
nic.br
Núcleo de Informação
e Coordenação do
Ponto BR
cgi.br
Comitê Gestor da
Internet no Brasil
registro.br cert.br cetic.br ceptro.br ptt.br

Antispoofing techniques for Internet Service Providers

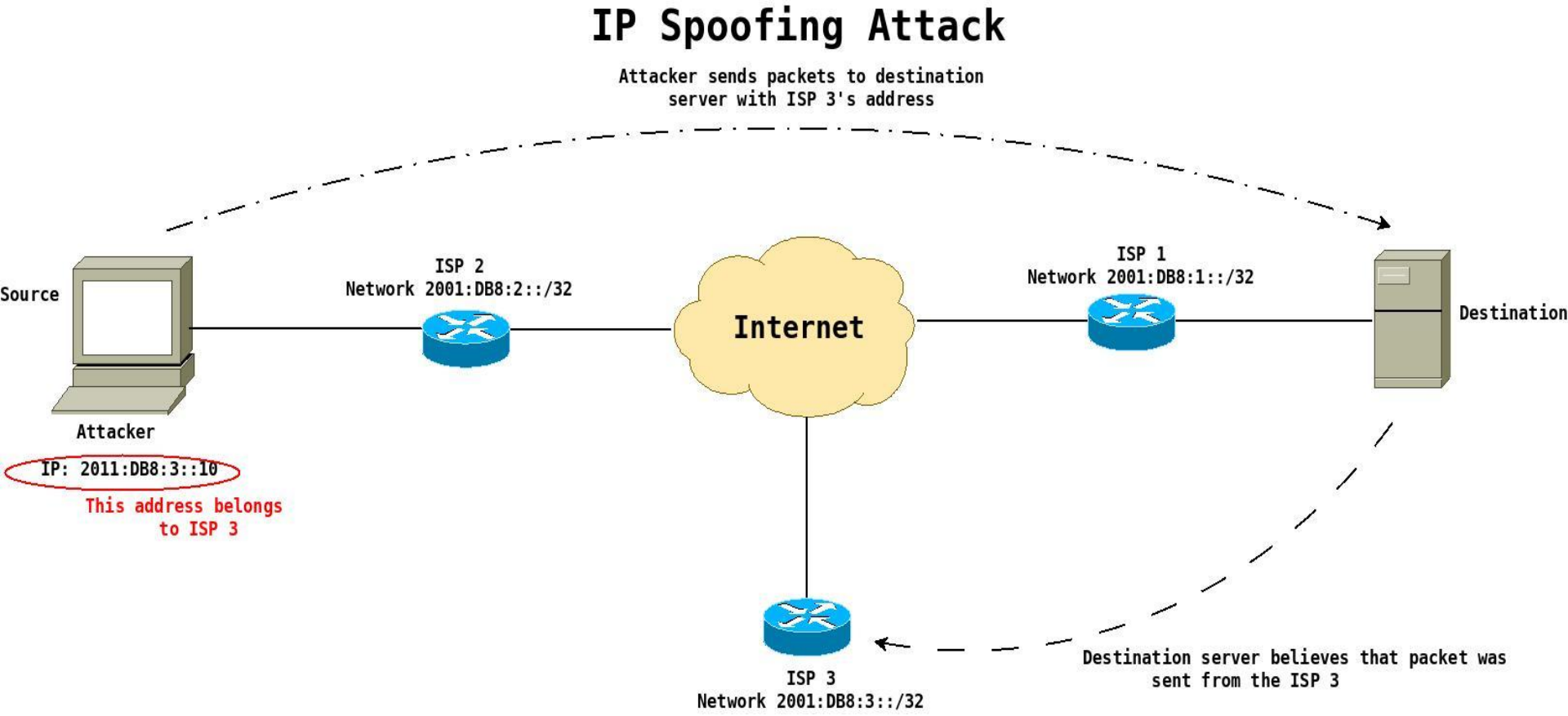
ceptro.br nic.br cgi.br

What is IP Spoofing?

- Packets with a **false IP source address**
  - **Misconfiguration**
    - Software problem
  - **Simulation and Test**
    - Performance test
  - **Malicious intent**
    - Hides the identity of the sender
    - Impersonates another computing system

- Most frequently used for **Denial Of Service attack**
  - **Anyone can be a victim!!!**

Understanding the problem



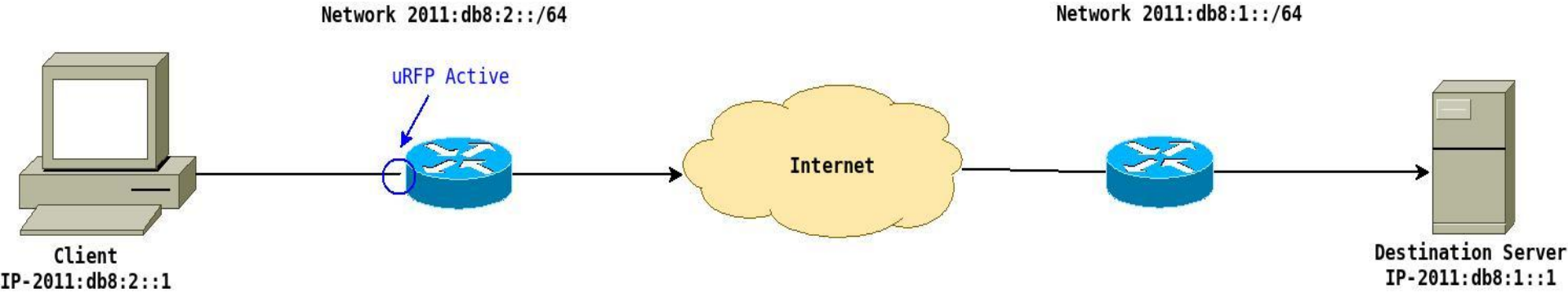
Proposed Solutions

- **Ingress Access Lists**
  - **Access Control List - ACLs**

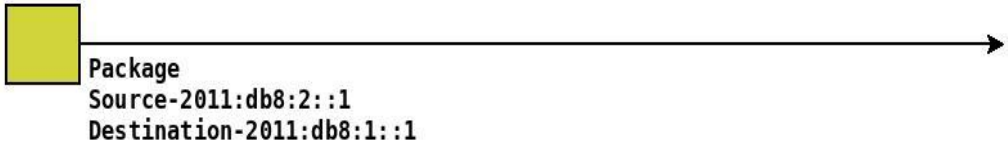
- **Unicast Reverse Path Forward (uRPF)**
  - **Strict Mode**
  - **Loose Mode**
  - **Feasible Path**
  - **VRF Mode**

- **Source Address Validation Improvement (SAVI)**

uRPF



The router searches for one route entry for the source address in the routing table.
If it founds, the packet is transmitted. Otherwise it discartds the packet.



uRPF commands

- **Cisco**
  - ip cef
    ipv6 cef
    interface GigabitEthernet0/1
    ip verify unicast source reachable-via rx
    ipv6 verify unicast source reachable-via rx

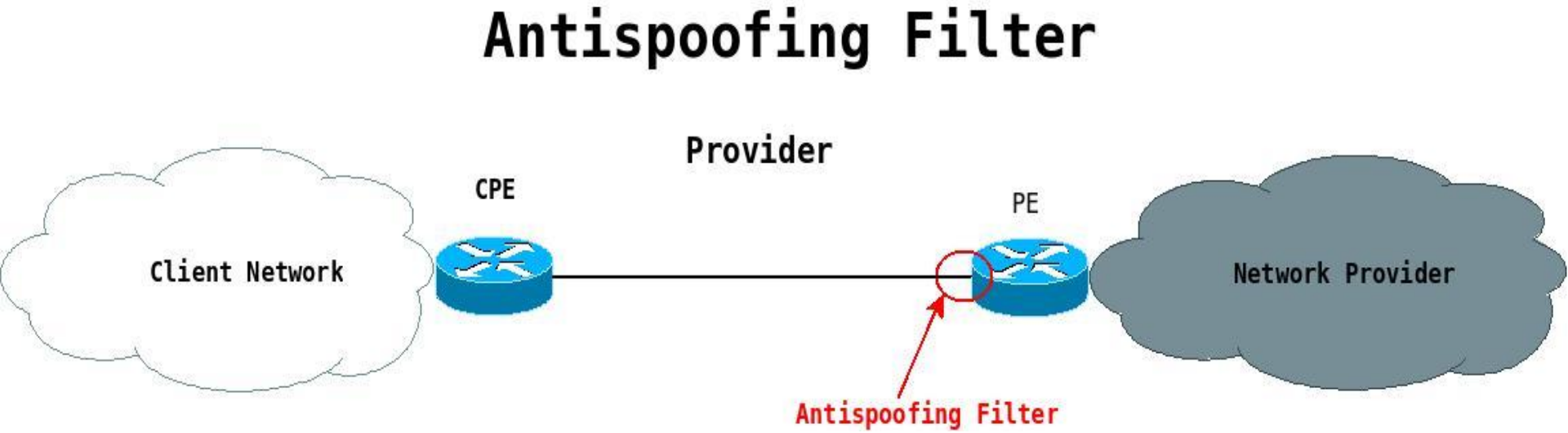
- **Juniper**
  - interfaces {
        ge-0/0/0 {
            unit 0 {
                family inet {
                    rpf-check;
                }
            }
        }
    }

uRPF commands

- **Juniper (continuation)**
  - interfaces {
    ge-0/0/0 {
    unit 0 {
    family inet6 {
    rpf-check;
    }
    }
    }
    }

- **Mikrotik**
  - **# beware this command apply rpf in all interfaces**
  - /ip settings set rp-filter=strict

Filter


Antispoofing Filter
Provider
CPE
PE
Client Network
Network Provider
Antispoofing Filter

Filter commands

- **Cisco**
  - interface GigabitEthernet0/1
    ip access-group FILTRO-CLIENTE-V4 in
    ipv6 traffic-filter FILTRO-CLIENTE-V6 in
    ...
    ip access-list extended FILTRO-CLIENTE-V4
    ! Your client IP address
    permit ip 192.0.2.2 0.0.0.0 any
    ! Your client range IP address
    permit ip 192.0.2.0 0.0.0.255 any
    ! Reject everything else
    deny ip any any
    ...
    ipv6 access-list extended FILTRO-CLIENTE-V6
    ! Your client IPv6 address
    permit ipv6 2001:DB8:CAFE:FACA::2/64 any
    ! Your client range IPv6 address
    permit ipv6 2001:DB8:CAFE::/48 any
    ! Reject everything else
    deny ipv6 any any

Filter commands

- **Mikrotik**
  - /ip firewall address-list
    # Your client IP address
    add address=192.0.2.2/32 list=FILTER-CLIENT-V4
    # Your client range IP address
    add address=192.0.2.0/24 list=FILTER-CLIENT-V4
    /ip firewall filter
    add chain=forward in-interface=ether1 src-address-list=FILTER-CLIENT-V4
    add action=drop chain=forward in-interface=ether1
    …
    /ipv6 firewall address-list
    # Your client IPv6 address
    add address=2001:DB8:CAFE:FACA::2/64 list=FILTRO-CLIENTE-V6
    # Your client range IPv6 address
    add address=2001:DB8:CAFE::/48 list=FILTRO-CLIENTE-V6
    /ipv6 firewall filter
    add chain=forward in-interface=ether1 src-address-list=FILTRO-CLIENTE-V6
    add action=drop chain=forward in-interface=ether1

Filter commands

- **Juniper**
  - interfaces {
    ge-0/0/0 {
    unit 0 {
    family inet {
    filter {
    input CLIENT-V4;
    }
    }
    family inet6 {
    filter {
    input CLIENTES-V6;
    }
    }
    }
    }
    }

Filter commands

- **Juniper (continuation)**

```
policy-options {
        prefix-list FILTRO-CLIENTE-V4{
                /* Your client IP address */
                192.0.2.2/32;
                /* Your client range IP address */
                192.0.2.0/24;
        }
        prefix-list FILTRO-CLIENTE-V6{
                /* Your client IPv6 address */
                2001:DB8:CAFE:FACA::2/64;
                /* Your client range IPv6 address */
                2001:DB8:CAFE::/48;
        }
}
```

Filter commands

- **Juniper (continuation)**
  - firewall {
    family inet {
    filter CLIENTES-V4{
    term 1 {
    from {
    source-prefix-list {
    FILTRO-CLIENTE-V4;
    }
    }
    then {
    accept;
    }
    }
    term DEFAULT{
    then {
    discard;
    }
    }
    }
    }
    }

Filter commands

- **Juniper (continuation)**

```
firewall {
    family inet6 {
        filter CLIENTES-V6{
            term 1 {
                from {
                    source-prefix-list {
                        FILTRO-CLIENTE-V6;
                    }
                }
                then {
                    accept;
                }
            }
            term DEFAULT{
                then {
                    discard;
                }
            }
        }
    }
}
```

Recommendations

- **Test your configuration**
  - **Caida**
    - https://www.caida.org/projects/spoofer/

- **Obtaining a peering session**
  - **Team Cymru**
    - https://www.team-cymru.com/bogon-reference.html
  - **Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF)**
    - https://tools.ietf.org/html/rfc5635

Recommendations

- **RFC 3704 - BCP 84**
  - https://tools.ietf.org/html/rfc3704

- **MANRS**
  - https://www.manrs.org/guide/antispoofing/

- **BCP -> NIC.BR**
  - https://bcp.nic.br/antispoofing

Questions?

Thank You

Eduardo Barasal Morales

emorales@nic.br

nic.br cgi.br

www.nic.br | www.cgi.br