1.0 Overview

This document is intended to give guidance on how to read log entries from a Cisco PIX / ASA. The specific model in this case was a PIX 501.

2.0 PIX Config

The following is the PIX config of the 501:

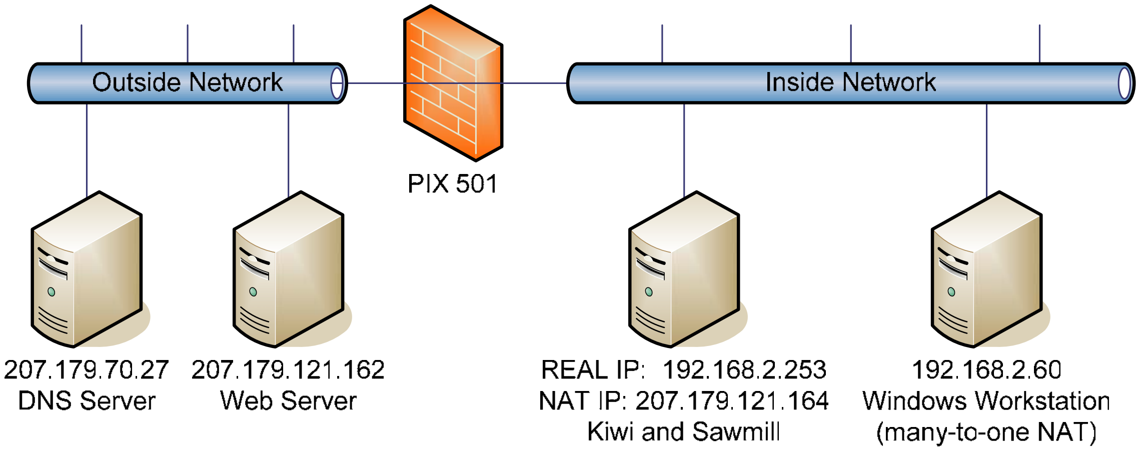
Result of firewall command: "wri te"

```
Building configuration...
: Saved
:
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 100full
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password REDACTED encrypted
passwd REDACTED encrypted
hostname pix
domain-name lachniet.com
clock timezone EST -5
clock summer-time EDT recurring
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
name 207.179.121.164 sawmill-nat
access-list inside_outbound_nat0_acl permit ip any 192.168.2.0 255.255.255.192
access-list REDACTED_splitTunnelAcl permit ip any any
access-list outside_cryptomap_dyn_40 permit ip any 192.168.2.0 255.255.255.192
access-list outside_access_in permit icmp any any
access-list outside_access_in permit tcp any host sawmill-nat eq 8987
access-list outside_access_in permit udp any host sawmill-nat eq syslog
```

```
pager lines 24
logging on
logging timestamp
logging trap debugging
logging host inside 192.168.2.253
mtu outside 1500
mtu inside 1500
ip address outside 207.179.121.163 255.255.255.248
ip address inside 192.168.2.254 255.255.255.0
ip audit name attack_signature attack action alarm
ip audit interface outside attack_signature
ip audit interface inside attack_signature
ip audit info action alarm
ip audit attack action alarm
ip local pool REDACTED-vpn-pool 192.168.2.31-192.168.2.40
pdm logging informational 100
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list inside_outbound_nat0_acl
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
static (inside,outside) sawmill-nat 192.168.2.253 netmask 255.255.255.255 0 0
access-group outside_access_in in interface outside
route outside 0.0.0.0 0.0.0.0 207.179.121.161 1
timeout xlate 0:05:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
ntp server 198.30.92.2 source outside prefer
http server enable
http 192.168.2.0 255.255.255.0 inside
http 192.168.2.62 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto dynamic-map outside_dyn_map 20 set transform-set ESP-AES-256-SHA
crypto dynamic-map outside_dyn_map 40 match address outside_cryptomap_dyn_40
crypto dynamic-map outside_dyn_map 40 set transform-set ESP-3DES-MD5
crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
crypto map outside_map client authentication LOCAL
crypto map outside_map interface outside
isakmp enable outside
isakmp nat-traversal 20
isakmp policy 20 authentication pre-share
isakmp policy 20 encryption aes-256
isakmp policy 20 hash md5
isakmp policy 20 group 2
isakmp policy 20 lifetime 86400
isakmp policy 40 authentication pre-share
isakmp policy 40 encryption 3des
isakmp policy 40 hash md5
isakmp policy 40 group 2
isakmp policy 40 lifetime 86400
vpngroup REDACTED address-pool REDACTED-vpn-pool
vpngroup REDACTED dns-server 192.168.2.60 35.8.2.42
vpngroup REDACTED wins-server 192.168.2.60
vpngroup REDACTED default-domain lachniet.com
vpngroup REDACTED split-tunnel REDACTED_splitTunnelAcl
vpngroup REDACTED idle-time 1800
vpngroup REDACTED password REDACTED
telnet timeout 5
ssh 0.0.0.0 0.0.0.0 outside
ssh 0.0.0.0 0.0.0.0 inside
ssh timeout 5
console timeout 0
dhcpd address 192.168.2.200-192.168.2.220 inside
dhcpd dns 207.179.71.27 207.179.70.27
dhcpd wins 192.168.2.60
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd auto_config outside
dhcpd enable inside
username REDACTED password REDACTED encrypted privilege 15
terminal width 80
Cryptochecksum:be5a4ac0f6c126654eb0f2b9833b8743
: end
[OK]
```

3.0 Network Configuration:

The following diagram details the test network configuration:



4.0 Commented Log Examples:

#1) Here are 2 outgoing DNS queries, 1:1 NAT, from the inside host 192.168.2.253 to the outside DNS server host 207.179.70.27:

```
2006-12-08 15:03:40     Local4.Info 192.168.2.254     Dec 08 2006
15:03:40: %PIX-6-302015: Built outbound UDP connection 28 for
outside:207.179.70.27/53 (207.179.70.27/53) to
inside:192.168.2.253/3548 (207.179.121.164/3548)
2006-12-08 15:03:40     Local4.Info 192.168.2.254     Dec 08 2006
15:03:40: %PIX-6-302016: Teardown UDP connection 28 for
outside:207.179.70.27/53 to inside:192.168.2.253/3548 duration 0:00:01
bytes 163
2006-12-08 15:03:43     Local4.Info 192.168.2.254     Dec 08 2006
15:03:43: %PIX-6-302015: Built outbound UDP connection 29 for
outside:207.179.70.27/53 (207.179.70.27/53) to
inside:192.168.2.253/3549 (207.179.121.164/3549)
2006-12-08 15:03:43     Local4.Info 192.168.2.254     Dec 08 2006
15:03:43: %PIX-6-302016: Teardown UDP connection 29 for
outside:207.179.70.27/53 to inside:192.168.2.253/3549 duration 0:00:01
bytes 142
2006-12-08 15:03:48     Local4.Info 192.168.2.254     Dec 08 2006
15:03:48: %PIX-6-302015: Built outbound UDP connection 30 for
outside:207.179.70.27/53 (207.179.70.27/53) to
inside:192.168.2.253/4367 (207.179.121.164/4367)
2006-12-08 15:03:48     Local4.Info 192.168.2.254     Dec 08 2006
15:03:48: %PIX-6-302016: Teardown UDP connection 30 for
outside:207.179.70.27/53 to inside:192.168.2.253/4367 duration 0:00:01
bytes 142
```

#2) Here is 1 outgoing HTTP connection, 1:1 NAT, from the inside host 192.168.2.253 to the outside web server host 207.179.121.162:

```
2006-12-08 15:03:48     Local4.Info 192.168.2.254     Dec 08 2006
15:03:48: %PIX-6-302013: Built outbound TCP connection 31 for
outside:207.179.121.162/80 (207.179.121.162/80) to
inside:192.168.2.253/3550 (207.179.121.164/3550)
2006-12-08 15:03:53     Local4.Info 192.168.2.254     Dec 08 2006
15:03:53: %PIX-6-302014: Teardown TCP connection 31 for
```

```
outside:207.179.121.162/80 to inside:192.168.2.253/3550 duration
0:00:04 bytes 512 TCP FINs
```

#3) Here is 1 incoming SYSLOG connection, 1:1 NAT, from the outside host 207.179.121.162 to the inside syslog server host 291.68.2.253:

```
2006-12-08 15:04:08     Local4.Info 192.168.2.254     Dec 08 2006
15:04:08: %PIX-6-302015: Built inbound UDP connection 32 for
outside:207.179.121.162/11484 (207.179.121.162/11484) to
inside:192.168.2.253/514 (207.179.121.164/514)
2006-12-08 15:06:09     Local4.Info 192.168.2.254     Dec 08 2006
15:06:09: %PIX-6-302016: Teardown UDP connection 32 for
outside:207.179.121.162/11484 to inside:192.168.2.253/514 duration
0:02:01 bytes 14
```

#4) Here are 4 incoming HTTP connections, 1:1 NAT, from the outside host 207.179.121.162 to the inside sawmill server host 192.168.2.253:

```
2006-12-08 15:04:14     Local4.Info 192.168.2.254     Dec 08 2006
15:04:14: %PIX-6-302013: Built inbound TCP connection 33 for
outside:207.179.121.162/25995 (207.179.121.162/25995) to
inside:192.168.2.253/8987 (207.179.121.164/8987)
2006-12-08 15:04:14     Local4.Info 192.168.2.254     Dec 08 2006
15:04:14: %PIX-6-302013: Built inbound TCP connection 34 for
outside:207.179.121.162/25996 (207.179.121.162/25996) to
inside:192.168.2.253/8987 (207.179.121.164/8987)
2006-12-08 15:04:14     Local4.Info 192.168.2.254     Dec 08 2006
15:04:14: %PIX-6-302013: Built inbound TCP connection 35 for
outside:207.179.121.162/25997 (207.179.121.162/25997) to
inside:192.168.2.253/8987 (207.179.121.164/8987)
2006-12-08 15:05:15     Local4.Info 192.168.2.254     Dec 08 2006
15:05:15: %PIX-6-302014: Teardown TCP connection 35 for
outside:207.179.121.162/25997 to inside:192.168.2.253/8987 duration
0:01:01 bytes 5030 TCP FINs
2006-12-08 15:05:15     Local4.Info 192.168.2.254     Dec 08 2006
15:05:15: %PIX-6-302014: Teardown TCP connection 33 for
outside:207.179.121.162/25995 to inside:192.168.2.253/8987 duration
0:01:01 bytes 7727 TCP FINs
2006-12-08 15:05:15     Local4.Info 192.168.2.254     Dec 08 2006
15:05:15: %PIX-6-302014: Teardown TCP connection 34 for
outside:207.179.121.162/25996 to inside:192.168.2.253/8987 duration
0:01:01 bytes 23852 TCP FINs
```

Case#5: A DNS lookup, many-to-one translation, from 192.168.2.60, which is then given a NAT entry (207.179.121.163/1032) and then sent to the destination (207.179.70.27/53)

```
2006-12-08 15:43:36     Local4.Info 192.168.2.254     Dec 08 2006
15:43:36: %PIX-6-305011: Built dynamic UDP translation from
inside:192.168.2.60/1041 to outside:207.179.121.163/1032
2006-12-08 15:43:36     Local4.Info 192.168.2.254     Dec 08 2006
15:43:36: %PIX-6-302015: Built outbound UDP connection 25 for
outside:207.179.70.27/53 (207.179.70.27/53) to inside:192.168.2.60/1041
(207.179.121.163/1032)
2006-12-08 15:43:36     Local4.Info 192.168.2.254     Dec 08 2006
15:43:36: %PIX-6-302016: Teardown UDP connection 25 for
```

```
outside:207.179.70.27/53 to inside:192.168.2.60/1041 duration 0:00:01
bytes 150
```

Case #6: A HTTP request, many-to-one translation, from 192.168.2.60, which is then given a NAT entry (207.179.121.163/1029) and then sent to the destination (207.179.121.162/80). You can also see that a URL was accessed.

```
2006-12-08 15:43:36     Local4.Info 192.168.2.254     Dec 08 2006
15:43:36: %PIX-6-305011: Built dynamic TCP translation from
inside:192.168.2.252/4952 to outside:207.179.121.163/1029
2006-12-08 15:43:36     Local4.Info 192.168.2.254     Dec 08 2006
15:43:36: %PIX-6-302013: Built outbound TCP connection 26 for
outside:207.179.121.162/80 (207.179.121.162/80) to
inside:192.168.2.252/4952 (207.179.121.163/1029)
2006-12-08 15:43:36     Local4.Notice     192.168.2.254     Dec 08 2006
15:43:36: %PIX-5-304001: 192.168.2.252 Accessed URL 207.179.121.162:/
2006-12-08 15:43:51     Local4.Info 192.168.2.254     Dec 08 2006
15:43:51: %PIX-6-302014: Teardown TCP connection 26 for
outside:207.179.121.162/80 to inside:192.168.2.252/4952 duration
0:00:15 bytes 3782 TCP Reset-I
```

5.0 Comments

As I see it, you basically have three possible types of connections to look for:

1) 1:1 NAT Incoming
2) 1:1 NAT Outgoing
3) Many:1 NAT Outgoing

There is also a fourth possibility, which is that someone is NAT’ing individual ports on their firewall to different internal hosts, so that the outside interface of the firewall (for example) will redirect port 25 to an internal mail server, and also redirect port 80 to a completely different internal HTTP server. I didn’t cover this possibility, and I’m not sure how that looks.

The log entries for many:1 NAT are totally different from 1:1 NAT. My take on it is this:

1) With 1:1 NAT, there will be 2 entries, each with the same connection ID. The connection ID is the index. You will have a "built inbound/built outbound" entry and then a "teardown". Pretty straightforward

3) With many:1 NAT, there will be 3 entries, that DON'T share the same connection ID - a "built dynamic" where the Index becomes the NAT'd address on the firewall (usually a specific port on the outside interface). You can link that index to the next line which is your "built outbound", which then identified your connection number. The connection number then becomes the new index for the "teardown" entry which is the third. So for this type, you really have to track 2 different unique identifier indexes, first the NAT port, then the connection ID.