Erro de sincronização de configuração ZTNA de acesso seguro com descriptografia SSL e túneis de rede

Contents

Problema

O Cisco Secure Client Zero Trust Access (ZTA) se inscreve com êxito, mas falha durante a sincronização da configuração com respostas HTTP 502 e estado de conectividade do servidor "BadResponse". Os logs do DART do endpoint do Windows 11 mostram o registro bem-sucedido, mas falhas repetidas de sincronização de configuração. O problema ocorre somente quando o endpoint é conectado ao caminho da rede corporativa usando o proxy Secure Access/Umbrella com túneis AutoVPN da Meraki, enquanto o mesmo endpoint conclui com êxito a sincronização de configuração em uma rede doméstica sem infraestrutura de proxy ou túnel.

Ambiente

- Cisco Secure Client ZTA versão 5.1.16.4434
- Ponto de extremidade do Windows 11 Enterprise
- Dispositivos Meraki MX com integração de AutoVPN
- Acesso seguro (SSE) com gateway de túneis de rede (NTG)
- DNS abrangente e segurança de acesso seguro à Web
- Descriptografia SSL e inspeção HTTPS habilitadas no caminho da rede corporativa
- Lista Não Descriptografar Fornecida pelo Sistema (DND) não configurada inicialmente

Resolução

A falha de sincronização de configuração foi resolvida com a implementação de desvios de descriptografia SSL adequados para domínios relacionados a ZTA ao usar Túneis de Rede com Acesso Seguro.

Passo 1: Identificar o impacto da descriptografia SSL

Verifique se a descriptografia SSL está causando as falhas de sincronização de configuração, revisando os logs de pesquisa de atividades no acesso seguro para eventos de descriptografia relacionados a domínios ZTA.

Passo 2: Configurar lista DND fornecida pelo sistema

Ao usar o Network Tunnels Gateway (NTG) com Acesso Seguro, o DND Fornecido pelo Sistema deve ser habilitado para ignorar adequadamente o tráfego relacionado a ZTA da inspeção de SSL.

Navegue até Secure Access Dashboard > Secure > Do Not Decrypt Lists e modifique a lista fornecida pelo sistema Do Not Decrypt.

Passo 3: Criar perfil de segurança para domínios ZTA

Adicione os domínios relacionados ao ZTA necessários a um novo perfil de segurança usando a lista DND fornecida pelo sistema:

- zpc.sse.cisco.com
- *.zpc.sse.cisco.com
- ztna.sse.cisco.com
- acme.sse.cisco.com
- devices.api.umbrella.com

Passo 4: Aplicar perfil de segurança à regra de teste

Atribua o perfil de segurança recém-criado contendo os desvios de domínio ZTA a uma regra de teste para validar a configuração.

Passo 5: Validar Sincronização de Configuração

Teste a inscrição ZTA e a sincronização da configuração a partir da rede corporativa. A sincronização agora pode ser concluída com êxito sem erros HTTP 502.

Passo 6: Coordenar com a equipe da Meraki

Para uma cobertura abrangente, coordene com o suporte da Meraki para validar URLs e domínios oficiais relacionados ao ZTA que podem ser ignorados na inspeção de acesso seguro. Consulte esta documentação da Meraki:

- Regras de firewall upstream para conectividade de nuvem
- Atualização de URL do painel Meraki - Conformidade com PCI

Causa

A falha de sincronização da configuração foi causada pela descriptografia SSL e proxy do tráfego de Acesso de Confiança Zero na rede corporativa. Quando o Network Tunnels Gateway (NTG) é usado com o Secure Access, os domínios relacionados ao ZTA devem ser ignorados usando a lista de endereços não criptografados fornecida pelo sistema (DND). Sem essa configuração de desvio, a inspeção SSL modifica as cadeias de certificados e interfere na comunicação do plano de controle ZTA, fazendo com que o cliente receba respostas HTTP 502 durante as tentativas de sincronização da configuração.

Conteúdo relacionado

- Solucionar problemas de descriptografia de acesso seguro e SSL

- Serviços de Registro com Base em Cliente Secure Access Zero Trust
- Requisitos de domínio ZTA para acesso seguro
- Solucionar Problemas de Registro de Erro de Acesso Seguro
- Solução de Problemas de Erro de Sincronização da Configuração do Cliente Seguro
- Coletar registros ZTNA detalhados para solução de problemas
- 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.