ANEXO 5

Configuración del Túnel IPsec y Reglas de Firewall

Proyecto: Interconexión Segura entre Dos Sedes (VPN Site-to-Site)

Fecha: Julio 2026 · Versión: 1.0

Elaborado por: Enrique Calabozo Orea – Administrador de Sistemas TIC / Project Manager

Este anexo recoge los parámetros de configuración de referencia del túnel IPsec Site-to-Site y la matriz de reglas de firewall, coherentes con el esquema de direccionamiento del Anexo 1. La sintaxis usada es genérica tipo Cisco/vendor-neutral a modo de referencia; debe adaptarse a la interfaz o CLI real del fabricante finalmente seleccionado. Las claves precompartidas se muestran como marcadores `[entre corchetes]` y deben gestionarse de forma segura (gestor de contraseñas / vault), nunca en texto plano en la documentación final.

1. Parámetros de Fase 1 (IKE)

Parámetro	Valor
Versión de IKE	IKEv2
Autenticación	Clave precompartida (PSK) robusta ≥ 20 caracteres, o certificados digitales
Cifrado	AES-256
Integridad / Hash	SHA-256
Grupo Diffie-Hellman	Grupo 14 (2048 bits) mínimo — recomendado Grupo 19/20 (curva elíptica)
Tiempo de vida (lifetime)	28.800 segundos (8 horas)
Dead Peer Detection (DPD)	Habilitado — intervalo 10 s, 3 reintentos

2. Parámetros de Fase 2 (IPsec / ESP)

Parámetro	Valor
Protocolo	ESP, modo túnel
Cifrado	AES-256-GCM
Perfect Forward Secrecy (PFS)	Habilitado — Grupo 14
Tiempo de vida (lifetime)	3.600 segundos (1 hora)

3. Redes de Interés del Túnel

Coherentes con el Anexo 1 (esquema de direccionamiento):

Extremo local (Sede Central)	Extremo remoto (Sucursal)
10.10.10.0/24 (Datos)	10.20.10.0/24 (Datos-Sucursal)
10.10.60.0/24 (Servidores)	10.20.10.0/24 (Datos-Sucursal)
10.10.60.0/24 (Servidores)	10.20.30.0/24 (WiFi-Corp-Sucursal)

4. Configuración de Referencia — Sede Central

```
! Interfaz WAN de cabecera
interface WAN
 description Enlace a Internet (IP publica fija)
!
! Definicion de la fase 1 (IKEv2)
```

```
crypto ikev2 proposal IKE-PROPOSAL
 encryption aes-256
 integrity sha256
 group 14
!
crypto ikev2 keyring VPN-SUCURSAL-KEYRING
 peer SUCURSAL
  address [IP-WAN-SUCURSAL]
  pre-shared-key [clave-precompartida-robusta]
!
crypto ikev2 profile IKE-PROFILE-SUCURSAL
 match identity remote address [IP-WAN-SUCURSAL] 255.255.255.255
 authentication local pre-share
 authentication remote pre-share
 keyring local VPN-SUCURSAL-KEYRING
 dpd 10 3 on-demand
!
! Definicion de la fase 2 (IPsec/ESP)
crypto ipsec transform-set TS-AES256GCM esp-gcm 256
 mode tunnel
!
crypto ipsec profile IPSEC-PROFILE-SUCURSAL
 set transform-set TS-AES256GCM
 set ikev2-profile IKE-PROFILE-SUCURSAL
 set pfs group14
 set security-association lifetime seconds 3600
!
! Interfaz de tunel virtual
interface Tunnel1
 description Tunel IPsec hacia Sucursal Remota
 ip address 169.254.100.1 255.255.255.252
 tunnel source WAN
 tunnel destination [IP-WAN-SUCURSAL]
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile IPSEC-PROFILE-SUCURSAL
!
! Enrutamiento hacia las redes de la sucursal
ip route 10.20.10.0 255.255.255.0 Tunnel1
ip route 10.20.30.0 255.255.255.0 Tunnel1
!
! Exencion de NAT para el trafico hacia el tunel (NAT exemption)
ip access-list extended NO-NAT-VPN
 permit ip 10.10.10.0 0.0.0.255 10.20.10.0 0.0.0.255
 permit ip 10.10.60.0 0.0.0.255 10.20.10.0 0.0.0.255
 permit ip 10.10.60.0 0.0.0.255 10.20.30.0 0.0.0.255
```

5. Configuración de Referencia — Sucursal Remota

Configuración simétrica en el equipo de cabecera de la sucursal (misma fase 1/fase 2, invirtiendo origen/destino), con la línea 4G/5G configurada como interfaz de respaldo:

```
interface WAN-PRIMARIA
 description Linea principal de Internet (IP dinamica)
!
interface WAN-RESPALDO
 description Modem 4G/5G de respaldo
!
! Mismos parametros de fase 1/2 que en la Sede Central, con peer invertido
crypto ikev2 keyring VPN-CENTRAL-KEYRING
 peer CENTRAL
  address [IP-WAN-SEDE-CENTRAL]
  pre-shared-key [clave-precompartida-robusta]
!
interface Tunnel1
 description Tunel IPsec hacia Sede Central
 ip address 169.254.100.2 255.255.255.252
 tunnel source WAN-PRIMARIA
 tunnel destination [IP-WAN-SEDE-CENTRAL]
```

```
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile IPSEC-PROFILE-CENTRAL
!
! Ruta de respaldo: si cae la deteccion DPD del tunel principal,
! se reestablece el tunel a traves de la interfaz 4G/5G (SLA/track configurado
! segun la sintaxis real del fabricante seleccionado)
track 1 interface WAN-PRIMARIA line-protocol
ip route 0.0.0.0 0.0.0.0 WAN-RESPALDO track 1
!
ip route 10.10.10.0 255.255.255.0 Tunnel1
ip route 10.10.60.0 255.255.255.0 Tunnel1
```

6. Matriz de Reglas de Firewall (Whitelist)

Política de denegación por defecto: solo se permite explícitamente el tráfico de la tabla siguiente; cualquier otro tráfico entre sedes queda bloqueado.

Nº	Origen	Destino	Servicio / Puerto	Acción
1	10.20.10.0/24 (Datos-Sucursal)	10.10.60.0/24 (Servidores)	TCP 445 (SMB), TCP 1433 (BD ERP)	Permitir
2	10.20.10.0/24 (Datos-Sucursal)	10.10.10.0/24 (Datos)	TCP 80/443 (intranet corporativa)	Permitir
3	10.20.30.0/24 (WiFi-Corp-Sucursal)	10.10.60.0/24 (Servidores)	TCP 443 (ERP web)	Permitir
4	10.10.10.0/24, 10.10.60.0/24	10.20.10.0/24, 10.20.30.0/24	ICMP (diagnóstico)	Permitir
5	any	any	any	Denegar (regla implícita final)

7. Alta Disponibilidad del Túnel

- El Dead Peer Detection (DPD) de fase 1 detecta la pérdida del peer remoto en un máximo de 30 segundos (10 s × 3 reintentos) y fuerza la renegociación del túnel.
- En la sucursal, la interfaz WAN principal se supervisa mediante un objeto de seguimiento (track); ante su caída, la ruta por defecto conmuta automáticamente a la línea 4G/5G de respaldo y el túnel se reestablece a través de ella.
- Se recomienda configurar una alerta (SNMP trap o correo) en el sistema de monitoreo ante cualquier caída del túnel, para que el equipo de operación pueda verificar la causa.

Nota: todas las configuraciones anteriores son plantillas de referencia elaboradas para este proyecto. Antes de aplicarlas en producción deben adaptarse a la sintaxis real del fabricante seleccionado, revisarse por el Ingeniero de Redes y probarse en un entorno controlado antes de desplegarlas (ver Memoria Técnica, sección 10).