Exemplo de configuração do recurso de desvio de estado do ASA 8.2.X

Contents

Introduction

Este documento descreve como configurar a característica de desvio do estado TCP. Esse recurso permite fluxos de saída e entrada por meio de dispositivos de segurança adaptáveis Cisco ASA 5500 Series separados.

Prerequisites

Requisitos de licença

Os dispositivos de segurança adaptável Cisco ASA 5500 Series devem ter pelo menos a licença básica.

Componentes Utilizados

As informações neste documento são baseadas no Cisco Adaptive Security Appliance (ASA) com a versão 8.2(1) e posterior.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Desvio de estado TCP

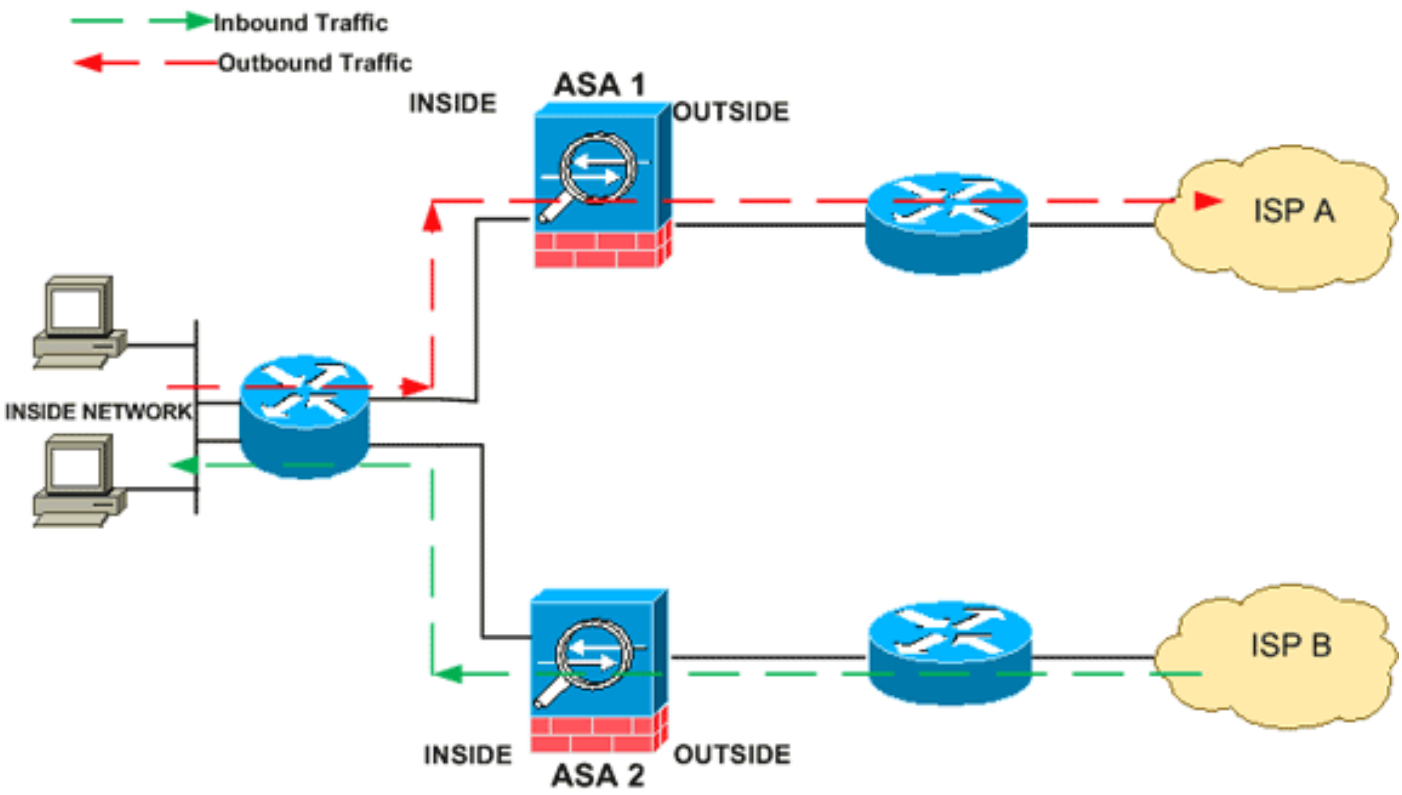
Por padrão, todo o tráfego que passa pelo Cisco Adaptive Security Appliance (ASA) é inspecionado usando o Adaptive Security Algorithm e é permitido através ou descartado com base na política de segurança. Para maximizar o desempenho do firewall, o ASA verifica o estado de cada pacote (por exemplo, essa é uma nova conexão ou uma conexão estabelecida?) e a atribui ao caminho de gerenciamento da sessão (um novo pacote SYN de conexão), ao caminho rápido (uma conexão estabelecida) ou ao caminho do plano de controle (inspeção avançada).

Os pacotes TCP que correspondem às conexões existentes no caminho rápido podem passar pelo dispositivo de segurança adaptável sem reverificar todos os aspectos da política de segurança. Este recurso maximiza o desempenho. No entanto, o método usado para estabelecer a sessão no caminho rápido (que usa o pacote SYN) e as verificações que ocorrem no caminho rápido (como o número de sequência TCP) podem atrapalhar as soluções de roteamento assimétrico: o fluxo de saída e de entrada de uma conexão deve passar pelo mesmo ASA.

Por exemplo, uma nova conexão vai para o *ASA 1*. O pacote SYN passa pelo caminho de gerenciamento da sessão e uma entrada para a conexão é adicionada à tabela de caminho rápido. Se os pacotes subsequentes dessa conexão passarem pelo *ASA 1*, os pacotes corresponderão à entrada no caminho rápido e serão passados. Se os pacotes subsequentes forem para o *ASA 2*, onde não havia um pacote SYN que passasse pelo caminho de gerenciamento da sessão, então não há entrada no caminho rápido para a conexão e os pacotes serão descartados.

Se você tiver o roteamento assimétrico configurado nos roteadores upstream e o tráfego alternar entre dois ASAs, você poderá configurar o desvio de estado do TCP para o tráfego específico. O desvio de estado do TCP altera a forma como as sessões são estabelecidas no caminho rápido e desabilita as verificações de caminho rápido. Este recurso trata o tráfego TCP da mesma forma que trata uma conexão UDP: quando um pacote não-SYN correspondente às redes especificadas entra no ASA e não há uma entrada de caminho rápido, o pacote passa pelo caminho de gerenciamento da sessão para estabelecer a conexão no caminho rápido. Uma vez no caminho rápido, o tráfego ignora as verificações de caminho rápido.

Essa imagem fornece um exemplo de roteamento assimétrico, em que o tráfego de saída passa por um ASA diferente do tráfego de entrada:



Observação: o recurso de desvio de estado TCP é desabilitado por padrão nos Cisco ASA 5500 Series Adaptive Security Appliances.

Informações de suporte

Esta seção fornece as informações de suporte para o recurso de desvio de estado TCP.

- Modo de contexto—Suportado em modo de contexto único e múltiplo.
- Modo de firewall—Suportado no modo roteado e transparente.
- Failover—Suporta failover.

Esses recursos não são suportados quando você usa desvio de estado TCP:

- Inspeção de aplicativos — A inspeção de aplicativos exige que o tráfego de entrada e saída passe pelo mesmo ASA, portanto, a inspeção de aplicativos não é suportada com o desvio de estado do TCP.
- Sessões autenticadas de AAA—Quando um usuário se autentica com um ASA, o tráfego que retorna via outro ASA será negado porque o usuário não se autenticou com esse ASA.
- Interceptação TCP, limite máximo de conexão embrionária, aleatorização do número de sequência TCP—O ASA não rastreia o estado da conexão, portanto esses recursos não são aplicados.
- Normalização de TCP—O normalizador de TCP está desabilitado.
- Funcionalidade SSM e SSC—Não é possível usar o desvio de estado TCP e qualquer aplicativo em execução em um SSM ou SSC, como IPS ou CSC.

Diretrizes de NAT: Como a sessão de conversão é estabelecida separadamente para cada ASA, certifique-se de configurar o NAT estático em ambos os ASAs para tráfego de desvio de estado TCP; se você usar NAT dinâmico, o endereço escolhido para a sessão no *ASA 1* será diferente do endereço escolhido para a sessão no *ASA 2*.

Configurar

Esta seção descreve como configurar o recurso de desvio de estado TCP no Cisco ASA 5500 Series Adaptive Security Appliance (ASA).

Configuração do recurso de desvio de estado TCP

Conclua estes passos para configurar o recurso de desvio de estado TCP no Cisco ASA 5500 Series Adaptive Security Appliance:

1. Use o comando class-map class_map_name para criar um *mapa de classes*. O mapa de classes é usado para identificar o tráfego para o qual você deseja desativar a inspeção de firewall stateful. O mapa de classes usado neste exemplo é *tcp_bypass*.
```
ASA(config)#class-map tcp_bypass
```

2. Use o comando match parameter para especificar o tráfego interessante no mapa de classes. Ao usar a Estrutura de política modular, use o comando **match access-list** no modo de configuração class-map para usar uma lista de acesso para identificar o tráfego ao qual você deseja aplicar ações. Aqui está um exemplo desta configuração:
```
ASA(config)#class-map tcp_bypass
ASA(config-cmap)#match access-list tcp_bypass
```

   tcp_bypass é o nome da lista de acesso usada neste exemplo. Consulte Identificação de Tráfego (Layer 3/4 Class Map) para obter mais informações sobre como especificar o tráfego interessante.
3. Use o comando policy-map name para adicionar um mapa de políticas ou editar um mapa de políticas (que já está presente) que defina as ações a serem tomadas com o tráfego de mapa de classes já especificado. Ao usar a Estrutura de Política Modular, use o comando **policy-map** (sem a palavra-chave type) no modo de configuração global para atribuir ações ao tráfego que você identificou com um mapa de classe de Camada 3/4 (o comando class-map ou class-map type management). Neste exemplo, o mapa de política é *tcp_bypass_policy*:
```
ASA(config-cmap)#policy-map tcp_bypass_policy
```

4. Use o comando class no modo de configuração de mapa de política para atribuir o mapa de classe (*tcp_bypass*) já criado ao mapa de política (*tcp_bypass_policy*) onde você pode atribuir ações ao tráfego de mapa de classe . Neste exemplo, o mapa de classes é *tcp_bypass*:
```
ASA(config-cmap)#policy-map tcp_bypass_policy
ASA(config-pmap)#class tcp_bypass
```

5. Use o comando set connection advanced-options tcp-state-bypass no modo de configuração de classe para ativar o recurso TCP state bypass. Esse comando foi introduzido na versão 8.2(1). O modo de configuração de classe pode ser acessado a partir do modo de configuração de mapa de política, como mostrado neste exemplo:
```
ASA(config-cmap)#policy-map tcp_bypass_policy
ASA(config-pmap)#class tcp_bypass
ASA(config-pmap-c)#set connection advanced-options tcp-state-bypass
```

6. Usar o service-policy policymap_name [global | interface *intf*] no modo de configuração

global para ativar um mapa de políticas globalmente em todas as interfaces ou em uma interface de destino. Para desabilitar a política de serviço, use a forma **no** desse comando. Use o comando **service-policy** para ativar um conjunto de políticas em uma interface.**global** aplica o mapa de políticas a todas as interfaces e **interface** aplica a política a uma interface. Apenas uma política global é permitida. Você pode substituir a política global em uma interface aplicando uma política de serviço a essa interface. Você pode aplicar apenas um mapa de política a cada interface.

```
ASA(config-pmap-c)#service-policy tcp_bypass_policy outside
```

Aqui está um exemplo de configuração para o desvio de estado TCP:

```
!--- Configure the access list to specify the TCP traffic !--- that needs to by-pass inspection
to improve the performance. ASA(config)#access-list tcp_bypass extended permit tcp 10.1.1.0
255.255.255.224 any

!--- Configure the class map and specify the match parameter for the !--- class map to match the
interesting traffic. ASA(config)#class-map tcp_bypass
ASA(config-cmap)#description "TCP traffic that bypasses stateful firewall"
ASA(config-cmap)#match access-list tcp_bypass

!--- Configure the policy map and specify the class map !--- inside this policy map for the
class map. ASA(config-cmap)#policy-map tcp_bypass_policy
ASA(config-pmap)#class tcp_bypass
!--- Use the set connection advanced-options tcp-state-bypass !--- command in order to enable
TCP state bypass feature.

ASA(config-pmap-c)#set connection advanced-options tcp-state-bypass
!--- Use the service-policy policymap_name [ global | interface intf ] !--- command in global
configuration mode in order to activate a policy map !--- globally on all interfaces or on a
targeted interface.

ASA(config-pmap-c)#service-policy tcp_bypass_policy outside

ASA(config-pmap-c)#static (inside,outside) 192.168.1.224 10.1.1.0 netmask
255.255.255.224
```

Verificar

O comando show conn exibe o número de conexões TCP e UDP ativas e fornece informações sobre conexões de vários tipos. Para exibir o estado da conexão para o tipo de conexão designado, use o comando show conn no modo EXEC privilegiado. Esse comando oferece suporte aos endereços IPv4 e IPv6. A exibição de saída para conexões que usam **desvio de estado TCP** inclui o sinalizador **b**.

Troubleshoot

Mensagem de erro

O ASA exibe essa mensagem de erro mesmo depois que o recurso TCP-state-bypass está ativado.

```
%PIX|ASA-4-313004:Denied ICMP type=icmp_type, from source_address oninterface
interface_name to dest_address:no matching session
```

Os pacotes ICMP foram descartados pelo Security Appliance devido a verificações de segurança adicionadas pelo recurso ICMP stateful que geralmente são respostas de eco ICMP sem uma solicitação de eco válida já passada pelo Security Appliance ou mensagens de erro ICMP não relacionadas a qualquer sessão TCP, UDP ou ICMP já estabelecida no Security Appliance.

O ASA exibe esse log mesmo se o desvio de estado do TCP estiver ativado porque não é possível desativar essa funcionalidade (ou seja, verificar as entradas de retorno do ICMP para o Tipo 3 na tabela de conexão). Mas o recurso de desvio de estado do TCP funciona corretamente.

Use este comando para evitar que essas mensagens apareçam:

```
hostname(config)#no logging message 313004
```

Informações Relacionadas

- Dispositivos de segurança adaptáveis Cisco ASA 5500 Series
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems