Engineering Note

Interoperability with Ingate SIParator and Cisco Pix

Revision History

Rev.	*Date*	*Signature*	*Comments*
0.1	2005-02-14	hebr	Initial version.

Introduction

The aim of this document is to assist the user during configurations of Ingate SIParator®, and Cisco Pix firewall.

Overview

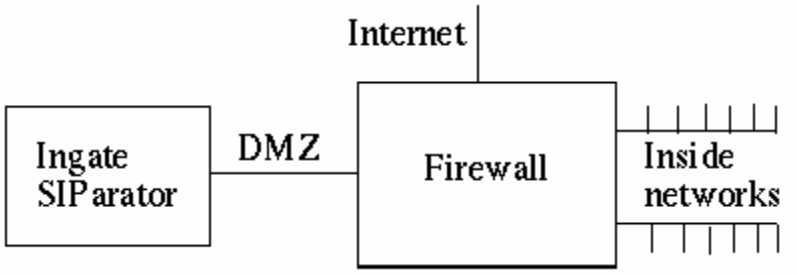
The following configuration supplement is meant to serve as an example and guide on how to configure a Cisco PIX for use with the Ingate SIParator in the DMZ and DMZ/LAN modes.

Ingate SIParator

The Ingate SIParator has to have a public routable ip-address assigned to it. Also when the SIParator is placed in DMZ mode, make sure no NAT is performed between the Cisco and the SIParator.

Please also make sure to open ports for SIP signaling and media from the Cisco Pix to the SIParator, and onto the LAN.

DMZ Mode



IMPORTANT NOTE:
The IP address assigned to the SIParator **MUST** be publicly addressable. In many/most configurations, the network in the DMZ of the PIX is private. Therefore, network address translation is performed. However, there can only be one network on the DMZ of a PIX unless there is a router present. Therefore, that DMZ network **HAS** to be a publicly addressable network even though NAT will be performed to all components except the SIParator. (If the DMZ was a private network, the SIParator could not have a public address. The PIX would not be able to route packets to it)

Cisco Pix

Turn off the SIP FIXUP in the Cisco PIX

Enter: [no] fixup protocol **[sip] [5060]**

If you would like to see the current settings for a specific protocol use the show fixup sip 5060 command which displays the configuration for an individual protocol.

For this example, assume the PIX has the following IP addresses assigned to its interfaces:
ip address outside 64.63.62.101 netmask 255.255.248.0
ip address inside 10.1.1.101 netmask 255.255.248.0
ip address dmz 31.32.33.254 netmask 255.255.248.0

The following entries are needed to allow the traffic to and from the SIParator *without* being NATed.
Static (inside,dmz) 10.1.0.0 10.1.0.0 netmask 255.255.248.0 0 0
static (dmz,inside) 31.32.33.1 31.32.33.1 netmask 255.255.255.255 0 0
static (dmz,outside) 31.32.33.1 31.32.33.1 netmask 255.255.255.255 0 0
static (outside,dmz) 64.63.62.0 64.63.62.0 netmask 255.255.248.0 0 0

Create an Access Group for each interface
access-group acl_out in interface outside
access-group acl_in in interface inside
access-group acl_dmz in interface dmz

Create access lists allowing traffic bi-directionally between the Internet and the SIParator and bi-directionally between the SIParator and the LAN. The following are examples of how these rules "could" be written.

Allow PC to configure SIParator (from LAN)
access-list acl_dmz permit tcp host 31.32.33.1 host 10.1.1.70
access-list acl_in permit tcp host 10.1.1.70 host 31.32.33.1

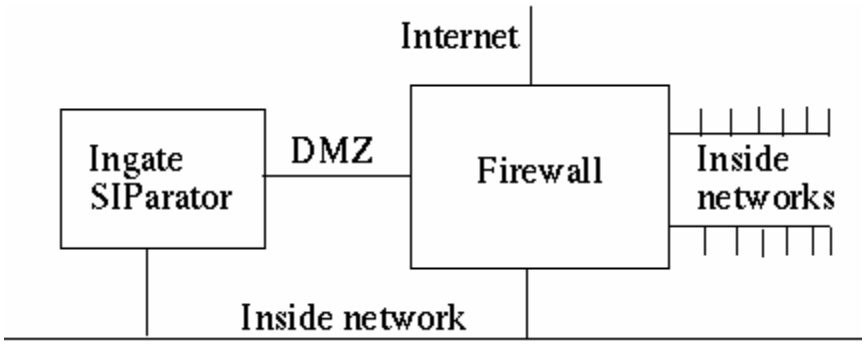
Internet->DMZ
access-list acl_out permit udp any host 31.32.33.1 eq 5060
access-list acl_out permit udp any host 31.32.33.1 port range 58024 60999
access-list acl_out permit udp any host 31.32.33.1 eq dnsix

SIParator-> Inside and Outside
access-list acl_dmz permit udp host 31.32.33.1 any eq 5060
access-list acl_dmz permit udp host 31.32.33.1 any range 58024 60999
access-list acl_dmz permit udp host 31.32.33.1 any eq dnsix

Inside-> SIParator
access-list acl_in permit udp any host 31.32.33.1 eq 5060
access-list acl_in permit udp any host 31.32.33.1 range 58024 60999
access-list acl_in permit udp any host 31.32.33.1 eq dnsix

Deny Lists (Following the "permits", it is good to write a list of "denies")
access-list acl_dmz deny udp any any
access-list acl_dmz deny tcp any any
access-list acl_in deny tcp host 10.1.1.70 any
access-list acl_out deny udp any any
access-list acl_out deny tcp any any
access-list acl_in deny udp any any

DMZ/LAN Mode



IMPORTANT NOTE:
The IP address assigned to the SIParator **MUST** publicly addressable. In many/most configurations, the network in the DMZ of the PIX is private. Therefore, network address translation is performed. However, there can only be one network on the DMZ of a PIX unless there is a router present. Therefore, that DMZ network **HAS** to be a publicly addressable network even though NAT will be performed to all components except the SIParator. (If the DMZ was a private network, the SIParator could not have a public address. The PIX would not be able to route packets to it)

For this example, assume the PIX has the following IP addresses assigned to its interfaces:
ip address outside 64.63.62.101 netmask 255.255.248.0
ip address inside 10.1.1.101 netmask 255.255.248.0
ip address dmz 31.32.33.254 netmask 255.255.248.0

The following entries are needed to allow the traffic to and from the SIParator without being NATed.
static (dmz,outside) 31.32.33.1 31.32.33.1 netmask 255.255.255.255 0 0
static (outside,dmz) 64.63.62.0 64.63.62.0 netmask 255.255.248.0 0 0

Create an Access Group for the external and DMZ interfaces
access-group acl_out in interface outside
access-group acl_dmz in interface dmz

Create access lists allowing traffic bi-directionally between the Internet and the SIParator. The following are examples of how these rules “could” be written.

Internet->DMZ
access-list acl_out permit udp any host 31.32.33.1 eq 5060
access-list acl_out permit udp any host 31.32.33.1 range 58024 60999
access-list acl_out permit udp any host 31.32.33.1 eq dnsix

SIParator->Outside
access-list acl_dmz permit udp host 31.32.33.1 any eq 5060
access-list acl_dmz permit udp host 31.32.33.1 any range 58024 60999
access-list acl_dmz permit udp host 31.32.33.1 any eq dnsix

Deny Lists (Following the “permits”, it is good to write a list of “denies”)

```
access-list acl_dmz deny udp any any
access-list acl_dmz deny tcp any any
access-list acl_out deny udp any any
access-list acl_out deny tcp any any
access-list acl_dmz deny udp any any
access-list acl_dmz deny tcp any any
```