Exemplo de configuração da característica do desvio do estado ASA 8.2.X TCP

Índice

Introdução

Este documento descreve como configurar a característica de desvio do estado TCP. Esta característica permite de partida e de entrada corre através do Dispositivos de segurança adaptáveis Cisco ASA série 5500 separado.

Pré-requisitos

Exigências da licença

O Dispositivos de segurança adaptáveis Cisco ASA série 5500 deve ter pelo menos a licença baixa.

Componentes Utilizados

A informação neste documento é baseada na ferramenta de segurança adaptável de Cisco (ASA) com versão 8.2(1) e mais recente.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Refira as convenções dos dicas técnicas da Cisco para obter informações sobre das convenções de documento.

O TCP indica o desvio

Àrevelia, todo o tráfego que passa através da ferramenta de segurança adaptável de Cisco (ASA) é inspecionado usando o algoritmo de segurança adaptável e é reservado completamente ou deixado cair baseado na política de segurança. A fim maximizar o desempenho do Firewall, o ASA verifica o estado de cada pacote (por exemplo, é este uma nova conexão ou uma conexão estabelecida?) e atribui-o ao trajeto do gerenciamento de sessão (um pacote SYN da nova conexão), ao caminho rápido (uma conexão estabelecida), ou ao trajeto do plano do controle (inspeção avançada).

Os pacotes de TCP que combinam conexões existentes no caminho rápido podem passar através da ferramenta de segurança adaptável sem verificar novamente cada aspecto da política de segurança. Esta característica maximiza o desempenho. Contudo, o método usado para estabelecer a sessão no caminho rápido (que usa o pacote SYN) e nas verificações que ocorrem no caminho rápido (tal como o número de sequência TCP) pode estar na maneira de soluções assimétricas do roteamento: o fluxo de partida e de entrada de uma conexão deve passar com o mesmo ASA.

Por exemplo, uma nova conexão vai a *ASA 1.* O pacote SYN passa através do trajeto do gerenciamento de sessão, e uma entrada para a conexão é adicionada à tabela do caminho rápido. Se os pacotes subsequente desta conexão atravessam *ASA 1*, os pacotes combinarão a entrada no caminho rápido e estão passados completamente. Se os pacotes subsequente vão a *ASA 2*, onde não havia um pacote SYN que atravesse o trajeto do gerenciamento de sessão, a seguir não há nenhuma entrada no caminho rápido para a conexão, e os pacotes são deixados cair.

Se você tem o roteamento assimétrico configurado em roteadores fluxo acima, e o tráfego alterna entre dois ASA, a seguir você pode configurar o desvio do estado TCP para o tráfego específico. O desvio do estado TCP altera a maneira que as sessões são estabelecidas no caminho rápido e desabilita as verificações do caminho rápido. Esta característica trata o tráfego TCP muito enquanto trata uma conexão de UDP: quando um pacote NON-SYN que combina as redes especificadas incorpora o ASA, e não há uma entrada do caminho rápido, a seguir o pacote atravessa o trajeto do gerenciamento de sessão estabelecer a conexão no caminho rápido. Uma vez no caminho rápido, o tráfego contorneia as verificações do caminho rápido.

Esta imagem fornece um exemplo do roteamento assimétrico, aonde o tráfego de saída atravessa um ASA diferente do que o tráfego de entrada:

Nota: A característica do desvio do estado TCP é desabilitada à revelia no Dispositivos de segurança adaptáveis Cisco ASA série 5500.

Informação da sustentação

Esta seção fornece a informação da sustentação para a característica do desvio do estado TCP.

- Modo do contexto — Apoiado em único e no modo de contexto múltiplo.

- Modo de firewall — Apoiado em roteado e no modo transparente.
- Failover — Apoia o Failover.

Estas características não são apoiadas quando você usa o desvio do estado TCP:

- Inspeção de aplicativo — A inspeção de aplicativo exige ambo o tráfego de entrada e de saída a passar com o mesmo ASA, assim que a inspeção de aplicativo não é apoiada com desvio do estado TCP.
- O AAA autenticou sessões — Quando um usuário autentica com um ASA, o tráfego que retorna através do outro ASA estará negado porque o usuário não autenticou com esse ASA.
- TCP Intercept, limite máximo da conexão embriônica, randomization do número de sequência TCP — O ASA não se mantém a par do estado da conexão, assim que estas características não são aplicadas.
- Normalização TCP — O normalizador TCP é desabilitado.
- Funcionalidade SS e de SSC — Você não pode usar o desvio do estado TCP e o nenhum aplicativo que são executado em um SS ou em SSC, tal como o IPS ou o CSC.

Diretrizes NAT: Porque a sessão de conversão é estabelecida separadamente para cada ASA, seja certo configurar o NAT estático em ambos os ASA para o tráfego do desvio do estado TCP; se você usa o NAT dinâmico, o endereço escolhido para a sessão em *ASA 1* diferirá do endereço escolhido para a sessão em *ASA 2.*

Configurar

Esta seção descreve como configurar a característica do desvio do estado TCP na ferramenta de segurança adaptável do 5500 Series de Cisco ASA (ASA).

Configuração da característica do desvio do estado TCP

Termine estas etapas a fim configurar a característica do desvio do estado TCP na ferramenta de segurança adaptável do 5500 Series de Cisco ASA:

1. Use o comando do **class_map_name do mapa de classe** a fim criar um *mapa da classe*. O mapa da classe é usado para identificar o tráfego para que você quer desabilitar a inspeção do firewall stateful. O mapa da classe usado neste exemplo é *tcp_bypass*.`ASA(config)#`**`class-map tcp_bypass`**
2. Use o **comando parameter do fósforo** a fim especificar o tráfego interessante no mapa da classe. Ao usar a estrutura de política modular, use o **comando access-list do fósforo no** modo da configuração de mapa de classe a fim usar uma lista de acessos para identificar o tráfego a que você quer aplicar ações. Está aqui um exemplo desta configuração:`ASA(config)#`**`class-map tcp_bypass`** `ASA(config-cmap)#`**`match access-list tcp_bypass`** *os tcp_bypass* são o nome da lista de acesso usada neste exemplo. Refira a identificação do tráfego (mapa da classe da camada 3/4) para obter mais informações sobre de especificar o tráfego interessante.
3. Use o **comando name do mapa de política** a fim adicionar um mapa de política ou editar um mapa de política (que está já atual) esse ajusta as ações para tomar com o tráfego do mapa da classe especificado já. Ao usar a estrutura de política modular, use o **comando policy-map** (sem o tipo palavra-chave) no modo de configuração global a fim atribuir ações para traficar que você identificou com um mapa da classe da camada 3/4 (o mapa de classe ou o tipo comando management do mapa de classe). 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 da configuração de mapa de política a fim atribuir o mapa da classe (*tcp_bypass*) já criado ao mapa de política (*tcp_bypass_policy*) onde você pode atribuir ações ao tráfego do mapa da classe. Neste exemplo, o mapa da classe é *tcp_bypass*:`ASA(config-cmap)#policy-map tcp_bypass_policy ASA(config-pmap)#class tcp_bypass`
5. Use o comando do TCP-estado-desvio das avançado-opções da conexão do grupo no modo de configuração de classe a fim permitir a característica do desvio do estado TCP. Este comando foi introduzido na versão 8.2(1). O modo de configuração de classe é acessível do modo da configuração de mapa de política segundo as indicações deste 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. Use o policymap_name da serviço-política [global | conecte o comando do *intf*] no modo de configuração global a fim ativar globalmente um mapa de política em todas as relações ou em uma relação visada. A fim desabilitar a política de serviços, não use **nenhum** formulário deste comando. Use o **comando service-policy** permitir um grupo de políticas em um interface.global aplica o mapa de política a todas as relações, e a **relação** aplica a política a uma relação. Somente uma política global é permitida. Você pode cancelar a política global em uma relação aplicando uma política de serviços a essa relação. Você pode aplicar somente um mapa de política a cada relação.`ASA(config-pmap-c)#service-policy tcp_bypass_policy outside`

Está aqui uma configuração de exemplo para o desvio do 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 indica o número de TCP ativo e de conexões de UDP e fornece a informação sobre conexões de vários tipos. A fim indicar o estado de conexão para o tipo de conexão designado, use o comando show conn no modo de exec privilegiado. Esse comando oferece suporte aos endereços IPv4 e IPv6. O indicador da saída para as conexões que usam o **desvio do estado TCP** inclui a bandeira **B.**

Troubleshooting

Mensagem de Erro

O ASA indica este Mensagem de Erro mesmo depois que a característica do TCP-estado-desvio é permitida.

```
%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 deixados cair pela ferramenta de segurança devido às verificações de segurança adicionadas pela característica do stateful ICMP que são geralmente respostas de eco ICMP sem uma requisição de eco válida já passada através da ferramenta de segurança ou mensagens de erro ICMP não relativos a toda a sessão TCP, UDP, ou ICMP já estabelecida na ferramenta de segurança.

O ASA indica este log mesmo se o desvio do estado TCP é permitido porque desabilitar esta funcionalidade (isto é, verificando o ICMP retorne entradas para o tipo 3 na tabela de conexão) não é possível. Mas a característica do desvio do estado TCP trabalha corretamente.

Use este comando a fim impedir que estas mensagens apareçam:

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

Informações Relacionadas

- Cisco ASA 5500 Series Adaptive Security Appliances
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems