Application Note

Calm During the Storm

Best Practices in Multicast Security

Lenny Giuliano

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
408 745 2000 or 888 JUNIPER
www.juniper.net

Part Number: 350051-001

Contents

Introduction

Multicast has changed the way business is conducted on the Internet by enabling many-to-many communications for applications such as distance learning and virtual business meetings. Security has been an obstacle to multicast's widespread acceptance and is the focus of this paper.

Internet multicast introduces a range of new security concerns to a network. JUNOS software offers the most comprehensive set of features in the industry for securing a multicast infrastructure. This expertise comes from lessons learned after more than six years of deployment experience in the world's largest Internet backbones. The following is a detailed set of recommended best practices for securing a multicast infrastructure of Juniper routers.

Calm During the Storm

The range of new security concerns that the deployment of Internet multicast brings to a network are not necessarily any more or less destructive than those found in unicast-only networks, but they represent a new class of threat that may be unfamiliar to those with minimal multicast experience. The following is a detailed set of recommended best practices for securing a multicast infrastructure of Juniper routers.

Originally, multicast deployment recommendations focused on filtering certain groups that should not be leaked in or out of a network. Some of these groups are protocol related, some are from legacy applications, and some are administratively scoped. Examples of these groups include:

224.0.1.2/32	SGI-Dogfight
224.0.1.3/32	RWHOD
224.0.1.8/32	SUN-NIS
224.0.1.22/32	SRVLOC
224.0.1.24/32	MICROSOFT-DS
224.0.1.25/32	NBC-PRO
224.0.1.35/32	SVRLOC-DA
224.0.1.39/32	AUTORP-Announce
224.0.1.40/32	AUTORP-Discovery
224.0.1.60/32	HP-Device-Discovery
224.0.2.1/32	RWHO
224.0.2.2/32	SUN-RPC
224.77.0.0/16	Norton-Ghost
226.77.0.0/16	Norton-Ghost
225.1.2.3/32	Altiris
229.55.150.208/32	Norton-Ghost
234.42.42.40/30	Phoenix/StorageSoft ImageCast
239.0.0.0/8	Administratively Scoped

This list gets added to periodically as providers find traffic floating around that shouldn't be on the Internet. You can find the updated list of inappropriate group addresses in the Internet Engineering Task Force (IETF) Internet draft document, "draft-ietf-mboned-ipv4-mcast-bcp".

Over the last few years, the primary threat seen on multicast networks has been Multicast Source Discovery Protocol (MSDP) storms. Internet worms, such as Ramen, Slammer, Sasser, etc, have most often caused these storms. Typically, these worms infect a host and propagate by using these infected hosts to discover and attack other vulnerable hosts. To discover other vulnerable hosts, they usually select a large block of addresses (such as a /16) at random, and port scan all hosts in that block. In just a few minutes, these infected hosts can scan up to tens or even hundreds of thousands of other hosts.

The coders of these worms often randomly select any IP address range, inadvertently including IP multicast addresses (224/4) in the possible range. When packets are transmitted with a destination address in 224/4 on a multicast-enabled network, multicast protocols use this data to drive the creation of a multicast state. For example, when a Protocol Independent Multicast-Sparse Mode (PIM-SM) router detects one of its locally connected hosts is transmitting multicast packets, it will encapsulate these packets in PIM register messages, and send these messages to the PIM-SM Rendezvous Point (RP), which will keep state of these local sources. The RP then creates an MSDP Source Address (SA) message for each source-group pair and floods it to all of its MSDP peers, which cache these messages and flood to all their respective peers, until MSDP speakers across the Internet have populated their SA caches. In this way, a single infected host that port scans only a single /16 of multicast addresses will generate over 65,000 MSDP SAs that are flooded and cached by all MSDP speaking routers on the Internet. As more hosts attack, and/or scan larger blocks of multicast addresses, this state explosion quickly causes MSDP speaking routers to run out of memory and crash. This attack, which is not even launched to intentionally affect the multicast infrastructure, is known as an MSDP SA storm. These storms are quite easy to launch and have been by far the most common type of attack seen on multicast networks to date.

Juniper has introduced a number of features in its implementation of MSDP to mitigate and even eliminate the damage caused by MSDP storms. These features will be described extensively in the following sections. Additionally, it should be noted that the damage done by MSDP storms is primarily "accidental". That is, attackers have damaged critical components of the network infrastructure without even targeting these components. Juniper recommends a two-fold approach to hardening a multicast deployment. First, by enabling features that will reduce or eliminate the damage caused by attacks, and second, by reducing the size of the target for accidental attacks by using the concept of "whitelisting".

The most common use of filtering in network security involves "blacklists". Blacklists simply contain a list of hosts or services that need to be denied, while all other hosts or services are permitted. Whitelists, on the other hand, contain a list of hosts or services that are permitted, while all other hosts or services are denied. So blacklists "allow everything except this list", while whitelists "block everything except this list".

Per Request for Comment 3171, the Internet Assigned Numbers Authority (IANA) has allocated addresses for global use only from the 224/8, 232/8 and 233/8 address ranges. Multicast groups outside of this range can be considered reserved from global use, and there is no legitimate reason to see this traffic on the Internet. Accordingly, Juniper strongly recommends only allowing forwarding and control traffic for groups in these whitelisted ranges. By permitting only 3/16 of the possible multicast address range to be routed, 81% of the accidental attacks should be prevented.

These recommendations assume static anycast RP is the RP-mapping mechanism used. An in-depth discussion of the operation of PIM-SM and MSDP is outside of the scope of this document. Additionally, for full documentation on the JUNOS commands listed, consult the JUNOS Multicast manual, "JUNOS Internet Software for J-series, M-series, and T-series Routing Platforms Multicast Protocols Configuration Guide" at http://www.juniper.net/techpubs/software/junos.

Throttling Multicast Source Discovery Protocol

The obvious solution to preventing damage caused by MSDP storms is to rate limit. However, whenever you rate limit control traffic, you inadvertently introduce new vulnerability since it is usually impossible to tell the difference between a good control message and a bad one. For example, if you blindly rate limit all MSDP (TCP port 639) traffic to 1 Mbps, you simply lower the bar for attack. An attacker must only send 1 Mbps of MSDP traffic to engage the rate limiter and all legitimate MSDP traffic is also blocked. Therefore, it is crucial that rate limiting is as intelligent as possible to deny the malicious, but permit the legitimate.

Per-Source Limits

The most important feature in realizing intelligent rate limiting is per-source SA limits. Per-source limits prevent an MSDP speaker from allowing any single host to generate more than a configured maximum number of SAs. For example, a per-source limit of 1,000 will not allow any individual host to generate more than 1,000 SAs. A worm infected host that port scanned a /16 of multicast addresses would then only generate 1,000 SAs instead of over 65,000. The configuration includes both a maximum and a threshold. SAs are randomly dropped using the Random Early Detection (RED) algorithm once they exceed the threshold value. MSDP per-peer and per-instance rate limits use the same "threshold" and "maximum" syntax and behavior.

It is difficult to imagine a host that legitimately sources more than 1,000 multicast streams. In the event that there are known hosts that legitimately transmit more than 1,000 multicast streams, these sources can be given larger limits. The following configuration allows the host 10.1.1.1 to generate up to 5,000 MSDP SAs, while all other hosts on the Internet are rate limited to 1,000 SAs.

```
msdp {
  source 0.0.0.0/0 {
    active-source-limit {
      maximum 1000;
      threshold 900;
     }
   }
   source 10.1.1.1/32 {
       active-source-limit {
         maximum 5000;
         threshold 4500;
        }
    }
}
```

To see the per-source limits as they apply to all known multicast sources, use the "show msdp source" command:

```
lenny@paix> show msdp source
Source address   /Len  Type        Maximum  Threshold  Exceeded
0.0.0.0           /0    Configured  1000     900        0
10.0.32.32       /32    Dynamic     1000     900        0
10.14.59.8       /32    Dynamic     1000     900        0
10.14.59.57      /32    Dynamic     1000     900        1243
10.39.0.144      /32    Dynamic     1000     900        0
10.89.2.245      /32    Dynamic     1000     900        13
```

To see only the hosts that exceed the per-source limits, use the "show msdp source | except "\ 0" regular expression:

```
lenny@paix> show msdp source | except "\ 0"
Source address   /Len   Type        Maximum  Threshold   Exceeded
10.14.68.99      /32    Dynamic     1000     900         81099693
10.51.171.149    /32    Dynamic     1000     900         540763
10.88.60.37      /32    Dynamic     1000     900         9080
10.88.176.175    /32    Dynamic     1000     900         1144711
10.58.5.249      /32    Dynamic     1000     900         425
```

Per-Peer Limits

Per-peer SA limits rate limit the number of SAs received from an MSDP peer. These limits are functionally analogous to Border Gateway Protocol (BGP) max-prefix limits. The following configuration prevents the router from accepting more than 100,000 SAs from peer 1.1.1.1.

```
msdp {
  group eMSDP-peer {
      local-address 2.2.2.2;
      peer 1.1.1.1 {
            active-source-limit {
               maximum 100000;
               threshold 90000;
             }
        }
    }
}
```

To apply the same per-peer limit to all MSDP peers, use apply groups.

Per-Instance Limits

Per-instance limits are the maximum number of SAs that a router allows in the entire routing instance. The following configuration prevents the router from installing more than 200,000 SAs in its default routing instance.

```
msdp {
       active-source-limit {
           maximum 200000;
           threshold 190000;
        }
  }
```

Disabling Multicast Source Discovery Protocol Data Encapsulation

In order to support bursty sources, MSDP SAs may also contain actual multicast data packets. Typically, the first packet in a multicast stream is added to the SA. MSDP SAs are placed in inet.4, the routing table that contains the MSDP SA cache. Additionally, SAs that include encapsulated data are placed in the forwarding table. The forwarding table generally has less capacity than the routing table. Therefore, it is recommended to prevent the creation of unnecessary forwarding table entries, as the forwarding table is a finite resource that also contains all the unicast forwarding entries. The following configuration prevents originating RPs from placing encapsulated data in SAs and ignores the encapsulated data in SAs received by peers. This sample configuration prevents forwarding table entries from being created by MSDP. Note, however, that the configuration may have an impact on bursty source applications such as when one multicast packet is transmitted every 20 minutes by the source. If support for bursty source applications is critical, leave MSDP data encapsulation enabled.

```
  msdp {
   data-encapsulation disable;
}
```

Multicast Source Discovery Protocol Filters

It is important to apply MSDP SA filters on all external MSDP sessions, inbound and outbound. MSDP SA filters will prevent SAs for groups and sources that should remain inside a network from leaking in or out. At a minimum, these filters should be applied to all external MSDP peerings. The following configuration will prevent SAs (for sources and groups that do not belong on the Internet) from being transmitted or received by all MSDP peers.

```
protocols {
       msdp {
               export sa-filter;
               import sa-filter;
       }
}
 policy-options {
                    policy-statement sa-filter {
                          term bad-groups {
                                 from {
                                       route-filter 224.0.1.2/32 exact;
                                       route-filter 224.0.1.3/32 exact;
                                       route-filter 224.0.1.8/32 exact;
                                       route-filter 224.0.1.22/32 exact;
                                       route-filter 224.0.1.24/32 exact;
                                       route-filter 224.0.1.25/32 exact;
                                       route-filter 224.0.1.35/32 exact;
                                       route-filter 224.0.1.39/32 exact;
                                       route-filter 224.0.1.40/32 exact;
                                       route-filter 224.0.1.60/32 exact;
                                       route-filter 224.0.2.1/32 exact;
                                       route-filter 224.0.2.2/32 exact;
                                       route-filter 224.77.0.0/16 orlonger;
                                       route-filter 226.77.0.0/16 orlonger;
                                       route-filter 225.1.2.3/32 exact;
                                       route-filter 229.55.150.208/32 exact;
                                       route-filter 232.0.0.0/8 orlonger;
                                       route-filter 234.42.42.40/30 orlonger;
                                       route-filter 239.0.0.0/8 orlonger;
                                }
                                then reject;
                           }
                          term bad-sources {
                                 from {
                                        source-address-filter 10.0.0.0/8 orlonger;
                                        source-address-filter 127.0.0.0/8 orlonger;
                                        source-address-filter 172.16.0.0/12 orlonger;
                                        source-address-filter 192.168.0.0/16 orlonger;
                                }
                                then reject;
                          }
                          term accept-everything-else {
                               then accept;
                          }
                    }
               }
```

Multicast Boundaries

Apply multicast boundary filters on all customer-facing interfaces by using multicast scoping. Multicast scoping prevents multicast packets from flowing into or out of an interface. Apply these scopes on all interfaces and on all routers in your network, since there is usually no good reason for these groups to flow on backbone links. The following configuration prevents multicast data packets from flowing into or out of all interfaces on the router for groups that do not belong on the Internet. This configuration also permits data packets in 239/8 to flow over backbone links, which is necessary on networks that allow 239/8-traffic for internal purposes.

```
routing-options {
    multicast {
         scope-policy boundary-filter;
    }
}
policy-options {
    policy-statement boundary-filter {
        term permit-239-on-backbone {
             from {
                  interface [ so-0/0/0.0 so-1/0/0.0 ];
                  route-filter 239.0.0.0/8 orlonger;
             }
             then accept;
        }
        term bad-groups {
             from {
                 route-filter 224.0.1.2/32 exact;
                 route-filter 224.0.1.3/32 exact;
                 route-filter 224.0.1.8/32 exact;
                 route-filter 224.0.1.22/32 exact;
                 route-filter 224.0.1.24/32 exact;
                 route-filter 224.0.1.25/32 exact;
                 route-filter 224.0.1.35/32 exact;
                 route-filter 224.0.1.39/32 exact;
                 route-filter 224.0.1.40/32 exact;
                 route-filter 224.0.1.60/32 exact;
                 route-filter 224.0.2.1/32 exact;
                 route-filter 224.0.2.2/32 exact;
                 route-filter 224.77.0.0/16 orlonger;
                 route-filter 226.77.0.0/16 orlonger;
                 route-filter 225.1.2.3/32 exact;
                 route-filter 229.55.150.208/32 exact;
                 route-filter 234.42.42.40/30 orlonger;
                 route-filter 239.0.0.0/8 orlonger;
            }
            then reject;
         }
         term accept-everything-else {
             then accept;
         }
     }
  }
```

Protocol Independent Multicast Bootstrap Router Filters

It is extremely important to make sure Bootstrap Router Filter (BSR) messages do not leak into or out of your network. The following configuration prevents BSR messages from getting into or out of a router. Use this configuration on all routers.

```
protocols {
    pim {
        rp {
            bootstrap-import no-bsr;
            bootstrap-export no-bsr;
        }
    }
}
policy-options {
    policy-statement no-bsr {
        then reject;
    }
}
```

Protocol Independent Multicast Join Filters

Multicast scopes prevent multicast data packets from flowing into or out of an interface. PIM join filters prevent the creation of PIM-SM state so multicast traffic is not transmitted across your network and dropped at a scope at the edge. Also, PIM join filters reduce the potential for denial-of-service (DOS) attacks and PIM state explosion. PIM join filters only apply to PIM-SM state. If you use them, apply them to all routers in your network. The following configuration will reject PIM joins sent by neighbors for groups that do not belong on the Internet. This same configuration permits PIM joins to flow over backbone links, which is necessary on networks that allow 239/8 traffic for internal purposes.

```
protocols {
    pim {
        import pim-join-filter;
    }
}
policy-options {
    policy-statement pim-join-filter {
        term permit-239-on-backbone {
            from {
                interface [ so-0/0/0.0 so-1/0/0.0 ];
                route-filter 239.0.0.0/8 orlonger;
            }
            then accept;
        }
        term bad-groups {
            from {
                route-filter 224.0.1.2/32 exact;
                route-filter 224.0.1.3/32 exact;
                route-filter 224.0.1.8/32 exact;
                route-filter 224.0.1.22/32 exact;
                route-filter 224.0.1.24/32 exact;
                route-filter 224.0.1.25/32 exact;
                route-filter 224.0.1.35/32 exact;
                route-filter 224.0.1.39/32 exact;
                route-filter 224.0.1.40/32 exact;
                route-filter 224.0.1.60/32 exact;
                route-filter 224.0.2.1/32 exact;
                route-filter 224.0.2.2/32 exact;
                route-filter 224.77.0.0/16 orlonger;
                route-filter 226.77.0.0/16 orlonger;
                route-filter 225.1.2.3/32 exact;
                route-filter 229.55.150.208/32 exact;
                route-filter 234.42.42.40/30 orlonger;
                route-filter 239.0.0.0/8 orlonger;
            }
            then reject;
        }
        term bad-sources {
            from {
                source-address-filter 10.0.0.0/8 orlonger;
                source-address-filter 127.0.0.0/8 orlonger;
                source-address-filter 172.16.0.0/12 orlonger;
                source-address-filter 192.168.0.0/16 orlonger;
            }
            then reject;
        }
        term accept-everything-else {
            then accept;
        }
    }
}
```

Forwarding Cache Limit

Inet.1 is the table that contains the multicast forwarding cache, which includes all PIM entries as well as MSDP SAs with encapsulated data. You limit the number of inet.1 entries on the router by configuring a forwarding cache limit. The multicast forwarding cache is added to the forwarding table, which the Packet Forwarding Engine (PFE) uses for unicast and multicast forwarding decisions. The following configuration limits the number of entries in the forwarding-cache to 150,000. Once this limit is met, the router cannot add entries until the forwarding-cache drops to 149,000.

```
routing-options {
          multicast {
            forwarding-cache {
              threshold {
                suppress 150000;
                reuse 149000;
              }
            }
          }
       }
```

Packet Filtering, Source Designated Router Filtering

You may use packet filters to deny certain multicast traffic based on values in the IP header. While scoping blocks multicast data packets based on group address, firewall filters block data packets based on values such as source address or protocol. Many worms use TCP packets when they probe. There is no legitimate reason for multicast TCP packets, so deny them on source-designated routers (DRs) and transit routers. Additionally, firewall filters enable register filtering at the source DR. Register filtering denies certain local sources from causing the DR to generate PIM register messages that are sent to the RP and prevents the creation of register state on the RP. In the following example, we want sources in the 10.1.1.0/24 range to create PIM register state on the RP, while all other sources in the 10.0.0.0/8 range cannot generate PIM register messages. By filtering packets at input on the source DR, the first hop router never gets a chance to receive the multicast packets, so it cannot create a PIM register message. Similarly, we filter all multicast packets with TCP, regardless of source address.

```
 interfaces {
     fe-0/0/0 {
         unit 0 {
             family inet {
                  filter {
                     input mcast-packet-filter;
                  }
                  address 10.0.0.1/8;
             }
         }
     }
}
firewall {
    filter mcast-packet-filter {
       term deny-tcp {
            from {
                destination-address {
                    224.0.0.0/4;
                }
                protocol tcp;
            }
            then {
                count mcast-tcp;
               discard;
            }
       }
       term allow-good-local-sources {
            from {
                source-address {
                    10.1.1.0/24;
                }
                destination-address {
                    224.0.0.0/4;
                }
            }
            then {
                count good-local-sources;
                accept;
            }
        }
        term deny-bad-local-sources {
            from {
                source-address {
                    10.0.0.0/8;
                }
                destination-address {
                    224.0.0.0/4;
                }
            }
            then {
                count bad-local-sources;
                discard;
            }
        }
        term allow-everything-else {
            then accept;
        }
    }
}
```

Routing Engine Filtering

Filtering control traffic to the routing engine (RE) is a critical component of securing routers. Firewall filters on loopback interfaces provide this functionality. In the case of MSDP, only configured peers should be allowed to send MSDP packets to a router. The following configuration only allows MSDP packets (TCP port 639) to be sent to the RE if the source address is one of its configured MSDP peers. Note the "apply path" command enables this filter to be automatically applied to all peers configured under MSDP, so there is no need to edit this filter when MSDP peers are added or removed.

```
interfaces {
    lo0 {
        unit 0 {
            family inet {
                filter {
                    input Protect-RE;
                }
            }
        }
    }
}
policy-options {
    prefix-list MSDP-Peers {
        apply-path "protocols msdp group <*> peer <*>";
    }
}
firewall {
    filter Protect-RE {
        term MSDP-Allow {
            from {
                source-prefix-list {
                    MSDP-Peers;
                }
                protocol tcp;
                port msdp;
            }
            then accept;
        }
    }
}
```

Use the "apply path" command for BGP peers also. The loopback filter should include all other protocols required to reach the router's control plane such as Protocol Independent Multicast (PIM), Internet Group Management Protocol (IGMP), Open Shortest Path First (OSPF), Secure Shell (SSH), Domain Naming System (DNS), Internet Control Message Protocol (ICMP), Simple Network Management Protocol (SNMP), etc.

Putting It All Together

The following configuration includes all of the aforementioned features along with a number of optimizations to maximize reuse of policies among all protocols. We use the whitelist approach so only multicast traffic from assigned address space is forwarded (224/8, 232/8 and 233/8), while all other multicast traffic is denied.

```
interfaces {
    lo0 {
        unit 0 {
            family inet {
                filter {
                    input Protect-RE;
                }
            }
        }
    }
}
routing-options {
    multicast {
         scope-policy [ SSM-Allow ASM-Allow ];
         forwarding-cache {
              threshold {
                  suppress 150000;
                  reuse 149000;
              }
         }
    }
 }
 protocols {
     msdp {
          apply-groups MSDP-Per-Peer-Limit;
          data-encapsulation disable;
          active-source-limit {
              maximum 200000;
              threshold 190000;
          }
          export [ Bogon-Sources ASM-Allow ];
          import [ Bogon-Sources ASM-Allow ];
          source 0.0.0.0/0 {
               active-source-limit {
                   maximum 1000;
                   threshold 900;
               }
          }
          group EMSDP-Peer1 {
                local-address 1.1.1.1;
                peer 2.2.2.2;
           }
       }
       pim {
            import [ Bogon-Sources SSM-Allow ASM-Allow ];
```

```
               rp {
                   bootstrap-import BSR-Deny;
                   bootstrap-export BSR-Deny;
                   local {
                        address 1.1.1.1;
                   }
               }
               interface all {
                    mode sparse;
                    version 2;
               }
        }
}
policy-options {
     prefix-list MSDP-Peers {
          apply-path "protocols msdp group <*> peer <*>";
    }
    prefix-list BGP-Peers {
        apply-path "protocols bgp group <*> neighbor <*>";
    }
    policy-statement ASM-Allow {
          term Bogon-Groups {
                from {
                      route-filter 224.0.1.2/32 exact;
                      route-filter 224.0.1.3/32 exact;
                      route-filter 224.0.1.8/32 exact;
                      route-filter 224.0.1.22/32 exact;
                      route-filter 224.0.1.24/32 exact;
                      route-filter 224.0.1.25/32 exact;
                      route-filter 224.0.1.35/32 exact;
                      route-filter 224.0.1.39/32 exact;
                      route-filter 224.0.1.40/32 exact;
                      route-filter 224.0.1.60/32 exact;
                      route-filter 224.0.2.1/32 exact;
                      route-filter 224.0.2.2/32 exact;
                      route-filter 224.77.0.0/16 orlonger;
              }
              then reject;
         }
         term ASM-Whitelist {
             from {
                    route-filter 224.0.0.0/8 orlonger;
                    route-filter 233.0.0.0/8 orlonger;
            }
            then accept;
         }
         term Deny-Everything-Else {
               then reject;
         }
    }
    policy-statement Bogon-Sources {
          term RFC-1918-Addresses {
                from {
                      source-address-filter 10.0.0.0/8 orlonger;
                      source-address-filter 127.0.0.0/8 orlonger;
                      source-address-filter 172.16.0.0/12 orlonger;
                     source-address-filter 192.168.0.0/16 orlonger;
               }
               then reject;
        }
  }
  policy-statement SSM-Allow {
       term SSM-Whitelist {
             from {
                    route-filter 232.0.0.0/8 orlonger;
             }
             then accept;
       }
  }
```

```
      policy-statement BSR-Deny {
          then reject;
      }
  }
  firewall {
     filter Protect-RE {
        term MSDP-Allow {
            from {
                source-prefix-list {
                   MSDP-Peers;
                }
               protocol tcp;
                 port msdp;
             }
             then accept;
         }
         term BGP-Allow {
             from {
                 source-prefix-list {
                     BGP-Peers;
                 }
                 protocol tcp;
                 port bgp;
            }
            then accept;
        }
        term PIM-Allow {
            from {
                 protocol pim;
            }
            then accept;
        }
        term IGMP-Allow {
            from {
                 protocol igmp;
            }
            then accept;
        }
        term Other-Protocols-Allow {
            from {
                 /* Add all other required unicast protocols */
            }
            then accept;
        }
        term Deny-Everything-Else {
            then {
               discard;
            }
        }
    }
}
```

References

"PIM-SM Multicast Routing Security Issues and Enhancements" draft-ietf-mboned-mroutesec-03.txt

"IPv4 Multicast Best Current Practice" draft-ietf-mboned-ipv4-mcast-bcp-02.txt

"JUNOS Internet Software for J-series, M-series, and T-series Routing Platforms Multicast Protocols Configuration Guide" http://www.juniper.net/techpubs/software/junos/junos71/swconfig71-multicast/frameset.htm

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.