

Práticas recomendadas contra ataques de borrifo de senhas que afetam os serviços de VPN de acesso remoto

Contents

[Introdução](#)

[Informações de Apoio](#)

[Padrões Incomuns Observados](#)

[Não é possível estabelecer conexões VPN com o Cisco Secure Client \(AnyConnect\) quando a postura do firewall \(HostScan\) está habilitada](#)

[Quantidade Incomum de Solicitações de Autenticação](#)

[Recomendações](#)

[1. Habilitar Registro em Log](#)

[2. Perfis de VPN de Acesso Remoto Padrão Seguro](#)

[3. Bloquear Tentativas de Conexão de Fontes Mal-Intencionadas](#)

[Implementar ACLs em nível de interface](#)

[Use o comando "shun"](#)

[Configurar ACL de Control-plane](#)

[Usar autenticação baseada em certificado para RAVPN \(Opcional\)](#)

[Informações adicionais](#)

Introdução

Este documento descreve as recomendações a serem consideradas contra ataques de spray de senha destinados aos serviços de VPN de acesso remoto (RAVPN) configurados no Cisco Secure Firewall.

Informações de Apoio

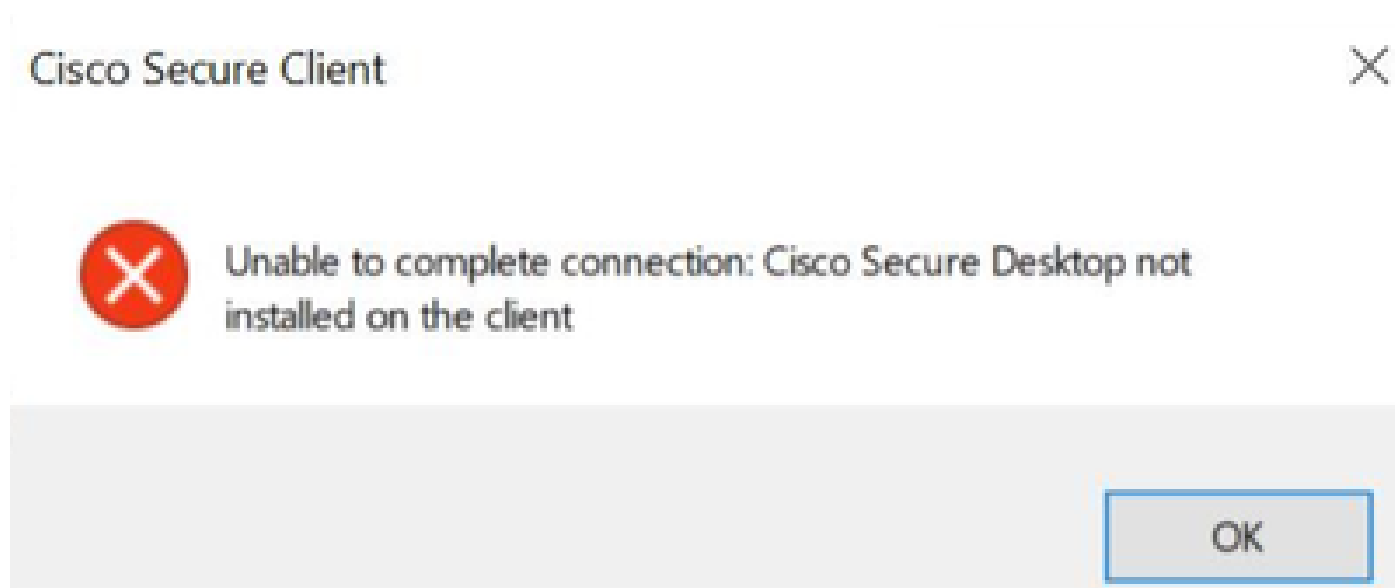
A Cisco foi informada sobre vários relatórios relacionados a ataques de pulverização de senhas direcionados a serviços RAVPN. O Talos observou que esses ataques não se limitam aos produtos da Cisco, mas também aos concentradores de VPN de terceiros.

Esta atividade parece estar relacionada com os esforços de reconhecimento.


Padrões Incomuns Observados

Não é possível estabelecer conexões VPN com o Cisco Secure Client (AnyConnect) quando a postura do firewall (HostScan) está habilitada

Ao tentar se conectar com o Cisco Secure Client (AnyConnect), os usuários são solicitados a receber o erro "Não é possível concluir a conexão. Cisco Secure Desktop não instalado no cliente.", impedindo o estabelecimento bem-sucedido de uma conexão VPN.



Esse sintoma parece ser um efeito colateral dos ataques tipo DoS descritos na próxima seção; uma investigação interna adicional ainda está em andamento.

 Observação: esse comportamento específico foi observado somente em cenários onde a postura do firewall (HostScan) está configurada no headend.

Quantidade Incomum de Solicitações de Autenticação

O headend da VPN Cisco Secure Firewall Adaptive Security Appliance (ASA) ou Threat Defense (FTD) mostra sintomas de ataques de spray de senha com 100 a milhares ou milhões de tentativas de autenticação rejeitadas.

A melhor maneira de detectar isso é observando o syslog. Procure um número incomum de qualquer um dos próximos IDs de syslog do ASA:

- %ASA-6-113015

<#root>

%ASA-6-113015

```
: AAA user authentication Rejected : reason = User was not found : local database :
```

```
user
```

```
= admin : user
```

```
IP
```

```
= x.x.x.x
```

- %ASA-6-113005

```
<#root>
```

```
%ASA-6-113005
```

```
: AAA user authentication Rejected : reason = Unspecified : server = x.x.x.x : user = ***** : user IP =
```


- %ASA-6-716039

```
<#root>
```

```
%ASA-6-716039
```

```
: Group <DfltGrpPolicy> User <admin> IP <x.x.x.x> Authentication: rejected, Session Type: WebVPN.
```

O nome de usuário está sempre oculto até que o comando no logging `hide username` seja configurado no ASA.

 Observação: isso fornecerá informações para entender se usuários válidos são gerados ou conhecidos por IPs ofensivos. No entanto, seja cauteloso, pois os nomes de usuário estarão visíveis nos logs.

Para verificar, faça login no ASA ou na Interface de Linha de Comando (CLI) do FTD, execute o comando `show aaa-server` e investigue um número incomum de solicitações de autenticação tentadas e rejeitadas para qualquer um dos servidores AAA configurados:

```
<#root>
```

```
ciscoasa# show aaa-server
```

```
Server Group: LOCAL - - - - - >>>> Sprays against the LOCAL database
Server Protocol: Local database
Server Address: None
Server port: None
Server status: ACTIVE, Last transaction at 16:46:01 UTC Fri Mar 22 2024
Number of pending requests 0
Average round trip time 0ms

Number of authentication requests 8473575 - - - - - >>>> Unusual increments

Number of authorization requests 0
Number of accounting requests 0
Number of retransmissions 0
Number of accepts 0

Number of rejects 8473574 - - - - - >>>> Unusual increments
```

<#root>

```
ciscoasa# show aaa-server
```

```
Server Group: LDAP-SERVER - - - - - >>>> Sprays against the LDAP server
Server Protocol: ldap
Server Hostname: ldap-server.example.com
Server Address: 10.10.10.10
Server port: 636
Server status: ACTIVE, Last transaction at unknown
Number of pending requests 0
Average round trip time 0ms

Number of authentication requests 2228536 - - - - - >>>> Unusual increments

Number of authorization requests 0
Number of accounting requests 0
Number of retransmissions 0
Number of accepts 1312

Number of rejects 2225363 - - - - - >>>> Unusual increments

Number of challenges 0
Number of malformed responses 0
Number of bad authenticators 0
Number of timeouts 1
Number of unrecognized responses 0
```

Recomendações

As ações listadas a seguir são recomendações para combater o impacto desses ataques direcionados aos dispositivos Cisco Secure Firewall:

1. Habilitar Registro em Log

O registro é uma parte crucial da segurança digital que envolve o registro de eventos que ocorrem em um sistema. A ausência de registros detalhados deixa lacunas na compreensão, dificultando uma análise clara do método de ataque. É recomendável habilitar o registro em um servidor syslog remoto para melhorar a correlação e a auditoria de incidentes de rede e segurança em vários dispositivos de rede.

Para obter informações sobre como configurar o registro em log, consulte os próximos guias específicos de plataforma:

Software Cisco ASA:

- [Use o guia para proteger o firewall ASA](#)
- Capítulo [Registro](#) do Guia de configuração da CLI de operações gerais do Cisco Secure Firewall ASA Series

Software Cisco FTD:


- [Configurar o registro no FTD usando o FMC](#)
- Seção [Configurar Syslog](#) no capítulo Configurações de plataforma do Guia de Configuração de Dispositivos do Cisco Secure Firewall Management Center
- [Configurar e verificar o Syslog no Gerenciador de dispositivos do Firepower](#)
- [Seção Definição de configurações de registro do sistema](#) no capítulo Configurações do sistema do Guia de configuração do Cisco Firepower Threat Defense para o Firepower Device Manager

2. Perfis de VPN de Acesso Remoto Padrão Seguro

Quando os perfis/grupos de túneis de conexão VPN de acesso remoto padrão DefaultRAGroup e DefaultWEBVPNGroup não são usados, é recomendável impedir tentativas de autenticação e o estabelecimento de sessão VPN de acesso remoto usando esses perfis/grupos de túneis de conexão padrão, apontando-os para um servidor AAA sinkhole. Para fazer isso, use as seguintes etapas:

1. Configure um servidor LDAP fictício, conforme mostrado no próximo exemplo:

```
<#root>
aaa-server
  AAA_Sinkhole
protocol ldap
```

 Observação: não adicione nenhuma configuração adicional para este servidor AAA.


2. Aponte o DefaultRAGroup e o DefaultWEBVPNGroup para este servidor LDAP fictício, como mostrado no próximo exemplo:

```
<#root>
tunnel-group
  DefaultWEBVPNGroup
general-attributes

authentication-server-group
  AAA_Sinkhole


tunnel-group
  DefaultRAGroup
general-attributes


authentication-server-group
  AAA_Sinkhole
```

 Observação: se os invasores atacarem perfis de conexão legítimos (grupos de túnel) depois que os grupos padrão forem redirecionados para o servidor AAA_Sinkhole, será necessário bloquear essas tentativas de conexão. Consulte a seção subsequente para obter mais detalhes.

3. Bloquear Tentativas de Conexão de Fontes Mal-Intencionadas

Para impedir tentativas de conexão de fontes não autorizadas, você pode implementar qualquer uma das opções listadas abaixo:

 Observação: inicialmente, você deve revisar os logs de segurança (syslog) para identificar os endereços IP problemáticos. Após a identificação, qualquer uma das três opções pode ser usada para bloqueá-las.

 Observação: você deve especificar e manter manualmente a lista de endereços IP a serem bloqueados.

Implementar ACLs em nível de interface

Implemente uma ACL de nível de interface no ASA/FTD para filtrar endereços IP públicos não autorizados e impedi-los de iniciar sessões de VPN remotas.

Use o comando "shun"

Essa é uma abordagem simples para bloquear um IP mal-intencionado, no entanto, ela deve ser feita manualmente. Leia a seção [Configuração alternativa para bloquear ataques para um firewall seguro usando o comando 'shun'](#) para obter mais detalhes.

Configurar ACL de Control-plane

Implemente uma ACL de plano de controle no ASA/FTD para filtrar endereços IP públicos não autorizados e impedi-los de iniciar sessões de VPN remotas. [Configure Políticas de Controle de Acesso de Plano de Controle para Secure Firewall Threat Defense e ASA.](#)

Usar autenticação baseada em certificado para RAVPN (opcional)

O uso de certificados para autenticação fornece uma abordagem mais robusta em comparação ao uso de credenciais. Para fortalecer seu ambiente, você pode alterar o método de autenticação para que o RAVPN seja baseado em certificados.

Para obter mais detalhes, verifique a seção [Configure AAA Settings for Remote Access VPN](#) no Cisco Secure Firewall Configuration Guide.

Informações adicionais

- [Procedimentos de investigação forense do Cisco ASA para socorristas](#)
- [Procedimentos de investigação forense do Cisco Firepower Threat Defense para socorristas](#)

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.