VPN de acesso seguro - impossível acessar o Jabber

Contents

Problema

Os usuários do Secure Client não conseguiram acessar aplicativos internos e privados, como Jabber e Epic, pelo túnel VPN do Secure Access, ao usar uma política de acesso privado. Os usuários experimentaram falhas de conectividade ao tentar acessar esses aplicativos empresariais críticos através da conexão VPN. Durante a solução de problemas, o tráfego unidirecional foi observado para recursos Epic, onde o tráfego de ping e TCP SYN foi visto saindo do túnel VPN de acesso seguro, mas problemas de validação de tráfego de retorno foram identificados no firewall Palo Alto. Além disso, problemas de acessibilidade do Jabber foram documentados onde os FQDNs do CUCM estavam sendo resolvidos via DNS interno, enquanto o direcionamento de tráfego foi configurado para roteamento baseado em IP, causando uma incompatibilidade no fluxo de tráfego.

Ambiente

- Cisco Secure Access com configuração de túnel VPN
- Cliente seguro para conectividade VPN
- Implementação da política de acesso privado
- Cisco Unified Communications Manager (CUCM) para serviços Jabber
- Recursos de aplicativos Epic
- Firewall Palo Alto para segurança de rede
- Resolução interna de DNS para FQDNs CUCM

Resolução

A resolução envolveu várias alterações de configuração e etapas de solução de problemas para restaurar a conectividade para aplicativos internos através do túnel VPN de acesso seguro:

Configuração de Sub-rede e Modificações de Túnel

Passo 1: Adicionar outras sub-redes ao túnel VPN

Sub-redes adicionais foram adicionadas à configuração do túnel VPN para os recursos afetados. Após implementar essa alteração, os recursos que estavam anteriormente inacessíveis começaram a ser carregados com êxito.

Configuração da direção do endereço IP do CUCM

Passo 2: Configurar a direção IP do CUCM

Para resolver o problema de conectividade do Jabber em que os FQDNs do CUCM estavam sendo resolvidos via DNS interno enquanto o direcionamento de tráfego era baseado em IP, os endereços IP do CUCM foram direcionados para o Secure Client. Essa alteração de configuração alinhou a resolução DNS com o mecanismo de direção de tráfego.

Passo 3: Criar Regra de Política de Acesso

Uma regra de política de acesso foi criada para permitir o acesso aos endereços IP do CUCM. Essa regra restaurou a conectividade adequada à infraestrutura do CUCM, habilitando a funcionalidade Jabber pelo túnel VPN.

Configuração de roteamento estático

Passo 4: Configurar o roteamento estático para a sub-rede CUCM

Certifique-se de que os endereços IP do CUCM e a sub-rede geral do CUCM estejam incluídos na tabela de roteamento estático para o túnel de rede. Essa configuração garante o roteamento adequado do tráfego entre o pool de usuários do Secure Client e a infraestrutura do CUCM.

Validação do tráfego de retorno

Passo 5: Valide o fluxo de pacotes e o tráfego de retorno

Valide a configuração do fluxo de pacotes para confirmar se o tráfego de retorno pode alcançar o pool de usuários do Secure Client. Isso inclui a revisão da configuração do firewall da Palo Alto para garantir a validação adequada do caminho de retorno para todos os recursos internos,

particularmente para a conectividade Epic onde o tráfego unidirecional foi observado.

Causa

Os problemas de conectividade foram causados por várias falhas de configuração na implementação da VPN de acesso seguro:

- A ausência de configurações de sub-rede no túnel VPN impediu o roteamento adequado para recursos de aplicativos internos
- A incompatibilidade entre a resolução DNS (baseada em FQDN) e a configuração de direcionamento de tráfego (baseada em IP) para serviços CUCM causou falhas de conectividade Jabber
- Regras de política de acesso incompletas que não permitiam o tráfego para endereços IP CUCM
- Entradas de roteamento estático ausentes para sub-redes CUCM na configuração do túnel de rede
- Problemas de validação da via de tráfego de retorno no firewall Palo Alto afetando a comunicação bidirecional

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.