Title: Configuring Multicast Routing Over IPSEC VPN
Document Number:
Version: 1.0 , November 28, 2004
OS Ver. Screen OS 5.1r1
Author: Choh Mun Kok
HW Platforms this Paper Applies to: All Platforms
Audience (Internal or E xternal): Internal

Configuring Multicast Routing Over IPSEC VPN

Introduction
This document describes how to configure multicast routing protocol over the route base IPSEC VPN between two Juniper Netscreen devices. Two 5GT running Screen OS 5.1r1 were use in the lab configuration and testing.

The paper does not intend to describe the multicast routing protocol in details. You are encouraged to read the RFCs and other resources related to multicasting technology. This paper describes the basic configuration and the mode of operation supported by Screen OS. Netscreen devices supported IGMP version 1 to version 3 and PIM Sparse Mode only.

Concept
VPN Provide a secure mean of communicating two devices over a non-secure network such as the Internet, Frame Relay network or Wireless network.

Some of the common multicast applications are multimedia video and phone conferencing, real time stock ticker information, gaming and simulation.

Multicasting is method of sending traffic from one source to a group of nodes that interested in getting these traffics.

IGMP (Internet Group Management Protocol) is the protocol that manages the group memberships. I.e. joining or leaving the group. RFC 1112 describe IGMP V1, RFC 2236 describe IGMP v2.

Protocol Independent Multicast (PIM) is one of the multicast routing protocol that use to build multicast routing table for forwarding multicast traffic in IP networks. Other multicast routing protocol includes, DVMRP, MOSPF and MBGP. PIM can operate in dense mode or sparse mode. Some devices supported sparse-dense mode as well. Netscreen devices only support PIM sparse mode.

The IP addresses ranges from 224.0.0.0 to 239.255.255.255 are multicast IP addresses; 224.0.0.0 to 224.0.0.255 is reserved by IANA and is called link local address. Packets with these multicast addresses will always have the Time to Live (TTL) of 1. For example 224.0.0.5 and 224.0.0.6 are reserve to be use by

OSPF. Other reserve multicast address are 224.0.1.0 to 224.0.1.255 and 239.0.0.0 to 239.255.255.255.

224.0.0.13 is use to transport PIM control packets between PIM enable devices. 224.0.0.1 is use by IGMP to solicit group membership.

All multicast packets will have the first 24 bit MAC address prefix by 0x01:00:5e.

Multicast distribution tree describe the path taken by IP multicast traffic from the source to a group of destination hosts. In general, we have two type of tree,

- source tree (also call Shortest Path Tree) and
- Share Tree

In the SPT model, the source is always the root of the tree. For example, the following (S,G)notation, (192.168.3.1, 224.1.1.55) describe that the source IP is 192.168.3.1 and is sending the multicast traffic to the multicast group 224.1.1.55.

Share Tree use any point within the network as root. This root is called Rendezvous Point (RP). Thus the source must send its traffic to the RP before this traffic could reach the receivers. The common notation for this traffic is (*,G). * mean all sources and G represent the multicast group. RP could be anywhere within the network but in most cases it would be closet to the source.

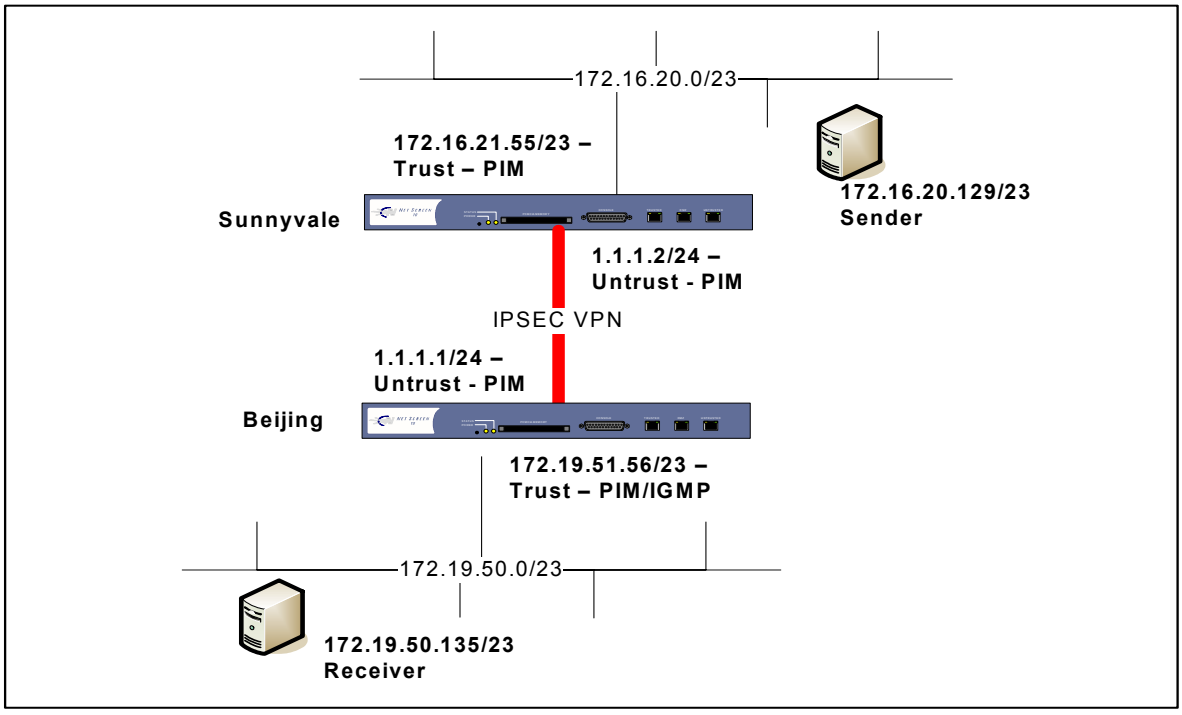
Reverse path forwarding is the mechanism to check the network path to reach the source IP address. Note that this process is opposite comparing to unicast routing mechanism. The unicast routing table is used to determine the incoming interface of the multicast traffic. Router will drop the packets if the RPF check is failed. Performing RPF check on each packet requires substantial router resources, thus it is common to perform the RPF on the first packet and RPF interface become the incoming interface. This information will be use to build the multicast routing table. There are more than one ways to determine the outgoing interface and is depend on the multicast routing protocol used. This information will be use by the multicast routing protocol such PIM to build the multicast routing table. Multicast routing table contain the information about the group, upstream, downstream, state and other related information.

IGMP proxy will enable the firewall to forward the multicast packet one hop beyond the local subnet. IGMP proxy can work without the use of PIM.

Example:
CLI: get vr trust proto pim mroute
[output from the receiving Netscreen]

(172.16.20.129/0, 225.0.0.37) 00:25:20/00:02:46 Flags: TLF
 Zone : Trust
 Upstream : tunnel.1 State : Joined
 RPF Neighbor : 172.16.21.55 Expires : 00:00:34
 Downstream :
 trust 00:07:26/- Join 0.0.0.0 172.16.20.129 FC

Network diagram



Configuration

The following describe the steps to configure both of the Nestcreen devices. Name the firewalls as Sunnyvale and Beijing. The multicast server is located behind the Sunnyvale firewall and the receiver is located behind the Beijing firewall.

Binding Interfaces into Zones

Interfaces will need to bind into its respective security zones.

Sunnyvale

```
set interf trust zone trust
set interf untrust zone untrust
```

Beijing

```
set interf trust zone trust
set interf untrust zone untrust
```

Assigning IP address to Interfaces

Sunnyvale

```
set interface trust ip 172.16.21.55/23
set interface untrust ip 1.1.1.2/24
```

Beijing

```
set interface trust ip 172.19.51.56/23
set interface untrust ip 1.1.1.1/24
```

Add default routes

Sunnyvale

```
set route  0.0.0.0/0 interface untrust gateway 1.1.1.1
```

Beijing

```
set route  0.0.0.0/0 interface untrust gateway 1.1.1.2
```

Build route base IPSEC tunnel

Sunnyvale

```
set interface "tunnel.1" zone "Trust"
set interface tunnel.1 ip unnumbered interface trust
set ike gateway "test" address 1.1.1.1 Main outgoing-interface "untrust" preshare
"hR5IC907NkImtbsDxxC09oWjZ2n2wW+FGQ==" sec-level standard
set vpn "test" gateway "test" no-replay tunnel idletime 0 sec-level standard
set vpn "test" monitor optimized rekey
set vpn "test" id 1 bind interface tunnel.1
set route  172.19.50.0/23 interface tunnel.1
```

Beijing

```
set interface "tunnel.1" zone "Trust"
set interface tunnel.1 ip unnumbered interface trust
set ike gateway "test" address 1.1.1.2 Main outgoing-interface "untrust" preshare
"2n9keJs4NT6A8Ksd3UCoZPbyLMnpytp9ZQ==" sec-level standard
set vpn "test" gateway "test" no-replay tunnel idletime 0 sec-level standard
set vpn "test" id 1 bind interface tunnel.1
set route  172.16.20.0/23 interface tunnel.1
```

Enable PIM on VR and interfaces

Sunnyvale

```
set interface Sunnyvale-> set vr trust
Sunnyvale(trust-vr)-> set proto pim
Sunnyvale(trust-vr/pim)-> set en
Sunnyvale(trust-vr/pim)-> end

set interface tunnel.1 protocol pim
set interface tunnel.1 protocol pim enable
set interface trust protocol pim
set interface trust protocol pim enable
```

Beijing

```
Beijing-> set vr trust
Beijing(trust-vr)-> set proto pim
Beijing(trust-vr/pim)-> set en
Beijing(trust-vr/pim)-> end

set interface tunnel.1 protocol pim
set interface tunnel.1 protocol pim enable
set interface trust protocol pim
set interface trust protocol pim enable
```

Enable IGMP on interface closet to receiver
Sunnyvale
No configuration needed

Beijing
set interface trust protocol igmp router
set interface trust protocol igmp enable

Add access list, and multicast policy
Sunnyvale
set vr trust
set access-list 5
set access-list 5 permit ip 224.0.0.0/4 1

** do not need if the traffic is intra zone and intra zone block if off*
set multicast-group-policy from "Trust" mgroup-list 5 to "Untrust" pim-message bsr-static-rp join-prune bi-directional

Beijing
set vr trust
set access-list 5
set access-list 5 permit ip 224.0.0.0/4 1

** do not need if the traffic is intra zone and intra zone block if off*
set multicast-group-policy from "Trust" mgroup-list 5 to "Untrust" pim-message bsr-static-rp join-prune bi-directional

Add RP
Sunnyvale
set vr trust
set proto pim
set zone "Trust" rp address 172.19.51.56 mgroup-list 5 always

Beijing
set vr trust
set proto pim
set zone "Trust" rp address 172.19.51.56 mgroup-list 5 always

Verification

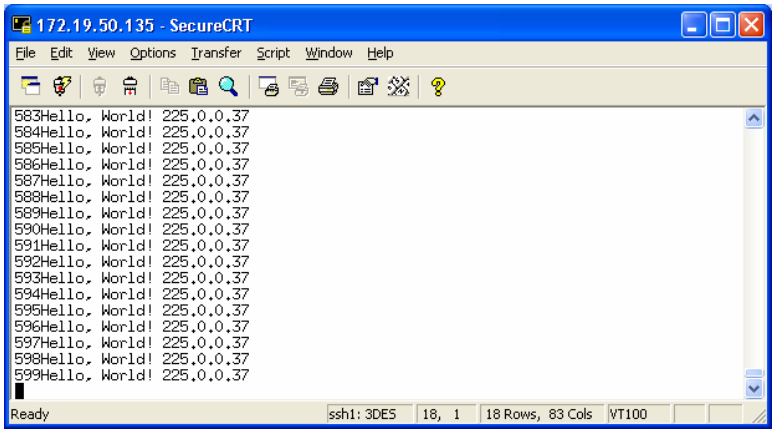
Testing tools

You can use any of the multicast applications such as IXIA or Microsoft Media Server to send multicast traffics across the firewalls. For the purpose of the lab test, we were using a much simplify tool running on Linux. Refer to Appendix-B on how to run this tool. This tool has two separate program, called sender and receiver, the sender will send "Hello, World" to the multicast group 225.0.0.37 and the receiver will join the multicast group. If the PIM and IGMP are configured correctly, the receiver should receive the message from the sender.

Example:

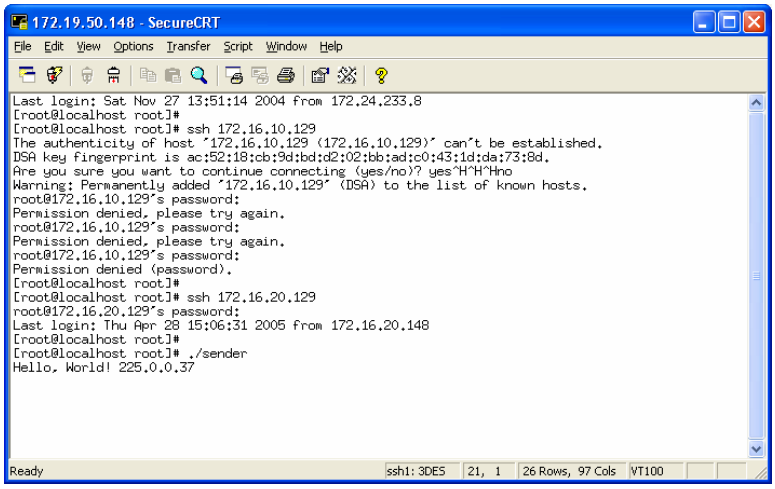
Receiver

The program is receiving multicast stream for the group 225.0.0.37



Sender

The sender is sending the word "Hello World" to the multicast group 225.0.0.37



Verify IGMP Group Joining

Screen OS command:	Get igmp group
Note:	The IGMP group should appear as one of the output. As in the example below, the multicast group 225.0.0.37 is learned from the interface trust and the client IP is 172.19.50.135

Example:

```
Beijing-> get igmp group
total groups matched: 3
multicast group interface        last reporter   expire ver query pkt   v1    v2    send
 224.0.0.2          trust        172.19.50.136    224s v2  ----- ----- -----  364s -----
 225.0.0.37         trust        172.19.50.135    227s v2  ----- ----- -----  367s -----
 239.255.255.254 trust           172.19.50.136    224s v2  ----- ----- -----  364s -----
Beijing->
```

Verify PIM operation

Screen OS command:	Get vr trust proto pim mroute
Note:	The multicast route, (172.16.20.129/23, 225.0.0.37) should appear in the output and the status is joined. The upstream and downstream interfaces are also identified.

```
Sunnyvale-> get vr trust proto pim mroute
trust-vr - PIM-SM routing table
------------------------------------------------------------------------
Register - R, Connected members - C, Pruned - P, Pending SPT Alert - G
Forward - F, Null - N , Negative Cache - E, Local Receivers - L
SPT - T, Proxy-Register - X, Imported - I, SGRpt state - Y, SSM Range Group - S
Turnaround Router - K
------------------------------------------------------------------------
Total PIM-SM mroutes: 2

(*, 225.0.0.37)  RP 172.19.51.56       00:04:50/-        Flags: E
  Zone          : Trust
  Upstream      : tunnel.1          State        : Not Joined
  RPF Neighbor  : 172.19.51.56      Expires      : -
  Downstream    :
  Null

(172.16.20.129/23, 225.0.0.37)        00:04:50/00:02:02  Flags: TF  Register Prune
  Zone          : Trust
  Upstream      : trust             State        : Joined
```

RPF Neighbor : local Expires : -
Downstream :
tunnel.1 00:04:50/00:03:09 Join 0.0.0.0 172.16.20.129 F

Sunnyvale->

Beijing-> get vr trust proto pim mroute
trust-vr - PIM-SM routing table

Register - R, Connected members - C, Pruned - P, Pending SPT Alert - G
Forward - F, Null - N , Negative Cache - E, Local Receivers - L
SPT - T, Proxy-Register - X, Imported - I, SGRpt state - Y, SSM Range Group - S
Turnaround Router - K

Total PIM-SM mroutes: 3

(*, 239.255.255.254) RP 172.19.51.56 21:23:39/- Flags: LF
Zone : Trust
Upstream : trust State : Joined
RPF Neighbor : local Expires : -
Downstream :
trust 21:23:39/- Join 0.0.0.0 FC

(*, 225.0.0.37) RP 172.19.51.56 00:07:18/- Flags: LF
Zone : Trust
Upstream : trust State : Joined
RPF Neighbor : local Expires : -
Downstream :
trust 00:07:18/- Join 0.0.0.0 FC

(172.16.20.129/0, 225.0.0.37) 00:04:04/00:02:16 Flags: TLF
Zone : Trust
Upstream : tunnel.1 State : Joined
RPF Neighbor : 172.16.21.55 Expires : 00:00:23
Downstream :
trust 00:04:04/- Join 0.0.0.0 172.16.20.129 FC

Sunnyvale-> get vr trust proto pim mroute
trust-vr - PIM-SM routing table

Register - R, Connected members - C, Pruned - P, Pending SPT Alert - G
Forward - F, Null - N , Negative Cache - E, Local Receivers - L
SPT - T, Proxy-Register - X, Imported - I, SGRpt state - Y, SSM Range Group - S
Turnaround Router - K

Total PIM-SM mroutes: 2

(*, 225.0.0.37) RP 172.19.51.56 00:04:50/- Flags: E
Zone : Trust

```
  Upstream       : tunnel.1          State        : Not Joined
  RPF Neighbor   : 172.19.51.56      Expires      : -
  Downstream     :
  Null

(172.16.20.129/23, 225.0.0.37)       00:04:50/00:02:02  Flags: TF  Register Prune
  Zone           : Trust
  Upstream       : trust             State        : Joined
  RPF Neighbor   : local             Expires      : -
  Downstream     :
  tunnel.1     00:04:50/00:03:09  Join        0.0.0.0          172.16.20.129 F

Sunnyvale->

Beijing-> get vr trust proto pim mroute
trust-vr - PIM-SM routing table
------------------------------------------------------------------------------
Register - R, Connected members - C, Pruned - P, Pending SPT Alert - G
Forward - F, Null - N , Negative Cache - E, Local Receivers - L
SPT - T, Proxy-Register - X, Imported - I, SGRpt state - Y, SSM Range Group - S
Turnaround Router - K
------------------------------------------------------------------------------
Total PIM-SM mroutes: 3

(*, 239.255.255.254)  RP 172.19.51.56  21:23:39/-        Flags: LF
  Zone           : Trust
  Upstream       : trust             State        : Joined
  RPF Neighbor   : local             Expires      : -
  Downstream     :
  trust       21:23:39/-       Join        0.0.0.0          FC

(*, 225.0.0.37)  RP 172.19.51.56      00:07:18/-        Flags: LF
  Zone           : Trust
  Upstream       : trust             State        : Joined
  RPF Neighbor   : local             Expires      : -
  Downstream     :
  trust       00:07:18/-       Join        0.0.0.0          FC

(172.16.20.129/0, 225.0.0.37)        00:04:04/00:02:16  Flags: TLF
  Zone           : Trust
  Upstream       : tunnel.1          State        : Joined
  RPF Neighbor   : 172.16.21.55      Expires      : 00:00:23
  Downstream     :
  trust       00:04:04/-       Join        0.0.0.0          172.16.20.129 FC

Beijing->
```

Verify PIM and IGMP is configured and enable on interfaces

Screen OS command:	Get interface <name>
Note:	Check if IGMP and PIM are enabled on the interfaces.

```
Sunnyvale-> get interf trust
Interface trust:
  number 2, if_info 176, if_index 0, mode nat
  link up, phy-link up/full-duplex
  vsys Root, zone Trust, vr trust-vr
  dhcp client disabled
  PPPoE disabled
  *ip 172.16.21.55/23   mac 0010.db7c.a022
  *manage ip 172.16.21.55, mac 0010.db7c.a022
  route-deny disable
  ping enabled, telnet enabled, SSH enabled, SNMP enabled
  web enabled, ident-reset disabled, SSL enabled
  DNS Proxy disabled, webauth disabled, webauth-ip 0.0.0.0
  OSPF disabled  BGP disabled  RIP disabled  mtrace disabled
  PIM: configured and enabled
  IGMP not configured
  bandwidth: physical 100000kbps, configured 0kbps, current 0kbps
          total configured gbw 0kbps, total allocated gbw 0kbps
  DHCP-Relay disabled
  DHCP-server enabled, status on.
Sunnyvale->
```

Verify PIM is enable on the VR

Screen OS command:	Get interface <name>
Note:	Check if PIM is enable on the VR.

```
Beijing-> get vr trust proto pim
PIM-SM enabled
Number of interfaces : 2
SPT threshold       : 1 Bps
PIM-SM Pending Register Entries Count : 0
Multicast group accept policy list: not set

Virtual Router trust-vr - PIM RP policy
-----------------------------------------------
Group Address      RP access-list

Virtual Router trust-vr - PIM source policy
-----------------------------------------------
Group Address      Source access-list
Beijing->
```

Verify multicast traffic flow

Screen OS command:	Get session
Note:	Check if the session using the multicast group is created successfully.

```
Sunnyvale-> get sess
alloc 8/max 2064, alloc failed 0, mcast alloc 4, di alloc failed 0
id 4/s**,vsys 0,flag 00001040/0882/21,policy 320002,time 178, dip 0
 20(0601):172.19.51.56/1->224.0.0.13/1,103,000000000000,2,vlan 0,tun 40000001,vsd 0,route 0
 3(0010):172.19.51.56/1<-224.0.0.13/1,103,000000000000,4,vlan 0,tun 0,vsd 0,route 0
id 60/s**,vsys 0,flag 00401040/0882/21,policy 320002,time 177, dip 0
 20(0601):172.19.51.56/1->172.16.21.55/1,103,000000000000,2,vlan 0,tun 40000001,vsd 0,route 0
 3(0010):172.19.51.56/1<-172.16.21.55/1,103,000000000000,4,vlan 0,tun 0,vsd 0,route 0
id 586/s**,vsys 0,flag 00000040/0020/00,policy 320002,time 6, dip 0
 2(a001):172.16.20.129/32795->225.0.0.37/12345,17,000102353cbe,2,vlan 0,tun 0,vsd 0,route 0
 20(2000):172.16.20.129/32795<-225.0.0.37/12345,17,000000000000,2,vlan 0,tun 40000001,vsd 0,route 121005448
id 587/s**,vsys 0,flag 00000050/0020/01,policy 320002,time 1, dip 0
 2(a001):172.16.20.129/32795->225.0.0.37/12345,17,000102353cbe,2,vlan 0,tun 0,vsd 0,route 0
 20(2000):255.255.255.255/32795<-255.255.255.255/12345,17,000000000000,2,vlan 0,tun 40000001,vsd 0,route 121005448
id 588/s**,vsys 0,flag 00000040/0020/00,policy 320002,time 6, dip 0
 2(a001):172.16.20.129/32795->225.0.0.37/12345,17,000102353cbe,2,vlan 0,tun 0,vsd 0,route 0
 20(2000):172.16.20.129/32795<-225.0.0.37/12345,17,000000000000,2,vlan 0,tun 40000001,vsd 0,route 121005448
id 589/s**,vsys 0,flag 00000040/0020/01,policy 320002,time 6, dip 0
 2(a001):172.16.20.129/32795->225.0.0.37/12345,17,000102353cbe,2,vlan 0,tun 0,vsd 0,route 0
 20(2000):255.255.255.255/32795<-255.255.255.255/12345,17,000000000000,2,vlan 0,tun 40000001,vsd 0,route 121005448
Total 6 sessions shown
Sunnyvale->
```

Limitation

The current multicast implementation does not map well into the hub and spoke base VPN networks. In the hub and spoke base VPN network, the hub would have many VPN connections to the spoke networks. Assume that the sender is located behind the hub firewall (5GT); it can only serve two of the spoke networks via the IPSEC tunnels concurrently. You can use the following command to check the maximum output interfaces for each platform.

```
Beijing-> get sys-cfg | i out
default period of timeout in cryptlib number: 200
max Multicast routing table owners number: 2
max output interfaces in multicast route number: 2
```

Troubleshooting

Debugging RP issue

Screen OS command:	Debug pim all
Note:	Receiver not able to received data from sender. On the debug output below, note that the RP for the group in 225.0.0.37 is not found. RP is configuring on per zone basis. On the example below the RP is configured on Trust zone but the receiver is located in the DMZ zone.

```
## 16:24:23 : trust-vr: PIMSM IGMP Group Info enqueued to PIM task
## 16:24:23 : trust-vr: PIMSM IGMP Event sent to PIM from IP
## 16:24:23 : IGMP: 225.0.0.37 create group_membership_timer on ethernet2
## 16:24:24 : PIMSM: Received events 50
## 16:24:24 : trust-vr: PIMSM IGMP Grp Specific msg Grp Join for G=225.0.0.37 received on
ethernet2
## 16:24:24 : trust-vr: PIMSM No Group Entry for 225.0.0.37 zone=DMZ
## 16:24:24 :                restore the sources pruned from the shared path
## 16:24:24 : trust-vr: PIMSM Process IGMP Join for G=225.0.0.37 on ifp=ethernet2
## 16:24:24 : trust-vr: PIMSM Group RPSet is not available
## 16:24:24 : trust-vr: PIMSM Static Group RPSet is not available
## 16:24:24 : trust-vr: PIMSM RP for group 225.0.0.37 not found in zone DMZ
## 16:24:24 : trust-vr: PIMSM No Group Entry for 225.0.0.37 zone=DMZ
## 16:24:24 : trust-vr: PIMSM zone DMZ No 225.0.0.37 Grp entry
## 16:24:24 : trust-vr: PIMSM  Destination Address is Zero
## 16:24:24 : trust-vr: PIMSM No Group Entry for 225.0.0.37 zone=DMZ
## 16:24:24 : trust-vr: PIMSM zone DMZ No 225.0.0.37 Grp entry
## 16:24:24 : trust-vr: PIMSM Group RPSet is not available
## 16:24:24 : trust-vr: PIMSM Static Group RPSet is not available
```

Debugging policy issue

Screen OS command:	Debug flow basic
Note:	Packet dropped denied by policy

```
Beijing-> get db str
****** 212779.0: <Untrust/untrust> packet received [104]******
  ipid = 26525(679d), @03c29b50
  packet passed sanity check.
  untrust:1.1.1.2/15519->1.1.1.1/37195,50<Root>
  existing session found. sess token 3
  flow got session.
  flow session id 1
  flow_decrypt: pipeline.
  Dec: SPI=3c9f914b, Data=104
  SA tunnel id=0x00000001, flag<00002063>
chip info: PIO. Tunnel id 00000001
ipsec decrypt prepare done
ipsec decrypt set engine done
  auth check pass!
ipsec decrypt engine released
  packet is decrypted
ipsec decrypt done
        put packet(3e126dc) into flush queue.
        remove packet(3e126dc) out from flush queue.

**** jump to packet:172.16.20.129->225.0.0.37
  tunnel.1:172.16.20.129/32795->225.0.0.37/12345,17<Root>
  chose interface tunnel.1 as incoming nat if.
  mcast packet. search mroute
  found mroute entry:
  mcast pak to out if: trust, mgroup 0.0.0.0
mcast pak, create session to trust
  policy search from zone 2-> zone 2
  No SW RPC rule match, search HW rule
  Searching global policy.
  packet dropped, deny by zone block
  packet dropped, null policy.

  **** pak processing end.
```

Debugging policy issue

Screen OS command:	Debug flow basic
Note:	Packet dropped, the multicast route do not have outgoing interface. Review the PIM/IGMP related configuration and Clear the multicast routing table. *clear vr <name> proto pim mroute all*

****** 78641.0: <Trust/trust> packet received [52]******
ipid = 0(0000), @03ca6d50
packet passed sanity check.
trust:172.16.20.129/32795->225.0.0.37/12345,17<Root>
chose interface trust as incoming nat if.
mcast packet. search mroute
found mroute entry:
packet dropped, mcast pak, no out if found

Debugging PIM and IGMP

Screen OS command:	Debug PIM all, Debug IGMP all, clear vr <name> proto pim mroute
Note:	There are a lot of data need to be analyzed. Some of the sample output is shown as below. If you think that all of the PIM/IGMP configuration is configured correctly, try to clear the mroute on all of the firewall. You may also need to restart the IGMP client if the client did not retry to re-join the group.

Sample PIM Hello trace

10:45:08 : trust-vr: PIMSM rx queued src=172.16.21.55 dst=224.0.0.13 ifp=tunnel.1
10:45:08 : PIMSM: Control packet enqueued to PIM task
10:45:08 : PIMSM: Control packet Event has been sent to PIM from IP
10:45:08 : PIMSM: Received events 40
10:45:08 : trust-vr: PIMSM Rx'ed PIM pkt 172.16.21.55->224.0.0.13 ver=2, type=hello, len=26
10:45:08 : trust-vr: PIMSM Hello received on tunnel.1 from 172.16.21.55
10:45:08 : NbrTimer restarted for 105 Sec
Beijing->

Sample Register message

10:45:24 : PIMSM: Control packet Event has been sent to PIM from IP
10:45:24 : PIMSM: Received events 40
10:45:24 : trust-vr: PIMSM Rx'ed PIM pkt 172.16.21.55->172.19.51.56 ver=2, type=register, len=28
10:45:24 : trust-vr: PIMSM rx'ed register from DR=172.16.21.55 ,RP=172.19.51.56, for G=225.0.0.37 S=172.16.20.129 on ifp trust
10:45:24 : trust-vr: PIMSM Group RPSet is not available
10:45:24 : trust-vr: PIMSM rx'ed null register from DR
10:45:24 : trust-vr: PIMSM Group RPSet is not available
10:45:24 : trust-vr: PIMSM zone Trust is static RP for group 225.0.0.37
10:45:24 : trust-vr: PIMSM Found (S,G) route S=172.16.20.129, G=225.0.0.37, ownerzone Trust
10:45:24 : trust-vr: PIMSM Register Stop Rate limit flag not set
10:45:24 : trust-vr: PIMSM Tx'ed PIM pkt 172.19.51.56->172.16.21.55, register stop, len=18
10:45:24 : trust-vr: PIMSM Sent Register Stop Message to DR 172.16.21.55
10:45:24 : trust-vr: PIMSM Register Stop rate limit timer is started
10:45:25 :

Summary
The multicast feature on Screen OS5.1 provides the ability to pass multicast traffic through the firewall configure in either route mode or NAT mode. Two simplify test are presented in this paper to provide the basic understanding about how to configure the multicast feature available on Screen OS.

Appendixes

Appendix A: Useful URL

Appendix B: Using the lab multicast tool

Appendix C: Using IGMP Proxy and IGMP Host

Appendix A: Useful URL

http://www.juniper.net/techpubs/software/screenos/screenos5.1.0/CE_v6.pdf
http://www.cisco.com/en/US/tech/tk828/tech_brief09186a00800a4415.html
http://www.juniper.net/solutions/literature/app_note/350034.pdf

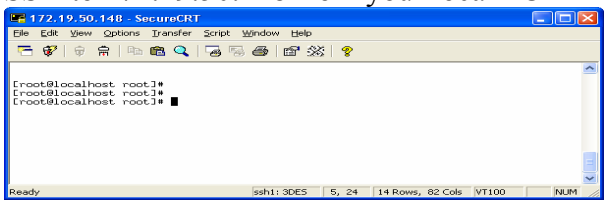
Appendix B: Using the lab multicast tool

Username: root
Password: netscreen

In order to use the multicast tool, the sender must be configure to VLAN 400 and the receiver must be configure to VLAN 200.

Step 1 – Start to send multicast packet to the network

- SSH to 172.19.50.148 from your local PC



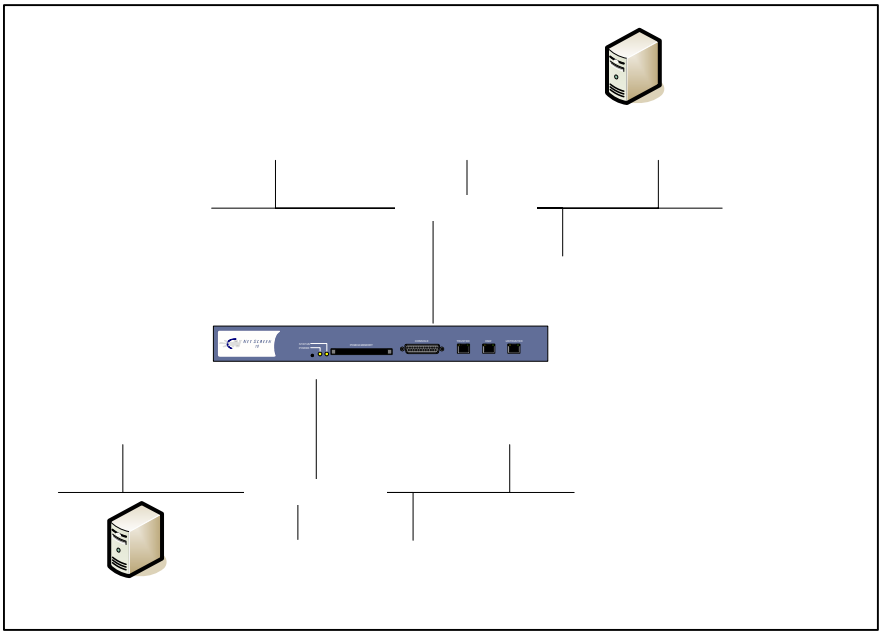
- SSH from 172.19.50.148 to 172.16.20.129
    - [root@localhost root]# ssh 172.16.20.129
- Start the multicast program; this will start the sending process to multicast group 225.0.0.37.
    - [root@localhost root]# sender
    - Hello, World! 225.0.0.37

Step 2 – Start the receiver

- SSH to 172.19.50.135
- Start the multicast receiver program;
    - [root@jasmine ckok]# receiver
    - 1Hello, World! 225.0.0.37
    - 2Hello, World! 225.0.0.37
    - 3Hello, World! 225.0.0.37
- If either the PIM and IGMP proxy is configured correctly. You should receive the work “nHello, World! 225.0.0.37” where n is the incremental numeric value.

Appendix C: Using IGMP Proxy and IGMP Host

Network Diagram



Configuration

set vrouter "trust-vr"
set access-list 5
set access-list 5 permit ip 224.0.0.0/4 5

set interface trust protocol igmp router
set interface trust protocol igmp proxy
set interface trust protocol igmp enable
set interface untrust protocol igmp host
set interface untrust protocol igmp enable
set multicast-group-policy from "Trust" mgroup-list 5 to "Untrust" igmp-message

set policy id 1 from "Trust" to "Untrust" "Any" "Any" "ANY" permit
set policy id 2 from "Untrust" to "Trust" "Any" "Any" "ANY" permit log

172.16.21.10
Untrust – IG
Host

Lab-5GT-01

Verification

Check the session table

```
Lab-5GT-01-> get sess
alloc 2/max 4064, alloc failed 0, mcast alloc 2, di alloc failed 0
id 115/s**,vsys 0,flag 00000040/0020/00,policy 2,time 6, dip 0
 1(a801):172.16.20.129/32798->225.0.0.37/12345,17,000102353cbe,3,vlan 0,tun 0,vsd
0,route 0
 2(2800):172.16.20.129/32798<-225.0.0.37/12345,17,000000000000,2,vlan 0,tun 0,vsd
0,route 121066544
id 116/s**,vsys 0,flag 00000040/0020/01,policy 2,time 6, dip 0
 1(a801):172.16.20.129/32798->225.0.0.37/12345,17,000102353cbe,3,vlan 0,tun 0,vsd
0,route 0
 2(2800):255.255.255.255/32798<-255.255.255.255/12345,17,000000000000,2,vlan
0,tun 0,vsd 0,route 121066544
Total 2 sessions shown
Lab-5GT-01->
```

Check the multicast routing table

Note the following two commands are different

- Get vr trust protocol pim mroute

  Example:

```
Lab-5GT-01-> get vr trust protocol pim mroute
PIM instance not configured in vrouter (trust-vr)
Lab-5GT-01->
```

- Get vr trust mroute

  Example:

```
Lab-5GT-01-> get vr trust mroute
 Flags:   P - PIM, S - Static, I - IGMP-Proxy
          F - Forwarding, U - Pruned, D - Down, B - Backup, T - Registering
          N - Negative Cache, M - Dummy route (Iif in another virtual router)
 Virtual router: trust-vr
 ---------------------------------------------------------------------------
 Total multicast routes : 4/system-max

 (*, 239.255.255.254)          06:19:31    RPF: 0.0.0.0        I
   Input Interface  : untrust              zone: Untrust
   Output Interfaces:
    zone       group          interface     source        uptime     flags
    Trust      239.255.255.254 trust         0.0.0.0       06:19:31   IF

 (172.16.20.129, 225.0.0.37)    00:17:37    RPF: 0.0.0.0        I
   Input Interface  : untrust              zone: Untrust
   Output Interfaces:
    zone       group          interface     source        uptime     flags
```

```
  Trust      225.0.0.37      trust         172.16.20.129  00:17:37   IF

(*, 225.0.0.37)              00:17:38   RPF: 0.0.0.0        I
  Input Interface  : untrust             zone: Untrust
  Output Interfaces:
   zone       group          interface     source        uptime     flags
   Trust      225.0.0.37      trust         0.0.0.0       00:17:38   IF

(*, 224.0.0.2)               06:19:33   RPF: 0.0.0.0        I
  Input Interface  : untrust             zone: Untrust
  Output Interfaces:
   zone       group          interface     source        uptime     flags
   Trust      224.0.0.2       trust         0.0.0.0       06:19:33   IF
```