Pesquisando defeitos configurações do Cisco IOS Firewall

Índice

Introdução

Este documento fornece a informação que você pode se usar a fim pesquisar defeitos configurações de firewall de Cisco IOS®.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Troubleshooting

Note: Consulte Informações Importantes sobre Comandos de Debugação antes de usar comandos **debug**.

- A fim inverter (para remover) uma lista de acessos, põe “não” na frente do **comando access-group no** modo de configuração da interface:

```
int <interface>
```

```
no ip access-group # in|out
```

- Se demasiado tráfego é negado, estude a lógica de sua lista ou tente-a definir uma lista ampla adicional, e aplique-a então pelo contrário. Por exemplo:

```
access-list # permit tcp any any
access-list # permit udp any any
access-list # permit icmp any any
int <interface>
ip access-group # in|out
```

- O comando show ip access-lists mostra que Listas de acesso são aplicadas e que tráfego é negado por elas. Se você olha o contagem de pacote de informação negado antes e depois de que a operação falhada com o endereço IP de origem e de destino, este número aumenta se a lista de acessos obstrui o tráfego.
- Se o roteador não estiver muito carregado, a depuração pode ser feita em um nível de pacote na lista de acesso de inspeção de ip ou estendida. Se o roteador é carregado pesadamente, o tráfego está retardado através do roteador. Use a discreção com comandos debugging.Adicionar temporariamente o comando no ip route-cache à relação:

```
int <interface>
no ip route-cache
```

  Então, permita dentro (mas não configuração) o modo:

```
term mon
debug ip packet # det
```

  produz a saída similar a esta:

```
term mon
debug ip packet # det
```

- As listas de acesso estendidas também podem ser usadas com a opção "log" no final das várias instruções.

```
access-list 101 deny ip host 171.68.118.100 host 10.31.1.161 log
access-list 101 permit ip any any
```

  Você vê consequentemente mensagens na tela para permitido e tráfego negado:

```
access-list 101 deny ip host 171.68.118.100 host 10.31.1.161 log
access-list 101 permit ip any any
```

- Se o IP inspeciona a lista é suspeita, o comando debug ip inspect <type_of_traffic> produz a saída tal como esta saída:

```
access-list 101 deny ip host 171.68.118.100 host 10.31.1.161 log
access-list 101 permit ip any any
```

Para estes comandos, junto com a outra informação de Troubleshooting, refira pesquisando defeitos o Proxy de autenticação.

Informações Relacionadas

- Sustentação do produto do Cisco IOS Firewall
- Suporte Técnico e Documentação - Cisco Systems