Desconexões intermitentes de acesso seguro atrás de firewalls corporativos com erros de timeout ocioso

Contents

- Problema
- Ambiente
- Resolução
  - Passo 1: Implementar configuração de buffer TTL MX
  - Passo 2: Configurar Exclusões de Domínio Necessárias
  - Passo 3: Verificar as permissões de porta e protocolo
  - Passo 4: Monitore e valide a resolução
- Causa
- Conteúdo relacionado

Problema

Os clientes do Cisco Secure Access experimentam desconexões intermitentes e reconexões imediatas quando os terminais estão conectados à rede corporativa. As desconexões ocorrem aleatoriamente, com o cliente se reconectando automaticamente após aproximadamente 5 segundos. Esse comportamento é observado quando o tráfego da Internet recebe proxy via ZTA (Zero Trust Access) para acesso seguro de endpoints posicionados atrás dos dispositivos Cisco FirePower e Meraki MX.

O log de eventos do Windows captura erros específicos de "idleTimeout" durante esses eventos de desconexão. O padrão de desconexão não ocorre quando os usuários se conectam de

conexões de Internet domésticas, indicando que o problema está especificamente relacionado à infraestrutura de rede corporativa.

O sintoma cria uma interrupção nos negócios para proteger a conectividade de acesso remoto para usuários que operam no ambiente de rede corporativo, enquanto os usuários remotos permanecem inalterados por esse problema de conectividade.

Ambiente

- Cisco Secure Access - Implantação vantajosa
- Software cliente Cisco Secure Internet Access (SIA)
- Infraestrutura de rede corporativa com dispositivos de segurança Cisco FirePower
- Dispositivos de segurança Meraki MX no caminho da rede
- Configuração ZTA (Zero Trust Access) que usa proxy no tráfego da Internet para acesso seguro
- Endpoints do Windows com recurso de registro de eventos
- Cenários de conectividade mista: rede corporativa (afetada) e conexões de internet residencial (não afetada)

Resolução

A resolução envolvia a implementação de alterações de configuração no dispositivo Meraki MX e a garantia de exclusões de domínio e permissões de porta adequadas para a integração do Secure Access.

Passo 1: Implementar configuração de buffer TTL MX

Configure um buffer TTL MX no dispositivo Meraki MX para lidar com o comportamento de cache TTL DNS que estava contribuindo para os problemas de desconexão intermitente. Essa alteração de configuração resolve os conflitos de temporização entre o cache de resolução DNS e as

expectativas de conectividade do cliente Secure Access.

Passo 2: Configurar Exclusões de Domínio Necessárias

Certifique-se de que esses domínios sejam adequadamente excluídos da interceptação e adicionados a listas de não descriptografia nos dispositivos Cisco FirePower e Meraki MX:

- ztna.sse.cisco.com
- zpc.sse.cisco.com
- Domínios de serviço de Acesso Seguro adicionais conforme identificados na configuração de política

Passo 3: Verificar as permissões de porta e protocolo

Configure a infraestrutura de firewall corporativa para permitir as portas e os protocolos de acesso seguro necessários por meio dos dispositivos FirePower e Meraki MX. Certifique-se de que o tráfego para a porta 443 para pontos de extremidade de serviço de Acesso Seguro seja tratado corretamente sem interferência da inspeção de segurança que poderia causar condições de timeout.

Passo 4: Monitore e valide a resolução

Após implementar a configuração do buffer TTL MX, monitore o comportamento do cliente Secure Access por vários dias para confirmar que o padrão de desconexão e reconexão intermitente parou.

Causa

As desconexões intermitentes foram causadas por conflitos de comportamento de cache DNS TTL (Time To Live, Tempo de Vida Restante) entre a infraestrutura de rede corporativa e as expectativas do serviço Secure Access. A análise de engenharia da Cisco revelou que os valores

TTL de DNS variam devido ao comportamento de cache do resolvedor, e endereços IP alternados são comportamento esperado devido a mecanismos de balanceamento de carga na arquitetura de serviço do Secure Access.

Quando os dispositivos de rede corporativa (Cisco FirePower e Meraki MX) processaram respostas DNS para endpoints do Secure Access, o armazenamento em cache e o tratamento TTL criaram incompatibilidades de temporização que resultaram em condições de "idleTimeout". Esse conflito de temporização fez com que o cliente Secure Access interpretasse a conexão como ociosa e iniciasse ciclos de desconexão/reconexão.

O problema era específico para ambientes de rede corporativa, pois as conexões de internet residenciais geralmente não implementam o mesmo nível de cache de DNS e inspeção de tráfego que pode interferir no gerenciamento do estado da conexão do cliente Secure Access.

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.