O bloqueio do Secure Access Application Protocol impede a conectividade com a Internet

Contents

Problema

Ambiente

Resolução

- Passo 1: Identificar a Regra de Bloqueio
- Passo 2: Modificar Configurações do Aplicativo
- Passo 3: Aplicar e verificar alterações

Causa

Conteúdo relacionado

- Problema
- Ambiente
- Resolução
  - Passo 1: Identificar a Regra de Bloqueio
  - Passo 2: Modificar Configurações do Aplicativo
  - Passo 3: Aplicar e verificar alterações
- Causa
- Conteúdo relacionado

Problema

Depois de migrar para o Cisco Secure Access, os usuários experimentaram conectividade com a Internet bloqueada ao tentar acessar serviços Web. O sintoma específico envolvia o bloqueio do tráfego HTTP pela política de segurança, impedindo o acesso a sites e aplicativos legítimos.

Os detalhes do evento de bloqueio mostraram estas características:

- Ação: Bloqueado
- Motivo do Bloqueio de Eventos: AC_RULE_MATCH_BLOCK
- Destino: http://www.bing.com/api/shopping/v1/user/shoppingsettings
- Porta de Destino: 443

- Categorias: Não categorizado
- Categoria do aplicativo: Busca
- Protocolo de aplicação: Protocolo HTTP
- Protocolo: TCP

Ambiente

- Implantação do Cisco Secure Access
- Política de segurança ativa com restrições do protocolo de aplicação

Resolução

A resolução envolve modificar a configuração da regra de segurança para permitir o tráfego do protocolo de aplicação HTTP, mantendo a postura de segurança para aplicações realmente não confiáveis.

Passo 1: Identificar a Regra de Bloqueio

Localize a regra específica que está causando o bloqueio na interface de gerenciamento do Secure Access:

- Nome da regra: Teste
- Configuração atual: Usando Bloco de Configurações do Aplicativo como Destino.

Passo 2: Modificar Configurações do Aplicativo

Acesse a configuração de regra e verifique o nome das Configurações de Aplicativo no Destino:

- Navegue até Resources > Internet and SaaS resources > Application Lists. Em seguida, clique no aplicativo.
- Localize as configurações do protocolo de aplicativo.
- Desmarque ou remova o HTTP da lista de protocolos de aplicativos bloqueados.
- Garanta que outros controles de segurança permaneçam em vigor para aplicativos não confiáveis reais.

Passo 3: Aplicar e verificar alterações

Salve as modificações da regra e teste a conectividade:

1.- Aplicar as alterações de configuração à política ativa.

2.- Teste a conectividade com a Internet para destinos bloqueados anteriormente.

3.- Monitore os registros de segurança para garantir que o tráfego HTTP legítimo agora seja permitido.

4.- Verifique se as outras proteções de segurança continuam em vigor.

Causa

A causa raiz foi uma configuração de regra de segurança excessivamente restritiva no Cisco Secure Access. A regra foi configurada para bloquear todo o tráfego do protocolo de aplicativo HTTP, o que impedia a navegação legítima na Web e o acesso do aplicativo. A ampla aplicação do bloqueio de protocolo HTTP afetou a conectividade normal da Internet para usuários que acessam serviços Web legítimos e aplicativos que utilizam protocolos HTTP/HTTPS.

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.