Configurar o Acesso a Recursos Internos para Usuários de VPN no FTD com Tráfego HairPin

Contents

Problema

O objetivo é permitir o acesso total dos usuários de VPN aos recursos de rede internos após a autenticação bem-sucedida de VPN usando RADIUS (em um servidor associado a um domínio do Windows) no FTD do Cisco Secure Firewall.

A configuração da VPN já está operacional; os usuários podem baixar e instalar o cliente VPN e se autenticar com êxito. O problema concentra-se na configuração do controle de acesso necessário e das regras de NAT para permitir o acesso de recurso interno necessário pela VPN.

Ambiente

- Produto: Cisco Secure Firewall Firepower (FTD), versão 7.6.0 (como um dispositivo CSF1220CX)
- Gerenciamento: Firepower Management Center (FMC), FMC fornecido na nuvem (cdFMC) ou Firepower Device Manager (FDM)
- VPN: configurado com autenticação RADIUS em um servidor associado a domínio (NPS) do Windows
- Pool de Endereços VPN: 192.168.250.1 - 192.168.250.200
- Exemplo de sub-rede interna de destino: 192.168.95.0/24
- Versão do software: 9.22.1 (conforme referenciado no fluxo de trabalho)
- Interfaces relevantes: interface 'externa' para entrada de VPN
- Acesso ao RDP e ao Ative Diretory necessário por conexão VPN

Resolução

Estas etapas detalham a configuração necessária para permitir que os usuários da VPN acessem recursos internos (como RDP e Ative Diretory) no Cisco FTD. Isso inclui a criação de regras de política de acesso, a configuração de isenções de NAT e o hairpin NAT para tráfego VPN e o uso de comandos de solução de problemas para validar a configuração.

Etapa 1: Adicione uma entrada de lista de acesso para permitir que o pool de endereços VPN acesse recursos internos.

```
access-list CSM_FW_ACL_ advanced permit ip object VPN_Pool any rule-id 268438528
access-list CSM_FW_ACL_ remark rule-id 268438528: ACCESS POLICY: Default Access Control Policy - Mandat
```

```
access-list CSM_FW_ACL_ remark rule-id 268438528: L7 RULE: Permit_VPN_Pool
```

Etapa 2: Adicione uma regra de lista de acesso para permitir que recursos internos enviem tráfego de retorno para o pool VPN:

```
access-list CSM_FW_ACL_ advanced permit ip any object VPN_Pool
```

Essas regras podem ser mais rígidas posteriormente para restringir origens e destinos específicos, conforme necessário.

Etapa 3: Configurar a isenção de NAT ou o NAT hairpin para o tráfego VPN

Há duas abordagens comuns:

- ◦ Opção A: Isenção de NAT para pool de VPN para sub-rede interna

```
nat (outside,inside) source static VPN_Pool VPN_Pool destination static Net_192.168.95.1-24 Net_192.168
```

- ◦ Opção B: Hairpin NAT para Pool VPN na Mesma Interface (no-proxy-arp)

```
nat (any,any) source static VPN_Pool VPN_Pool no-proxy-arp
```

- ◦ Opção C: NAT Hairpin Dinâmico para Pool VPN na Interface Externa

```
nat (outside,outside) dynamic VPN_Pool interface
```

O método correto depende se os recursos internos estão na mesma interface física (exigindo hairpin NAT) ou em interfaces diferentes (isenção de NAT).

Etapa 4: Use o comando `packet-tracer` para simular fluxos de tráfego do pool VPN para recursos internos e validar se o tráfego é permitido pela regra desejada, NAT e rota.

```
packet-tracer input outside icmp 192.168.250.1 8 0 192.168.95.1
packet-tracer input outside tcp 192.168.250.1 12345 192.168.95.1 80
packet-tracer input inside icmp 192.168.95.1 8 0 192.168.250.1
packet-tracer input inside tcp 192.168.250.1 54321 192.168.95.1 443
--
```

```
Phase 5
ID: 5
Type: ACCESS-LIST
Result: ALLOW
Config: access-group CSM_FW_ACL_ globalaccess-list CSM_FW_ACL_ advanced permit ip object VPN_Pool any r
Additional Information:  This packet will be sent to snort for additional processing where a verdict wi
Elapsed Time: 0 ns
--
Phase 7
ID: 7
Type: NAT
Result: ALLOW
Config: nat (outside,outside) dynamic VPN_Pool interface
Additional Information: Static translate 192.168.250.1/12345 to 192.168.250.1/12345 Forward Flow based
Elapsed Time: 0 ns
```

Observação: a saída do packet-tracer para a fase WebVPN pode mostrar um "DROP" para o tráfego VPN na interface externa. Esse é o comportamento esperado para o tráfego de texto simples na interface externa e ainda pode ser usado para validar o NAT.

Observações Adicionais:

- É possível que as capturas de pacotes na interface do usuário do Threat Defense mostrem apenas solicitações de entrada. Se nenhuma queda for observada, mas o tráfego não atingir o recurso interno, verifique as regras de NAT e de lista de acesso.
- Quando o SSH não está disponível, toda a solução de problemas pode ser executada através dos recursos da interface de usuário do Threat Defense no cdFMC, mas o uso do comando é limitado.
- É possível que algumas modificações sejam necessárias em dispositivos adjacentes para conectividade fim-a-fim.

Causa

A causa raiz foi a política de acesso insuficiente e a configuração de NAT para o tráfego do pool de VPN para interno e interno para VPN. A configuração padrão não permitia a comunicação bidirecional completa do pool VPN para recursos internos e vice-versa, nem tratava dos requisitos de NAT hairpin para entrada e saída de tráfego na mesma interface.

Conteúdo relacionado

- Configurar a isenção de NAT no FTD
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.