



NETWORKERS 2004

CISCO PIX FIREWALL SOLUTIONS

Session CERT-2001

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

1

Agenda

Cisco.com

- Review of PIX Firewall Technology
- PIX Firewall Capabilities and Good Practices
- New Features in PIX Firewall 6.2 & 6.3
- Question & Answer

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

2

Associated Sessions

Cisco.com

- **SEC-2020 – Deploying Firewalls**

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

3

REVIEW OF PIX FIREWALL TECHNOLOGY



CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

4

The PIX Firewall

Cisco.com

- The PIX Firewall is a dedicated hardware and software security solution that delivers high-level security **without impacting** network performance

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

5

PIX Firewall Benefits

Cisco.com

The Cisco PIX Firewall family delivers enterprise-class security for small-to-medium business and enterprise networks in a modular, purpose-built appliance. Some of the PIX Firewall family product highlights are as follows:

- Proprietary operating system
- Stateful inspection
- Protocol and application inspection
- User-based authentication
- Virtual private networking
- Web-based management solutions
- Stateful failover capabilities

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

6

Finesse Operating System

Cisco.com

- **Dedicated Proprietary OS**
No underlying OS (UNIX, NT) required to access memory, network devices, etc.
- **Hardened**
All access to or through the PIX Firewall must be defined by the administrator
- **Small**
PIX Firewall 6.3 image is less than 2 MB (Compressed)
- **Fast**
PIX 515E rated at 188 Mbps, 130,000 concurrent connections

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

7

Adaptive Security Algorithm (ASA)

Cisco.com

- **Provides stateful connection security**
Tracks source and destination ports and addresses, TCP sequence numbers, and additional TCP flags
Randomizes TCP initial sequence numbers
Monitors the session, ensuring both sides are obeying TCP/IP 'rules'
- **Dynamically permits stateful response traffic**
- **Supports Authentication, Authorization and Accounting (AAA)**

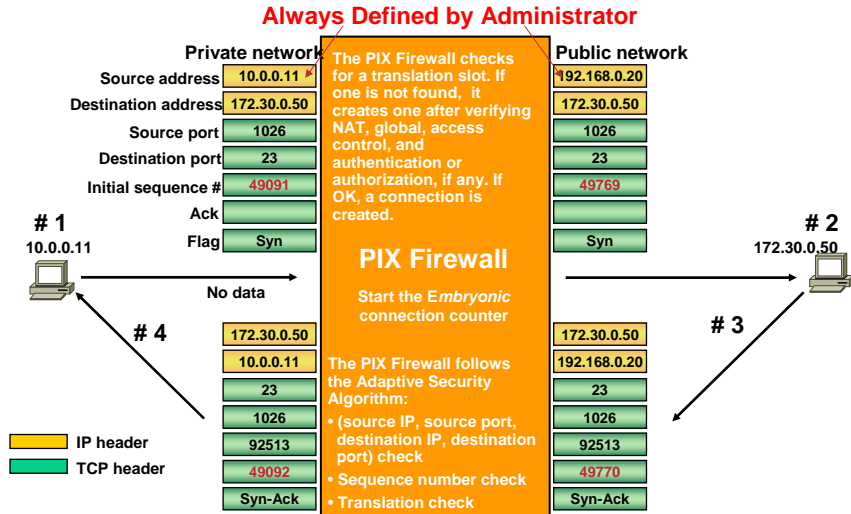
CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

8

TCP Initialization: Inside to Outside

Cisco.com



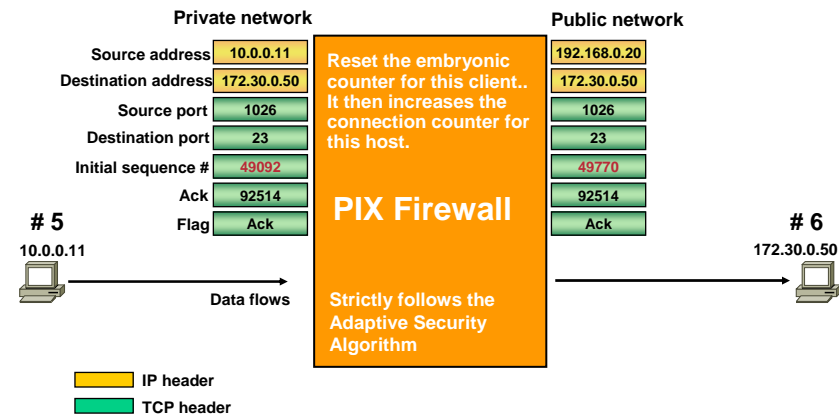
CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

9

TCP Initialization: Inside to Outside (Cont)

Cisco.com



CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

10

Cut-Through Proxy

Cisco.com

- **User-based authentication of inbound or outbound connections using TACACS+ or RADIUS**
Authentication occurs via HTTP, HTTPS (v6.3), FTP or Telnet
- **Per-user authorization**
Defines what the user is allowed to access
- **Authenticated/Authorized connections are fast (cut-through)**

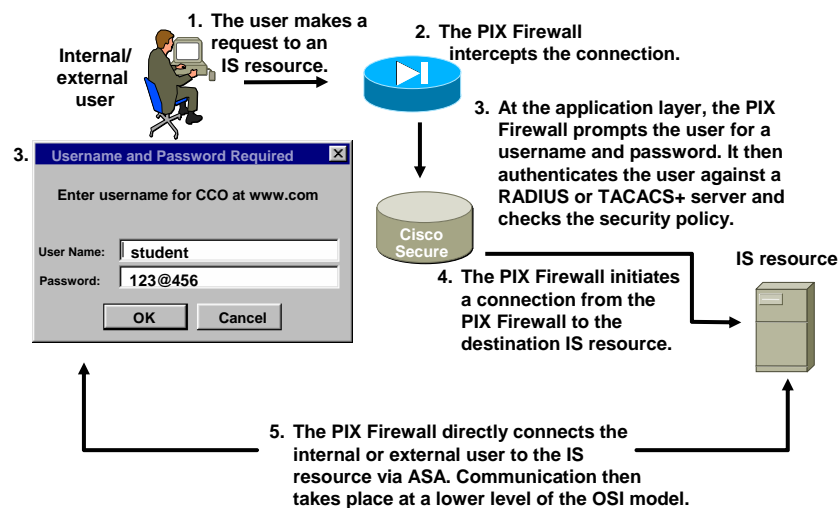
CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

11

Cut-Through Proxy

Cisco.com



CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

12

VPN Solution

Cisco.com

- **Supports PPTP, IPSec, IKE and L2TP/IPSec**
- **Site-to-Site tunneling**
- **Easy VPN Server for VPN Clients**
- **Easy VPN Remote**
 - 501 and 506E only**
 - Comparable to VPN 3002 HW Client**

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

13

Intrusion Detection System (IDS)

Cisco.com

- **Inline Intrusion Protection**
 - Provides protection from over 55 different types of popular network-based attacks ranging from malformed packet attacks to DoS attacks**
- **Integrates with Cisco IDS sensors for the ability to dynamically block/shun hostile network nodes via the firewall**

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

14

Application Inspection (Fixups)

Cisco.com

- **The PIX Firewall can inspect upper layer communications for certain protocols or applications to:**

Securely open and close negotiated ports or IP addresses for legitimate client-server connections through the firewall

Modify NAT/PAT relevant instances of IP addresses inside a packet (payload)

Inspect packets for signs of malicious application misuse

- **Some of the applications supported:**

CTIQBE (JTAPI), DNS, FTP, H.323, HTTP, ICMP, ILS (LDAP), MGCP, NetBIOS, PPTP, RSH, RTSP, SIP, SKINNY, SMTP, SQL*NET

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

15

PIX CAPABILITIES AND GOOD PRACTICES



CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

16

XLATE Fundamentals

Cisco.com

- **No communication (connection) is allowed without an XLATE**
- **NAT/global and static (translation rules) define XLATEs**
- **An XLATE is not created until traffic occurs that matches a translation rule**
- **Traffic that conforms to an XLATE is allowed outbound (HI to LOW) unless denied by an ACL**

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

17

XLATE Fundamentals (Cont.)

Cisco.com

- **Traffic that conforms to an XLATE is allowed inbound only if it's a stateful response or permitted by a conduit/ACL**
- **An XLATE, once created, can remain in place without a translation rule – use 'clear xlate' to force re-evaluation of translation rules**
- **Good Practice – Control outbound traffic with translation rules**

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

18

Translation Rules

Cisco.com

- **NAT/global**
 - For dynamic NAT/PAT assignments
 - Used mostly for end-user communications
- **static**
 - For 'permanent' NAT/PAT assignments
 - Used mostly for service communications
- **Both methods can be used bi-directionally (v6.2)**
- **Both methods can be configured to 'not-NAT' (i.e. nat 0)**

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

19

NAT/global

Cisco.com

```
nat [(if_name)] nat_id local_ip [mask [dns] [outside] [max_conns [emb_limit  
[norandomseq]]]]
```

```
global [(if_name)] nat_id {global_ip [-global_ip] [netmask global_mask]} |  
interface
```

- **Reflects PIX v6.2 syntax**
- **nat_id is used for 'binding'**
- **dns converts DNS replies that match the XLATE**
- **outside used for reverse NAT**

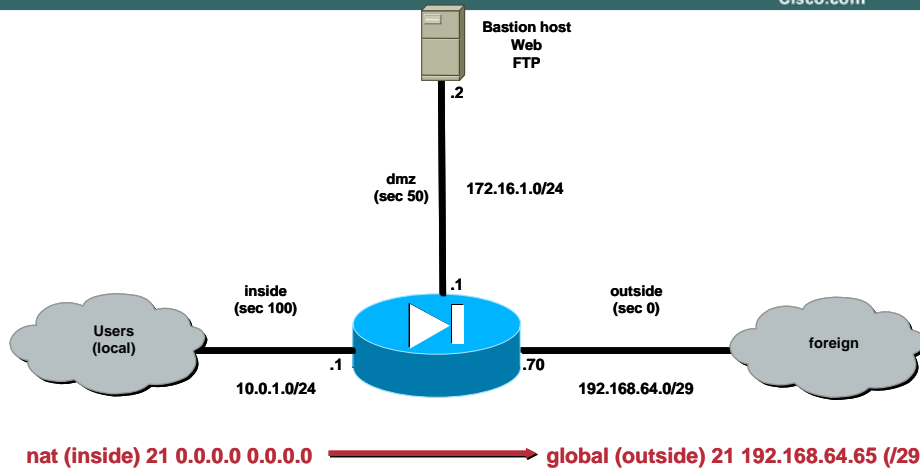
CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

20

NAT/global (Cont)

Cisco.com



Allows everything outbound!

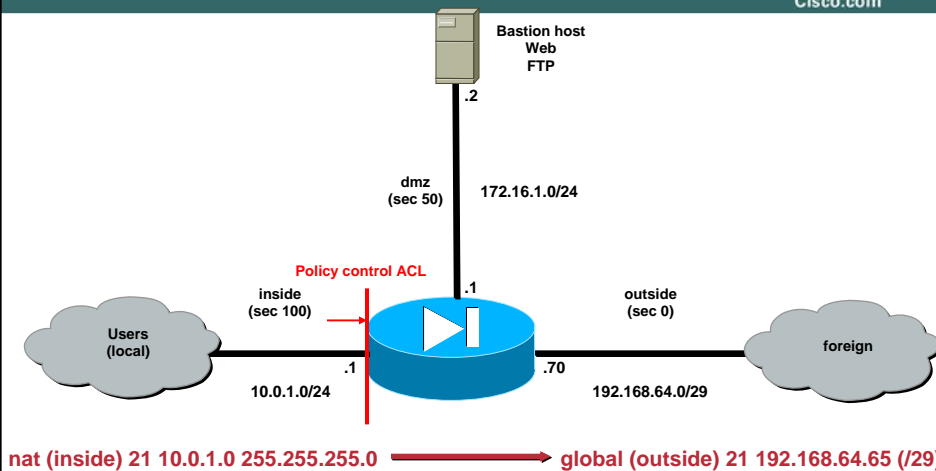
CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

21

NAT/global (Cont)

Cisco.com



Better – prevents IP spoofing
global (dmz) 21 required for communication to Bastion

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

22

NAT/global (Cont)

Cisco.com

- PIX Firewall ARP replies for addresses in 'global'
- global does not have to be the same address space as the outside interface
- nat IDs can be varied to define/control the 'exit' interface and global address(es)
- Can be used for outside or reverse NAT – i.e nat (outside) to global (inside) – v6.2
- Can PAT to the outside IP address – 'global (outside) 21 interface'
- static can be used instead

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

23

Static

Cisco.com

```
static [(prenat-interface, postnat-interface)] {mapped_address} interface}
  real_address [dns] [netmask mask] [norandomseq] [connection_limit
  [em_limit]]
```

- Reflects PIX v6.2 syntax
- Typically used to represent services
- A conduit or ACL permit is required to access the service inbound (lower to higher)
- Defines an outbound XLATE

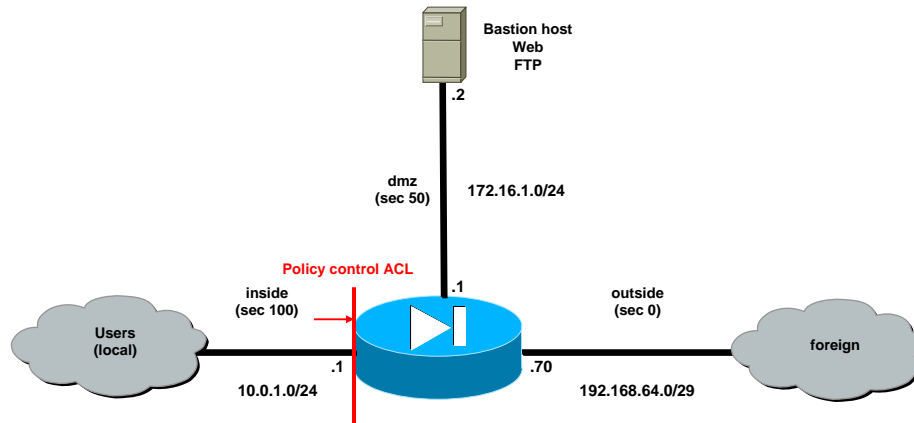
CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

24

Static (Cont)

Cisco.com



static (inside,outside) 192.168.64.65 10.0.1.11 → (192.168.64.65)

netmask can be modified to create a 'net static'

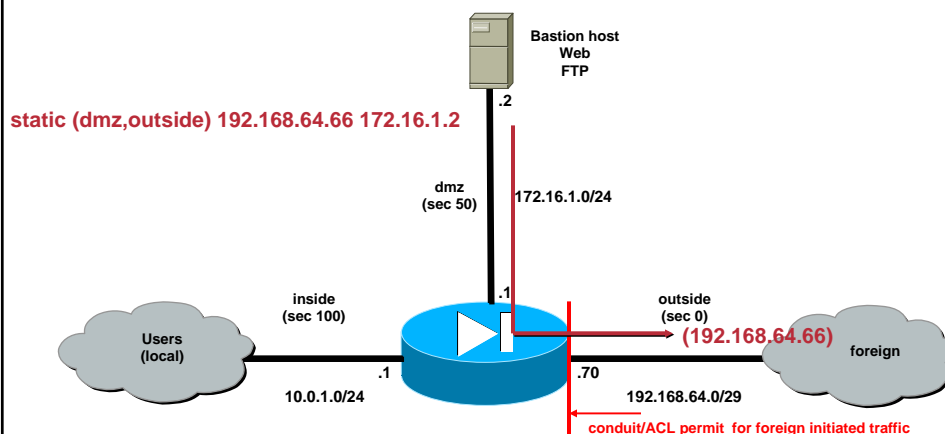
CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

25

Static (Cont)

Cisco.com



static (dmz,outside) 192.168.64.66 172.16.1.2

Defines an XLATE for the Bastion!
- it can initiate any traffic to the outside
- stateful responses are always permitted

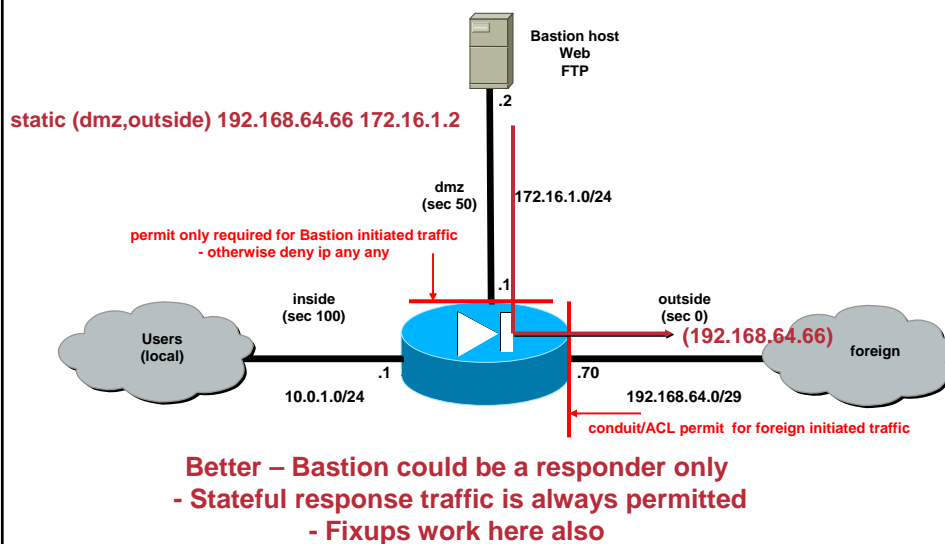
CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

26

Static (Cont)

Cisco.com



CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

27

Port Redirection

Cisco.com

```
static [(prenat-interface, postnat-interface)] tcp | udp global_ip | interface  
global_port local_ip local_port [netmask mask]
```

- Provides a method to map multiple services to a single global IP
- Can be used to limit the outbound XLATE
- Available in PIX v6.0

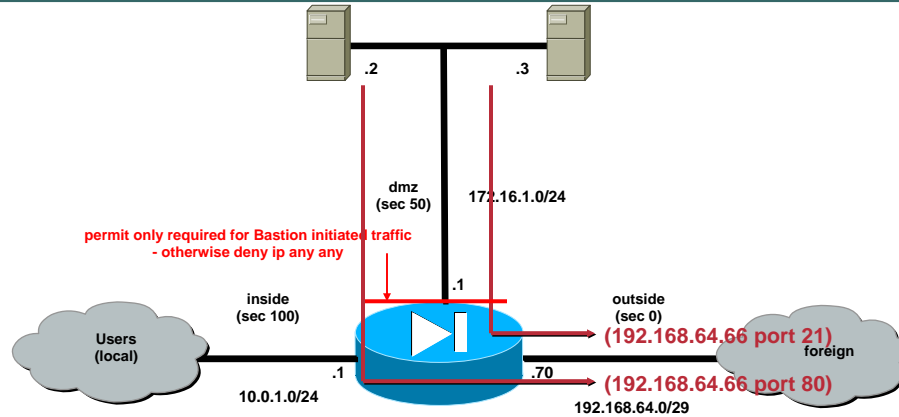
CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

28

Port Redirection Example

Cisco.com



static (dmz,outside) tcp 192.168.64.66 ftp 172.16.1.3 ftp
static (dmz,outside) tcp 192.168.64.66 www 172.16.1.2 www

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

29

No-NAT (identity NAT)

Cisco.com

- **nat (inside) 0 10.0.1.11 255.255.255.255**
no global – so valid for outbound to any interface
- **nat (inside) 0 access-list *acl_id***
Better – ACL defines when to nat 0
Used for tunneling
- **static (inside,outside) 10.0.1.11 10.0.1.11**
Also good – controls exit interface but 'permanent'
- **The PIX uses more specific entries always – i.e. static preferred over nat/global**

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

30

DoS Prevention

Cisco.com

```
pix1# sh static
static (dmz,outside) 192.168.64.66 172.16.1.2 netmask 255.255.255.255 0 0
```

- **The last two values represent *conn_limit* & *em_limit***
0 = unlimited - no DoS protection provided by the PIX
- **When *em_limit* is exceeded the PIX will force initiators to complete the 3-way handshake first**
- **Limits work in both directions**
- **Will generate a syslog event when limits have been exceeded**

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

31

clear xlate

Cisco.com

```
pix1# clear xlate ?
Usage: show|clear xlate [global | local <ip1[-ip2]> [netmask <mask>]]
      [gport | lport <port1[-port2]>]
      [interface <if1[,if2]>]
      [state <static [,portmap] [,norandomseq] [,identity]>]
      [debug]
      [count]
```

- **Once the XLATE is created it will remain in place until the timeout xlate expires – default = 3 hours**
- **Use when an existing translation rule has been modified**
- **All connections using that xlate will be cleared also**

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

32

Access Lists vs Conduits?

Cisco.com

- **ACLs**
 - Hierarchy required, evaluated top to bottom – first match
 - Evaluates the specific interface ACL is applied to
 - More like IOS
 - Editing simplified in 6.2 and 6.3
 - Used for more than interface control
- **Conduits**
 - No hierarchy required, evaluated as a group – best match - quicker?
 - Permits access only from lower security to higher security interfaces – control is defined by global destination address
 - Backwards syntax vs IOS (destination address first)
 - Not a filtering utility
- Cisco recommends using ACLs
- ACLs take precedence over conduits for the same direction
- PDM does not support both ACLs and conduits
- VMS uses only ACLs – conduit to ACL converter provided

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

33

Unicast Reverse Path Forwarding

Cisco.com

```
ip verify reverse-path interface <if_name>
```

- **IP spoofing protection**
- **Does a route lookup based on the source address**
- **Packets are dropped if there is no route found for the packet or the route found does not match the interface on which the packet arrived**

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

34

ICMP

Cisco.com

- **ICMP traffic not allowed to XLATES i.e. through the PIX**
 - Must use ACL permits to override – ICMP not stateful
- **ICMP permitted to PIX interface IP addresses**
 - Should limit using 'icmp' command

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

35

ICMP Example

Cisco.com

- **ICMP uses a hierarchy – first match with an implicit deny all**
- **To block all ICMP to the outside IP**
 - `icmp deny any outside`
- **To deny all ping requests and permit all unreachables to the outside**
 - `icmp deny any echo-reply outside`
 - `icmp permit any unreachable outside`
 - Recommended for Path MTU discovery
- **To permit subnet 172.22.0.0/16 to ping the outside**
 - `icmp permit 172.22.0.0 255.255.0.0 echo-reply outside`
 - host keyword can be used for a single address

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

36

IP Fragmentation

Cisco.com

```
pix1(config)# fragment ?
```

```
Usage: fragment {size | chain | timeout} <limit> [<interface>]
```

```
show fragment [<interface>]
```

```
clear fragment
```

```
size <limit> - maximum number of blocks in database (def = 200)
```

```
chain <limit> - maximum number of element in a fragment set (def = 24)
```

```
timeout <limit> - number of seconds to assemble a fragment set (def = 5)
```

- **By default the PIX accepts up to 24 fragments to reconstruct a full IP packet (chain)**
- **To prevent IP fragmentation through the PIX, set the chain to 1**

Use 'show fragment' first to determine if fragmentation is occurring – limit as much as possible

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

37

VPN: More than Site-to-Site

Cisco.com

- **The recommended Cisco VPN box before Altiga was purchased**
- **Same capabilities as the VPN 3000 series except for:**
 - IPSec over TCP/UDP 10000 (not the same as NAT-T)**
 - Client Firewall management**
 - Local LAN access (modified split-tunneling)**
 - Ease of management**
- **Configurable with the PDM VPN Wizard**

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

38

Easy VPN Server Example

Cisco.com

```
access-list INSIDE_OUTBOUND_NAT0_ACL permit ip 192.168.0.0  
255.255.255.0 10.62.62.0 255.255.255.0
```

```
ip local pool VPN-POOL 10.62.62.1-10.62.62.30
```

```
nat (inside) 0 access-list INSIDE_OUTBOUND_NAT0_ACL
```

```
sysopt connection permit-ipsec
```

```
isakmp enable outside  
isakmp identity address  
isakmp nat-traversal 20  
isakmp policy 20 authentication pre-share  
isakmp policy 20 encryption aes  
isakmp policy 20 hash sha  
isakmp policy 20 group 2  
isakmp policy 20 lifetime 86400
```

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

39

Easy VPN Server Example (Cont.)

Cisco.com

```
crypto ipsec transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac  
crypto dynamic-map OUTSIDE_DYN_MAP 20 set transform-set ESP-AES-128-  
SHA
```

```
crypto map OUTSIDE_MAP 20 ipsec-isakmp dynamic OUTSIDE_DYN_MAP  
crypto map OUTSIDE_MAP client configuration address respond  
crypto map OUTSIDE_MAP client authentication LOCAL  
crypto map OUTSIDE_MAP interface outside
```

```
vpngroup VPNCLIENT address-pool VPN-POOL  
vpngroup VPNCLIENT dns-server 192.168.0.2  
vpngroup VPNCLIENT default-domain sunsetlearning.com  
vpngroup VPNCLIENT split-dns sunsetlearning.com  
vpngroup VPNCLIENT idle-time 1800  
vpngroup VPNCLIENT password *****
```

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

40

IDS

Cisco.com

```
ip audit name audit_name attack [action [alarm] [drop] [reset]]
ip audit name audit_name info [action [alarm] [drop] [reset]]
ip audit interface if_name audit_name
```

- PIX can provide inline intrusion detection
- Evaluated before interface ACL
- Can take any combination of 'action' for a given family (attack or informational) of signatures
- Can audit multiple interfaces
- Currently sends alarms only to syslog

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

41

IDS Example

Cisco.com

```
ip audit name I-HACK attack action alarm
ip audit name I-SNOOP info action alarm

ip audit name SNOOP info action alarm
ip audit name HACK attack action alarm drop reset

ip audit interface outside SNOOP
ip audit interface outside HACK

ip audit interface inside I-SNOOP
ip audit interface inside I-HACK
```

Use 'show ip audit count' to see signature matches
For detailed signature information – requires customer login
<http://www.cisco.com/cgi-bin/front.x/csec/idsHome.pl>

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

42

PIX FIREWALL 6.2 AND 6.3 NEW FEATURES



CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

43

Management Authentication

Cisco.com

```
aaa-server LOCAL protocol local ← default – cannot be renamed
aaa authentication enable console LOCAL
aaa authentication http console LOCAL
aaa authentication serial console LOCAL
aaa authentication ssh console LOCAL
```

```
username rdeterman password cisc0123 ← password encrypted in
config
```

- **PIX 6.2 has 'local' username/password capability**
Provides some AAA without TACACS+/RADIUS

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

44

Object-Grouping

Cisco.com

- Allows discontinuous named ranges of protocols, addresses, ports or ICMP types for use in an ACL or conduit
- Groups can be nested
- ACL reflects each combination as a unique 'element'
- Can be combined with non-grouped access-list statements
- Available in PIX v6.2

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

45

Object-Grouping Example

Cisco.com

```
(config)# object-group network THEM
(config-network)# description The Potential BAD Guys
(config-network)# network-object 172.26.0.0 255.255.0.0

(config)# object-group network US
(config-network)# description The GOOD guys
(config-network)# network-object host 10.0.3.3
(config-network)# network-object 172.16.3.0 255.255.255.0

(config)# object-group service SERVICES tcp
(config-service)# port-object eq www
(config-service)# port-object eq ftp
(config-service)# port-object eq telnet

config)#access-list THEM-to-US deny tcp object-group THEM object-
group US object-group SERVICES
(config)#access-list THEM-to-US permit ip any any
```

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

46

ACL Editing

Cisco.com

- **ACL Line Numbers**

- Used for ACL editing

- PIX automatically creates line numbers

- Allows full editing on the console

- Similar capability introduced in IOS 12.2.15T

- **Remarks**

- Allows commenting of your 'code'

- Can be placed anywhere in the ACL without evaluation overhead

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

47

ACL Editing Example

Cisco.com

```
pix1(config)# sh access-list TEST
access-list TEST; 1 elements
access-list TEST line 1 deny ip any any (hitcnt=0)
```

```
pix1(config)# access-list TEST line 1 permit tcp any host 192.168.1.11 eq www
```

```
pix1(config)# sh access-list TEST
access-list TEST; 2 elements
access-list TEST line 1 permit tcp any host 192.168.1.11 eq www (hitcnt=0)
access-list TEST line 2 deny ip any any (hitcnt=0)
```

```
pix1(config)# access-list TEST line 2 remark Place all entries above this line!
```

```
pix1(config)# sh access-list TEST
access-list TEST; 2 elements
access-list TEST line 1 permit tcp any host 192.168.1.11 eq www (hitcnt=0)
access-list TEST line 2 remark Place all entries above this line!
access-list TEST line 3 deny ip any any (hitcnt=0)
```

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

48

TurboACL

Cisco.com

- TurboACL compiles ACLs into a set of lookup tables, while maintaining first-match requirements
- Packet headers enable access to these tables in a small, fixed number of lookups, independently of the existing number of ACL entries
- Minimum memory required = 2.1 MB
 - ~1 MB for every 2000 elements
- Can be enabled globally for all ACLs or per ACL
 - access-list compiled
 - access-list TEST compiled
- Use 'show access-list' to view memory utilization

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

49

VLAN-Based Virtual Interfaces

Cisco.com

pix1(config)# interface ?

Usage: interface <hardware_id> [<hw_speed> [shutdown]]

[no] interface <hardware_id> <vlan_id> [logical|physical] [shutdown]

interface <hardware_id> change-vlan <old_vlan_id> <new_vlan_id>

show interface

pix1(config)# interface e4 vlan22 physical ← ensures all frames are tagged from the PIX Firewall

pix1(config)# interface e4 vlan21 logical ← creates new interface vlan21

- Provides 802.1q tagging
- Extends number of interfaces supported
 - Chassis dependant

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

50

Improved Cisco AVVID Support

Cisco.com

- **DHCP Option 66 and 150 support**
For Skinny and SIP based IP Phones
- **IGMP v2 and Stub Multicast Routing**
- **Fixups for H.323v3/4, MGCP, Skinny, and SIP**

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

51

VPN NAT Traversal (NAT-T): 6.3

Cisco.com

```
pix1(config)# isakmp nat-traversal 20 ← 20 second keepalives
```

- **Support for standard IPSec transparent tunneling**
- **Detects translation (NAT/PAT) in the path via the IKE tunnel**
- **If translation is detected, will automatically encapsulate with UDP/4500**
- **www.ietf.org/html.charters/ipsec-charter.html**

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

52

Management-access

Cisco.com

```
pix1(config)# management-access inside
```

- **Enables administrators to remotely manage firewalls over a VPN tunnel using the inside interface IP address of the remote PIX**
- **Works for PDM, SSH, Telnet, and SNMP**
- **Don't have to 'wildcard' access to outside any more. i.e. ssh 0.0.0.0 0.0.0.0 outside**

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

53

AES (Advanced Encryption Standard) Support

Cisco.com

- **AES 128, 192 & 256 key lengths supported for IKE and ESP**
- **Hardware encryption support with PIX Firewall VAC+**
- **Automatically enabled in 6.3 if your PIX Firewall is activated for 3-DES**
- **Supported in Cisco VPN Client 3.6+**
- **A brute force attack at 256 keys/second**
 - DES = 1 second
 - AES 128 = 149 trillion years
 - Age of the universe = 13.7 billion years

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

54

NTP and Timezone Support

Cisco.com

```
pix1(config)# clock timezone MST -7  
pix1(config)# clock summer-time MDT recurring  
pix1(config)# ntp server 172.26.26.100 source inside
```

- **Supported in PIX v6.2**
 - previously only UTC was relevant
- **Supports NTP v3 and MD5 authentication**

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

55

OSPF Routing

Cisco.com

- **Available in PIX v6.3**
- **More resilient than static routing or RIP**
- **Supports**
 - Virtual links
 - OSPF authentication
 - DR, ABR, ASBR
 - Stub areas and NSSA
 - Load balancing among 3 peers using ECMP

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

56

OSPF Routing: Example

Cisco.com

```
routing interface outside
  ospf priority 0
  ospf message-digest-key 1 md5 PIXOSPF
  ospf authentication message-digest
routing interface inside
routing interface dmz
router ospf 100
  network 10.0.7.1 255.255.255.255 area 1
  network 192.168.0.0 255.255.0.0 area 0
  area 0 authentication message-digest
  router-id 3.3.3.3
  log-adj-changes
```

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

57

Packet Capture

Cisco.com

- Available in PIX v6.2
- Provides the ability to sniff any traffic on any interface accepted or blocked by the PIX Firewall
- Can view captures on the console or HTTPS
- Can copy via TFTP to PCAP format file

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

58

Packet Capture: Example

Cisco.com

```
capture capture_name [access-list acl_id] [buffer bytes] [ethernet-type type][interface name] [packet-length bytes]
```

```
copy capture:<capture-name> tftp://<location>/<pathname> [pcap]
```

```
pix1# sh capture
capture PCAP access-list UNREACH interface outside
pix1# sh access-list UNREACH
access-list UNREACH turbo-configured; 1 elements
access-list UNREACH line 1 permit icmp any any unreachable (hitcnt=9)
pix1# sh capture PCAP
9 packets captured
17:57:21.375712 172.18.126.90 > 207.225.27.67: icmp: host 205.188.158.130
unreachable - admin prohibited filter
20:13:27.166586 207.225.27.67 > 198.6.1.4: icmp: 207.225.27.67 udp port 3025
unreachable
01:42:43.016768 207.225.27.67 > 198.6.1.4: icmp: 207.225.27.67 udp port 3172
unreachable
```

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

59

show Command Output Filter

Cisco.com

```
pix1(config)# sh ?
```

At the end of show <command>, use the pipe character '|' followed by: begin|include|exclude|grep [-v] <regular_exp>, to filter show output.

```
pix1(config)# sh run | include nat
nat (inside) 0 access-list CRYPTO-ACL
nat (inside) 1 10.0.1.0 255.255.255.0 0 0
isakmp nat-traversal 20
```

- **New in PIX v6.3**

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

60

Information Sources

Cisco.com

- <http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/index.htm>
- <http://www.cisco.com/warp/public/707/ref.html>
- <http://www.cisco.com/go/csec>
- <http://www.cisco.com/go/safe>

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

61

QUESTIONS



CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

62

Thank You for Your Attendance

Cisco.com

Ryan J. Determan, CCSI 98950
CCIE #5276

Sunset Learning
Cisco Learning Solutions Partner
Booth# 209

www.sunsetlearning.com
1.800.569.1894

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

63

Complete Your Online Session Evaluation!

Cisco.com

- WHAT:** Complete an online session evaluation and your name will be entered into a daily drawing
- WHY:** Win fabulous prizes! Give us your feedback!
- WHERE:** Go to the Internet stations located throughout the Convention Center
- HOW:** Winners will be posted on the onsite Networkers Website; four winners per day

CERT-2001
9978_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

64

CISCO SYSTEMS

