Campanha Anti-Spoofing

Anexo B.2 – Tutorial de configuração para Clientes

Roteadores Cisco

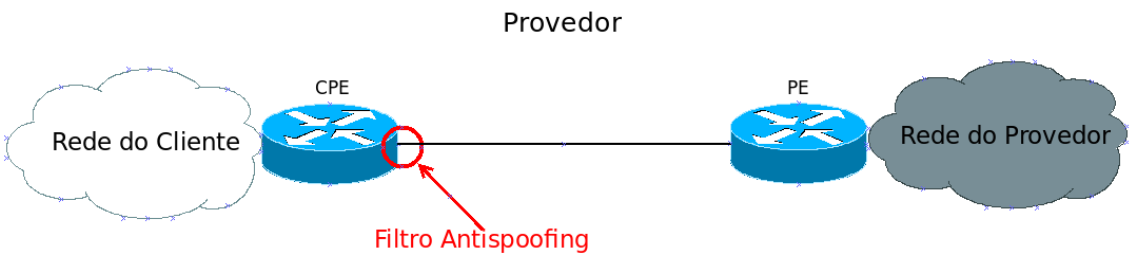
RNP MINISTÉRIO DA DEFESA MINISTÉRIO DA CULTURA MINISTÉRIO DA SAÚDE MINISTÉRIO DA EDUCAÇÃO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES BRASIL GOVERNO FEDERAL

Anexo A.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 Cisco.

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

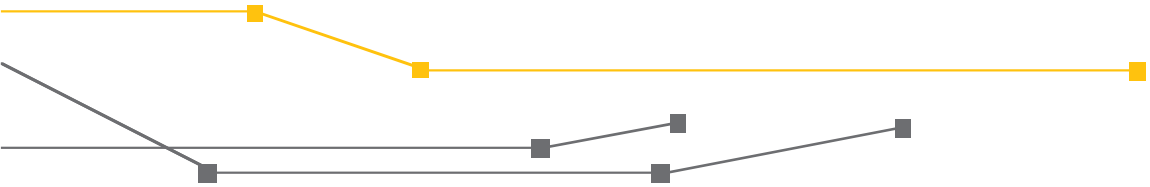


Fonte: Portal de Boas Práticas para a Internet no Brasil

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

```
! CEF é preciso para uRPF strict
ip cef
interface GigabitEthernet0/1
! Endereço da interface do roteador
! Troque este endereço pelo que é usado em sua rede!
ip address 192.0.2.1 255.255.255.252
 ! Aplicando Filtro estatico baseado no endereço alocado para o cliente
ip access-group FILTRO-BOGONS-V4 in
 ! habilitando Strict uRPF
ip verify unicast source reachable-via rx
```

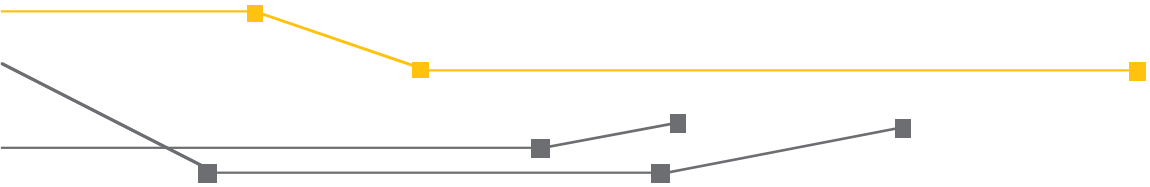


```
…
! Filtro de rede estático
! Caso use enderecos privados na sua rede tome cuidado para nao filtrar trafe
go valido. Remova a linha do prefixo utilizado
ip access-list extended FILTRO-BOGONS-V4
! faixa de enderecos reservados para identificar que o host pertence a rede l
ocal
deny ip 0.0.0.0 0.255.255.255 any
! faixa de enderecos privados
deny ip 10.0.0.0 0.255.255.255 any
! faixa de enderecos privados do CGNAT
deny ip 100.64.0.0 0.63.255.255 any
! faixa de enderecos reservados para loopback
deny ip 127.0.0.0 0.255.255.255 any
! faixa de enderecos reservados para escopo local
deny ip 169.254.0.0 0.0.255.255 any
! faixa de enderecos privados
deny ip 172.16.0.0 0.15.255.255 any
! faixa de enderecos reservado para atribuição a protocolos específicos
deny ip 192.0.0.0 0.0.0.255 any
! faixa de enderecos reservado para documentação
deny ip 192.0.2.0 0.0.0.255 any
! faixa de enderecos privados
deny ip 192.168.0.0 0.0.255.255 any
! faixa de enderecos reservado para testes - benchmarking
deny ip 198.18.0.0 0.1.255.255 any
! faixa de enderecos reservado para documentação
deny ip 198.51.100.0 0.0.0.255 any
! faixa de enderecos reservado para documentação
deny ip 203.0.113.0 0.0.0.255 any
! faixa de enderecos reservado da antiga classe D de multicast e uso futuro
deny ip 224.0.0.0 31.255.255.255 any
! permite todo o resto
permit ip any any
```

Fonte: Portal de Boas Práticas para a Internet no Brasil

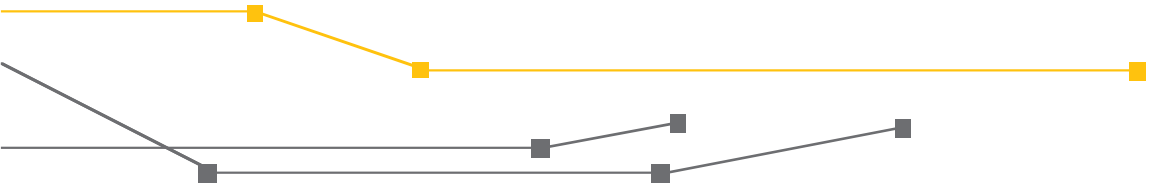
Configuração para IPv6

```
! CEF é necessário para uRPF strict
ipv6 cef
interface GigabitEthernet0/1
! Endereço da interface do roteador
! Troque este endereço pelo que é usado em sua rede!
ipv6 address 2001:DB8:CAFE:FACA::1/64
! Aplicando Filtro estatico baseado no endereço alocado para o cliente
ipv6 traffic-filter FILTRO-BOGONS-V6
! habilitando Strict uRPF
```



```
ipv6 verify unicast source reachable-via rx
…
! bloqueia tudo e permite as faixas
! já liberadas para os RIRs
! Filtro de rede estático
ipv6 access-list extended FILTRO-BOGONS-V6
! faixa de endereços reservada para documentacao
deny ipv6 2001:db8::/32 any
! faixa de endereços dos enderecos globais
permit ipv6 2000::/3 any
! faixa de endereços dos enderecos link local
permit ipv6 fe80::/64 any
! Endereco nao especificado
permit ipv6 ::/128 any
! bloqueia todo o resto
deny ipv6 ::/0 any
```

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