IPSec Tunnel Authentication Fails Between Secure Access and FortiGate Firewall

Issue

IPSec tunnel establishment is failing between Cisco Secure Access and a FortiGate firewall with authentication errors. The FortiGate firewall debug logs show "authentication failed" messages, despite verification that the Pre-Shared Keys (PSKs) match on both sides. The Phase 1 negotiation is failing with an INVALID_KE_PAYLOAD error, preventing the tunnel from coming up. The proposals for the connection appear to match between both endpoints, but the tunnel establishment process is not completing successfully.

Environment

- Cisco Secure Access
- FortiGate firewall (managed by third party)
- IPSec tunnel configuration with redundant primary and backup endpoints

Resolution

The IPSec tunnel connectivity issue was resolved by making specific configuration adjustments to address the INVALID_KE_PAYLOAD error and authentication problems.

Phase 1 DH Group Configuration

Configure only one Diffie-Hellman (DH) group for Phase 1 negotiation. Set DH group 20 on Phase 1 instead of using multiple DH groups or the previously configured DH group 14.

Configuration Fix

```
config vpn ipsec phase1-interface
```

```
    edit "sse-tunnel"
        set dhgrp 20
    next
end
```

NAT Traversal Configuration

Enable NAT Traversal (NAT-T) on the IPSec tunnel configuration. This was previously disabled but needs to be enabled for proper tunnel establishment.

Perfect Forward Secrecy Configuration

Disable Perfect Forward Secrecy (PFS) in the Phase 2 configuration to eliminate potential negotiation conflicts.

Cause

The IPSec tunnel failure was caused by multiple configuration mismatches and incompatibilities:

- INVALID_KE_PAYLOAD Error: This Phase 1 error occurred due to Diffie-Hellman group negotiation conflicts between the Cisco Secure Access and FortiGate endpoints
- DH Group Mismatch: Multiple DH groups configured and use of DH group 14 in the original configuration was not compatible with the Cisco Secure Access requirements
- NAT Traversal Settings: NAT Traversal was disabled, which prevented proper tunnel establishment in the network environment

Related Content

- Configure Secure Access with FortiGate Firewall
- Cisco Technical Support & Downloads