Túneis IPSec oscilam entre o Secure Access e o C8000Vs hospedado no Azure/AWS

Contents

Problema

Os túneis de rede IPsec entre os roteadores C8000V/Cisco IOS-XE e a rede Cisco Secure Access na região us-east-2 estão oscilando.

Todos os grupos de túneis são afetados, resultando em túneis inativos entre os roteadores no local e a rede Cisco Secure Access.

Ambiente

- Tecnologia: suporte à solução (SSPT - contrato necessário)
- Subtecnologia: Acesso seguro - Túneis de rede (IPSEC, site a site, recurso privado)
- Família de produtos: SECACCS
- Roteadores: C8000V / roteadores Cisco IOS-XE (no local)
- Endpoint remoto: rede Cisco Secure Access (região leste-2 dos eua)
- Versão do Software: Não especificada
- Mensagens de erro, logs, depurações observadas
- Nenhum usuário final afetado durante a interrupção

Resolução

A partir dos registros de entroncamento CNHE

porta = 1409

sourceIpAddr = x.x.x.x

porta = 1408

sourceIpAddr = x.x.x.x

1. Foi detectada uma alteração de ponto de extremidade remoto (a porta foi atualizada)
2. O Cortex aciona uma nova chave filha nesta atualização
3. Nenhuma resposta do cliente em novas chaves usando a nova porta para que o cortex esgote as novas tentativas e termine o túnel
4. Logo após a reinicialização do cliente, usando a nova porta onde o túnel é ativado

A partir dos logs de tronco CSA.

2026-02-02T16:36:02.188+00:00 disparando uma nova chave filha para atualização do ike com o IP local: x.x.x.x, ike_spi:new_datanode:

2026-02-02T16:36:04.207+00:00 retransmitir 1 de solicitação com ID de mensagem 0

2026-02-02T16:36:08.207+00:00 retransmitir 2 da solicitação com ID de mensagem 0

2026-02-02T16:36:16.207+00:00 retransmitir 3 da solicitação com ID de mensagem 0

2026-02-02T16:36:32.207+00:00 retransmitir 4 de solicitação com ID de mensagem 0

2026-02-02T16:37:04.207+00:00 retransmitir 5 da solicitação com ID de mensagem 0

2026-02-02T16:38:08.208+00:00 desistindo após 5 retransmissões

2026-02-02T16:38:08.208+00:00 terminando IKE, falha na rechave SA filho

A partir do log de depuração 1769305781091_vJY_CENTRAL_R2.log:

Erros SPI inválidos - Ocorrem com muita frequência:

*Jan 24 07:55:04.209: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: o pacote IPSEC gravado tem spi inválido para destaddr=x.x.x.x prot=50, spi=, srcaddr=x.x.x.x, interface de entrada=Tunnel12

*Jan 24 07:56:06.829: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: o pacote IPSEC gravado tem spi inválido para destaddr=x.x.x.x, prot=50, spi=, srcaddr=x.x.x.x, interface de entrada=Tunnel11

Não-sincronização de túnel - Várias instâncias de túneis sendo desativadas/ativadas:

* 24 de janeiro 08:33:12.069: %LINEPROTO-5-UPDOWN: protocolo de linha no túnel de interface12, estado alterado para inativo

* 24 de janeiro 08:33:14.459: %LINEPROTO-5-UPDOWN: protocolo de linha no túnel de interface11, estado alterado para inativo

*Jan 24 08:33:15.275: %LINEPROTO-5-UPDOWN: protocolo de linha no túnel de interface11, estado alterado para ativo

Causa

Isso parecerá um problema de cliente com defeito se a porta estiver oscilando.

A oscilação parece ser estável por enquanto após fazer uma alteração no Azure.

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.