

O proxy Umbrella bloqueia a conectividade de aplicativos Ninja

Contents

Problema

Os usuários não podem executar um sistema remoto usando um arquivo de instalação baixado quando conectados pelo Cisco Umbrella. O aplicativo não funciona sob a proteção Umbrella, afetando especificamente o acesso ao sistema remoto. O mesmo sistema remoto funciona perfeitamente sem nenhum problema quando o proxy do Cisco Umbrella está desativado.

As tentativas de solução de problemas incluíram o teste com uma política separada em que a segurança e o destino do sistema foram definidos como QUALQUER UM, mas o problema persistiu. Além disso, houve uma tentativa de rotear o tráfego através do acesso de confiança zero (ZTA), mas o problema permaneceu inalterado. O tráfego foi permitido através do Acesso Seguro no TCP/443, mas as conexões ainda estavam bloqueadas no endpoint.

Ambiente

- Cisco Umbrella com funcionalidade de proxy ativada
- Configuração do Zero Trust Access (ZTA)
- Políticas de acesso seguro configuradas para tráfego TCP/443

Resolução

A resolução envolve a exclusão de domínios específicos relacionados ao NinjaOne do proxy Umbrella para permitir a conectividade direta para o aplicativo de acesso remoto.

Passo 1: Identificar domínios afetados

A análise da captura de pacotes e dos arquivos HAR revela que esses domínios relacionados ao NinjaOne estão sendo afetados pelo proxy Umbrella:

- ninjarmm.net
- ninjarmm.com
- app.ninjarmm.com
- ninjaone.com
- agent-app.ninjaone.com

Passo 2: Configurar isenções de domínio

Exclua os domínios identificados das políticas de Segurança da Internet do Secure Web Gateway (SWG) e da direção do tráfego da Internet ZTA. Essa alteração de configuração permite que esses domínios ignorem o proxy Umbrella e estabeleçam conexões diretas.



Note: Uma configuração de lista Não descriptografar (NaoPtb) foi considerada ineficaz para resolver esse problema. A orientação do tráfego e a isenção são a abordagem recomendada.

Passo 3: Aplicar alterações de configuração

Implemente as isenções de domínio na configuração Umbrella para excluir o tráfego relacionado ao NinjaOne do processamento de proxy. Isso permite que o aplicativo de acesso remoto estabeleça conexões diretas com os serviços necessários.

Passo 4: Validar Resolução

Teste a funcionalidade do aplicativo de acesso remoto depois de aplicar as isenções para garantir que a conectividade apropriada seja restaurada enquanto mantém a proteção Umbrella para outro tráfego.

Causa

O problema ocorre porque os aplicativos de acesso remoto do NinjaOne rejeitam conexões com proxy quando o tráfego é roteado através do proxy do Cisco Umbrella. O aplicativo requer conectividade direta com domínios NinjaOne específicos para funcionar corretamente. Quando essas conexões são intermediadas por proxy através do Umbrella, o serviço de acesso remoto não pode estabelecer os canais de comunicação necessários, resultando em falha do aplicativo mesmo quando as políticas de segurança são configuradas para permitir o tráfego.

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.