Problemas de conectividade de cliente completo Omnissa através de acesso seguro

Contents

Problema

O cliente completo Omnissa não consegue carregar desktops virtuais quando conectado através do Cisco Secure Access. Os usuários experimentam falhas de conectividade ao tentar estabelecer conexões com ambientes virtuais usando o aplicativo cliente completo. No entanto, o acesso por meio do cliente HTML/Web continua a funcionar normalmente, indicando que a infraestrutura de desktop virtual subjacente está funcional, mas há um problema específico que afeta a capacidade total do cliente de estabelecer conexões por meio da solução Cisco Secure Access.

Ambiente

- Tecnologia: Suporte à solução (SSPT - contrato necessário)
- Subtecnologia: Acesso seguro da Cisco
- Linha de produtos: SECACCS
- Versão de software: Todas as versões afetadas
- Aplicativo cliente: Omnissa cliente completo
- Ambiente de desktop virtual: Desktops virtuais Omnissa
- Infraestrutura de Rede: Túneis IPsec e FTD (Firepower Threat Defense, Defesa contra ameaças do Firepower)

Resolução

A resolução envolve a implementação de alterações de configuração de rede específicas para permitir o roteamento apropriado para o cliente completo Omnissa através do Cisco Secure Access. Estas etapas foram executadas para resolver o problema de conectividade:

- Defina as configurações de túnel dividido. Adicione configurações de túnel dividido para permitir que o cliente omnissa completo estabeleça conexões diretas com os hosts de destino necessários. Essa configuração garante que o tráfego destinado a clientes de desktop virtual específicos seja roteado corretamente através dos caminhos de rede apropriados.
- Implementar configurações de rota estática. Configure rotas estáticas para clientes específicos que precisam estabelecer conexões com áreas de trabalho virtuais. O principal requisito é configurar rotas não apenas para o downstream do servidor de agregação, mas diretamente para os hosts de destino que os clientes de desktop virtual precisam alcançar.
- Limpe os túneis IPsec. Depois de implementar as alterações de configuração, limpe os túneis IPsec no FTD para garantir que as novas configurações de roteamento entrem em vigor corretamente.
- Valide a conectividade. Teste a conectividade completa do cliente Omnissa após implementar as alterações para confirmar se as conexões de desktop virtual podem ser estabelecidas com sucesso através do Cisco Secure Access.

Cronograma de implementação

As alterações de configuração devem ser implementadas durante uma janela de manutenção programada para minimizar o impacto nos usuários. Após a implementação, valide a acessibilidade e a conectividade completa do cliente Omnissa para garantir que a resolução seja bem-sucedida.

Causa

O problema de conectividade foi causado por configurações insuficientes de roteamento no ambiente Cisco Secure Access. Especificamente, a rede foi configurada com rotas somente para o downstream do servidor de agregação, mas não tinha as configurações necessárias de túnel dividido e rota estática para os clientes específicos que o cliente completo Omnissa precisava para estabelecer conexões. Essa lacuna de roteamento impediu que o cliente completo acessasse corretamente os hosts de desktop virtual, enquanto o cliente HTML/Web ainda poderia funcionar porque usava caminhos de conexão diferentes que foram configurados corretamente.

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.