La autenticación del túnel IPSec falla entre el acceso seguro y el firewall FortiGate

Problema

El establecimiento del túnel IPSec falla entre Cisco Secure Access y un firewall FortiGate con errores de autenticación. Los registros de depuración del firewall FortiGate muestran mensajes de "fallo de autenticación", a pesar de la verificación de que las claves precompartidas (PSK) coinciden en ambos lados. La negociación de la fase 1 está fallando con un error INVALID_KE_PAYLOAD, que impide que el túnel se active. Las propuestas para la conexión parecen coincidir entre ambos puntos finales, pero el proceso de establecimiento del túnel no se ha completado correctamente.

Entorno

- Acceso seguro de Cisco
- Firewall FortiGate (gestionado por terceros)
- Configuración de túnel IPSec con terminales principales y de reserva redundantes

Resolución

El problema de conectividad del túnel IPSec se resolvió realizando ajustes de configuración específicos para resolver el error INVALID_KE_PAYLOAD y los problemas de autenticación.

Configuración de Grupo DH de Fase 1

Configure sólo un grupo Diffie-Hellman (DH) para la negociación de fase 1. Establezca el grupo DH 20 en la fase 1 en lugar de utilizar varios grupos DH o el grupo DH 14 configurado anteriormente.

Corrección de configuración

```
config vpn ipsec phase1-interface
    edit "sse-tunnel"
        set dhgrp 20
    next
end
```

Configuración transversal de NAT

Active NAT Traversal (NAT-T) en la configuración del túnel IPSec. Anteriormente se deshabilitó, pero debe habilitarse para establecer correctamente el túnel.

Configuración Perfecta De Confidencialidad Directa

Deshabilite Perfect Forward Secrecy (PFS) en la configuración de la fase 2 para eliminar posibles conflictos de negociación.

Causa

La falla del túnel IPSec fue causada por múltiples discordancias e incompatibilidades de la configuración:

- Error INVALID_KE_PAYLOAD: Este error de fase 1 se produjo debido a conflictos de negociación de grupo Diffie-Hellman entre los terminales de Cisco Secure Access y FortiGate
- Discordancia de grupo DH: Varios grupos DH configurados y el uso del grupo DH 14 en la configuración original no era compatible con los requisitos de Cisco Secure Access
- Configuración transversal de NAT: NAT Traversal estaba desactivado, lo que impedía el establecimiento correcto del túnel en el entorno de red

Contenido relacionado

- Configuración del acceso seguro con el firewall FortiGate
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).