ips-category-action)#end
Do you want to accept these changes? [confirm]
```

- **Never unretire the "all" signature category**
- For routers with 128MB memory, start with the IOS IPS Basic category
- For routers with 256MB or more memory, start with the IOS IPS Advanced category

IOS IPS Best Practices – Summary

- Then use CCP/CSM to customize the signature set by unretiring /retiring few signatures at a time according to your network needs
- Pay attention to the free memory every time after you unretiring/ retiring signatures
- When router free memory drops below 10% of the total installed memory, then stop unretiring signatures. Adding more memory will not necessarily increase the number of signatures that can be loaded significantly
- You must **unretire** and **enable** a signature to have it loaded and take configured actions when triggered. Enabling it does not load a signature
- If using IOS IPS in a network with a lot of *out-of-order* packets, note:

  You must use 12.4(9)T2 or 12.4(11)T or later T-Train releases. You may not use Mainline image. If Firewall will be also configured, you must configure Classic IOS Firewall. Zone Based Firewall will not work with out-of-order packets


CISCO