Campanha Anti-Spoofing

Anexo A.1 – Tutorial de configuração para Provedores/PoPs

Roteadores Juniper

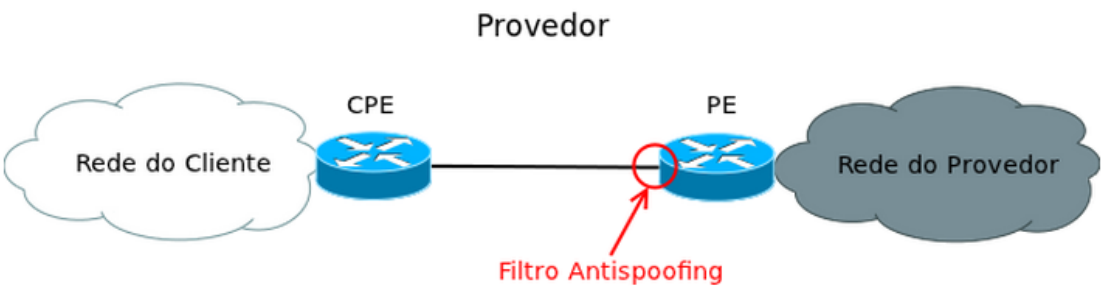
RNP MINISTÉRIO DA DEFESA MINISTÉRIO DA CULTURA MINISTÉRIO DA SAÚDE MINISTÉRIO DA EDUCAÇÃO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES BRASIL GOVERNO FEDERAL

Anexo A.1 – Tutorial de configuração para Provedores/PoPs

O CAIS/RNP visando apoiar a disseminação de boas práticas em Segurança da Informação, está fornecendo este tutorial baseado no Portal de Boas Práticas para a Internet no Brasil auxiliando a implantação de controles de segurança para mitigação de ataques realizados através da técnica do IP Spoofing para redes que utilizam equipamentos do fabricante Juniper.

Abaixo estão disponíveis as configurações relacionadas a implementação do RPF (Reverse Path Forwarding) e de um filtro que restringe a comunicação para que somente os endereços atribuídos ao cliente como origem sejam permitidos e encaminhados para Internet (IP do roteador do cliente e o range de IP do mesmo), conforme as recomendações de boas práticas dos documentos BCP38 e BCP84.

Filtro para ser aplicado na interface do PE conectado ao CPE



Fonte: Portal de Boas Práticas para a Internet no Brasil

Os comandos a seguir são exemplos genéricos de configuração, informamos que ambientes Multihomed necessitam de maior atenção na implantação do RPF, e caso não se aplique, recomendamos a configuração dos demais filtros após uma avaliação prévia de impacto em seu cenário.

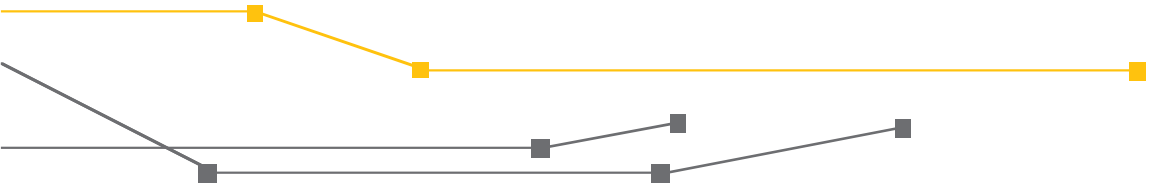
Configuração para IPv4

```
interfaces {
   ge-0/0/0 {
             unit 0 {
          family inet {
              filter {
                  input CLIENTES-V4;
              }
             /* Endereço da interface do roteador */
             /* Precisa trocar */
```

```
                address 192.0.2.1/30;
                /* habilitando Strict uRPF  */
                 rpf-check;
            }
        }
    }
}
policy-options {


     prefix-list FILTRO-CLIENTE-V4{
          /* Permite o IP alocado para o CPE do cliente */
          /* Troque este endereço pelo que é usado em sua rede! */
         192.0.2.2/32;
         /* Permite o range de IPs alocados para o seu cliente */
         /* Troque este endereço pelo que é usado em sua rede! */
         192.0.2.0/24;
     }
}
firewall {
   family inet {
       filter CLIENTES-V4{
           term 1 {
               from {
                   source-prefix-list {
                       FILTRO-CLIENTE-V4;
                   }
               }
               then {
                  accept;
               }
           }
           term DEFAULT{
                then {
                       /* Rejeita todo os outros endereços que o cliente pode
usar para fazer ataque */
                       discard;
                }
           }
       }
   }
}
```

Fonte: Portal de Boas Práticas para a Internet no Brasil



Configuração para IPv6

```
interfaces {
   ge-0/0/0 {
             unit 0 {
          family inet6 {
              filter {
                  input CLIENTES-V6;
              }
             /* Endereço da interface do roteador */
             /* Precisa trocar */
             address 2001:DB8:CAFE:FACA::1/64;
             /* habilitando Strict uRPF  */
              rpf-check;
          }
       }
   }
}
policy-options {
     prefix-list FILTRO-CLIENTE-V6{
          /* Permite o IP alocado para o CPE do cliente */
          /* Troque este endereço pelo que é usado em sua rede! */
         2001:DB8:CAFE:FACA::2/64;
         /* Permite o range de IPs alocados para o seu cliente */
         /* Troque este endereço pelo que é usado em sua rede! */
         2001:DB8:CAFE::/48;
    }
}
firewall {
   family inet6 {
       filter CLIENTES-V6{
           term 1 {
               from {
                   source-prefix-list {
                       FILTRO-CLIENTE-V6;
                   }
               }
               then {
                  accept;
               }
           }
           term DEFAULT{
               then {
                   /* Rejeita todo os outros endereços que o cliente pode us
ar para fazer ataque */
                   discard;
               }
           }
         }
```

```
    }
}
```

Fonte: Portal de Boas Práticas para a Internet no Brasil

Fontes:

Portal de Boas Práticas para a Internet no Brasil. Disponível em: <http://bcp.nic.br/>. Acesso em: 04/12/2017.

IETF Tools. Disponível em: <https://tools.ietf.org>. Acesso em 04/12/2017.

Créditos:

RNP
Rede Nacional de Ensino e Pesquisa

Realização:

CAIS
Centro de Atendimento a Incidentes de Segurança da RNP

Apoio

GO
Gerência de Operações de Redes

GER
Gerência de Engenharia de Redes