Configurar a detecção de ameaças para VPN de acesso remoto no Secure Firewall ASA

Contents

Introdução

Este documento descreve o processo de configuração dos recursos de detecção de ameaças para VPN de acesso remoto no Cisco Secure Firewall ASA.

Informações de Apoio

Os recursos de detecção de ameaças para serviços VPN de acesso remoto permitem que você se proteja contra qualquer um dos próximos cenários:

1. O Connection tenta invalidar os serviços VPN de acesso remoto. Ou seja, tentativas de conexão com serviços destinados apenas a uso interno.
2. Ataques de iniciação do cliente, em que o invasor inicia mas não conclui as tentativas de conexão com um ponto inicial de VPN de acesso remoto repetidas vezes a partir de um único host.
3. Tentativas repetidas de autenticação com falha para acesso remoto aos serviços VPN (ataques de verificação de nome de usuário/senha de força bruta).

Esses ataques, mesmo quando mal sucedidos em sua tentativa de obter acesso, podem consumir recursos computacionais e impedir que usuários válidos se conectem aos serviços VPN de acesso remoto.

Quando você habilita esses serviços, o Firewall Seguro automaticamente ignora o host (endereço IP) que excede os limites configurados, para evitar novas tentativas até que você remova manualmente o shun do endereço IP.

Observação: todos os serviços de detecção de ameaças para VPN de acesso remoto são desabilitados por padrão.

Pré-requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Secure Firewall Adaptive Security Appliance (ASA)
- VPN de acesso remoto (RAVPN) no ASA

Requisitos

Esses recursos de detecção de ameaças são suportados nas versões do Cisco Secure Firewall ASA listadas a seguir:

- versão de treinamento 9.16 -> suportado na versão 9.16(4)67 e mais recente
- versão de treinamento 9.20 -> compatível com a versão 9.20(3) e mais recente

Componentes Utilizados

As informações descritas neste documento são baseadas nestas versões de hardware e software:

- Cisco Secure Firewall ASA versão 9.20(3)

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 rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Faça login na Secure Firewall Command Line Interface (CLI) no modo de configuração global e ative um ou mais dos serviços de detecção de ameaças disponíveis para VPN de acesso remoto:

Detecção de ameaças para tentativas de conexão com serviços VPN somente internos (inválidos)

Para habilitar este serviço, execute o comando threat detection service invalid-vpn-access.

Detecção de ameaças para ataques de início de cliente VPN de acesso remoto

Para habilitar este serviço, execute o comando threat detection service remote-access-client-initiations hold-down <minutes> threshold <count>, onde:

- hold-down <minutes> define o período após a última tentativa de início durante o qual as tentativas consecutivas de conexão são contadas. Se o número de tentativas de conexão consecutivas atingir o limite configurado dentro desse período, o endereço IPv4 do invasor será ignorado. Você pode definir esse período entre 1 e 1440 minutos.
- threshold <count> é o número de tentativas de conexão necessárias dentro do período de retenção para disparar um shun. Você pode definir o limite entre 5 e 100.

Por exemplo, se o período de retenção for de 10 minutos e o limite for 20, o endereço IPv4 será automaticamente ignorado se houver 20 tentativas de conexão consecutivas em qualquer intervalo de 10 minutos.

Observação: ao definir os valores de hold-down e de limite, leve em consideração o uso do NAT. Se você usar PAT, que permite muitas solicitações do mesmo endereço IP, considere valores mais altos. Isso garante que usuários válidos tenham tempo suficiente para se conectar. Por exemplo, em um hotel, vários usuários podem tentar se conectar em um curto período.

Detecção de ameaças para falhas de autenticação de VPN de acesso remoto

Para habilitar este serviço, execute o comando threat detection service remote-access-authentication hold-down<minutes> threshold <count>, onde:

- hold-down <minutes> define o período após a última tentativa com falha durante o qual as falhas consecutivas são contadas. Se o número de falhas consecutivas de autenticação atingir o limite configurado nesse período, o endereço IPv4 do invasor será ignorado. Você pode definir esse período entre 1 e 1440 minutos.
- threshold <count> é o número de tentativas de autenticação com falha necessárias dentro do período de retenção para disparar um shun. Você pode definir o limite entre 1 e 100.

Por exemplo, se o período de retenção for de 10 minutos e o limite for 20, o endereço IPv4 será automaticamente ignorado se houver 20 falhas de autenticação consecutivas em qualquer intervalo de 10 minutos.

Observação: ao definir os valores de hold-down e de limite, leve em consideração o uso do NAT. Se você usar PAT, que permite muitas solicitações do mesmo endereço IP, considere valores mais altos. Isso garante que usuários válidos tenham tempo suficiente para se conectar. Por exemplo, em um hotel, vários usuários podem tentar se conectar em um curto período.

Observação: ainda não há suporte para falhas de autenticação via SAML.

A configuração do próximo exemplo ativa os três serviços de detecção de ameaças disponíveis para VPN de acesso remoto com um período de retenção de 10 minutos e um limite de 20 para iniciação do cliente e tentativas de autenticação com falha.

```
threat-detection service invalid-vpn-access
threat-detection service remote-access-client-initiations hold-down 10 threshold 20
threat-detection service remote-access-authentication hold-down 10 threshold 20
```

Verificar

Para exibir estatísticas de serviços RAVPN de detecção de ameaças, execute o comando show threat-detection service [service] [entries|details]. Onde o serviço pode ser: remote-access-authentication, remote-access-client-initiations ou invalid-vpn-access.

Você pode limitar ainda mais a view adicionando estes parâmetros:

- entries — Exibe somente as entradas que estão sendo rastreadas pelo serviço de detecção de ameaças. Por exemplo, os endereços IP que tiveram tentativas de autenticação com falha.
- detalhes — Exibe os detalhes e as entradas de serviço.

Execute o comando de serviço show threat-detection para exibir estatísticas de todos os serviços de detecção de ameaças habilitados.

```
ciscoasa# show threat-detection service
Service: invalid-vpn-access
    State     : Enabled
    Hold-down : 1 minutes
    Threshold : 1
    Stats:
        failed      :          0
        blocking    :          0
        recording   :          0
        unsupported :          0
        disabled    :          0
    Total entries: 0
Service: remote-access-authentication
    State     : Enabled
    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          1
        recording   :          4
        unsupported :          0
```

```
        disabled    :          0
    Total entries: 2
Name: remote-access-client-initiations
    State     : Enabled
    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          0
        recording   :          0
        unsupported :          0
        disabled    :          0
    Total entries: 0
```

Para exibir mais detalhes de possíveis invasores que estão sendo rastreados para o serviço de autenticação de acesso remoto, execute o comando show threat-detection service <service> entries.

```
ciscoasa# show threat-detection service remote-access-authentication entries
Service: remote-access-authentication
    Total entries: 2

Idx Source              Interface            Count          Age         Hold-down
--- ------------------- -------------------- -------------- ----------- ---------
  1 192.168.100.101/ 32              outside              1        721         0
  2 192.168.100.102/ 32              outside              2        486       114
Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.
```

Para exibir as estatísticas e os detalhes gerais de um serviço VPN de acesso remoto com detecção de ameaças específico, execute o comando show threat-detection service <service> details.

```
ciscoasa# show threat-detection service remote-access-authentication details
Service: remote-access-authentication
    State     : Enabled
    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          1
        recording   :          4
        unsupported :          0
        disabled    :          0
     Total entries: 2
```

```
Idx Source              Interface            Count          Age         Hold-down
--- ------------------- -------------------- -------------- ----------- ---------
  1 192.168.100.101/ 32              outside              1         721           0
  2 192.168.100.102/ 32              outside              2         486         114
Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.
```

Observação: as entradas exibem apenas os endereços IP que estão sendo rastreados pelo serviço de detecção de ameaças. Se um endereço IP atender às condições para ser rejeitado, a contagem de bloqueio aumenta e o endereço IP não é mais exibido como uma entrada.

Além disso, você pode monitorar shuns aplicados pelos serviços VPN e remover shuns para um único endereço IP ou todos os endereços IP com os próximos comandos:

- show shun [ip_address]

Mostra os hosts evitados, incluindo aqueles evitados automaticamente pela detecção de ameaças para serviços VPN, ou manualmente usando o comando shun. Como opção, você pode limitar a exibição a um endereço IP especificado.

- no shun ip_address [interface if_name]

Remove o shun somente do endereço IP especificado. Opcionalmente, você pode especificar o nome da interface para o shun, se o endereço for shun em mais de uma interface e você quiser deixar o shun em algumas interfaces.

- clear shun

Remove o shun de todos os endereços IP e de todas as interfaces.

Observação: os endereços IP evitados pela detecção de ameaças para serviços VPN não aparecem no comando show threat-detection shun, que se aplica somente à verificação da detecção de ameaças.

Para ler todos os detalhes da saída de cada comando e as mensagens de syslog disponíveis relacionadas aos serviços de detecção de ameaças para VPN de acesso remoto, consulte o Guia de Configuração CLI do Cisco Secure Firewall ASA Firewall, 9.20. Capítulo: Documento de detecção de ameaças.

Informações Relacionadas

- Para obter assistência adicional, entre em contato com o Centro de Assistência Técnica (TAC). É necessário um contrato de suporte válido:Cisco Worldwide Support Contacts.

- Você também pode visitar a comunidade de VPN da Cisco aqui.

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.