

Campanha Anti-Spoofing

Anexo A.2 – Tutorial de configuração para Clientes

Roteadores Juniper



RNP

MINISTÉRIO DA
DEFESA

MINISTÉRIO DA
CULTURA

MINISTÉRIO DA
SAÚDE

MINISTÉRIO DA
EDUCAÇÃO

MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA,
INOVAÇÕES E COMUNICAÇÕES

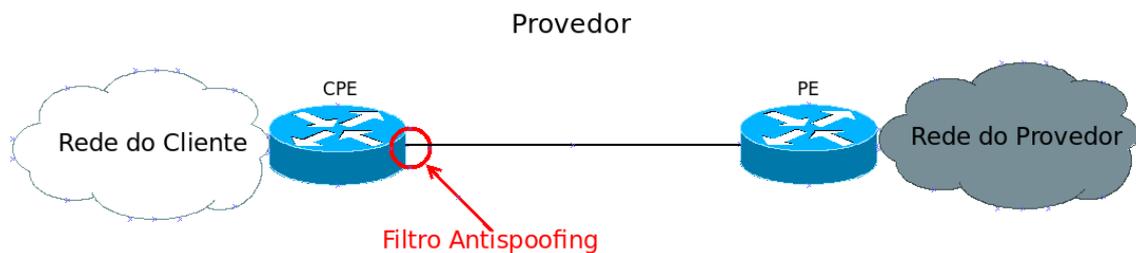


Anexo A.2 – Tutorial de configuração para Clientes

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 de pacotes com origem de endereços reservados que não devem ser roteados pela internet, conforme as recomendações de boas práticas dos documentos BCP38 e BCP84.

Filtro para ser aplicado na interface do CPE conectado ao PE



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 BOGONS;
        }
        /* Endereço da interface do roteador */
        /* Precisa trocar */
      }
    }
  }
}
```

```

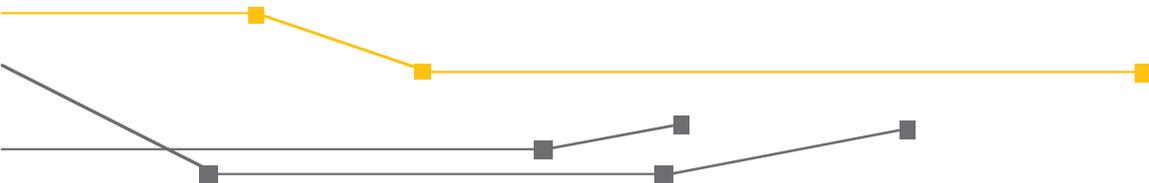
        address 192.0.2.1/30;
        /* habilitando Strict uRPF */
        rpf-check;
    }
}
}
}
policy-options {
    prefix-list FILTRO-BOGONS-V4{
        /* faixa de endereços reservados para identificar que o host pertence a rede local */
        0.0.0.0/8;
        /* faixa de endereços privados */
        10.0.0.0/8;
        /* faixa de endereços privados do CGNAT */
        100.64.0.0/10;
        /* faixa de endereços reservados para loopback */
        127.0.0.0/8;
        /* faixa de endereços reservados para escopo local */
        169.254.0.0/16;
        /* faixa de endereços privados */
        172.16.0.0/12;
        /* faixa de endereços reservado para atribuição a protocolos específicos */
        192.0.0.0/24;
        /* faixa de endereços reservado para documentação */
        192.0.2.0/24;
        /* faixa de endereços privados */
        192.168.0.0/16;
        /* faixa de endereços reservado para testes - benchmarking */
        198.18.0.0/15;
        /* faixa de endereços reservado para documentação */
        198.51.100.0/24;
        /* faixa de endereços reservado para documentação */
        203.0.113.0/24;
        /* faixa de endereços reservado da antiga classe D de multicast e uso futuro */
        224.0.0.0/3;
    }
}
firewall {
    family inet {
        filter BOGONS{
            term 1 {
                from {
                    source-prefix-list {
                        FILTRO-BOGONS-V4;
                    }
                }
                then {
                    discard;
                }
            }
        }
    }
}

```



```
FILTRO-BOGONS-V6-DENY;
}
}
then {
  discard;
}
}
}
term 2{
  from {
    source-prefix-list {
      LISTA-BOGONS-V6-ACCEPT;
    }
  }
  then {
    accept;
  }
}
term DEFAULT{
  then {
    /* bloqueia todo o resto */
    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



MINISTÉRIO DA
DEFESA

MINISTÉRIO DA
CULTURA

MINISTÉRIO DA
SAÚDE

MINISTÉRIO DA
EDUCAÇÃO

MINISTÉRIO DA
**CIÊNCIA, TECNOLOGIA,
INOVAÇÕES E COMUNICAÇÕES**

