Configurar portas de proxy para tráfego de porta fora do padrão no WSA 1000V

Contents

Problema

Um proxy WSA 1000V hospedado no VMware estava processando o tráfego do cliente corretamente nas portas 80 e 443, mas não estava processando o tráfego em portas fora do padrão, como a porta 8890. Quando o acesso a um destino usando uma porta não padrão foi inicialmente bloqueado pela política, o WSA registrou corretamente a solicitação bloqueada. No entanto, depois de adicionar o endereço IP e o URL a uma política de permissão, o tráfego ainda falhou e nenhum registro correspondente foi gerado no proxy. Esse comportamento sugeriu que o tráfego não estava chegando ou sendo processado pelo WSA após a criação da política de permissão, afetando o acesso do cliente aos aplicativos que usam portas fora do padrão.

Ambiente

- Proxy Cisco WSA 1000V hospedados no VMware
- Software versão 15.0.0
- Tráfego nas portas 80 e 443 processando normalmente.
- O tráfego de porta não padrão (por exemplo, porta 8890) não está sendo processado pelo proxy.
- Permitir políticas configuradas para os destinos afetados.

Resolução

O problema foi resolvido com a configuração do WSA para oferecer suporte a portas fora do padrão nas configurações do Perfil de identificação. A configuração das portas de proxy precisava

ser atualizada para incluir os números de porta não padrão necessários.

Configuration Steps

Passo 1: Acesse a interface do Web Security Manager.

Passo 2: Navegue até a configuração Perfis de identificação.

Navegue até Web Security Manager > Identification Profiles.

Passo 3: Selecione o perfil de identificação desejado que requer suporte de porta não padrão.

Passo 4: Expanda as opções de configuração avançada.

Na página do perfil de identificação, expanda a guia Avançado.

Passo 5: Defina a configuração Proxy Ports.

Selecione o link ao lado de Proxy Ports para acessar a configuração da porta.

Passo 6: Adicione os números de porta não padrão necessários.

Adicione os números de porta específicos que os clientes usam para conexões de porta não padrão (por exemplo, 8890).

Passo 7: Salve e confirme as alterações de configuração.

Após implementar essas alterações de configuração, o WSA é capaz de processar e inspecionar o tráfego nas portas não padrão especificadas, permitindo que o proxy manipule corretamente as conexões de clientes e aplique políticas ao tráfego usando essas portas.

Causa

O WSA 1000V foi configurado com as configurações de porta de proxy padrão que incluíam

apenas portas HTTP (porta 80) e HTTPS (porta 443) padrão. A configuração das portas proxy do perfil de identificação não incluiu as portas não padrão exigidas pelos aplicativos cliente. Sem que essas portas sejam explicitamente configuradas nas configurações avançadas do perfil de identificação, o WSA não conseguiu interceptar, processar ou aplicar políticas ao tráfego usando portas não padrão, mesmo quando as políticas de permissão foram configuradas para os destinos.

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.