

Acesso VPN do AnyConnect de Cliente Seguro Negado Devido a Problemas de Conformidade de Postura de Segurança do Ponto de Extremidade

Contents

Problema

Vários usuários não conseguem se conectar ao AnyConnect VPN e ao Zero Trust Access (ZTA) e recebem a mensagem de erro "Login negado. Seu ambiente não atende aos critérios de acesso definidos pelo administrador."

O problema está relacionado à conformidade da postura do endpoint, em que o requisito do Agente de Segurança de Endpoint é relatado como não correspondente. Os usuários experimentam VPN e negação de acesso ZTA ao tentar se conectar por meio do Cisco Secure Client.

A avaliação de postura mostra que a postura de segurança do ponto final do Trellix está falhando nos pontos finais afetados, impedindo a autenticação bem-sucedida para o serviço VPN.

Ambiente

- Cisco Secure Client (AnyConnect e acesso sem confiança)
- Agente de Segurança de Ponto Final Trellix versão 5.8.4.505
- Perfil de postura da VPN: KFIN_SECURE_VPN com imposição de agente de segurança de ponto de extremidade
- Requisito de postura: Agente de segurança de endpoint em execução com atualizações nos últimos 14 dias

- Pontos de extremidade do Windows com o Serviço do Agente Trellix em execução
- Processos do Umbrella Agent detectados em endpoints

Resolução

O problema foi resolvido resolvendo-se os problemas de conformidade de postura do agente de segurança do endpoint Trellix. As etapas de solução de problemas e resolução descritas nas próximas seções foram implementadas.

Passo 1: Validar Configuração de Perfil de Situação

Revise o perfil de postura da VPN para confirmar os requisitos do agente de segurança do ponto final. O perfil KFIN_SECURE_VPN impõe que um agente de segurança de ponto de extremidade esteja em execução e atualizado nos últimos 14 dias.

Passo 2: Verifique o status de segurança do ponto de extremidade do Trellix

Verifique o status atual do agente Trellix Endpoint Security nos pontos de extremidade afetados:

```
Trellix Agent Service: masvc.exe  
Version: 5.8.4.505  
Install Location: C:\Program Files\McAfee\Agent\  
Display Name: Trellix Agent  
Publisher: Trellix
```

Passo 3: Reinstalar Segurança de Ponto de Extremidade do Trellix

Execute uma reinstalação completa do Trellix Endpoint Security nos endpoints afetados:

1. Desinstale totalmente o agente de Segurança de Ponto de Extremidade Trellix existente.

2. Reinicialize o sistema.

3. Instalar a versão mais recente aprovada do agente Trellox de acordo com os padrões organizacionais.

4. Verifique se o agente está sendo executado com êxito após a instalação.

5. Confirme se as atualizações de assinatura/conteúdo foram concluídas com êxito.

Passo 4: Ativar o registro TRACE para o Cisco Secure Client (ZTA)

Habilite o log detalhado para capturar detalhes da avaliação da postura.

Crie o arquivo logconfig.json com este conteúdo:

```
{ "global": "DBG_TRACE" }
```

Coloque o arquivo no diretório apropriado:

- Windows: C:\ProgramData\Cisco\Cisco Secure Client\ZTA
- MacOS: /opt/cisco/secureclient/zta

Reinicie o serviço Cisco Secure Client/ZTA após criar o arquivo.

Passo 5: Coletar pacote DART atualizado

Depois de implementar as alterações, colete um novo pacote DART para validar a resolução e confirmar a detecção apropriada de conformidade de postura.

Causa

A causa raiz foi identificada como problemas de conformidade de postura do agente do Trellix Endpoint Security. O perfil de postura de VPN exigia que um agente de segurança de ponto final estivesse em execução com atualizações nos últimos 14 dias, mas o agente de Segurança de Ponto Final do Trellix não estava atendendo a esses critérios de conformidade. O módulo de avaliação de postura não pôde detectar ou validar corretamente o status do agente de segurança do ponto de extremidade, resultando em uma negação de acesso para conexões VPN e ZTA. O problema estava especificamente relacionado à configuração do agente do Trellix e exigia intervenção da equipe de suporte do Trellix para resolver os problemas subjacentes de conformidade do agente.

Conteúdo relacionado

- [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.