Autenticazione tunnel IPSec non riuscita tra Secure Access e il firewall FortiGate

Problema

Errore durante la definizione del tunnel IPSec tra Cisco Secure Access e un firewall FortiGate con errori di autenticazione. I registri di debug del firewall di FortiGate visualizzano messaggi di "autenticazione non riuscita", nonostante la verifica della corrispondenza delle chiavi già condivise (PSK) su entrambi i lati. Negoziazione fase 1 non riuscita con un errore INVALID_KE_PAYLOAD. Impossibile completare il tunnel. Le proposte per la connessione sembrano corrispondere tra entrambi gli endpoint, ma il processo di definizione del tunnel non è stato completato correttamente.

Ambiente

- Cisco Secure Access
- Firewall FortiGate (gestito da terze parti)
- Configurazione del tunnel IPSec con endpoint primari e di backup ridondanti

Risoluzione

Il problema di connettività del tunnel IPSec è stato risolto apportando modifiche di configurazione specifiche per risolvere l'errore INVALID_KE_PAYLOAD e i problemi di autenticazione.

Configurazione gruppo DH fase 1

Configurare un solo gruppo Diffie-Hellman (DH) per la negoziazione della fase 1. Impostare il gruppo DH 20 sulla fase 1 anziché utilizzare più gruppi DH o il gruppo DH 14 configurato in precedenza.

Correzione configurazione

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

Configurazione trasversale NAT

Abilitare NAT Traversal (NAT-T) nella configurazione del tunnel IPSec. Questa funzionalità è stata disabilitata in precedenza, ma è necessario abilitarla per stabilire correttamente il tunnel.

Configurazione Perfect Forward Secrecy

Disabilitare Perfect Forward Secrecy (PFS) nella configurazione della fase 2 per eliminare potenziali conflitti di negoziazione.

Causa

L'errore del tunnel IPSec è stato causato da più incompatibilità e mancata corrispondenza della configurazione:

- Errore INVALID_KE_PAYLOAD: Questo errore di fase 1 si è verificato a causa di conflitti di negoziazione del gruppo Diffie-Hellman tra gli endpoint Cisco Secure Access e FortiGate
- Gruppo DH non corrispondente: Più gruppi DH configurati e l'utilizzo del gruppo DH 14 nella configurazione originale non è compatibile con i requisiti di Cisco Secure Access
- Impostazioni attraversamento NAT: NAT Traversal disabilitato. Impossibile stabilire il tunnel corretto nell'ambiente di rete

Contenuto correlato

- Configurazione di Secure Access con FortiGate Firewall
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).