Example 13-1 - Components That Make Up The ZBF

```
! The class map "classifies" or "identifies" the traffic
! In this example, this class map will match on either TELNET traffic or
! any type of ICMP traffic
R3(config)# class-map type inspect match-any MY-CLASS-MAP
R3(config-cmap)# match protocol telnet
R3(config-cmap)# match protocol icmp
R3(config-cmap)# exit

! The policy map calls on a specific class map that it wants to use
! to identify which traffic the policy applies to, and then specifies the
! policy action. In this example, it is to inspect the traffic
R3(config)# policy-map type inspect MY-POLICY-MAP
R3(config-pmap)# class type inspect MY-CLASS-MAP
R3(config-pmap-c)# inspect
R3(config-pmap-c)# exit
R3(config-pmap)# exit

! Create the security zones, they can be named whatever you want to
! name them. In this example, I named them inside and outside.
R3(config)# zone security inside
R3(config-sec-zone)# exit
R3(config)# zone security outside
R3(config-sec-zone)# exit

! Create the zone-pair, specifying the zones and the direction
R3(config-sec-zone)# zone-pair security in-to-out source inside destination
outside

! Apply the policy map you want to use for traffic that matches this zone-pair
R3(config-sec-zone-pair)# service-policy type inspect MY-POLICY-MAP
R3(config-sec-zone-pair)# exit

! Configure the interfaces, so they become members of the respective zones
R3(config)# interface GigabitEthernet3/0
R3(config-if)# description Belongs to outside zone
R3(config-if)# zone-member security outside
R3(config-if)# exit
R3(config)# interface GigabitEthernet1/0
R3(config-if)# description Belongs to inside zone
R3(config-if)# zone-member security inside
R3(config-if)# exit
R3(config)#
```

Example 13-2 - Literal CLI Commands That the CCP Basic Zone-Based Firewall Creates

```
access-list 100 remark CCP_ACL Category=128
access-list 100 permit ip host 255.255.255.255 any
access-list 100 permit ip 127.0.0.0 0.255.255.255 any
access-list 100 permit ip 34.0.0.0 0.0.0.255 any
ip domain lookup
ip name-server 8.8.8.8
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 ads1.vip.scd.yahoo.com
 server name radio1.launch.vip.dal.yahoo.com
 server name in1.msg.vip.re2.yahoo.com
 server name data1.my.vip.sc5.yahoo.com
 server name address1.pim.vip.mud.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
 exit
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
 exit
parameter-map type protocol-info msn-servers
 server name messenger.hotmail.com
 server name gateway.messenger.hotmail.com
 server name webmessenger.msn.com
 exit
class-map type inspect match-any ccp-cls-protocol-im
 match protocol ymsgr yahoo-servers
 match protocol msnmsgr msn-servers
 match protocol aol aol-servers
 exit
class-map type inspect edonkey match-any ccp-app-edonkeydownload
 match file-transfer
 exit
class-map type inspect match-any ccp-h323annexe-inspect
 match protocol h323-annexe
 exit
class-map type inspect http match-any ccp-http-blockparam
 match request port-misuse im
 match request port-misuse p2p
 match req-resp protocol-violation
 exit
class-map type inspect aol match-any ccp-app-aol-otherservices
 match service any
 exit
class-map type inspect match-all ccp-protocol-pop3
 match protocol pop3
 exit
class-map type inspect msnmsgr match-any ccp-app-msn
 match service text-chat
 exit
class-map type inspect match-any ccp-cls-icmp-access
 match protocol icmp
 match protocol tcp
 match protocol udp
 exit
class-map type inspect match-all ccp-icmp-access
 match class-map ccp-cls-icmp-access
 exit
class-map type inspect match-all ccp-protocol-imap
 match protocol imap
 exit
class-map type inspect match-any ccp-cls-insp-traffic
```

```
 match protocol cuseeme
 match protocol dns
 match protocol ftp
 match protocol https
 match protocol icmp
 match protocol imap
 match protocol pop3
 match protocol netshow
 match protocol shell
 match protocol realmedia
 match protocol rtsp
 match protocol smtp extended
 match protocol sql-net
 match protocol streamworks
 match protocol tftp
 match protocol vdolive
 match protocol tcp
 match protocol udp
 exit
class-map type inspect aol match-any ccp-app-aol
 match service text-chat
 exit
class-map type inspect edonkey match-any ccp-app-edonkey
 match file-transfer
 match text-chat
 match search-file-name
 exit
class-map type inspect kazaa2 match-any ccp-app-kazaa2
 match file-transfer
 exit
class-map type inspect fasttrack match-any ccp-app-fasttrack
 match file-transfer
 exit
class-map type inspect match-any ccp-h323-inspect
 match protocol h323
 exit
class-map type inspect match-any ccp-h323nxg-inspect
 match protocol h323-nxg
 exit
class-map type inspect match-all ccp-insp-traffic
 match class-map ccp-cls-insp-traffic
 exit
class-map type inspect edonkey match-any ccp-app-edonkeychat
 match search-file-name
 match text-chat
 exit
class-map type inspect match-any ccp-h225ras-inspect
 match protocol h225ras
 exit
class-map type inspect msnmsgr match-any ccp-app-msn-otherservices
 match service any
 exit
class-map type inspect ymsgr match-any ccp-app-yahoo-otherservices
 match service any
 exit
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 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 trace
 match request method unedit
 match request method unlock
 match request method unsubscribe
 exit
class-map type inspect match-any ccp-skinny-inspect
 match protocol skinny
 exit
class-map type inspect match-all ccp-protocol-im
 match class-map ccp-cls-protocol-im
 exit
class-map type inspect match-any ccp-cls-protocol-p2p
 match protocol edonkey signature
 match protocol gnutella signature
 match protocol kazaa2 signature
 match protocol fasttrack signature
 match protocol bittorrent signature
 exit
class-map type inspect http match-any ccp-http-allowparam
 match request port-misuse tunneling
 exit
class-map type inspect gnutella match-any ccp-app-gnutella
 match file-transfer
 exit
class-map type inspect match-any ccp-sip-inspect
 match protocol sip
 exit
class-map type inspect match-all ccp-invalid-src
 match access-group 100
 exit
class-map type inspect ymsgr match-any ccp-app-yahoo
 match service text-chat
 exit
class-map type inspect pop3 match-any ccp-app-pop3
 match invalid-command
 exit
class-map type inspect imap match-any ccp-app-imap
```

```
 match invalid-command
 exit
class-map type inspect match-all ccp-protocol-p2p
 match class-map ccp-cls-protocol-p2p
 exit
class-map type inspect match-all ccp-protocol-http
 match protocol http
 exit
policy-map type inspect http ccp-action-app-http
 class type inspect http ccp-http-blockparam
  log
  reset
  exit
 class type inspect http ccp-app-httpmethods
  log
  reset
  exit
 class type inspect http ccp-http-allowparam
  log
  allow
  exit
 exit
policy-map type inspect imap ccp-action-imap
 class type inspect imap ccp-app-imap
  log
  exit
 exit
policy-map type inspect pop3 ccp-action-pop3
 class type inspect pop3 ccp-app-pop3
  log
  exit
 exit
policy-map type inspect p2p ccp-action-app-p2p
 class type inspect edonkey ccp-app-edonkeychat
  log
  allow
  exit
 class type inspect edonkey ccp-app-edonkeydownload
  log
  allow
  exit
 class type inspect fasttrack ccp-app-fasttrack
  log
  allow
  exit
 class type inspect gnutella ccp-app-gnutella
  log
  allow
  exit
 class type inspect kazaa2 ccp-app-kazaa2
  log
  allow
  exit
 exit
policy-map type inspect im ccp-action-app-im
 class type inspect aol ccp-app-aol
  log
  allow
  exit
 class type inspect msnmsgr ccp-app-msn
  log
  allow
 exit
```

```
 class type inspect ymsgr ccp-app-yahoo
  log
  allow
  exit
 class type inspect aol ccp-app-aol-otherservices
  log
  reset
  exit
 class type inspect msnmsgr ccp-app-msn-otherservices
  log
  reset
  exit
 class type inspect ymsgr ccp-app-yahoo-otherservices
  log
  reset
  exit
 exit
policy-map type inspect ccp-inspect
 class type inspect ccp-invalid-src
  drop log
  exit
 class type inspect ccp-protocol-http
  no drop
  inspect
  service-policy http ccp-action-app-http
  exit
 class type inspect ccp-protocol-imap
  no drop
  inspect
  service-policy imap ccp-action-imap
  exit
 class type inspect ccp-protocol-pop3
  no drop
  inspect
  service-policy pop3 ccp-action-pop3
  exit
 class type inspect ccp-protocol-p2p
  no drop
  inspect
  service-policy p2p ccp-action-app-p2p
  exit
 class type inspect ccp-protocol-im
  no drop
  inspect
  service-policy im ccp-action-app-im
  exit
 class type inspect ccp-insp-traffic
  no drop
  inspect
  exit
 class type inspect ccp-sip-inspect
  no drop
  inspect
  exit
 class type inspect ccp-h323-inspect
  no drop
  inspect
  exit
 class type inspect ccp-h323annexe-inspect
  no drop
  inspect
  exit
 class type inspect ccp-h225ras-inspect
```

```
  no drop
  inspect
  exit
 class type inspect ccp-h323nxg-inspect
  no drop
  inspect
  exit
 class type inspect ccp-skinny-inspect
  no drop
  inspect
  exit
 exit
policy-map type inspect ccp-permit
 class class-default
 exit
policy-map type inspect ccp-permit-icmpreply
 class type inspect ccp-icmp-access
  no drop
  inspect
  exit
 class class-default
  no drop
  pass
 exit
exit
zone security in-zone
zone security out-zone
zone-pair security ccp-zp-out-self source out-zone destination self
 service-policy type inspect ccp-permit
 exit
zone-pair security ccp-zp-in-out source in-zone destination out-zone
 service-policy type inspect ccp-inspect
 exit
zone-pair security ccp-zp-self-out source self destination out-zone
 service-policy type inspect ccp-permit-icmpreply
 exit
interface GigabitEthernet3/0
 description $FW_OUTSIDE$
 zone-member security out-zone
 exit
interface GigabitEthernet1/0
 description $FW_INSIDE$
 zone-member security in-zone
 exit
```

Example 13-3 - Verifying the Configuration from the Command Line

```
R3# show class-map type inspect
Class Map type inspect match-any ccp-cls-protocol-p2p (id 27)
 Match protocol edonkey signature
 Match protocol gnutella signature
 Match protocol kazaa2 signature
 Match protocol fasttrack signature
 Match protocol bittorrent signature
Class Map type inspect match-any ccp-skinny-inspect (id 25)
 Match protocol skinny
Class Map type inspect match-all ccp-insp-traffic (id 19)
 Match class-map ccp-cls-insp-traffic
Class Map type inspect match-any ccp-h323nxg-inspect (id 18)
 Match protocol h323-nxg
Class Map type inspect match-any ccp-cls-icmp-access (id 8)
 Match protocol icmp
```

```
 Match protocol tcp
 Match protocol udp
Class Map type inspect match-any ccp-cls-protocol-im (id 1)
 Match protocol ymsgr yahoo-servers
 Match protocol msnmsgr msn-servers
 Match protocol aol aol-servers
Class Map type inspect match-all ccp-protocol-pop3 (id 6)
 Match protocol pop3
Class Map type inspect match-any ccp-h225ras-inspect (id 21)
 Match protocol h225ras
Class Map type inspect match-any ccp-h323annexe-inspect (id 3)
 Match protocol h323-annexe
Class Map type inspect match-any ccp-cls-insp-traffic (id 12)
 Match protocol cuseeme
 Match protocol dns
 Match protocol ftp
 Match protocol https
 Match protocol imap
 Match protocol pop3
 Match protocol netshow
 Match protocol shell
 Match protocol realmedia
 Match protocol rtsp
 Match protocol smtp extended
 Match protocol sql-net
 Match protocol streamworks
 Match protocol tftp
 Match protocol vdolive
 Match protocol tcp
 Match protocol udp
Class Map type inspect match-all ccp-protocol-p2p (id 35)
 Match class-map ccp-cls-protocol-p2p
Class Map type inspect match-any ccp-h323-inspect (id 17)
 Match protocol h323
Class Map type inspect match-all ccp-protocol-im (id 26)
 Match class-map ccp-cls-protocol-im
Class Map type inspect match-all ccp-icmp-access (id 9)
 Match class-map ccp-cls-icmp-access
Class Map type inspect match-all ccp-invalid-src (id 31)
 Match access-group 100
Class Map type inspect match-any ccp-sip-inspect (id 30)
 Match protocol sip
Class Map type inspect match-all ccp-protocol-imap (id 11)
 Match protocol imap
Class Map type inspect match-all ccp-protocol-http (id 36)
 Match protocol http
R3#
! In the example content below, we see the detailed information
! regarding a telnet session that is currently going through the firewall,
! as well as a PING that is being sent through the firewall.

R3# show policy-map type inspect zone-pair ccp-zp-in-out sessions
policy exists on zp ccp-zp-in-out
 Zone-pair: ccp-zp-in-out
 Service-policy inspect : ccp-inspect
<snip>
Inspect
 Class-map: ccp-insp-traffic (match-all)
  Match: class-map match-any ccp-cls-insp-traffic
  Match: protocol cuseeme
   0 packets, 0 bytes
   30 second rate 0 bps
  Match: protocol dns
```

```
   0 packets, 0 bytes
   30 second rate 0 bps
  Match: protocol ftp
   0 packets, 0 bytes
   30 second rate 0 bps
<-----snip>
  Match: protocol tcp
   0 packets, 0 bytes
   30 second rate 0 bps
  Match: protocol udp
   0 packets, 0 bytes
   30 second rate 0 bps
Inspect
  Number of Established Sessions = 2
  Established Sessions
   Session 673BBD00 (10.0.0.11:29333)=>(34.0.0.4:23) tacacs:tcp SIS_
OPEN
    Created 00:02:20, Last heard 00:00:37
    Bytes sent (initiator:responder) [39:273572]
   Session 673BC100 (10.0.0.22:8)=>(34.0.0.4:0) icmp SIS_OPEN
    Created 00:00:40, Last heard 00:00:00
    ECHO request
    Bytes sent (initiator:responder) [69912:69912]
<-----snip>
```

Example 14-4 Implementing Additional Firewall Interfaces

```
ASA-1(config)#  configure terminal
ASA-1(config)#  ! Configure the logical SVI, the Layer 3 interface)
ASA-1(config)#  interface Vlan1
ASA-1(config-if)#  no shutdown
ASA-1(config-if)#  description Connect to the dmz
ASA-1(config-if)#  nameif dmz
ASA-1(config-if)#  security-level 50
ASA-1(config-if)#  ip address 192.168.1.254 255.255.255.0
ASA-1(config-if)#  exit
! Repeat this process for the other interfaces
ASA-1(config)#  interface Vlan2
ASA-1(config-if)#  no shutdown
ASA-1(config-if)#  description Connects to my private network
ASA-1(config-if)#  nameif inside
ASA-1(config-if)#  security-level 100
ASA-1(config-if)#  ip address 10.0.0.1 255.255.255.0
ASA-1(config-if)#  exit
ASA-1(config)#  interface Vlan4
ASA-1(config-if)#  no shutdown
ASA-1(config-if)#  description Connects to the Internet
ASA-1(config-if)#  no forward interface Vlan2
ASA-1(config-if)#  nameif outside
ASA-1(config-if)#  security-level 0
ASA-1(config-if)#  ip address 23.1.2.3 255.255.255.240
ASA-1(config-if)#  exit
ASA-1(config)#  ! Assign access ports of built-in switch to VLANs that you
! want them to belong to, repeat for all switch ports you intend to use.
ASA-1(config)# interface Ethernet0/1
ASA-1(config-if)#  switchport access vlan 4
ASA-1(config-if)#  exit
ASA-1(config)#
ASA-1(config)#  interface range Ethernet0/2-7
ASA-1(config-if)#  switchport access vlan 2
ASA-1(config-if)#  exit
! To verify your work:
```

```
ASA-1(config)#  show run interface
! Note the E0/0 is assigned to VLAN 1 (the dmz interface) and because the
! default is for a port to be assigned to VLAN 1, there is no specific
! configuration that shows up in the interface belonging to VLAN 1
```

Example 14-5 Configuring the ASA as a DHCP Server for Inside Clients

```
! specifies pool range, enables feature and specifies interface
ASA-1(config)# dhcpd address 10.0.0.101-10.0.0.132 inside
ASA-1(config)# dhcpd enable inside
ASA-1(config)# dhcpd dns 8.8.8.8 interface inside
ASA-1(config)# dhcpd domain iins.com interface inside
! tell the ASA that default route will use next hop of 23.1.2.7
! which is located off of the outside interface (on that same subnet)
ASA-1(config)# route outside 0.0.0.0 0.0.0.0 23.1.2.7
```

Example 14-7 CLI Equivalent for Implementing Dynamic PAT

```
! creates a network object that refers to the 10.0.0.0/24 network
ASA-1(config)# object network Inside_Hosts
ASA-1(config-network-object)# subnet 10.0.0.0 255.255.255.0
ASA-1(config-network-object)# description Inside_Hosts
ASA-1(config-network-object)# exit
! creates a NAT rule that says any traffic sourced from devices
! from the Inside_Hosts object group (network the 10.0.0.0/24 network),
! and coming in on the inside interface, as well as exiting (being routed
! through) the outside interface (based on the routing table of the ASA),
! it would then translate the source address of these packets, and
! substitute the source address of the outside interface of the ASA.
! Additionally it would track this in a NAT/PAT table, that is separate
! from the stateful database, and the ASA would manage both of these
! tables.
ASA-1(config)# nat (inside,outside) 1 source dynamic Inside_Hosts interface
! With the NAT on version 8.3 and newer, there are multiple options of
! configuring the NAT, including a NAT command done within object group
! configuration mode. These additional options, including advanced ASA NAT
! configuration are covered in the CCNP Security curriculum.
```

Example 14-8 Creating and Applying an ACL at the CLI

```
ASA-1(config)# access-list inside_access_in deny tcp any any eq telnet
ASA-1(config)# access-list inside_access_in permit ip any any
ASA-1(config)# access-group inside_access_in in interface inside
! Note: the optional elements of line number, and extended are optional.
! ASA assumes the ACL is an extended (if keyword "standard" isn't used)
! In absence of a "line" command, ASA adds new entries to the end
! To apply the ACL, the ASA uses a global access-group command, which is
! different than on an IOS router, where applying an ACL is done in
! interface configuration mode.
```

Example 14-9 Using the ASA Packet Tracer Utility at the CLI

```
! Checks to see if a packet, inbound on the inside interface,
! that is coming from host 10.0.0.101 and going to 22.33.44.55, and is
! TCP based and from port 1065 going to 80, and tell us if it would make
! it through the firewall
ASA-1# packet-tracer input inside tcp 10.0.0.101 1065 22.33.44.55 80
! Here are the results of each of the tests it internally checks (based on
! the current, configured and default rules in place)
Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
```

```
in 0.0.0.0 0.0.0.0 outside

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group inside_access_in in interface inside
access-list inside_access_in extended permit ip any any
Additional Information:

Phase: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,outside) source dynamic Inside_Hosts interface
Additional Information:
Dynamic translate 10.0.0.101/1065 to 23.1.2.3/5069

Phase: 5
Type: HOST-LIMIT
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1427, packet dispatched to next module

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

Example 14-9 Using the Packet Tracer Utility at the CLI

```
! Checks to see if a packet, inbound on the inside interface,
! that is coming from host 10.0.0.101 and going to 22.33.44.55, and is
! TCP based and from port 1065 going to 80, and tell us if it would make
! it through the firewall
ASA-1#
packet-tracer input inside tcp 10.0.0.101 1065 22.33.44.55
80
! Here are the results of each of the tests it internally checks (based on
! the current, configured and default rules in place)
Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in 0.0.0.0 0.0.0.0 outside
Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group inside_access_in in interface inside
access-list inside_access_in extended permit ip any any
Additional Information:
Phase: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 4
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,outside) source dynamic Inside_Hosts interface
Additional Information:
Dynamic translate 10.0.0.101/1065 to 23.1.2.3/5069
Phase: 5
Type: HOST-LIMIT
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 7
Type: FLOW-CREATION
```

```
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1427, packet dispatched to next module
Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```