

Configurar e examinar o proxy SOCKS no dispositivo da Web seguro

Contents

[Introdução](#)

[Como o proxy SOCKS funciona em um alto nível](#)

[Configuração do proxy SOCKS em SWA/WSA](#)

[Solucionar problemas relacionados ao proxy SOCKS](#)

[Não suportado na implementação SWA SOCKS](#)

[Informações adicionais](#)

[Referência](#)

Introdução

Este documento descreve como o proxy SOCKS funciona no Cisco SWA e fornece uma visão geral de como ele roteia o tráfego entre um cliente e o servidor final

Como o proxy SOCKS funciona em um alto nível

Soquete Seguro (SOCKS) é um protocolo de rede que facilita a comunicação com servidores através de um proxy SOCKS (aqui, é SWA/WSA) roteando o tráfego de rede para o servidor real em nome de um cliente. O SOCKS foi projetado para rotear qualquer tipo de tráfego da camada de aplicação gerado por qualquer programa.

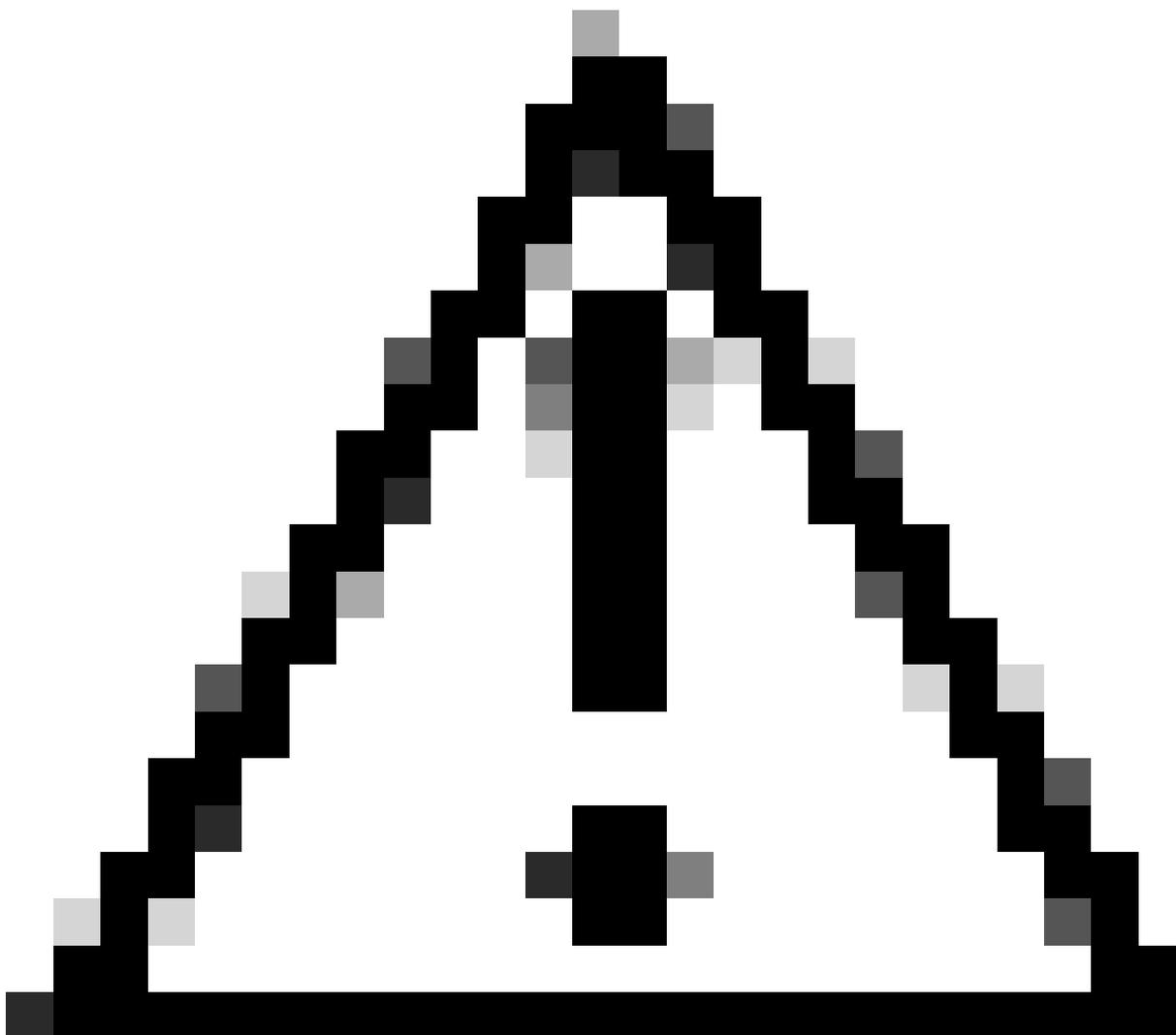
O SWA, por padrão, usa a porta TCP 1080 para escutar o tráfego SOCKS do cliente. Os clientes podem configurar o envio do tráfego socks para o WSA na porta TCP 1080. Você pode adicionar números de porta adicionais, se necessário.

O SOCKS versão 5 também suporta o tunelamento UDP para que o cliente possa usar a porta UDP também para enviar o tráfego para o proxy. Por padrão, é 16000-16100.

Quando você deseja retransmitir um tráfego UDP sobre o proxy SOCKS5, o cliente faz uma solicitação de associação UDP sobre a porta de controle TCP 1080. O servidor SOCKS5 (SWG/WSA) retorna uma porta UDP disponível para o cliente para onde enviar os pacotes UDP. Por padrão, é 16000-16100. Você pode modificar os números de porta.

O cliente então começa a enviar os pacotes UDP que precisam ser retransmitidos para a nova porta UDP que está disponível no servidor SOCKS5. O servidor SOCKS5 redireciona esses pacotes UDP para o servidor remoto e redireciona os pacotes UDP vindos do servidor remoto de volta para o PC.

Quando você deseja encerrar a conexão, o PC envia um pacote FIN pelo TCP. O servidor SOCKS5 termina a conexão UDP criada para o cliente e, em seguida, termina a conexão TCP.



Cuidado: as informações neste documento foram criadas a partir dos dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configuração do proxy SOCKS em SWA/WSA

Você pode navegar para [Serviços de segurança > proxy SOCKS](#) para configurar a porta de controle SOCKS e as portas de solicitação UDP. Isso também permite configurar os tempos limite.

1. O SOCKS versão 5 é suportado. Não há suporte para a versão 4.
2. O protocolo SOCKS só suporta conexões diretas de encaminhamento, portanto ele não suporta redirecionamentos.
3. O proxy SOCKS não oferece suporte a proxies de upstream, portanto, você não pode enviar o tráfego de socks do WSA para outro proxy de upstream. Você deve sempre usar a política de roteamento de conexão direta.
4. Você não pode utilizar as funcionalidades do WSA, como varredura, AVC, DLP e detecção de malware.
5. O rastreamento de política não pode funcionar com proxy socks.
6. Não há suporte à descryptografia SSL disponível como túneis de tráfego do cliente para o servidor.
7. Proxy Socks suporta apenas autenticação básica.

Informações adicionais

Por padrão, ao tentar enviar tráfego SOCKS via Firefox, a resolução DNS é feita localmente, portanto, o WSA não vê nenhum nome de host nos relatórios ou logs de acesso. Se habilitarmos o DNS Remoto no Firefox, o WSA poderá fazer a resolução DNS e poderemos exibir o nome do host nos logs de relatório/acesso. A opção de DNS remoto está disponível nas versões mais recentes do Firefox. Se não estiver disponível, tente estas etapas.

sobre:config

Nome de preferência de pesquisa: proxy, localize network.proxy.socks_remote_dns e defina-o como True.

O navegador Google Chrome, por padrão, executa a resolução DNS no proxy SOCKS para que nenhuma alteração seja necessária.

De acordo com o documento de suporte do Google Chrome Proxy, o SOCKSv5 é usado somente para solicitações de URL baseadas em TCP de proxy. Ele não pode ser usado para retransmitir o tráfego UDP.

Referência

<https://www.rfc-editor.org/rfc/rfc1928#section-4>

<https://chromium.googlesource.com/chromium/src+/HEAD/net/docs/proxy.md#SOCKSv5-proxy-scheme>

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.