PIX Firewall
IP Multicast Case Study

Peter Fyffe (pfyffe@cisco.com)

Cisco Advanced Services

Multicast Security – Firewalls

Unicast Firewalls

- Unicast

  Flows are inherently bidirectional.

  Firewall must be used to guard against unwanted connections that can "push" or "pull" traffic into/out of network.

  Prevented by the use "statefull" inspection of flows by the Firewall.

Multicast Firewalls

Flows are naturally "stateful" and unidirectional.

Traffic can only come into the network:

If requested by a host inside of the network.

Traffic can only go out of network:

If explicitly sent by a host inside of the network

AND

PIM Joins for the traffic are permitted to come into the network.

PIM Routers already perform these functions.

PIM-SM is a "stateful" protocol.

Uses the ip pim multicast boundary command to control incoming PIM Joins.

PIX Firewalls

- PIX Firewall v7.0

  Adds PIM support.

  No need to "tunnel" multicast and PIM Control traffic through PIX Firewall.

  Allows PIX to function as a PIM router.

  Provides "stateful" control of all multicast crossing Firewall boundary.

PIX Multicast Feature Summary

Multicast Support in PIXOS 7.0

IGMP Support

Stub multicast routing – IGMP Proxy Agent

IGMPv2

IGMP Access group

IGMP Limit

PIM Support

PIM Sparse Mode

Bidirectional PIM

DR Priority

Accept Register Filter

Multicast Source NAT

515, 525, 535 and ASA platforms

PIX Multicast Feature Summary (cont)

Multicast Support in PIXOS 7.2

Multicast Boundary with autorp filter

PIM Neighbor filters

PIM Bidir Neighbor filters

Future Support ?

IGMPv3/SSM
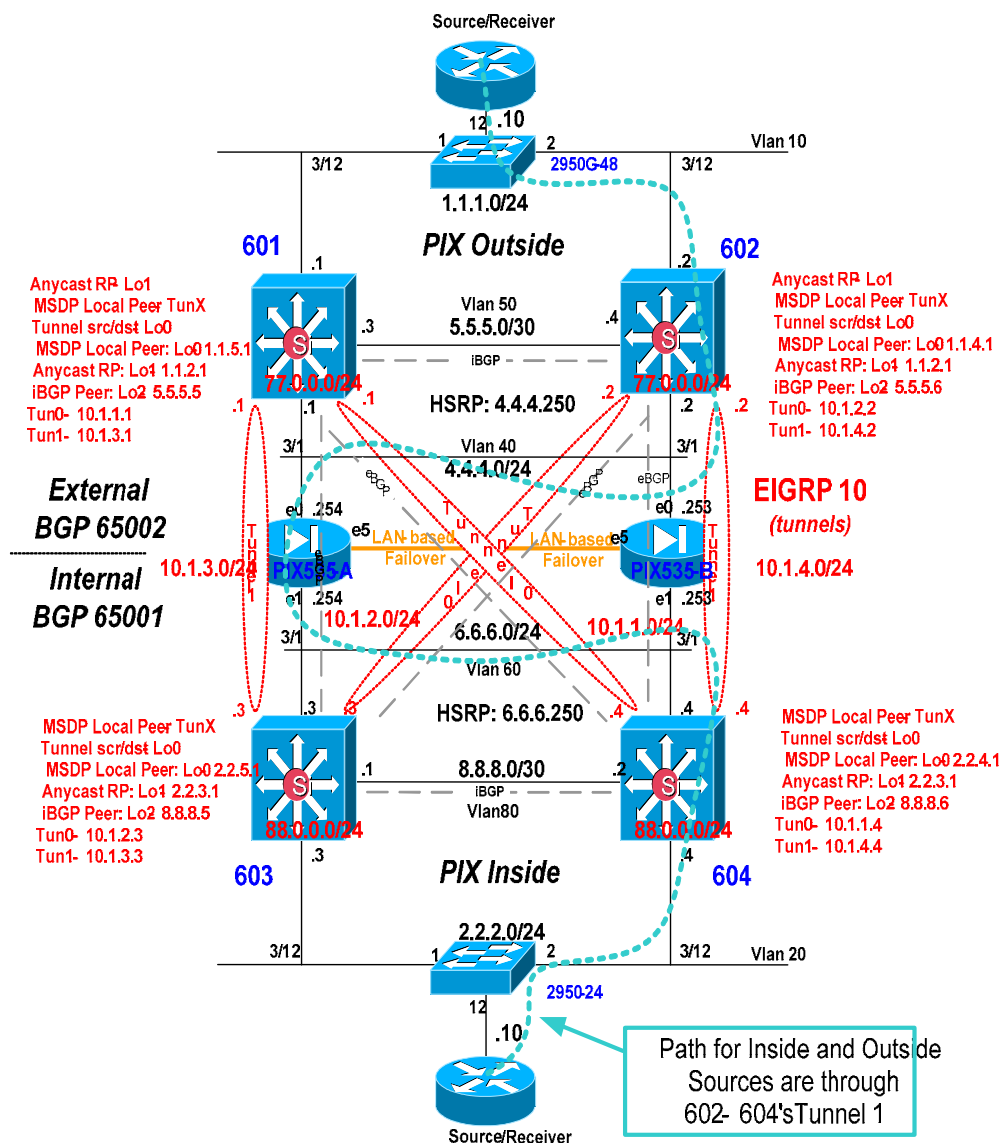
IPv6 Multicast

Stateful MSDP inspection

MSDP

FSWM 3.1 supports multicast similar to PIXOS 7.0

Multicast forwarding before native PIM support

Multicast forwarding using GRE Tunnels

Path for Inside and Outside Sources are through 602- 604'sTunnel 1

PIX Firewall Multicast Configuration

PIX Firewall configuration for IP Multicast

Enabling Multicast Routing

hostname(config)# multicast-routing

Rendezvous Point

hostname(config)# pim rp-address **ip_address [acl]** [bidir**]**

Static Mroutes

hostname(config)# mroute **src_ip src_mask input_if_name [distance]**

Forwarding IP Multicast

access-list <acl-out> extended permit udp host <source> host <group>

Note: **When multicast routing is configured on PIX Firewall, PIM and IGMP v2 are automatically enabled on all interfaces**