

Guía de Configuración IPsec - pfSense

Esta guía describe cómo configurar correctamente la Fase 2 de una VPN IPsec entre dos dispositivos pfSense. El ejemplo parte de la red local 192.168.111.0/24 y la red remota 192.168.113.0/24.

Las capturas muestran cómo establecer manualmente las redes implicadas y los algoritmos adecuados para la fase de intercambio de claves (SA).

Captura: Configuración Fase 2 - Red y Algoritmos

The screenshot shows the pfSense web interface for configuring the Phase 2 of an IPsec VPN. The browser address bar shows the URL `192.168.111.1/vpn_ipsec_phase2.php?p2index=6819616b1a53d`. The configuration is divided into several sections:

- Networks:**
 - Local Network:** Set to 'Address' with the value '192.168.111.0 / 24'.
 - NAT/BINAT translation:** A dropdown menu is open, showing options: 'Address', 'Network', 'WAN subnet', and 'LAN subnet'. Below it, a note states: 'If NAT/BINAT is required on this network specify the address to be translated'.
 - Remote Network:** Set to 'Network' with the value '192.168.113.0 / 24'.
- Phase 2 Proposal (SA/Key Exchange):**
 - Protocol:** Set to 'ESP'. A note below states: 'Encapsulating Security Payload (ESP) performs encryption and authentication, Authentication Header (AH) is authentication only.'
 - Encryption Algorithms:**
 - ☒ AES (256 bits)
 - ☐ AES128-GCM (Auto)
 - ☐ AES192-GCM (Auto)
 - ☐ AES256-GCM (Auto)
 - ☐ CHACHA20-POLY1305
 - Hash Algorithms:**
 - ☐ SHA1
 - ☒ SHA256
 - ☐ SHA384
 - ☐ SHA512
 - ☐ AES-XCBC

Note: Hash is ignored with GCM algorithms. SHA1 provides weak security and should be avoided.
 - PFS key group:** Set to '14 (2048 bit)'.

Note: Groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.
- Expiration and Replacement:** This section is partially visible at the bottom of the screenshot.

Parámetros recomendados:

- Local Network: Tipo 'Address', valor 192.168.111.0/24 (se especifica a mano para evitar ambigüedades).
- Remote Network: Tipo 'Network', valor 192.168.113.0/24 (la red remota del otro firewall).

- Protocol: ESP
- Encryption Algorithm: AES (256 bits)
- Hash Algorithm: SHA256
- PFS Key Group: 14 (2048 bits)

En el otro extremo (el otro firewall), deben invertirse las redes local/remota (espejo exacto).

Nota: Evitá seleccionar 'LAN subnet' directamente si no estás seguro que pfSense la interpreta correctamente. Usar 'Address' con la red escrita es más fiable.