Troubleshooting Firewalls

Session SEC-340

Agenda

• Advanced Concepts of PIX Packet Processing
• Common Troubleshooting Techniques
• Understanding and Troubleshooting PIX Failover
• Cisco IOS Firewall
Agenda

- Advanced Concepts of PIX Packet Processing
- Common Troubleshooting Techniques
- Understanding and Troubleshooting PIX Failover
- Cisco IOS Firewall

PIX Packet Flow

- Initial process
- Security level process
  - Inbound process
  - or
  - Outbound process
**Initial Process**

- **Incoming packet**
- Parse packet for errors (source/destination ip/port and protocol)
- If errors exist ➔ Drop packet
- Otherwise, perform xlate lookup

**Xlate Lookup**

- Output from the ‘show xlate’ command

```
pix515c# show xlate
PAT Global 172.16.171.234(1028) Local 172.16.171.1(37378)
PAT Global 172.16.171.234(1026) Local 10.19.226.250(1207)
Global 209.165.201.30 Local 209.165.201.30 static nconns 4 econns 0
pix515c#
```
Understanding the Xlate Table

- Xlate means “translation slot”
- Translation slots may still be active even after changes in the following commands:
  - aaa-server, access-list, alias, conduit, global, nat, route, or static
- Always use “clear xlate” to reset translation slots
- Adjust timeout value from 3 hour default to as low as 1 minute

Security Level Processing

```plaintext
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security10
```
Understanding Security Levels

- Level 0 and 100 are reserved the 'outside' and 'inside', respectively
- Security level does not indicate the level of the security algorithm for the interface, only the trust level in relation to the other perimeters

Lower to Higher Security Level

Access from lower to higher security level requires a static translation and an access-list/conduit

- No translation for destination host will produce an ICMP unreachable syslog message:

```
3020125: ICMP unreachable (code 3)
171.68.9.137 > 172.16.171.54
```

- Translation but no access will produce a deny statement like the following:

```
106001: Inbound TCP connection denied from 172.16.171.235/11004
to 172.16.171.1/23 flags SYN on interface outside
```
Higher to Lower Security Level

Access from higher to lower security level requires a translation (nat/global or static translation)

- Source packet not part of a nat/global or static translation

```
305005: No translation group found for tcp src inside:172.16.171.3/21012 dst outside:172.16.171.235/23
```

Inbound or Outbound?

Communication between two interfaces with the same security level is not allowed

```
```
Inbound Packet Processing

- Inbound packets are assigned the following variables:
  - faddr = ip source
  - laddr = ip dest/alias
- faddr = 192.168.1.135
- laddr = 172.16.1.82

Outbound Packet Processing

- Outbound packets are assigned the following variables:
  - laddr = ip source
  - faddr = ip dest/alias
- laddr = 172.16.1.67
- faddr = 192.168.1.135
TCP Fixup Protocol Success

- Adjust sequence numbers
- Update connection statistics
- Check for FIN bit
- TCP fixup success!

Agenda

- Advanced Concepts of PIX Packet Processing
- Common Troubleshooting Techniques
- Understanding and Troubleshooting PIX Failover
- Cisco IOS Firewall
Valid NAT or Static Statement

- global (outside) 1 192.168.1.50-192.168.1.250
- nat (inside) 1 172.16.0.0 255.255.0.0
- static (inside,outside) 192.168.1.40

Verify Route Statements

- route outside 0.0.0.0 0.0.0.0 192.168.1.2
- route inside 172.20.0.0 255.255.0.0 172.16.1.5
Show Route

- Output from ‘show route’ command

```simple
pix515c# show route
inside 10.0.0.0 255.0.0.0 172.16.171.1 1 OTHER static
inside 171.68.9.0 255.255.255.0 172.16.171.1 1 OTHER static
inside 172.16.171.0 255.255.255.192 172.16.171.54 1 CONNECT static
outside 172.16.171.232 255.255.255.248 172.16.171.233 1 CONNECT static
pix515c#
```

Access List Applied to Interface

- Output of the ‘show access-list’ command

```simple
pix515c# sh access-list
access-list in_acl permit tcp host 172.16.171.1 any eq www (hitcnt=0)
pix515c# sh access-group
access-group in_acl in interface inside
106023: Deny tcp src inside:172.16.171.1/38402 dst outside:172.16.171.235/23 by access-group "in_acl"
pix515c#sh access-list
access-list in_acl permit tcp host 172.16.171.1 any eq www (hitcnt=0)
access-list in_acl permit tcp host 172.16.171.1 any eq telnet (hitcnt=0)
302003: Built outbound TCP connection 8 for faddr 172.16.171.235/23
gaddr 172.16.171.1/38914 laddr 172.16.171.1/38914
pix515c#sh access-list
access-list in_acl permit tcp host 172.16.171.1 any eq www (hitcnt=0)
access-list in_acl permit tcp host 172.16.171.1 any eq telnet (hitcnt=1)
```
Verify Timeout Values

• Check timeout for site usage
  
  timeout xlate 3:00:00
  timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
  rpc 0:10:00 h323 0:05:00 sip 0:30:00 sip_media 0:02:00
  timeout uauth 0:05:00 absolute

• Recommended timeout values for average usage
  
  timeout xlate 00:30:00
  timeout conn 00:15:00 half-closed 0:10:00 udp 0:02:00
  rpc 0:10:00 h323 0:05:00 sip 0:30:00 sip_media 0:02:00
  timeout uauth 0:05:00 absolute

Possible Events for Log Messages

• AAA events
• Connection events
• Failover events
• FTP/URL events
• Mail guard/SNMP events
• PIX firewall management events
• Routing errors
## Log Message Severity Levels

<table>
<thead>
<tr>
<th>Level Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>alert</td>
</tr>
<tr>
<td></td>
<td>Immediate action required</td>
</tr>
<tr>
<td>2</td>
<td>critical</td>
</tr>
<tr>
<td></td>
<td>Critical condition</td>
</tr>
<tr>
<td>3</td>
<td>error</td>
</tr>
<tr>
<td></td>
<td>Error condition</td>
</tr>
<tr>
<td>4</td>
<td>warning</td>
</tr>
<tr>
<td></td>
<td>Warning condition</td>
</tr>
<tr>
<td>5</td>
<td>notification</td>
</tr>
<tr>
<td></td>
<td>Normal but significant condition</td>
</tr>
<tr>
<td>6</td>
<td>informational</td>
</tr>
<tr>
<td></td>
<td>Informational message only</td>
</tr>
<tr>
<td>7</td>
<td>debugging</td>
</tr>
<tr>
<td></td>
<td>Appears during debugging only</td>
</tr>
</tbody>
</table>

**Log Message Severity Levels**

<table>
<thead>
<tr>
<th>Log Message Severity Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>pix515c# show logging</td>
</tr>
<tr>
<td>Syslog logging: enabled</td>
</tr>
<tr>
<td>Timestamp logging: disabled</td>
</tr>
<tr>
<td>Standby logging: disabled</td>
</tr>
<tr>
<td>Console logging: level debugging, 404 messages logged</td>
</tr>
<tr>
<td>Monitor logging: disabled</td>
</tr>
<tr>
<td>Buffer logging: level debugging, 5 messages logged</td>
</tr>
<tr>
<td>Trap logging: level debugging, facility 20, 404 messages logged</td>
</tr>
<tr>
<td>Logging to inside 171.68.9.137</td>
</tr>
<tr>
<td>History logging: disabled</td>
</tr>
<tr>
<td>302002: Teardown TCP connection 1 faddr 172.16.171.235/23 gaddr 172.16.171.234/1025 laddr 172.16.171.3/22548 duration 0:00:23 bytes 274 (TCP FINs)</td>
</tr>
<tr>
<td>302010: 0 in use, 1 most used</td>
</tr>
<tr>
<td>305004: Teardown portmap translation for global 172.16.171.234/1024 local 172.16.171.3/22036</td>
</tr>
<tr>
<td>305001: Portmapped translation built for gaddr 172.16.171.234/1026 laddr 172.16.171.3/23060</td>
</tr>
<tr>
<td>305001: Built outbound TCP connection 2 for laxaddr 172.16.171.235/23 gaddr 172.16.171.234/1026 laddr 172.16.171.3/23060</td>
</tr>
</tbody>
</table>

**Display Current Logging Level**

pix515c# show logging
Syslog logging: enabled
  Timestamp logging: disabled
  Standby logging: disabled
  Console logging: level debugging, 404 messages logged
  Monitor logging: disabled
  Buffer logging: level debugging, 5 messages logged
  Trap logging: level debugging, facility 20, 404 messages logged
  Logging to inside 171.68.9.137
  History logging: disabled
302002: Teardown TCP connection 1 faddr 172.16.171.235/23 gaddr 172.16.171.234/1025 laddr 172.16.171.3/22548 duration 0:00:23 bytes 274 (TCP FINs)
302010: 0 in use, 1 most used
305004: Teardown portmap translation for global 172.16.171.234/1024 local 172.16.171.3/22036
305001: Portmapped translation built for gaddr 172.16.171.234/1026 laddr 172.16.171.3/23060
305001: Built outbound TCP connection 2 for laxaddr 172.16.171.235/23 gaddr 172.16.171.234/1026 laddr 172.16.171.3/23060
ICMP Types Values

- What are the most common icmp types?

<table>
<thead>
<tr>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>echo</td>
<td>8</td>
</tr>
<tr>
<td>echo-reply</td>
<td>0</td>
</tr>
<tr>
<td>time-exceeded</td>
<td>11</td>
</tr>
<tr>
<td>unreachable</td>
<td>3</td>
</tr>
<tr>
<td>redirect</td>
<td>5</td>
</tr>
</tbody>
</table>

ICMP Can Be Your Friend

- Syslog messages with ‘debug icmp trace’ enabled

```
05002: Translation built for gaddr 192.168.1.50 to laddr 172.16.1.5
20: Outbound ICMP echo request (len 72 id 43039 seq 9753)
   172.16.1.5 > 192.168.1.50 > 192.168.1.2
21: Inbound ICMP echo reply (len 72 id 43295 seq 9753)
   172.16.1.5 > 192.168.1.50 > 192.168.1.2
```
Enable Packet Debugs

- Packet debugs are very CPU intensive
- Packet debug can be enabled for the following parameters:
  - source IP address, destination IP address, source port, destination port, protocol, and direction (rx/tx)

Packet Debug Data Format

- Packet debugs display data in hexadecimal format

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Decimal Value</th>
<th>Hexadecimal Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>http</td>
<td>80</td>
<td>50</td>
</tr>
<tr>
<td>ssl</td>
<td>443</td>
<td>1BB</td>
</tr>
<tr>
<td>smtp</td>
<td>25</td>
<td>19</td>
</tr>
<tr>
<td>telnet</td>
<td>23</td>
<td>17</td>
</tr>
<tr>
<td>ftp</td>
<td>21</td>
<td>15</td>
</tr>
<tr>
<td>ftp-data</td>
<td>20</td>
<td>14</td>
</tr>
</tbody>
</table>
Debug Packet Output

The output of the debug packet command resembles a packet analyzer in that you are able to see the protocol headers for both layer 3 and layer 4, as well as the data they contain in hex format.

Ex.
Dest port = 0x19syn
Under the TCP header

-------- PACKET --------
-- IP --
172.16.1.5      ==>     192.168.1.2
ver = 0x4       hlen = 0x5      tos = 0xc0
tlen = 0x2c
id = 0x0        flags = 0x0     frag off=0x0
ttl = 0xff      proto=0x6       chksum = 0x4c4c
-- TCP --
source port = 0x2af9    dest port = 0x19syn
seq = 0x471c8bbb
ack = 0x0
hlen = 0x6              window = 0x1020
chksum = 0x1ef9       urg = 0x0
tcp options:    0x2     0x4     0x2     0x18
-- DATA --
0000002c: 00 00 cc
| ... 00000002c: 00 00 cc
-------- END OF PACKET --------

Passing Traffic Outbound

- Verify default gateway and proper routing
- Packet must be part of a translation statement
  Static translations take precedence over a nat/global translation
  Perform “clear xlate” if changes have been made to translation methods
Passing Traffic Outbound (Cont.)

Translations built for outbound connections

Translation creation failure produces syslog message

305002: Translation built for gaddr 172.16.171.236 to laddr 172.16.171.1
305002: Translation built for gaddr 172.16.171.237 to laddr 172.16.171.3
305006: regular translation creation failed for tcp src inside:172.16.171.102 dst outside:172.16.171.235

Passing Traffic Outbound (Cont.)

Output of ‘show xlate’ and ‘show global’ shows no available global addresses for new translations

pix515c# show xlate
Global 172.16.171.236 Local 172.16.171.1
Global 172.16.171.237 Local 172.16.171.3
pix515c# show global
  global (outside) 1 172.16.171.236-172.16.171.237
  netmask 255.255.255.248
Passing Traffic Outbound (Cont.)

• Add a Port Address Translation (PAT) address to the global for the outside

```
pix515c# global (outside) 1 172.16.171.238
Global 172.16.171.238 will be Port Address Translated
305001: Portmapped translation built for gaddr
172.16.171.238/1024 laddr 171.68.9.110/1074
302001: Built outbound TCP connection 14 for faddr
172.16.171.235/80 gaddr 172.16.171.238/1024 laddr
171.68.9.110/1074
304001: 171.68.9.110 Accessed URL 172.16.171.235:
```

Inbound SMTP

```
static (dmz,outside) 192.168.1.42 172.17.1.82
access-list out_acl permit tcp any host 192.168.1.42 eq smtp
access-group out_acl in interface outside
```
Inbound SMTP (Cont.)

Telnet to tcp port 25 on the mail server from the internet

The server should respond with a 220 message

Send a HELO command

The server should respond with a 250 OK

Inbound SMTP (Cont.)

• If you are still unable to pass smtp mail inbound, temporarily disable fixup for smtp:
  
  no fixup protocol smtp 25
Understanding Fixup for SMTP

- Only allows the following commands per RFC 821:
  
  HELO, MAIL, RCPT, DATA, RSET, NOOP, and QUIT

- Unknown commands in the SMTP banner are replaced with asterisks

- Mail and rcpt commands are inspected
  
  Bad characters are removed

Agenda

- Advanced Concepts of PIX Packet Processing
- Common Troubleshooting Techniques
- Understanding and Troubleshooting PIX Failover
- Cisco IOS Firewall
Detecting a Failed State

- Primary and secondary perform the following interface tests:
  - Network interface status test
  - Network activity test
  - Address Resolution Protocol (ARP) test
  - Ping test

Monitor Failover Status

- Output of ‘show failover’ command

```
Failover On
Cable status: Normal
Reconnect timeout 0:00:00

This host: Primary - Standby (Failed)
  Active time: 7140 (sec)
  Interface 0 (192.168.1.1): Normal (Waiting)
  Interface 1 (172.16.171.54): Failed (Waiting)

Other host: Secondary - Active
  Active time: 30 (sec)
  Interface 0 (192.168.1.3): Normal (Waiting)
  Interface 1 (172.16.171.55): Normal (Waiting)
```
Failover Debug Options

- ‘Debug fover’ options

debug fover <sub option>

- tx  Failover cable xmit
- rx  Failover cable receive
- open Failover device open
- cable Failover cable status
- txdmp Cable xmit message dump (serial console only)
- rxdmp Cable recv message dump (serial console only)
- ifc Network interface status trace
- rxip IP network failover packet recv
- txip IP network failover packet xmit
- get IP network packet received
- put IP network packet xmit
- verify Failover message verify
- switch Failover Switching status
- fail Failover internal exception
- fmsg Failover message

Verify Failover Communication

- Output of ‘debug fover cable’ command

32: fover_thread: cstatus = 0xb, normal
33: fover_thread: cstatus = 0xb, normal
34: fover_thread: cstatus = 0xb, normal
35: fover_thread: cstatus = 0xb, normal

- Output of ‘debug fover rxip’ command

116: fover_ip0: fover_ip(): ifc 0 172.16.171.226 -> 172.16.171.225
117: fover_ip0: fover_ip(): ifc 0 got FHELLO
118: fover_ip1: fover_ip(): ifc 1 172.16.171.35 -> 172.16.171.53
119: fover_ip1: fover_ip(): ifc 1 got FHELLO
Syslog Messages for Failed Interface

- Syslog messages from primary with failed interface 2

0005: (Primary) Lost Failover communications with mate on interface 2
105008: (Primary) Testing Interface 2
103004: (Primary) Other firewall reports this firewall failed.
104002: (Primary) Switching to STNDBY - switch to failed state
105009: (Primary) Testing on interface 2 Failed
105003: (Primary) Monitoring on interface 0 waiting
105003: (Primary) Monitoring on interface 1 waiting
104004: (Primary) Switching to groove.
105003: (Primary) Monitoring on interface 0 waiting
104003: (Primary) Switching to FAILED.
105003: (Primary) Monitoring on interface 0 waiting
105004: (Primary) Monitoring on interface 1 normal
105004: (Primary) Monitoring on interface 2 normal

Debug Output for Interface Testing

This output signifies that we have the interface and line protocol up, but failed to increase the counters for the traffic test

This next output shows that pix increased the traffic counters, however, it could not arp for the secondary address

10360: fover_thread: ifc_test(2) - LINKTEST
361: fover_thread: ifc_test(2) - TRAFFICTEST
362: fover_thread: ifc_test(2) - ENDTST
363: fover_thread: ifc_test(2) completed: test state 0, ifc status 1
364: fover_parse: parse_thread_helper() - mate ifc 2
link status change form 1 to 0

102423: fover_thread: ifc_test(2) - LINKTEST
2424: fover_thread: ifc_test(2) - TRAFFICTEST
2425: fover_thread: ifc_test(2) - ARPTEST
2426: fover_thread: ifc_test(2) - 192.168.1.2
2427: fover_thread: ifc_test(2) - WRCHNT
2428: fover_thread: ifc_test(2) 9 8 8
2429: fover_parse: parse_thread_helper() - mate ifc 2
link status change form 1 to 0
2430: fover_thread: ifc_test(2) - G0RESULT
Stateful Failover Statistics

- Output from ‘sh failover’ on the secondary PIX

```
Stateful Failover Logical Update Statistics
Link : intf2
Stateful Obj   xmit  xerr  rcv  rerr
General       975    0    143   0
sys cmd       962    0    130   0
up time       0    0    2    0
xlate         4    0    11    0
tcp conn      9    0    0    0
udp conn      0    0    0    0
ARP tbl       0    0    0    0
RIP tbl       0    0    0    0

Logical Update Queue Information
   Queue Information
      Cur  Max  Total
Recv Q:  0    1   143
Xmit Q:  0    2   975
```

Best Practices for Failover Communication

- Hardcode transmission speed and duplex settings on PIX and switch ports
  PIX:
  ‘interface ethernet0 100full’
  Cat6K:
  ‘set port speed 3/25 100’
  ‘set port duplex 3/25 full’

- Disable Spanning Tree for switch VLAN connected to PIX
  Cat6K:
  ‘set spantree disable 50’
Agenda

- Advanced Concepts of PIX Packet Processing
- Common Troubleshooting Techniques
- Understanding and Troubleshooting PIX Failover
- Cisco IOS Firewall

The Most Common Configuration Error Is the Direction of Inspection!

Protected Network

Unprotected Network

e0

e1

Inspect Inbound on e0 ➔ and ➔ Access List Inbound on e1

or

Inspect outbound on e1 ➔ and ➔ Access List Inbound on e1
CBAC Process

- CBAC will create openings for return traffic

```
ip inspect name firewall tcp
ip inspect name firewall udp
interface s0
ip access-group 150 in
ip inspect firewall out
access-list 150 deny any any
```

Object Creation and Deletion

- Output of ‘debug ip inspect object-creation’ and ‘debug ip inspect object-deletion’

```
CBAC Pak 80DFC034 sis 80D8F678 initiator_addr (171.68.9.156:1054) responder_addr (172.16.171.225:23) initiator_alt_addr (171.68.9.156:1054) responder_alt_addr (172.16.171.225:23) CBAC OBJ_CREATE: create sis 80D8F678 CBAC OBJ_CREATE: create acl wrapper 80CDF00C -- acl item 80CDEB34 CBAC Src 172.16.171.225 Port [23:23] CBAC Dst 171.68.9.156 Port [1054:1054] CBAC OBJ_CREATE: create host entry 80CDC6A0 addr 172.16.171.225 bucket 246 CBAC OBJ_DELETE: delete host entry 80CDC6A0 addr 172.16.171.225
```
Half Open Connections

- TCP sessions get created with the SYN packet and are not established until the handshake is complete

TCP Session Debugging

- Output of ‘debug ip inspect tcp’

CBAC OBJ_CREATE: create sis 80DF678
CBAC sis 80DF678 pak 80DFC034 TCP S seq 609986712(0) (171.68.9.156:1100) => (172.16.171.229:23)
CBAC OBJ_CREATE: create acl wrapper 80CDEE1C -- acl item 80CDE7E4
CBAC Src 172.16.171.229 Port [23:23]
CBAC Dst 171.68.9.156 Port [1100:1100]
CBAC OBJ_CREATE: create host entry 80CDC7C4 addr 172.16.171.229 bucket 242
CBAC* sis 80DF678 pak 80D52DC8 TCP S seq 609986712(0) (171.68.9.156:1100) => (172.16.171.229:23)

CBAC OBJ_CREATE: create sis 80D8F678
CBAC sis 80D8F678 pak 80DFC034 TCP S seq 3071996006(0) (171.68.9.156:1059) => (172.16.171.225:23)
CBAC* sis 80D8F678 pak 80D8CF20 TCP S ack 3071996007 seq 967618911(0) (171.68.9.156:1059) => (172.16.171.225:23)
CBAC* sis 80D8F678 pak 80D52DC8 TCP S seq 3071996007(0) (171.68.9.156:1059) => (172.16.171.225:23)

CBAC* sis 80D8F678 pak 80DFC034 TCP F P ack 3071996052 seq 967618984(0) (171.68.9.156:1059) => (172.16.171.225:23)
CBAC sis 80D8F678 pak 80DFC034 TCP F P ack 3071996052 seq 967618984(0) (171.68.9.156:1059) => (172.16.171.225:23)
CBAC sis 80D8F678 pak 80DFC034 TCP F ack 967618985 seq 3071996052(0) (171.68.9.156:1059) => (172.16.171.225:23)
CBAC sis 80D8F678 pak 80DFC034 TCP F ack 967618985 seq 3071996052(0) (171.68.9.156:1059) => (172.16.171.225:23)
CBAC sis 80D8F678 pak 80DFC034 TCP F P ack 3071996053 seq 967618985(0) (171.68.9.156:1059) => (172.16.171.225:23)
Session Idle-Timeout

- To view more information regarding the CBAC sessions, use:
  ‘show ip inspect session detail’

Established Sessions
Session 8D8F678 (171.68.9.156:1054)=>(172.16.171.225:23) tcp S IS_OPEN
Created 00:00:25, Last heard 00:00:23
Bytes sent (initiator:responder) [41:69] acl created 1
Inbound access-list 100 applied to interface FastEthernet0/1

Summary

- PIX outbound packets must be part of a translation rule
- PIX security level rules
- ICMP is a different animal
- PIX ‘show failover’ to monitor status and state information
- IOS Firewall requires established sessions
- Logging, logging, logging
Useful Links for Troubleshooting

- PIX top ten issues:

- PIX product support page:
  http://www.cisco.com/cgi-bin/Support/PSP/psp_view.pl?p=Hardware:PIX

- PIX failover document:

- Cisco TAC:
  http://www.cisco.com/kobayashi/support/tac/home.shtml

Troubleshooting Firewalls

Session SEC-340
Please Complete Your Evaluation Form

Session SEC-340