

Métodos de Distribuição Segura de Cliente para Acesso Seguro RAVPN

Contents

Problema

Ao configurar o acesso de fornecedor externo à VPN de acesso remoto (RAVPN) no Cisco Secure Access, os administradores precisam de um método para que os fornecedores baixem o software AnyConnect/Secure Client. Diferentemente das implantações anteriores do ASA, em que a URL da VPN fornecia downloads diretos de clientes, as URLs de headend da VPN de acesso seguro da Cisco não fornecem uma função de download de cliente. Essa limitação afeta o processo de integração para fornecedores externos que exigem recursos de acesso remoto.

Os administradores esperam que os URLs de configuração de VPN no Secure Access concedam aos fornecedores acesso para baixar o cliente AnyConnect, semelhante ao comportamento anteriormente disponível com implantações baseadas em ASA, onde o URL de VPN permitiria downloads de clientes antes da conexão.

Ambiente

- Configuração do Cisco Secure Access com RAVPN
- Requisitos de acesso de fornecedor externo
- Migração da implantação de VPN baseada em ASA
- Necessidades de distribuição do AnyConnect/Secure Client

Resolução

O Cisco Secure Access não hospeda pacotes do Secure Client nos URLs de headend da VPN. A

solução usa a tecnologia hostscan em vez de fornecer downloads diretos de clientes através da URL da VPN. Para distribuir o software Secure Client para fornecedores externos, use um destes métodos aprovados.

Método 1: Distribuição do painel de controle de acesso seguro

- 1.- Obtenha pacotes de instalação diretamente do painel do Secure Access para distribuição manual.
- 2.- Navegue até Conectividade do usuário final e clique no botão Cisco Secure Client para fazer o download dos pacotes do instalador para distribuição aos fornecedores.

Método 2: Site de download de software da Cisco

Os fornecedores podem fazer o download de pacotes diretamente se tiverem os direitos adequados:

- O fornecedor deve ter uma conta da Cisco com qualificação para software
- Acesse pacotes por meio de software.cisco.com
- Requer planejamento de pré-implantação e configuração de conta da Cisco do fornecedor

Método 3: Distribuição manual

Distribua o software Secure Client para fornecedores externos manualmente ou através de canais de distribuição alternativos fora da URL da VPN. Esse método oferece o maior controle sobre o processo de distribuição e não exige contas de fornecedores da Cisco.

Causa

Os URLs de headend da VPN de Acesso Seguro da Cisco são projetados de forma diferente das

implantações baseadas em ASA. A solução Secure Access não hospeda pacotes do instalador do cliente nos headends e, em vez disso, usa a tecnologia hostscan. Essa diferença de arquitetura significa que os URLs de VPN não podem fornecer a mesma funcionalidade de download do cliente que estava disponível nas implantações do ASA.

Conteúdo relacionado

- [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.