Grupo de Túnel de Rede de Acesso Seguro não Sincronizado Intermitentemente com o Gateway VPN do Azure Durante Eventos de Rechaveamento IKE

Contents

Problema

Um Network Tunnel Group recém-configurado entre o Cisco Secure Access e o Azure VPN Gateway passa por um túnel intermitente oscilando aproximadamente a cada 4 horas durante eventos de rechaveamento de IKE.

Estas mensagens de erro e sintomas específicos são observados:

- Emparelhamento via protocolo BGP desativado, temporizador de espera expirado
- Alerta: rechaveamento de IKE com falha
- Túnel IKE desconectado

A oscilação de túnel resulta em interrupções periódicas, falhas de rechaveamento de IKE, falhas de verificação de integridade, desconexões de túnel e quedas de peering de BGP, afetando a conectividade estável aos recursos do Azure. Falhas de autenticação são observadas durante negociações de rechaveamento.

Ambiente

- Grupo de Túnel de Rede do Cisco Secure Access (CSA) configurado para o Gateway VPN do Azure
- Túneis VPN Site a Site IPsec usando IKEv2

- Gateway VPN do Azure com criptografia AES-GCM-256 configurada nas políticas do Modo Principal (MM)
- NAT-T (NAT Traversal) habilitada em ambos os lados usando a porta 4500
- Correspondência BGP configurada entre pontos finais
- Tempo de vida padrão de IKE SA de 4 horas (28800 segundos)
- Configuração inicial do tempo de vida de SA do IPsec, modificado posteriormente para 10800 segundos
- PFS (Perfect Forward Secrecy) não habilitado no Azure

Resolução

O problema foi resolvido por meio de uma alteração de configuração para evitar cifras AES-GCM nas políticas do Modo Principal, com base na identificação de um bug no Gateway VPN do Azure.

Passo 1: Análise de Depuração do Gateway VPN do Azure

As depurações de IKE foram coletadas do lado do Gateway VPN do Azure, revelando esse comportamento durante tentativas de rechaveamento:

```
SESSION_ID :{} Remote x.x.x.x:500: Local x.x.x.x:500: [SEND]Sending IPSec policy Payload for tunnel Id
SESSION_ID :{} Remote x.x.x.x:4500: Local x.x.x.x:4500: [SEND][CHILD_SA MM_REKEY] Sending IKE rekey res
SESSION_ID :{} Remote x.x.x.x:4500: Local x.x.x.x:4500: [LOCAL_MSG] IKE Tunnel closed for tunnelId x3 w
```

Passo 2: Identificação da causa raiz

O suporte do Azure investigou as falhas de rechaveamento. A análise do Azure identificou que quando o Azure inicia um MM-REKEY usando AES-GCM-256, o pacote de rechaveamento está malformado. O dispositivo local não responde à solicitação de rechaveamento malformada, resultando na desconexão do túnel.

Passo 3: Implementação da solução alternativa de configuração

Com base nas recomendações do Azure, esta mitigação foi implementada:

- Remova as cifras AES-GCM das políticas do Modo Principal (MM) na configuração do Grupo de Túneis de Rede.
- Configure métodos de criptografia alternativos que não usem o modo GCM.

Consulte a Etapa 17 em https://securitydocs.cisco.com/docs/csa/olh/121327.dita.

Passo 4: Opções alternativas de mitigação

O Azure também forneceu estratégias de mitigação adicionais que podem ser consideradas:

- Configure o tempo de vida do MM local para ser maior que 28800 segundos para que o Azure sempre inicie uma nova chave.
- Defina o Gateway VPN do Azure para o modo somente de resposta com vida útil de SA local menor do que a vida útil do Azure.

Causa

A causa raiz é um bug no Gateway VPN do Azure que afeta as operações de rechaveamento AES-GCM. Quando o Azure inicia um MM-REKEY usando AES-GCM-256, o pacote de rechaveamento é malformado, fazendo com que o dispositivo Cisco Secure Access local não responda à solicitação de rechaveamento malformada. Isso resulta em falhas de rechaveamento de IKE, erros de autenticação e desconexões de túnel subsequentes.

O Azure confirmou isso como um bug existente e documentou uma correção planejada em uma futura versão do gateway, prevista para meados de 2026.

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.