

JUNOS Strict ISP Prefix Filter Template

v. 2.2 Updated: Mar 30, 2005

Change History:

2.2 – 73/8 allocated to ARIN. Bogon route filters moved to a separate URL.
2.1 – 124/8, 125/8, 126/8 allocated to APNIC.
2.0 – 71/8, 72/8 allocated to ARIN.
1.9 – 58/8, 59/8 allocated to APNIC.
1.8 – 85/8, 86/8, 87/8, 88/8 allocated to RIPE.
1.7 – 70/8 allocated to ARIN.
1.6 – 83/8 and 84/8 allocated to RIPE.
1.5 – Corrected typo in Phase 7 for 128.0.0.0/2 and 192.0.0.0/3.
1.4 – 223/8 returned to ARIN; 60/8 allocated to APNIC.
1.3 – 201/8 allocated to LACNIC; 173/8 - 187/8 and 189/8 – 190/8 DE-allocated by IANA.
1.2 - Updated F-Root prefix from 192.5.4.0/23 to 192.5.5.0/24
1.1 – Added several prefix entries for GTLDs

See the following URLs for Updates:

Cisco <ftp://ftp-eng.cisco.com/cons/isp/security/Ingress-Prefix-Filter-Templates/>
Juniper <http://www.cymru.com/gillsr/documents.html>

To be applied on ingress eBGP sessions with other ISPs

Developed by Barry Greene [bgreene@cisco.com]

Adapted to JUNOS by Stephen Gill [gillsr@cymru.com]

Instructions: Use this template as a "get started" guide. Each provider's network has unique properties that may require some of the template statements to be commented out or tuned to the unique network requirements.

Phase 1 - Deny Special Prefixes
Phase 2 - Deny Your Own Blocks
Phase 3 - Deny IXP Blocks
Phase 4 - Deny Bogon Prefixes
Phase 5 - Permit Critical Infrastructure Blocks
Phase 6 - Permit RIR Blocks on the minimal allocation block to a /24
Phase 7 - Permit the rest between /8 and /24

Phase 1 - Deny Special Prefixes

Reference Documents:

<http://www.ietf.org/internet-drafts/draft-manning-dsua-08.txt>
<http://www.ietf.org/internet-drafts/draft-iana-special-ipv4-05.txt>

```
/* ----- Begin Prefix-Filter ----- */

/* Strict Mode Prefix Filter for ISP Peers v1.1 - 12-10-2002 */
[edit policy-options policy-statement loose-prefix-filter]
/* Phase 1 - Deny Special Prefixes */
term phase-1 {
  from {
    /* Default Route */
    route-filter 0.0.0.0/0 exact reject;
    /* RFC 1918 Address Range */
    route-filter 10.0.0.0/8 orlonger reject;
    route-filter 172.16.0.0/12 orlonger reject;
    route-filter 192.168.0.0/16 orlonger reject;
    /* Multicast - remove if running multicast */
    route-filter 224.0.0.0/4 orlonger reject;
    /* Experimental */
    route-filter 240.0.0.0/4 orlonger reject;
    /* Loopback Range */
    route-filter 127.0.0.0/8 orlonger reject;
    /* Link Local Network Address */
    route-filter 169.254.0.0/16 orlonger reject;
    /* Test-Net */
    route-filter 192.0.2.0/24 orlonger reject;
    /* NeXT-Default */
    route-filter 192.42.172.0/24 orlonger reject;
    /* RFC-2544 - BMWG Addresses */
    route-filter 198.18.0.0/15 orlonger reject;
    /* Block 29-32 bit prefixes */
```

```

route-filter 0.0.0.0/0 prefix-length-range /29-/32 reject;
/* Block 0-5 bit prefixes from the table */
route-filter 0.0.0.0/0 prefix-length-range /0-/5 reject;
}
}
/* ----- snip snip ----- */

```

Phase 2 - Deny Your own Prefixes

You may wish to keep your blocks from coming back to you with the exception of multihomed customers where more specifics might be desired. Change this prefix to match your advertisements.

```
from route-filter XX.YY.ZZ./20 prefix-length-range /26-/32 reject;
```

One option for multihomed customers would be to limit the prefixes to a certain range of acceptable lengths to restrict large aggregates and small specifics.

For example:

```
from route-filter XX.YY.ZZ./20 prefix-length-range /0-/20 reject;
from route-filter XX.YY.ZZ./20 prefix-length-range /26-/32 reject;
```

```

/* ----- snip snip ----- */

/* Phase 2 - Deny Your own Prefixes */
term phase-2 {
  /* see examples */
  from {
  }
}
/* ----- snip snip ----- */

```

Phase 3 - Deny IXP Prefixes

REQUIRED

Block IXP Prefixes from whom you connect. Other ISPs should not be sending you IXP prefixes from IXPs that you are connected. While you might want to filter other IXPs, people hijacking them will not have a direct impact on your network. People hijacking prefixes from your IXPs will have an impact.

Change and un-comment this prefix(s) of IXP networks you are connected adding it to the list below.

```
route-filter XX.YY.ZZ.0/20 prefix-length-range /0-/32 reject;
```

OPTIONAL

This is a list of IXPs micro allocations that should not be globally advertised on the Internet. Putting these on the global Internet would open the door for traffic games, DOS attacks, and other mischief that would disrupt operations, services, and the interconnection of the Internet.

Filtering these are optional. The filter makes hijacking difficult - which protects the Internet in general. It may or may not have a direct effect on your network, while hijacking prefixes that are directly connected to your network will have a direct impact.

APNIC's IXP Allocation Block

```
route-filter 218.100.0.0/16 prefix-length-range /0-/32 reject;
```

```

/* ----- snip snip ----- */

term phase-3 {
  /* see examples */

  from {
  }
}
/* ----- snip snip ----- */

```

Phase 4 - Deny Bogon Prefixes

Sources:
Bogon List

<http://www.cymru.com/Documents/bogon-list.html>

Secure JUNOS BGP Template

<http://www.cymru.com/gillsr/documents/junos-bgp-template.pdf>

The bogons prefix list prevents the acceptance of obviously bogus routing updates. This can be modified to fit local requirements.

While aggregation is possible - certainly desirable - IANA tends to allocate netblocks on a /8 boundary. For this reason, I have listed the bogons largely as /8 netblocks. This will make changes to the bogons prefix-list easier to accomplish and less intrusive.

Please see the IANA IPv4 netblock assignment document at:

<http://www.iana.org/assignments/ipv4-address-space>

Bogon filters should be used to protect an ISP from the outside.

```
/* ----- snip snip ----- */

/* Phase 4 - Deny Bogon Prefixes */
term phase-4 {
    from {
        /* Use: http://www.cymru.com/gillsr/documents/junos-bogon-route-filters.txt */
    }
}

/* ----- snip snip ----- */
```

Phase 5 - Critical Infrastructure

Some services and parts of the Internet are critical. They should be permitted but not allowed to be hijacked.

Sources:

<http://www.cymru.com/gillsr/documents/golden-networks>

All prefixes that are more specific than the known root server blocks will be discarded.

Prefixes that are already found elsewhere in this template are placed here for reference purposes only.

```
/* biz – already exist */
route-filter 209.173.58.0/24 exact accept;
/* com, net – already exist */
route-filter 192.5.6.0/24 exact accept;
route-filter 192.33.14.0/24 exact accept;
route-filter 192.26.92.0/24 exact accept;
route-filter 192.31.80.0/24 exact accept;
route-filter 192.12.94.0/24 exact accept;
route-filter 192.35.51.0/24 exact accept;
route-filter 192.42.93.0/24 exact accept;
route-filter 192.54.112.0/24 exact accept;
route-filter 192.43.172.0/24 exact accept;
route-filter 192.48.79.0/24 exact accept;
route-filter 192.52.178.0/24 exact accept;
route-filter 192.41.162.0/24 exact accept;
route-filter 192.55.83.0/24 exact accept;
/* coop – already exist */
route-filter 192.100.59.0/24 exact accept;
/* gov, edu – already exist */
route-filter 192.5.6.0/24 exact accept;
route-filter 192.33.14.0/24 exact accept;
route-filter 192.26.92.0/24 exact accept;
route-filter 192.31.80.0/24 exact accept;
route-filter 192.12.94.0/24 exact accept;
route-filter 192.55.83.0/24 exact accept;
route-filter 192.5.6.0/24 exact accept;
route-filter 192.5.6.0/24 exact accept;
/* int – already exist */
route-filter 128.9.0.0/16 exact accept;
/* name – already exist */
route-filter 192.5.6.0/24 exact accept;
route-filter 192.35.51.0/24 exact accept;
route-filter 192.42.93.0/24 exact accept;
route-filter 192.41.162.0/24 exact accept;
/* org – already exist */
route-filter 192.5.6.0/24 exact accept;
route-filter 192.26.92.0/24 exact accept;
```

```

route-filter 192.12.94.0/24 exact accept;
route-filter 192.35.51.0/24 exact accept;
route-filter 192.42.93.0/24 exact accept;
route-filter 192.43.172.0/24 exact accept;
route-filter 192.48.79.0/24 exact accept;
route-filter 192.41.162.0/24 exact accept;
route-filter 192.55.83.0/24 exact accept;
/* pro – already exist */
route-filter 192.0.34.0/24 exact accept;
route-filter 193.0.0.0/21 exact accept;

/* ----- snip snip ----- */

/* Phase 5 - Critical Infrastructure */
term phase-5 {
  from {
    /* a.root */
    route-filter 198.41.0.0/24 exact accept;
    /* b.root */
    route-filter 128.9.0.0/16 exact accept;
    /* c.root */
    route-filter 192.33.4.0/24 exact accept;
    /* d.root */
    route-filter 128.8.0.0/16 exact accept;
    /* e.root */
    route-filter 192.203.230.0/24 exact accept;
    /* f.root */
    route-filter 192.5.5.0/24 exact accept;
    /* g.root */
    route-filter 192.112.36.0/24 exact accept;
    /* h.root */
    route-filter 128.63.0.0/16 exact accept;
    /* i.root */
    route-filter 192.36.148.0/24 exact accept;
    /* j.root */
    route-filter 192.58.128.0/24 exact accept;
    /* k.root */
    route-filter 193.0.14.0/24 exact accept;
    /* l.root */
    route-filter 198.32.64.0/24 exact accept;
    /* m.root */
    route-filter 202.12.27.0/24 exact accept;
    /* a.gtld */
    route-filter 192.5.6.0/24 exact accept;
    /* b.gtld */
    route-filter 192.33.14.0/24 exact accept;
    /* c.gtld */
    route-filter 192.26.92.0/24 exact accept;
    /* d.gtld */
    route-filter 192.31.80.0/24 exact accept;
    /* e.gtld */
    route-filter 192.12.94.0/24 exact accept;
    /* f.gtld */
    route-filter 192.35.51.0/24 exact accept;
    /* g.gtld */
    route-filter 192.42.93.0/24 exact accept;
    /* h.gtld */
    route-filter 192.54.112.0/24 exact accept;
    /* i.gtld */
    route-filter 192.43.172.0/24 exact accept;
    /* j.gtld */
    route-filter 192.48.79.0/24 exact accept;
    /* k.gtld */
    route-filter 192.52.178.0/24 exact accept;
    /* l.gtld */
    route-filter 192.41.162.0/24 exact accept;
    /* m.gtld */
    route-filter 192.55.83.0/24 exact accept;
    /* aero */
    route-filter 192.55.83.0/24 exact accept;
    route-filter 130.59.0.0/16 exact accept;
    route-filter 194.64.105.0/24 exact accept;
    route-filter 192.100.59.0/24 exact accept;
    /* biz */
    route-filter 209.173.53.0/24 exact accept;
    route-filter 209.173.57.0/24 exact accept;
    route-filter 209.173.60.0/24 exact accept;
    route-filter 213.86.0.0/16 exact accept;

```

```

route-filter 209.173.58.0/24 exact accept;
/* coop */
route-filter 198.133.199.0/24 exact accept;
/* gov, edu */
route-filter 192.35.51.0/24 exact accept;
/* info */
route-filter 204.74.112.0/24 exact accept;
route-filter 204.74.113.0/24 exact accept;
/* int */
route-filter 137.39.0.0/16 exact accept;
route-filter 128.86.0.0/16 exact accept;
route-filter 193.60.0.0/14 exact accept;
route-filter 128.16.0.0/16 exact accept;
route-filter 192.0.34.0/24 exact accept;
route-filter 193.0.0.0/21 exact accept;
/* mil */
route-filter 199.252.128.0/18 exact accept;
route-filter 199.252.154.0/24 exact accept;
route-filter 199.252.180.0/24 exact accept;
route-filter 199.252.155.0/24 exact accept;
/* museum */
route-filter 153.10.0.0/16 exact accept;
route-filter 195.7.64.0/19 exact accept;
route-filter 130.242.0.0/15 exact accept;
route-filter 204.152.184.0/21 exact accept;
/* name */
route-filter 193.109.220.0/24 exact accept;
route-filter 202.71.192.0/18 exact accept;
}
}
/* ----- snip snip ----- */

```

Phase 6 - RIR Allocation Blocks

Explicitly permit only those advertisements that have been allocated by IANA and the RIRs.

This is a very Strict Net Police filter - allowing prefixes from a /9 to the minimal prefix size allocated by the RIR. A /8 from any of these block would be bogus.

ISPs can modify this section to have a range of /8 to the RIR's Minimal Allocation Size. Strict Mode will mitigate some forms of prefix garbage attack and save RIB and FIB memory in the router. The trade off is that other ISP's customers could not use some forms of more specific prefix advertisements to do their traffic engineering.

This assumes ISPs have a clue and will advertise their allocated CIDR block vs advertising lots of more specifics. So clueless ISPs might have problems reach your customers (and visa versa).

APNIC

<http://www.apnic.net/db/min-alloc.html>

ARIN

<http://www.arin.net/statistics/index.html#cidr>

ARIN Micro Allocations

http://www.arin.net/registration/ipv4/micro_alloc.html

The following blocks have been allocated to organizations under ARIN's micro-allocation policy for exchange points. NOTE: Some of these will be duplicates of the IXP Deny phase. They are listed here and `_commented_` out just in case (you never know when you might to make exceptions).

```

route-filter 206.223.116.0/24 exact accept;
route-filter 206.223.117.0/24 exact accept;
route-filter 206.223.118.0/24 exact accept;
route-filter 206.223.120.0/24 exact accept;
route-filter 206.223.121.0/24 exact accept;
route-filter 206.223.122.0/24 exact accept;
route-filter 206.223.124.0/24 exact accept;
route-filter 206.223.128.0/24 exact accept;
route-filter 206.223.129.0/24 exact accept;
route-filter 206.223.130.0/24 exact accept;
route-filter 206.223.132.0/22 exact accept;

```

Micro-allocations for Critical Internet Infrastructure

The following blocks of IP address space have been allocated to organizations under ARIN's micro-allocation policy for gTLDs, ccTLDs, RIRs, and ICANN, as well as all named servers of the domain.

These prefixes should _never_ be filtered. Global Access is critical! We put them here and limit them to /24 to keep people from injecting a more specific prefix (i.e. less than /24) to DOS or hijack a critical Internet resource.

```
/* micro critical – already exist */
route-filter 192.12.94.0/24 exact accept;
route-filter 192.26.92.0/24 exact accept;
route-filter 192.31.80.0/24 exact accept;
route-filter 192.33.14.0/24 exact accept;
route-filter 192.35.51.0/24 exact accept;
route-filter 192.41.162.0/24 exact accept;
route-filter 192.42.93.0/24 exact accept;
route-filter 192.43.172.0/24 exact accept;
route-filter 192.48.79.0/24 exact accept;
route-filter 192.5.6.0/24 exact accept;
route-filter 192.52.178.0/24 exact accept;
route-filter 192.54.112.0/24 exact accept;
route-filter 192.55.83.0/24 exact accept;
route-filter 192.58.128.0/24 exact accept;
```

RIPE NCC

<http://www.ripe.net/ripe/docs/smallest-alloc-sizes.html>

```
/* ----- snip snip ----- */

/* Phase 6 - RIR Allocation Blocks */
term phase-6 {
  from {
    /* APNIC */
    route-filter 61.0.0.0/8 prefix-length-range /9-/22 accept;
    route-filter 202.0.0.0/8 prefix-length-range /9-/24 accept;
    route-filter 203.0.0.0/8 prefix-length-range /9-/24 accept;
    route-filter 210.0.0.0/8 prefix-length-range /9-/20 accept;
    route-filter 211.0.0.0/8 prefix-length-range /9-/20 accept;
    route-filter 218.0.0.0/8 prefix-length-range /9-/20 accept;
    route-filter 219.0.0.0/8 prefix-length-range /9-/20 accept;
    route-filter 220.0.0.0/8 prefix-length-range /9-/20 accept;
    route-filter 221.0.0.0/8 prefix-length-range /9-/20 accept;
    /* APNIC Specials - Shownet and Temp Allocations */
    route-filter 169.208.0.0/16 upto /20 accept;
    route-filter 169.209.0.0/16 upto /20 accept;
    route-filter 169.210.0.0/16 upto /20 accept;
    route-filter 169.211.0.0/16 upto /20 accept;
    route-filter 169.212.0.0/16 upto /20 accept;
    route-filter 169.213.0.0/16 upto /20 accept;
    route-filter 169.214.0.0/16 upto /20 accept;
    route-filter 169.215.0.0/16 upto /20 accept;
    route-filter 169.216.0.0/16 upto /20 accept;
    route-filter 169.217.0.0/16 upto /20 accept;
    route-filter 169.218.0.0/16 upto /20 accept;
    route-filter 169.219.0.0/16 upto /20 accept;
    route-filter 169.220.0.0/16 upto /20 accept;
    route-filter 169.221.0.0/16 upto /20 accept;
    route-filter 169.222.0.0/16 upto /20 accept;
    route-filter 169.223.0.0/16 upto /20 accept;
    /* ARIN */
    route-filter 24.0.0.0/8 prefix-length-range /9-/20 accept;
    route-filter 63.0.0.0/8 prefix-length-range /9-/19 accept;
    route-filter 64.0.0.0/8 prefix-length-range /9-/20 accept;
    route-filter 65.0.0.0/8 prefix-length-range /9-/20 accept;
    route-filter 66.0.0.0/8 prefix-length-range /9-/20 accept;
    route-filter 67.0.0.0/8 prefix-length-range /9-/20 accept;
    route-filter 68.0.0.0/8 prefix-length-range /9-/20 accept;
    route-filter 69.0.0.0/8 prefix-length-range /9-/20 accept;
    route-filter 196.0.0.0/8 prefix-length-range /9-/24 accept;
    route-filter 198.0.0.0/8 prefix-length-range /9-/24 accept;
    route-filter 199.0.0.0/8 prefix-length-range /9-/24 accept;
    route-filter 200.0.0.0/8 prefix-length-range /9-/24 accept;
    route-filter 204.0.0.0/8 prefix-length-range /9-/24 accept;
    route-filter 205.0.0.0/8 prefix-length-range /9-/24 accept;
    /* for 206.0.0.0-8 see micro-allocation list */
    route-filter 206.0.0.0/8 prefix-length-range /9-/24 accept;
    route-filter 207.0.0.0/8 prefix-length-range /9-/24 accept;
    route-filter 208.0.0.0/8 prefix-length-range /9-/20 accept;
    route-filter 209.0.0.0/8 prefix-length-range /9-/20 accept;
    route-filter 216.0.0.0/8 prefix-length-range /9-/20 accept;
    /* micro critical internet infrastructure */
    route-filter 192.31.177.0/24 exact accept;
```

```

route-filter 192.31.178.0/24 exact accept;
route-filter 192.31.179.0/24 exact accept;
route-filter 206.223.136.0/24 exact accept;
/* RIPE */
route-filter 62.0.0.0/8 prefix-length-range /9-/19 accept;
route-filter 80.0.0.0/8 prefix-length-range /9-/20 accept;
route-filter 81.0.0.0/8 prefix-length-range /9-/20 accept;
route-filter 82.0.0.0/8 prefix-length-range /9-/20 accept;
route-filter 83.0.0.0/8 prefix-length-range /9-/20 accept;
route-filter 84.0.0.0/8 prefix-length-range /9-/20 accept;
route-filter 193.0.0.0/8 prefix-length-range /9-/29 accept;
route-filter 194.0.0.0/8 prefix-length-range /9-/29 accept;
route-filter 195.0.0.0/8 prefix-length-range /9-/29 accept;
route-filter 212.0.0.0/8 prefix-length-range /9-/19 accept;
route-filter 213.0.0.0/8 prefix-length-range /9-/19 accept;
route-filter 217.0.0.0/8 prefix-length-range /9-/20 accept;
}
}
/* ----- snip snip ----- */

```

Phase 7 - Permit the Legacy Prefixes

These are the legacy prefixes allocated before the CIDR, RIR's and RFC 2050. These are mostly from the old Class B and Class C allocations (pre-RFC 2050). The prefix filters here are one way of putting a boundary around these prefixes.

```

/* ----- snip snip ----- */

/* Phase 7 - Permit the Legacy Prefixes */
term phase-7 {
  from {
    /* Old Class B Space */
    route-filter 128.0.0.0/2 prefix-length-range /21-/32 reject;
    route-filter 128.0.0.0/16 upto /32 reject;
    route-filter 191.255.0.0/16 upto /32 reject;
    /* Old Class C Space */
    route-filter 192.0.0.0/3 prefix-length-range /25-/32 reject;
    route-filter 192.0.0.0/24 upto /32 reject;
    /* Permit pre-RIR/RFC2050 allocations through */
    route-filter 0.0.0.0/0 upto /24 accept;
  }
}

/* ----- End Prefix-List ----- */

```