RIPE Anti-Spoofing Task Force HOW-TO

Fernando García (Tecnocom) and Juan P. Cerezo (BT GS)

Document ID: ripe-431
Date: 9 Mai 2008

Table of Contents

1. Introduction

This document presents practical recommendations for the implementation of anti-spoofing mechanisms at the critical points of the network infrastructure of carriers and/or ISPs.

These practical recommendations are based on the experience of the editors and collaborators and on previous existing work, like existing best common practices [1].

2. Overview

This document starts with an enumeration of the most common attacks that networks connected to the Internet suffer today, followed by a brief description of the countermeasures that can be used to avoid or, at least, reduce the impact of these attacks.

Finally, a set of recipes implementing these countermeasures in mainstream routers is presented in a way that is easy to deploy in a network.

3. Definitions

CEF: Cisco Express Forwarding: a packet switching mode used in Cisco routers that increases the transmission speed while reducing CPU load.

CPE: Customer Premises Equipment: a router placed in an end-user office that connects to both the end-user network and the provider network, usually through a point-to-point link.

DFZ: Default Free Zone: the set of routers in the Internet that do not use a default route and that need to keep the full routing table in their memory.

PE: Provider Edge: a router located in the provider network that connects directly with one or more CPEs.

4. Common aspects related to IP networking

4.1. Filtering prefixes

4.1.1. Why to filter

The amount and severity of security incidents involving spoofed IP addresses is increasing. This suggests that applying some level of control over the correctness of the source IP address of packets can mitigate the impact of the attacks on the infrastructure. Also, the blocking of spoofed address would help to find the origin of such attacks.

4.1.2. What to filter

IP traffic with a source address belonging to prefixes that should not be on the routing table of routers connected to (or that forward traffic from/to) the public Internet should be filtered. The most common list of these prefixes is the so-called bogon list [2].

4.1.3. Where to filter

Filtering should be applied, where possible, on at least one of:

- The hosts in the network
- The customer’s routers (CPE)
- The ISP infrastructure equipment (access routers and concentrators, DFZ routers)

The nearer the filters are applied to the origination of the spoofed traffic, the better the effects on the security and reliability of the hosts and the network will be.

4.2. Unicast Reverse Path Forwarding (uRPF) mechanism(s)

uRPF [3] is a mechanism where routers check whether the source address of a received packet exists in the routing table. If it does not appear in the routing table, the packet is blocked. Various options exist regarding the strictness:

- Strict uRPF will drop the packet unless the best route to the source address is through the interface on which the packet was received
- Feasible path uRPF will drop the packet unless a route (not necessarily the best) to the source address is through the interface on which the packet was received. Feasible path uRPF prevents issues in asymmetric and multihomed scenarios
- Loose uRPF will drop the packet unless a route to the source address exists. The interface is irrelevant for this type. A variation of this mechanism allows ignoring the existence of default routes in the forwarding table.

The exact conditions for choosing one of these mechanisms are hard to describe, but the following rules of thumb apply:

- Networks that apply strict uRPF must keep their routing symmetric. Strict uRPF can be problematic on peering routers that exchange routes with other ISPs (“hot potato“ routing, BGP filtering in both directions of the peering due to different routing policies). It can also cause problems in networks that have different links to other networks
- Loose uRPF applied to interfaces in border routers will allow asymmetric routing, but will limit the automatic “pseudo-filtering” benefits of uRPF to private (RFC 1918) and unallocated (“bogon“) IP addresses [4]

4.3. Other filters: bogon prefix filtering

4.3.1. What are bogon prefixes

A bogon prefix as defined by Cymru [1] is “a route that should never appear in the Internet routing table. A packet routed over the public Internet (not including over VPN or other tunnels) should never have a source address in a bogon range. These are commonly found as the source addresses of DDoS attacks”.

For the purpose of this how-to, a packet received on an interface of a router is considered bogon if it’s source address should not be routable through that interface. This definition of bogon includes “martian” addresses (as listed in RFC 1918 and RFC 3330) and unallocated addresses as explained in the next subsection. Also included are addresses from networks that are always connected to other interfaces of the router.

4.3.2. Why filter bogons

The Cymru document states that, according to some measurements, up to 60% of the IP addresses used in attacks are bogon. Filtering these addresses will greatly reduce the impact of such attacks.

4.3.3. How to build the filters

There are two basic methods:

- On interfaces connected to the Internet, the easiest way is to create a list of denied networks and block these
- On interfaces connected to a reduced set of networks, or only internal networks, it is usually easier create a list of allowed networks and allowing only these networks

In the first case, the filters have a static part and a dynamic part. The static part contains the martian addresses and the static networks inside the organisation. The dynamic part contains, at least, the list of otherwise valid addresses that have not been allocated from the IANA to the RIRs yet (see next section).

4.3.4. Unallocated addresses

One special case of bogon networks is unallocated address space. Unallocated addresses are blocks of public address space that have not been allocated by the IANA to the RIRs yet, but that could be allocated in the future. This means that some of the networks that make up this list today should be removed once they have been assigned. If they are not removed after being allocated, there is a risk that portions of the Internet will be blocked to customers. For transit providers, this problem can be very difficult to debug.

Therefore, it is important to keep these lists up-to-date. Manual maintenance often comes with problems, so it is strongly recommended to use some kind of automation. The Team Cymru Bogon Reference Page [2] provides more information on automatic generation of these filters.

5. Vendor specifics

5.1. Cisco features

Cisco routers support both strict and loose uRPF. CEF is necessary for uRPF. Therefore, uRPF is incompatible with solutions that disable CEF.

Source routing is disabled by default in Cisco routers, although it can be enabled in the configuration.

On Cisco routers, it is possible to filter packets based on source IP address without loading the router CPU too much.

5.2. Juniper features

Juniper routers support both strict and loose uRPF, if they are equipped with the (relatively) new Internet Processor II ASIC.

Source routing is enabled by default in Juniper routers. This can be a threat for connected networks. Therefore, it is recommended to disable this feature.

On Juniper routers, it is possible to filter packets based on source IP address without loading the router CPU too much.

6. Scenarios

Several different scenarios are examined, each with examples of how the filtering can be configured.

6.1. Customer/provider scenarios

The scenarios in this section all focus on a clear separation between router(s) at the customer's side (CPE) and the connected router(s) on the provider side (PE).

6.1.1. One customer router, single provider with one router

In this scenario, there is a single link between the customer and the provider's access router. This would often be done with a /30 or /31 from the provider's PA range.

In many cases, the link will use public addresses, but in some cases, NAT is used with private addresses.

The routing between the customer and the provider in this scenario is static.

On both routers in this scenario, filters can either be maintained manually and/or uRPF can be used to filter automatically. The former can be more accurate, but it is harder to maintain. It will also put a bigger load on the router. Manual lists are recommended over uRPF when the traffic exceeds 1 Mbit/s. If access lists are implemented, uRPF is mostly redundant.

Cisco version

Configuration on the customer router (CPE)

```
! CEF is needed for uRPF
ip cef
interface ATM0/1.1 point-to-point
```

```
 description Interface to provider
 ip address 89.107.53.2 255.255.255.252
  ! Packets are filtered based on a static list
 ip access-group bogons in
  ! Strict uRPF can also be used, although
  ! it is redundant in this case
  ! Note that allow-default is set, to permit
  ! uRPF to allow a packet based on a default route
 ip verify unicast reachable-via rx allow-default
...
 ! Default route to the provider
ip route 0.0.0.0 0.0.0.0 ATM0/1.1
...
! Manually maintained list of networks to be filtered
! These are the private and reserved networks
ip access-list extended bogons
 deny ip 10.0.0.0 0.255.255.255 any
 deny ip 192.168.0.0 0.0.255.255 any
 deny ip 172.16.0.0 0.15.255.255 any
 deny ip 127.0.0.0 0.255.255.255 any
 deny ip 169.254.0.0 0.0.255.255 any
 deny ip 192.0.2.0 0.0.0.255 any
 deny ip 198.18.0.0 0.1.255.255 any
 deny ip 240.0.0.0 15.255.255.255 any
 ! If a public range was assigned to this network,
 ! these addresses can’t be received from the outside
 deny ip 89.107.52.0 0.0.0.255 any
 ! External address of this router
 deny ip 89.107.53.2 0.0.0.0 any
 permit ip any any
```

Configuration on the provider router (PE)

```
! CEF is needed for uRPF
ip cef
interface ATM0/1.1 point-to-point
 description Interface to customer
 ip address 89.107.53.1 255.255.255.252
  ! Static filter based on the public addresses
  ! of the customer
 ip access-group customer-routes in
  ! Strict uRPF can also be used here
  ! allow-default is not used, because a customer link
  ! should not be a default route
 ip verify unicast reachable-via rx
...
! Static networks to filter
ip access-list extended customer-routes
 ! Allow the IP address of the customer’s router
 permit ip 89.107.53.2 0.0.0.0 any
 ! If the customer has a public range assigned, allow it
 permit ip 89.107.52.0 0.0.0.255 any
 ! Deny anything else
 deny   ip any any
```

Juniper Version

Configuration on the customer router (CPE)

```
interfaces {
    e3-0/0/0 {
        description "Interface to provider";
        hold-time up 200 down 200;
        clocking internal;
        encapsulation ppp;
        e3-options {
            compatibility-mode kentrox;
            payload-scrambler;
            fcs 32;
        }
        unit 0 {
            family inet {
                filter {
                    input bogons;
                }
                address 89.107.53.2/30;
                /* Strict uRPF can be used, */
                /* but it is redundant */
                rpf-check;
            }
        }
    }
}
chassis {
    no-source-route;
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop e3-0/0/0;

    }
}
policy-options {
    prefix-list bogon-list {
        10.0.0.0/8;
        192.168.0.0/16;
        172.16.0.0/12;
        127.0.0.0/8;
        169.254.0.0/16;
        192.0.2.0/24;
        198.18.0.0/15;
        240.0.0.0/4;
    }
}
firewall {
    family inet {
        filter bogons {
            term bogons {
                from {
                    prefix-list {
                        bogon-list;
                    }
                }
                then {
                    discard;
                }
            }
            term our-own {
                from {
                    source-address {
                        89.107.52.0/24;
                    }
                }
                then {
                    discard;
                }
            }
            term the-router {
                from {
                    source-address {
                        89.107.53.2/32;
                    }
                }
                then {
                    discard;
                }
            }
            term default {
                then {
                    accept;
                }
            }
        }
    }
}
```

Configuration on the provider router (PE)

```
interfaces {
    e3-0/0/0 {
        description "Interface to customer";
        hold-time up 200 down 200;
        clocking internal;
        encapsulation ppp;
        e3-options {
            compatibility-mode kentrox;
            payload-scrambler;
            fcs 32;
        }
        unit 0 {
            family inet {
                filter {
                    input customer;
                }
                address 89.107.53.1/30;
                /* Strict uRPF can be used, */
                /* but it is redundant */
                rpf-check;
            }
        }
    }
}
chassis {
    no-source-route;
}
routing-options {
    static {
        route 89.107.52.0/24 next-hop e3-0/0/0;

    }
}
firewall {
    family inet {
        filter customer {
            term network {
                from {
                    source-address {
                        89.107.52.0/24;
                    }
                }
                then {
                    accept;
                }
            }
            term router {
                from {
                    source-address {
                        89.107.53.2/32;
                    }
                }
                then {
                    accept;
                }
            }
        }
    }
}
```

6.1.2. Multiple customer routers, single provider with one router

In this scenario, multiple routers at the customer's side are connected to one router at the provider's side. Each route between the customer's and the provider's routers will be static and will have different metrics for each path, with one path being the default active in both ways and the other path the default passive in both ways. Using the same kind of metrics on both sides is important: If one side would use one path as "best" and the other side would use the other one, strict uRPF would block the traffic.

Each router has a link between customer's and provider's router, commonly using /30 or /31 range from the provider's PA range. The customer will have a public range from the PA space allocated to the provider.

The CPEs would often use VRRP or a similar mechanism to provide automatic failover. More weight would be on the CPE with the best link. The CPEs each have two default routes: one through its link to the provider and another through the other router with a lower weight.

On the PE, routes are set to the customer's network through both links. The preferred link has a higher weight.

```
        +----------+
        | Provider |
        | router   |
        ++--------++
          |       |
+---------++      ++----------+
| Customer |     | Customer |
| router A |     | router B |
+--------+-+      +---+------+
        |            |
        |            |
        |  --------  |
        |//        \\|
       /|           \\
       ||            ||
            customer
            network
       ||            ||
       \\            //
          \\        //
           --------
```

The customer's routers can implement the same filtering that was described for the previous scenario. Filtering is only applied to the incoming routes from the provider network; no filtering is applied to the routes coming from the customer network itself. uRPF is enabled, in strict mode.

Cisco version

Configuration on customer router A (CPE)

```
! CEF is needed for uRPF
ip cef
interface ATM0/1.1 point-to-point
 description Interface to provider
 ip address 89.107.53.2 255.255.255.252
 ! Packets are filtered based on a static list
 ip access-group bogons in
 ! Strict uRPF is enabled
 ! Note that allow-default is set, to permit
 ! uRPF to allow a packet based on a default route
 ip verify unicast reachable-via rx allow-default
[...]
! Default route to the provider
ip route 0.0.0.0 0.0.0.0 ATM0/1.1 10
! Default route to the other router
ip route 0.0.0.0 0.0.0.0 89.107.52.3 20
[...]
! Manually maintained list of networks to be filtered
! These are the private and reserved networks
ip access-list extended bogons
 deny ip 10.0.0.0 0.255.255.255 any
 deny ip 192.168.0.0 0.0.255.255 any
 deny ip 172.16.0.0 0.15.255.255 any
 deny ip 127.0.0.0 0.255.255.255 any
 deny ip 169.254.0.0 0.0.255.255 any
 deny ip 192.0.2.0 0.0.0.255 any
 deny ip 198.18.0.0 0.1.255.255 any
 deny ip 240.0.0.0 15.255.255.255 any
 ! External address of this router
 deny ip 89.107.53.2 0.0.0.0 any
 ! Public address range of the customer
 deny ip 89.107.52.0 0.0.0.255 any
 permit ip any any
...
interface FastEthernet0/0
 ip address 89.107.52.2 255.255.255.0
 standby 1 ip 89.107.52.1
 standby 1 preempt
 standby 1 priority 150
 standby 1 track ATM0/1.1
```

Configuration on customer router B (CPE)

```
! CEF is needed for uRPF
ip cef
interface ATM0/1.1 point-to-point
 description Interface to provider
 ip address 89.107.53.6 255.255.255.252
 ! Packets are filtered based on a static list
 ip access-group bogons in
 ! Strict uRPF is enabled
 ! Note that allow-default is set, to permit
 ! uRPF to allow a packet based on a default route
 ip verify unicast reachable-via rx allow-default
[...]
! Default route to the provider
ip route 0.0.0.0 0.0.0.0 ATM0/1.1
[...]
! Manually maintained list of networks to be filtered
! These are the private and reserved networks
ip access-list extended bogons
 deny ip 10.0.0.0 0.255.255.255 any
 deny ip 192.168.0.0 0.0.255.255 any
 deny ip 172.16.0.0 0.15.255.255 any
 deny ip 127.0.0.0 0.255.255.255 any
 deny ip 169.254.0.0 0.0.255.255 any
 deny ip 192.0.2.0 0.0.0.255 any
 deny ip 198.18.0.0 0.1.255.255 any
 deny ip 240.0.0.0 15.255.255.255 any
 ! External address of this router
 deny ip 89.107.53.6 0.0.0.0 any
 ! Public address range of the customer
 deny ip 89.107.52.0 0.0.0.255 any
 permit ip any any
[...]
interface FastEthernet0/0
 ip address 89.107.52.3 255.255.255.0
 standby 1 ip 89.107.52.1
 standby 1 preempt
 standby 1 priority 75
 standby 1 track ATM0/1.1
```

Filters on provider router (PE)

Only filtering on routes sent by the customer is shown.

```
! CEF is needed for uRPF
ip cef
interface ATM0/1.1 point-to-point
 description Interface to customer
 ip address 89.107.53.1 255.255.255.252
 ! Packets are filtered based on a static list
 ip access-group customer-routes in
 ! uRPF filtering
 ip verify unicast reachable-via rx
[...]
interface ATM0/2.1 point-to-point
 description Interface to customer
 ip address 89.107.53.5 255.255.255.252
 ! Packets are filtered based on a static list
 ip access-group customer-routes in
 ! uRPF filtering
 ip verify unicast reachable-via rx
[...]
! Route to customer router A
ip route 89.107.52.0 255.255.255.0 ATM0/1.1 10
! Route to customer router B
ip route 89.107.52.0 255.255.255.0 ATM0/2.1 20
! Static networks to filter
! Public addresses of the CPE routers
ip access-list extended customer-routes
 permit ip 89.107.53.2 0.0.0.0 any
 permit ip 89.107.53.6 0.0.0.0 any
 ! Public range of the customer
 permit ip 89.107.52.0 0.0.0.255 any
 deny ip any any
```

Juniper version

Filters on customer router A (CPE)

```
interfaces {
    e3-0/0/0 {
        description "Interface to provider";
        hold-time up 200 down 200;
        clocking internal;
        encapsulation ppp;
        e3-options {
            compatibility-mode kentrox;
            payload-scrambler;
            fcs 32;
        }
        unit 0 {
            family inet {
                filter {
                    input bogons;
                }
                address 89.107.53.2/30;
                /* Enable strict uRPF */
                rpf-check;
            }
        }
    }
    fe-1/3/0 {
        unit 0 {
            family inet {
                filter {
                    input voip;
                }
                address 89.107.52.2/24 {
                    vrrp-group 1 {
                        virtual-address 89.107.52.1;
                        priority 150;
                        track {
                            interface e3-0/0/0.0 {
                                priority-cost 100;
                            }
                        }
                    }
                }
            }
        }
    }
}
chassis {
    no-source-route;
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop e3-0/0/0 preference 10;
        route 0.0.0.0/0 next-hop 89.107.52.3 preference 20;
    }
}
policy-options {
    prefix-list bogon-list {
        10.0.0.0/8;
        192.168.0.0/16;
        172.16.0.0/12;
        127.0.0.0/8;
        169.254.0.0/16;
        192.0.2.0/24;
        198.18.0.0/15;
        240.0.0.0/4;
    }
}
firewall {
    family inet {
        filter bogons {
            term bogons {
                from {
                    prefix-list {
                        bogon-list;
                    }
                }
                then {
                    discard;
                }
            }
            term our-own {
                from {
                    source-address {
                        89.107.52.0/24;
                    }
                }
                then {
                    discard;
                }
            }
            term the-router {
                from {
                    source-address {
                        89.107.53.2/32;
                    }
                }
                then {
                    discard;
                }
            }
            term default {
                then {
                    accept;
                }
            }
        }
    }
}
```

Filters on customer router B (CPE)

```
interfaces {
    e3-0/0/0 {
        description "Interface to provider";
        hold-time up 200 down 200;
        clocking internal;
        encapsulation ppp;
        e3-options {
            compatibility-mode kentrox;
            payload-scrambler;
            fcs 32;
        }
        unit 0 {
            family inet {
                filter {
                    input bogons;
                }
                address 89.107.53.6/30;
                /* Enable strict uRPF */
                rpf-check;
            }
        }
    }
    fe-1/3/0 {
        unit 0 {
            family inet {
                filter {
                    input voip;
                }
                address 89.107.52.3/24 {
                    vrrp-group 1 {
                        virtual-address 89.107.52.1;
                        priority 125;
                        track {
                            interface e3-0/0/0.0 {
                                priority-cost 100;
                            }
                        }
                    }
                }
            }
        }
    }
}
chassis {
    no-source-route;
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop e3-0/0/0 preference 10;
        route 0.0.0.0/0 next-hop 89.107.52.2 preference 20;
    }
}
policy-options {
    prefix-list bogon-list {
        10.0.0.0/8;
        192.168.0.0/16;
        172.16.0.0/12;
        127.0.0.0/8;
        169.254.0.0/16;
        192.0.2.0/24;
        198.18.0.0/15;
        240.0.0.0/4;
    }
}
firewall {
    family inet {
        filter bogons {
            term bogons {
                from {
                    prefix-list {
                        bogon-list;
                    }
                }
                then {
                    discard;
                }
            }
            term our-own {
                from {
                    source-address {
                        89.107.52.0/24;
                    }
                }
                then {
                    discard;
                }
            }
            term the-router {
                from {
                    source-address {
                        89.107.53.6/32;
                    }
                }
                then {
                    discard;
                }
            }
            term default {
                then {
                    accept;
                }
            }
        }
    }
}
```

Filters on provider router (PE)

Only filtering on routes sent by the customer is shown.

```
interfaces {
    e3-0/0/0 {
        description "Interface to customer";
        hold-time up 200 down 200;
        clocking internal;
        encapsulation ppp;
        e3-options {
            compatibility-mode kentrox;
            payload-scrambler;
            fcs 32;
        }
        unit 0 {
            family inet {
                filter {
                    input customer;
                }
                address 89.107.53.1/30;
                /* Strict uRPF can be used, */
                /* but it is redundant */
                rpf-check;
            }
        }
    }
    e3-0/0/1 {
        description "Interface to customer";
        hold-time up 200 down 200;
        clocking internal;
        encapsulation ppp;
        e3-options {
            compatibility-mode kentrox;
            payload-scrambler;
            fcs 32;
        }
        unit 0 {
            family inet {
                filter {
                    input customer;
                }
                address 89.107.53.5/30;
                /* Strict uRPF can be used, */
                /* but it is redundant */
                rpf-check;
            }
        }
    }
}
chassis {
    no-source-route;
}
routing-options {
    static {
        route 89.107.52.0/24 next-hop e3-0/0/0 preference 10;
        route 89.107.52.0/24 next-hop e3-0/0/1 preference 20;
    }
}
firewall {
    family inet {
        filter customer {
            term network {
                from {
                    source-address {
                        89.107.52.0/24;
                    }
                }
                then {
                    accept;
                }
            }
            term router {
                from {
                    source-address {
                        89.107.53.2/32;
                    }
                }
                then {
                    accept;
                }
            }
            term router {
                from {
                    source-address {
                        89.107.53.6/32;
                    }
                }
                then {
                    accept;
                }
            }
        }
    }
}
```

6.1.3. Multiple routers, single provider with multiple routers

In this scenario, multiple routers at the customer's side connect to multiple routers on the provider's side. On the customer's side, this scenario is almost the same as the previous scenario.

On the provider's side, a system like HSRP or VRRP can be used. However, the use of a dynamic routing protocol inside the provider's network is more common. This would then be used to announce the customer's networks into the provider's network. A higher weight is used for the preferred link.

Even though both scenarios are different at a routing level, they are similar when seen from the spoofing security level; strict uRPF and similar static filters can be used.

It is important to keep in mind that, for the uRPF configuration to work, both sides (customer and provider) must select the same link as "active". If they select a different link as active, uRPF will block all traffic.

```
               ---------
            ///         \\\
          //              \\
          //                \\
          |                  |
        |    Provider        |
        |    network          |
        |                    |
          |                  |
          \|                //
          |\              //
           | \\\         ///|
           |    ---------   |
           |               |
           |               |
 +---------+-+           +-+---------+
 |Provider   |           |Provider   |
 |router A   |           |router B   |
 |           |           |           |
 +-----+-----+           +----+------+
       |                      |
       |                      |
 +-----+-----+            +----+------+
 |Customer   |           |Customer   |
 |router A   |           |router B   |
 |           |           |           |
 +-----------++          +--+---------+
           |                |
           |                |
           |   ---------    |
           |//          \   |
          /|              \ |
          |    Customer    \|
          |    network      |
          |                 |
           \\             //
            \\          //
               ---------
```

Cisco version

Filters on provider router A (PE)

```
! CEF is needed for uRPF
ip cef
router ospf 10
 network 89.107.54.0 0.0.0.255 area 1
 redistribute static
interface ATM0/1.1 point-to-point
 description Interface to customer
 ip address 89.107.53.1 255.255.255.252
 ! Packets are filtered based on a static list
 ip access-group customer-routes in
  ! Strict uPRF filtering
 ip verify unicast reachable-via rx
...
interface FastEthernet0/0
 ip address 89.107.54.2 255.255.255.0
 standby 1 ip 89.107.54.1
 standby 1 preempt
 standby 1 priority 150
 standby 1 track ATM0/1.1
...
! Routes for the customer prefix
ip route 89.107.52.0 255.255.255.0 ATM0/1.1 10
ip route 89.107.52.0 255.255.255.0 89.107.54.3 20
! Static list of networks to filter
! Public address of the CPE router
```

```
ip access-list extended customer-routes
 permit ip 89.107.53.2 0.0.0.0 any
 ! Public address range of the customer
 permit ip 89.107.52.0 0.0.0.255 any
 deny ip any any
```

Filters on provider router B (PE)

```
! CEF is needed for uRPF
ip cef
router ospf 10
 network 89.107.54.0 0.0.0.255 area 1
 redistribute static
interface ATM0/1.1 point-to-point
 description Interface to customer
 ip address 89.107.53.5 255.255.255.252
 ! Packets are filtered based on a static list
 ip access-group customer-routes in
  ! Strict uRPF filtering
 ip verify unicast reachable-via rx
...
interface FastEthernet0/0
 ip address 89.107.54.3 255.255.255.0
 standby 1 ip 89.107.54.1
 standby 1 preempt
 standby 1 priority 75
 standby 1 track ATM0/1.1
...
ip route 89.107.52.0 255.255.255.0 ATM0/1.1 10
ip route 89.107.52.0 255.255.255.0 89.107.54.2 20
! Static list of networks to filter
! Public address of the CPE router
ip access-list extended customer-routes
 permit ip 89.107.53.6 0.0.0.0 any
 ! Public address range of the customer
 permit ip 89.107.52.0 0.0.0.255 any
 deny ip any any
```

Juniper version

Filters on provider router A (PE)

```
interfaces {
    e3-0/0/0 {
        description "Interface to customer";
        hold-time up 200 down 200;
        clocking internal;
        encapsulation ppp;
        e3-options {
            compatibility-mode kentrox;
            payload-scrambler;
            fcs 32;
        }
        unit 0 {
            family inet {
                filter {
                    input customer;
                }
                address 89.107.53.1/30;
                /* Strict uRPF can be used here, */
                /* although it is redundant */
                rpf-check;
            }
        }
    }
    fe-0/3/0 {
        description ”Provider network";
        unit 0 {
            family inet {
                address 89.107.54.2/24;
            }
        }
    }
}
protocols {
    ospf {
        import statics;
        area 0.0.0.1 {
            interface fe-0/3/0.0;
        }
    }
}
chassis {
    no-source-route;
}
routing-options {
    static {
        route 89.107.52.0/24 next-hop e3-0/0/0;
    }
}
firewall {
    family inet {
        filter customer {
            term network {
                from {
                    source-address {
                        89.107.52.0/24;
                    }
                }
                then {
                    accept;
                }
            }
            term router {
                from {
                    source-address {
                        89.107.53.2/32;
                    }
                }
                then {
                    accept;
                }
            }
        }
    }
}
policy-options {
    policy-statement statics {
        from protocol static;
        then accept;
    }
}
```

Filters on provider router B (PE)

```
interfaces {
    e3-0/0/0 {
        description "Interface to customer";
        hold-time up 200 down 200;
        clocking internal;
        encapsulation ppp;
        e3-options {
            compatibility-mode kentrox;
            payload-scrambler;
            fcs 32;
        }
        unit 0 {
            family inet {
                filter {
                    input customer;
                }
                address 89.107.53.5/30;
                /* Strict uRPF can be used here, */
                /* although it is redundant */
                rpf-check;
            }
        }
    }
    fe-0/3/0 {
        description "Provider network";
        unit 0 {
            family inet {
                address 89.107.54.3/24;
            }
        }
    }
}
protocols {
    ospf {
        import statics;
        area 0.0.0.1 {
            interface fe-0/3/0.0;
        }
    }
}
chassis {
    no-source-route;
}
routing-options {
    static {
        route 89.107.52.0/24 next-hop e3-0/0/0;
    }
}
firewall {
    family inet {
        filter customer {
            term network {
                from {
                    source-address {
                        89.107.52.0/24;
                    }
                }
                then {
                    accept;
                }
            }
            term router {
                from {
                    source-address {
                        89.107.53.6/32;
                    }
                }
                then {
                    accept;
                }
            }
        }
    }
```

```
}
policy-options {
    policy-statement statics {
        from protocol static;
        then accept;
    }
}
```

6.1.4. Single customer outer, multiple providers, load balancing

In this scenario, a single router (CPE) has links to separate links to different providers. This is one of the most common multihoming scenarios. The CPE selects the best route through various mechanisms, like static routing or BGP. The CPE can peer with each ISP over BGP, announcing the customer's PI space, PA space assigned to the customer or a combination of these.

```
     +--------+
     |        | 1
     | isp A  +--------------------+
     |        |                    |          |
     |        |                    |          |
     +--------+                    |  3       |
                              +----+----+     |
                              |         |5    |
                              | cust    +-----+
                              |         |     |
                              |         |     |
                              +----+----+     |
                                   |  4       |
     +--------+                    |          |
     |        |                    |
     |        | 2                  |
     | isp B  +--------------------+
     |        |
     +--------+
```

Figure 6.1-1

CPE interfaces to the transit providers

The CPE will accept a set of routes from the transit providers. In some cases, default routes can be assigned to one or more (in case of resilient links) of the provider interfaces. In other cases, BGP will select the best available route.

At these transit interfaces, anti-spoofing measures can include:

- Bogon filtering via access-lists (see section 4.3)
- Loose uRPF, or if available, feasible path uRPF. This can be activated for each interface that is connected to one of the providers (interfaces 3 and 4 of the Figure 5.1-1) by using the following commands:

Cisco routers

```
ip cef
interface FastEthernet0/0
 ! Configure the interface (IOS versions 12.2T+)
 ip verify unicast source reachable-via any
```

Juniper routers

```
[edit routing-options forwarding-table]
    unicast-reverse-path feasible-paths;
```

```
/* And */
[edit interfaces fe-0/0/0]
    unit 0 {
        family inet {
            rpf-check; {
                mode loose;
            }
        }
    }
```

CPE interfaces to the customer's network

If the CPE has interfaces that connect to the customer's network, using public addressing, various anti-spoofing measures can be used.

Which measures fit best, depend on whether there is more than one CPE interface per network. In this context, two networks are seen as separate when they use different addresses.

Single interface per network

When no more than one interface per network is used, strict uRPF can be applied to each of the CPE interfaces that are connected to the customer's networks. This will help drop spoofed traffic from hosts inside the customer's networks, generated by, for example, botnets.

Cisco routers

```
ip cef
interface FastEthernet0/0
 ! Configure the interface with strict uRPF
 ip verify unicast source reachable-via rx
```

Juniper routers

```
[edit routing-options forwarding-table]
    unicast-reverse-path feasible-paths;
/* And */
[edit interfaces fe-0/0/0]
    unit 0 {
        family inet {
            rpf-check;
        }
    }
```

Multiple interfaces per network

Where more than one interface per network is used, asymmetric routing may occur. Therefore, strict uRPF may drop legitimate traffic in situations where no default route is present. Feasible-path uRPF will have to be used or, if feasible-path is unavailable, loose uRPF.

In the figure 5.1-2, all the interfaces will operate in loose or feasible-path uRPF mode. In case the customer's routers have a default route configured, only interfaces 9 and 10 will have loose or feasible-path uRPF configured.

```
      +--------+
      |        |1                                |
      | isp A  +------------------------+        |
      |        |                       |  5      |
      +-----+---+                +----+---+     |
           |2                   |        |      |
           |                   6| cust   +------+
        +------------------------+       |9     |
        |  |                    +--------+      |
        |  |                                    |
        |  |                    +--------+      |
        |  |                   7|        |      |
        |  +---------------------+ cust   +------+
        |                       |        |10    |
        |3                      +----+---+      |
      +--+-----+                     |8         |
      |        |                     |          |
      |        |4                    |          |
      | isp B  +-----------------------+        |
      |        |
```

Figure 5.1-2

6.2. Customer access networks

Customer access networks are the equipment deployed by ISPs and carriers to aggregate a large number of customers (e.g. broadband concentrators, dial-up RAS, etc.)

This equipment generally has:

- Point-to-point interfaces to customers, one interface per customer, with a prefix assigned to each customer interface
- One or more transit interfaces connected to the Internet

In this case, strict uRPF can be configured on the interfaces facing customers. These interfaces are one of the best-suited uses for uRPF, as IP addresses are often assigned dynamically (for example, with a RADIUS server). This makes the use of static filters impossible.

Cisco configuration

For a Cisco AS5300 the configuration would be as follows:

```
! CEF is needed for uRPF
ip cef
! Configure a dial-in group
interface Group-Async1
 ip unnumbered Loopback0
 no ip directed-broadcast
 ! The IP address is dynamically assigned, so static
 ! filters can not be used.
 ! Therefore, enable strict uRPF
 ip verify unicast source reachable-via rx
 encapsulation ppp
 async mode interactive
 peer default ip address pool dialin_pool
 no cdp enable
 ppp authentication chap pap
 group-range 1 96
```

6.3. Core networks

Core networks are not as clearly split as customer/provider scenarios. In most cases, packets with any valid address can arrive on any interface.

Therefore, the recommendation is to filter only the well-known bogon prefixes, and work with customers to help them implement stricter rules in their access networks.

The basic recommended configuration for a core router is:

Cisco version

```
! CEF is needed for uRPF
ip cef
interface ATM0/1.1 point-to-point
 description Interface to core A
 ip address 89.107.53.2 255.255.255.252
 ! Packets are filtered based on a static list
 ip access-group bogons in
interface ATM0/2.1 point-to-point
 description Interface to core B
 ip address 89.107.54.2 255.255.255.252
 ! Packets are filtered based on a static list
 ip access-group bogons in
...
! Manually maintained list of networks to be filtered
! These are the private and reserved networks
ip access-list extended bogons
 deny ip 10.0.0.0 0.255.255.255 any
 deny ip 192.168.0.0 0.0.255.255 any
 deny ip 172.16.0.0 0.15.255.255 any
 deny ip 127.0.0.0 0.255.255.255 any
 deny ip 169.254.0.0 0.0.255.255 any
 deny ip 192.0.2.0 0.0.0.255 any
 deny ip 198.18.0.0 0.1.255.255 any
 deny ip 240.0.0.0 15.255.255.255 any
 ! External address of this router
 deny ip 89.107.53.2 0.0.0.0 any
 deny ip 89.107.54.2 0.0.0.0 any
 permit ip any any
```

Juniper version

```
interfaces {
    e3-0/0/0 {
        description "Interface to provider";
        hold-time up 200 down 200;
        clocking internal;
        encapsulation ppp;
        e3-options {
            compatibility-mode kentrox;
            payload-scrambler;
            fcs 32;
        }
        unit 0 {
            family inet {
                filter {
                    input bogons;
                }
                address 89.107.53.2/30;
            }
        }
    }
    e3-0/1/0 {
        description "Interface to provider";
        hold-time up 200 down 200;
        clocking internal;
        encapsulation ppp;
        e3-options {
            compatibility-mode kentrox;
            payload-scrambler;
            fcs 32;
        }
        unit 0 {
            family inet {
                filter {
                    input bogons;
                }
                address 89.107.54.2/30;
            }
        }
    }
}
chassis {
    no-source-route;
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop e3-0/0/0;

    }
}
policy-options {
    prefix-list bogon-list {
        10.0.0.0/8;
        192.168.0.0/16;
        172.16.0.0/12;
        127.0.0.0/8;
        169.254.0.0/16;
        192.0.2.0/24;
        198.18.0.0/15;
        240.0.0.0/4;
    }
}
firewall {
    family inet {
        filter bogons {
            term bogons {
                from {
                    prefix-list {
                        bogon-list;
                    }
                }
                then {
                    discard;
                }
            }
            term default {
                then {
                    accept;
                }
            }
        }
    }
}
```

7. IPv6

Although IPv6 is not very widely deployed yet, the recommendation is to implement anti-spoofing filters for it. The preferred solution is uRPF, but static filters based on martian addresses and bogon lists are also possible. A large part of the content of this chapter is extracted from the excellent page created by Gert

Döring [5]. A complete list of bogon addresses in IPv6 can be obtained from Team Cymru [6].

Many of the recommendations for IPv6 are similar to those stated for IPv4.

7.1. uRPF

Cisco routers

uRPF is available for IPv6 on Cisco high end series (12000, 7600 and so on) as of release 12.0(31)S.

The commands to configure uRPF for IPv6 are almost exactly the same as for IPv4. The only difference is that "ip" should be replaced by "ipv6". For example, to use uRPF for IPv4 and IPv6, replace:

```
ip verify unicast source reachable-via rx
```

with:

```
ip verify unicast source reachable-via rx
ipv6 verify unicast source reachable-via rx
```

Juniper routers

To enable uRPF for IPv6 on Juniper routers, simply replace "inet" with "inet6" in the previous examples. For example, to use uRPF for IPv4 and IPv6, replace:

```
[edit interfaces fe-0/0/0]
    unit 0 {
        family inet {
            rpf-check;
        }
    }
```

with:

```
[edit interfaces fe-0/0/0]
    unit 0 {
        family inet {
            rpf-check;
        }
        family inet6 {
            rpf-check;
        }
    }
```

7.2. Routes from customers

For routes received from customers, simple filters can be used. The customer's prefix is accepted, anything else is denied.

Cisco routers

```
ipv6 prefix-list ipv6-from-customer permit 2001:db8::/32
ipv6 prefix-list ipv6-from-customer deny 0::/0 le 128
```

Juniper routers

```
policy-statement ipv6-from-customer {
    from {
        family inet6;
        route-filter 2001:db8::/32 exact next policy;
    }
    then reject;
}
```

7.3. Routes from peers

If static filters are used for routes received from peers, a strategy similar to that for IPv4 must be applied. These filters block packets using bogon addresses, but do not take possible other issues into account.

7.3.1. Blocking martians

In the simplest case, all known martians are blocked. The martians are:

- 3FFE::/16 - used for 6bone in the past
- 2001:db8::/32 – reserved for documentation
- 0000::/8 – used for loopback, IPv4 mapping, etc.
- FE00::/9 and FF00::/8
- 2001:4030:f::/48 – example range for the internal network in this example

When setting up filters for this, the result is:

Cisco version

```
ipv6 prefix-list ibv6-ebgp deny 2001:4030:f::0/48 le 128
ipv6 prefix-list ipv6-ebgp deny 3ffe::/16 le 128
ipv6 prefix-list ipv6-ebgp deny 2001:db8::/32 le 128
ipv6 prefix-list ipv6-ebgp deny 0000::/8 le 128
ipv6 prefix-list ipv6-ebgp deny fe00::/9 le 128
ipv6 prefix-list ipv6-ebgp deny ff00::/8 le 128
ipv6 prefix-list ipv6-ebgp permit any
```

Juniper version

```
policy-statement ipv6-ebgp {
   from {
        family inet6;
        route-filter 3ffe::/16 orlonger;
        route-filter ::/8 orlonger;
        route-filter 2001:db8::/32 orlonger;
        route-filter fe00::/9 orlonger;
        route-filter ff00::/8 orlonger;
        route-filter ::/0 upto /48 next policy;
    }
   then reject;
}
```

7.3.2. Blocking martians and bogons

A more extensive filter can also include the IPv6 bogons: the pool of addresses that IANA has not yet assigned. However, when using this list, it is essential to keep it up-to-date.

Cisco version

```
ipv6 prefix-list ibv6-ebgp deny 2001:4030:f::0/48 le 128
ipv6 prefix-list ipv6-ebgp deny 3ffe::/16 le 128
ipv6 prefix-list ipv6-ebgp deny 2001:db8::/32 le 128
ipv6 prefix-list ipv6-ebgp permit 2001::/32
ipv6 prefix-list ipv6-ebgp permit 2002::/16
ipv6 prefix-list ipv6-ebgp permit 2003::/16
ipv6 prefix-list ipv6-ebgp permit 2400::/12
ipv6 prefix-list ipv6-ebgp permit 2600::/12
ipv6 prefix-list ipv6-ebgp permit 2610::/23
ipv6 prefix-list ipv6-ebgp permit 2620::/23
ipv6 prefix-list ipv6-ebgp permit 2800::/12
```

```
ipv6 prefix-list ipv6-ebgp permit 2a00::/12
ipv6 prefix-list ipv6-ebgp permit 2c00::/12
ipv6 prefix-list ipv6-ebgp deny 0000::/8 le 128
ipv6 prefix-list ipv6-ebgp deny fe00::/9 le 128
ipv6 prefix-list ipv6-ebgp deny ff00::/8 le 128
ipv6 prefix-list ipv6-ebgp deny 0::/0 le 128
```

Juniper version

```
policy-statement ipv6-ebgp {
    term pass-some {
        from {
            family inet6;
            route-filter 3ffe::/16 orlonger reject;
            route-filter 2001:500::/30 prefix-length-range /48-
/48;
            route-filter 2001:db8::/32 orlonger reject;
            route-filter 2001::/32 longer;
            route-filter 2002::/16 longer;
            route-filter 2003::/16 longer;
            route-filter 2400::/12 longer;
            route-filter 2600::/12 longer;
            route-filter 2610::/23 longer;
            route-filter 2620::/23 longer;
            route-filter 2800::/12 longer;
            route-filter 2a00::/12 longer;
            route-filter 2c00::/12 longer;
        }
        then next policy;
    }
    term reject-rest {
        from family inet6;
        then reject;
    }
}
```

8. Conclusion

The application of one or more of these guidelines will not assure that all attacks can be stopped. Even some attacks that use spoofed addresses will not be stopped. For example, if the attack comes from a different network, that did not apply the recommendations as stated in this document, the computers in that network can use any address on the Internet without being detected.

However, if all ISPs would implement these measures, the usability of spoofed IP addresses for attacks would be dramatically limited and the origin of malicious packets would be a lot easier to discover. Even if not all ISPs implement these guidelines, their use can still prevent some attacks. This includes one of the most dangerous attacks: those that use spoofed addresses from your own networks.

9. References

[1] Savola & Baker, RFC 3704

[2] http://www.cymru.com/Bogons/index.html

[3]
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fothersf/scfrpf.htm

[4] Savola, draft-savola-bcp84-urpf-experiences-03.txt (updated version)

[5] http://www.space.net/~gert/RIPE/ipv6-filters.html

[6] http://www.cymru.com/Bogons/ipv6.txt