Cisco Configuration Professional: Zone-Based Firewall Blocking Peer to Peer Traffic Configuration Example

Document ID: 112237

Contents

Introduction
Prerequisites
  Requirements
  Router Configuration to Run Cisco CP
  Components Used
  Conventions
Background Information
Configure
  Network Diagram
Configuration through Cisco Configuration Professional
  Command-Line Configuration of ZFW Router
Verify
Related Information

Introduction

This document provides a step-by-step approach to configure a Cisco IOS Router as a zone-based firewall to block Peer-to-Peer (P2P) traffic by using the Advanced Firewall configuration wizard in the Cisco Configuration Professional (Cisco CP).

Zone-Based Policy Firewall (also known as Zone-Policy Firewall, or ZFW) changes the firewall configuration from the older interface-based model to a more flexible, more easily understood zone-based model. Interfaces are assigned to zones, and inspection policy is applied to traffic moving between the zones. Inter-zone policies offer considerable flexibility and granularity. Therefore, different inspection policies can be applied to multiple host groups connected to the same router interface. Zones establish the security borders of your network. A zone defines a boundary where traffic is subjected to policy restrictions as it crosses to another region of your network. ZFWs default policy between zones is deny all. If no policy is explicitly configured, all traffic moving between zones is blocked.

P2P applications are some of the most widely used applications on the Internet. P2P networks can act as a conduit for malicious threats such as worms, offering an easy path around firewalls and causing concerns about privacy and security. Cisco IOS Software Release 12.4(9)T introduced ZFW support for P2P applications. P2P inspection offers Layer 4 and Layer 7 policies for application traffic. This means ZFW can provide basic stateful inspection to permit or deny the traffic, as well as granular Layer 7 control on specific activities in the various protocols, so that certain application activities are allowed while others are denied.

Cisco CP offers an easy-to-follow, step-by-step approach to configure the IOS Router as a zone-based firewall by using the Advanced Firewall configuration wizard.

Prerequisites
Requirements

Ensure that you meet these requirements before you attempt this configuration:

- The IOS Router must have the software version as 12.4(9)T or later.
- For IOS Router models that support Cisco CP, refer to the Cisco CP Release Notes.

Router Configuration to Run Cisco CP

**Note:** Perform these configuration steps in order to run Cisco CP on a Cisco router:

```
Router(config)# ip http server
Router(config)# ip http secure-server
Router(config)# ip http authentication local
Router(config)# username <username> privilege 15 password 0 <password>
Router(config)# line vty 0 4
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet
Router(config-line)# transport input telnet ssh
Router(config-line)# exit
```

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 1841 IOS Router that runs IOS Software Release 12.4(15)T
- Cisco Configuration Professional (Cisco CP) Release 2.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Background Information

For this document’s example, the router is configured as a zone–based firewall to block the P2P traffic. The ZFW Router has two interfaces, an inside(trusted) interface in In–zone and an outside (untrusted) interface in Out–zone. The ZFW Router blocks P2P applications such as edonkey, fasttrack, gnutella and kazaa2 with logging action for the traffic that is passing from In–zone to the Out–zone.

Configure

In this section, you are presented with the information to configure the features described in this document.

**Note:** Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.
Configuration through Cisco Configuration Professional

This section contains the step–by–step procedure on how to use the wizard to configure the IOS Router as a zone–based firewall.

Complete these steps:

1. Go to Configure > Security > Firewall and ACL. Then, choose the Advanced Firewall radio button. Click Launch the selected task.

2. This next screen shows a brief introduction about the Firewall Wizard. Click Next to start configuring the firewall.
3. Select the interfaces of the router to be part of zones and click **Next**.

4. The default Policy with High Security along with the set of commands is shown in the next window. Click **Close** to proceed.
5. Enter the details of the DNS Server and click **Next**.

6. The Cisco CP provides a configuration summary such as the one shown here. Click **Finish** to complete the configuration.
The detailed configuration summary is provided in this table. This is the default configuration as per the High Security policy of the Cisco CP.

<table>
<thead>
<tr>
<th>Configuration Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong> Do not select the interface through which you accessed Cisco CP as the outside (untrusted) interface. If you do, you will not be able to launch Cisco CP from that interface after you complete the Firewall Wizard.</td>
</tr>
</tbody>
</table>

**Inside (trusted) Interfaces:**
- FastEthernet0/1 (10.77.241.114)

**Outside (untrusted) Interfaces:**
- FastEthernet0/0 (209.165.201.2)

**Service Policy Configuration:**

**In-zone -> Out-zone:**
- Inspect TCP, UDP, H323, SIP, SCCP and other protocols
- Deny packets with invalid ip address as source

**Application Inspection for HTTP:**
- Block HTTP port-misuse for IP, P2P
- Block HTTP protocol violation
- Block HTTP request methods other than post, head, get
- Block http request response containing non-ascii characters

**Application Inspection for Instant Messaging:**
- Block all services of msn, yahoo, aol with log action

**Application Inspection for P2P:**
- **Block file transfer over edonkey, fasttrack, gnutella and kazaa**
- **Block text-chat over edonkey**

**Application Inspection for Email:**
- Block invalid command for imap, pop3
- Block SMTP session with data length over 5 MB

**Self -> Out-zone:**
- Inspect router generated ICMP traffic

**Out-zone -> Self:**
- Deny all other traffic.

**DNS Configuration:**
- Primary DNS: 10.77.230.45
7. Check the **Save the running config to router's startup config** check box. Click **Deliver** to send this configuration to the router.

The entire configuration is delivered to the router. This takes some time to process.

8. Click **OK** to proceed.
9. Click **OK** again.

The configuration is now in effect and is shown as the rules under the Firewall Policy tab.

10. The zones along with the zone pairs they are associated can be viewed if you go to **Configure** > **Security** > **Advanced Security** > **Zones**. You can also add new zones by clicking **Add**, or modify the existing zones by clicking **Edit**.
11. Go to **Configure > Security > Advanced Security > Zone Pairs** to view the details of the zone pairs.

Instant help on how to modify/add/delete zones/zone pairs and other related information is readily available with the built-in web pages in the Cisco CP.
12. In order to modify the application specific inspection capabilities for certain P2P applications, go to Configuration > Security > Firewall and ACL. Then, click Edit Firewall Policy and choose the respective rule in the policy map. Click Edit.

This shows the current P2P applications that will blocked by default configuration.
13. You can use the Add and Remove buttons to add/remove specific applications. This screenshot shows how to add the winmx application to block that.
14. Instead of choosing the drop action, you can also choose the Inspect action to apply different options for deep packet inspection.
P2P inspection offers Layer 4 and Layer 7 policies for application traffic. This means ZFW can provide basic stateful inspection to permit or deny the traffic, as well as granular Layer 7 control on specific activities in the various protocols, so that certain application activities are allowed while others are denied. In this application inspection, you can apply different types of specific header level inspections for P2P applications. An example for the gnutella is shown next.

15. Check the P2P option and click Create in order to create a new policy-map for this.
16. Create a new policy-map for deep packet inspection for the gnutella protocol. Click **Add** and then choose **New Class Map**.

17. Give a new name for the class-map and click **Add** to specify a match criteria.
18. Use file-transfer as the match criterion and the string used is .exe. This indicates that all gnutella file transfer connections containing the .exe string match for the traffic policy. Click OK.

19. Click OK again to complete the class-map configuration.
20. Choose the **Reset** or **Allow** option, which depends on the Security policy of your company. Click **OK** to confirm the action with the policy-map.

![Configure Deep Packet Inspection - Peer-to-Peer](image)

In this same way you can add other policy−maps to implement deep inspection features for other P2P protocols by specifying different regular−expressions as the match criterion.

**Note:** P2P applications are particularly difficult to detect, as a result of port−hopping behavior and other tricks to avoid detection, as well as problems introduced by frequent changes and updates to P2P applications which modify the protocols behaviors. ZFW combines native firewall stateful inspection with Network−Based Application Recognition (NBAR)′s traffic−recognition capabilities to deliver P2P application control.

**Note:** P2P Application Inspection offers application−specific capabilities for a subset of the applications supported by Layer 4 Inspection:

- edonkey
- fasttrack
- gnutella
- kazaa2

**Note:** Currently, ZFW does not have an option to inspect the "bittorrent" application traffic.

BitTorrent clients usually communicate with trackers (peer directory servers) via HTTP running on some non−standard port. This is typically TCP 6969, but you might need to check the torrent−specific tracker port. If you wish to allow BitTorrent, the best method to accommodate the additional port is to configure HTTP as one of the match protocols and add TCP 6969 to HTTP using this ip port−map command: `ip port−map http port tcp 6969`. You will need to define http and bitTorrent as the match criteria applied in the class−map.

21. Click **OK** to complete the Advanced Inspection configuration.
The corresponding set of commands is delivered to the router.

22. Click OK to complete copying the set of commands to the router.

23. You can observe the new rules taking place from the Edit Firewall Policy tab under Configure > Security > Firewall and ACL.
Command–Line Configuration of ZFW Router

The configuration in the previous section from Cisco CP results in this configuration on the ZFW Router:

```
ZBF Router#show run
Building configuration...

Current configuration : 9782 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ZBF-Router
!
boot-start-marker
boot-end-marker
!
logging buffered 51200 warnings
!
no aaa new-model
ip cef
!
!
!
ip name-server 10.77.230.45
!
multilink bundle-name authenticated
parameter-map type protocol-info msn-servers
  server name messenger.hotmail.com
  server name gateway.messenger.hotmail.com
  server name webmessenger.msn.com

parameter-map type protocol-info aol-servers
  server name login.oscar.aol.com
  server name toc.oscar.aol.com
  server name oam-d09a.blue.aol.com
```
parameter-map type protocol-info yahoo-servers
server name scs.msg.yahoo.com
server name scsa.msg.yahoo.com
server name scsb.msg.yahoo.com
server name scsc.msg.yahoo.com
server name scsd.msg.yahoo.com
server name cs16.msg.dcn.yahoo.com
server name cs19.msg.dcn.yahoo.com
server name cs42.msg.dcn.yahoo.com
server name cs53.msg.dcn.yahoo.com
server name cs54.msg.dcn.yahoo.com
server name adsl.vip.scd.yahoo.com
server name radiol.launch.vip.dal.yahoo.com
server name in1.msg.vip.re2.yahoo.com
server name edit.messenger.yahoo.com
server name messenger.yahoo.com
server name http.pager.yahoo.com
server name privacy.yahoo.com
server name csa.yahoo.com
server name csb.yahoo.com
server name csc.yahoo.com

parameter-map type regex ccp-regex-nonascii
pattern [\x00-\x80]
!
!
crypto pki trustpoint TP-self-signed-1742995674
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-1742995674
revocation-check none
rsakeypair TP-self-signed-1742995674
!
!
crypto pki certificate chain TP-self-signed-1742995674
certificate self-signed 02
30820242 308201AB A0030201 02020102 300D0609 2A864886 F70D0101 04050003
3132F30 2D060355 04031326 494F532D 53656C66 2D5369676E65642D 43657274
69666963 6174652D 31373432 39393536 3734301E 170D3130 31313236 310332
32315A17 0D323030 31303130 300D0609 2A864886 F70D0101 01050003 81890281
8100A4A 980D15F0 6A6B5F18 5A3359DE 5D552EFE FAA8079B DA927DA2 4AF210F0
408131CE BB5B0189 FD82E22D 6A684AE3 5F4DB2A7 7517772B 1BC5624E A1A6382E
6A07EE71 E93A98C9 B8494A55 0CD6B4C 442065AA DBC9D9CC 14D10B65 2FEFEC8
AA9B3064 59105FBF B9B30219 2FD53ECA 06720CA1 A6D30DA5 564F0CE4 E53FC7FD
835B0203 010001A3 6A306830 0F060355 1D30101F FF040530 030101FF 30150030
551D1104 0E300C82 0A5A4246 2D526F75 74657230 1F060355 1D230418 30150030
0BDBE585 15377DCA 5F00A1A2 6644EC22 36DE590 301D0603 551D0E04 1604140B
DBE58515 377DC5A5 00A12A66 44EC2236 6DE59030 0D06092A 864896F7 0D010104
50000381 810037F4 8E8C7A5F 85429563 F78F2F41 A060E2EB F23DFB3E 09193E11
A143FC44 8CCE71C3 A5E9D9F7 C2A8CD38 C272A375 4FC4D59B E02A9427 56E2F1A0
DA190B50 FA091669 CD8C066E CDA10955 4E01350D 77B3E567 DFD55A71 5220F8F6
F006D31E 02CB739E 19D633D6 61E49B66 C31AD865 DC7F4380 FFEDDBAB 89E3B3E9
6139E472 DC62
quit
!
!
username cisco privilege 15 password 0 cisco123
archive
log config
hidekeys
!
class-map type inspect match-all sdm-cls-im
  match protocol ymsgr
class-map type inspect imap match-any ccp-app-imap
  match invalid-command
class-map type inspect match-any ccp-cls-protocol-p2p
  match protocol gnutella signature
  match protocol kazaa2 signature
  match protocol fasttrack signature
  match protocol bitTorrent signature
class-map type inspect smtp match-any ccp-app-smtp
  match data-length gt 5000000
class-map type inspect http match-any ccp-app-nonascii
  match req-resp header regex ccp-regex-nonascii
class-map type inspect match-any CCP-Voice-permit
  match protocol h323
  match protocol skinny
  match protocol sip
class-map type inspect gnutella match-any ccp-class-gnutella
  match file-transfer .exe
class-map type inspect match-any ccp-cls-insp-traffic
  match protocol dns
  match protocol https
  match protocol icmp
  match protocol imap
  match protocol pop3
  match protocol tcp
  match protocol udp
class-map type inspect match-all ccp-insp-traffic
  match class-map ccp-cls-traffic
class-map type inspect match-any ccp-cls-icmp-access
  match protocol icmp
  match protocol tcp
  match protocol udp
!
!--- Output suppressed
!
class-map type inspect match-all sdm-cls-p2p
  match protocol gnutella
class-map type inspect match-all ccp-protocol-pop3
  match protocol pop3
class-map type inspect kazaa2 match-any ccp-cls-p2p
  match file-transfer
class-map type inspect pop3 match-any ccp-app-pop3
  match invalid-command
class-map type inspect match-all ccp-protocol-p2p
  match class-map ccp-cls-protocol-p2p
class-map type inspect match-all ccp-protocol-im
  match class-map ccp-cls-protocol-im
class-map type inspect match-all ccp-invalid-src
  match access-group 100
class-map type inspect match-all ccp-icmp-access
  match class-map ccp-cls-icmp-access
class-map type inspect http match-any ccp-app-httpmethods
  match request method bcopy
  match request method bdelete
  match request method bmove
  match request method bpropfind
  match request method bproppatch
  match request method connect
  match request method copy
  match request method delete
  match request method edit
  match request method getattribute
match request method getattributenames
match request method getproperties
match request method index
match request method lock
match request method mkcol
match request method mkdir
match request method move
match request method notify
match request method options
match request method poll
match request method post
match request method propfind
match request method proppatch
match request method put
match request method revadd
match request method revlabel
match request method revlog
match request method revnum
match request method save
match request method search
match request method setattribute
match request method startrev
match request method stoprev
match request method subscribe
match request method unedit
match request method unlock
match request method unsubscribe

class-map type inspect http match-any ccp-http-blockparam
match request port-misuse im
match request port-misuse p2p
match request port-misuse tunneling
match req-resp protocol-violation

class-map type inspect match-all ccp-protocol-imap
match protocol imap

class-map type inspect match-all ccp-protocol-smtp
match protocol smtp

class-map type inspect match-all ccp-protocol-http
match protocol http
!

policy-map type inspect ccp-permit-icmpreply
class type inspect ccp-icmp-access
  inspect
  class class-default
  pass
!
!--- Output suppressed

!

policy-map type inspect http ccp-action-app-http
class type inspect http ccp-http-blockparam
  log
  reset
class type inspect http ccp-app-httpmethods
  log
  reset
class type inspect http ccp-app-nonascii
  log
  reset
class class-default

policy-map type inspect smtp ccp-action-smtp
class type inspect smtp ccp-app-smtp
  reset
  class class-default

policy-map type inspect imap ccp-action-imap
class type inspect imap ccp-app-imap
  log
  reset
class class-default
policy-map type inspect pop3 ccp-action-pop3
class type inspect pop3 ccp-app-pop3
  log
  reset
class class-default
policy-map type inspect ccp-inspect
class type inspect ccp-invalid-src
  drop log
class type inspect ccp-protocol-http
  inspect
  service-policy http ccp-action-app-http
class type inspect ccp-protocol-smtp
  inspect
  service-policy smtp ccp-action-smtp
class type inspect ccp-protocol-imap
  inspect
  service-policy imap ccp-action-imap
class type inspect ccp-protocol-pop3
  inspect
  service-policy pop3 ccp-action-pop3
class type inspect sdm-cls-p2p
  inspect
!
!--- Output suppressed
!
class type inspect ccp-protocol-im
  drop log
class type inspect ccp-insp-traffic
  inspect
class type inspect CCP-Voice-permit
  inspect
class class-default
  pass
policy-map type inspect ccp-permit
  class class-default
policy-map type inspect p2p ccp-pmap-gnutella
  class type inspect gnutella ccp-class-gnutella
!
zone security out-zone
zone security in-zone
zone-pair security ccp-zp-self-out source self destination out-zone
  service-policy type inspect ccp-permit-icmprep
zone-pair security ccp-zp-in-out source in-zone destination out-zone
  service-policy type inspect ccp-inspect
zone-pair security ccp-zp-out-self source out-zone destination self
  service-policy type inspect ccp-permit
!
!
interface FastEthernet0/0
  description $FW_OUTSIDE$
  ip address 209.165.201.2 255.255.255.224
  zone-member security out-zone
duplex auto
  speed auto
!
interface FastEthernet0/1
  description $FW_INSIDE$
  ip address 10.77.241.114 255.255.255.192
  zone-member security in-zone
duplex auto
speed auto
!

!--- Output suppressed
!

ip http server
ip http authentication local
ip http secure-server
!

!--- Output suppressed
!

!
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
  privilege level 15
  login local
  transport input ssh
!
scheduler allocate 20000 1000
!
webvpn cef
end

ZBF-Router#

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain show commands. Use the OIT to view an analysis of show command output.

- ZBF–Router#show policy–map type inspect zone–pair sessionsDisplays the runtime inspect type policy–map statistics for all existing zone pairs.

Related Information

- Zone–Based Policy Firewall Design and Application Guide
- Cisco IOS Firewall Classic and Zone–Based Virtual Firewall Application Configuration Example
- Cisco Configuration Professional Home Page
- Cisco Configuration Professional User Guide
- Technical Support & Documentation – Cisco Systems