EJEMPLO DE CONFIGURACIÓN BÁSICA DE CORTAFUEGOS

Vamos a describir cómo el software pfSense® realiza la correspondencia de reglas y un conjunto básico estricto de reglas. El enfoque descrito en este documento no es el más seguro, pero ayudará a mostrar cómo se configuran las reglas.

Las reglas en las pestañas de Interfaz son comparadas en la interfaz entrante.

BLOQUEO BÁSICO DE LAS REGLAS SALIENTES LAN Y DMZ

LAN SALIENTE

Asegúrese de que la regla Default LAN > any está desactivada o eliminada.

1. Permitir el acceso DNS:
   - Si pfSense es el servidor DNS:
     - Permitir TCP/UDP 53 (DNS) desde la subred LAN a la dirección LAN.
   - Si se utilizan servidores DNS ascendentes:
     - Permitir TCP/UDP 53 (DNS) desde la subred LAN a los servidores DNS ascendentes.
   - En caso contrario:
     - Permitir TCP/UDP 53 (DNS) desde la subred LAN a cualquier lugar.
2. Permitir a todos los usuarios navegar por páginas web en cualquier lugar:
   - Permitir TCP 80 (HTTP) desde la subred LAN a cualquier lugar.
3. Permitir a los usuarios navegar por páginas web seguras en cualquier lugar:
   - Permitir TCP 443 (HTTPS) desde la subred LAN a cualquier lugar.
4. Permitir a los usuarios acceder a sitios FTP desde cualquier lugar:
   - Permitir TCP 21 (FTP) desde la subred LAN a cualquier lugar.
5. Permitir a los usuarios acceder a SMTP en un servidor de correo en cualquier lugar:
   - Permitir TCP 25 (SMTP) desde la subred LAN a cualquier lugar.
6. Permitir a los usuarios acceder a POP3 en un servidor de correo en algún lugar:
   - Permitir TCP 110 (POP3) desde la subred LAN a cualquier lugar.
7. Permitir a los usuarios acceder a IMAP en un servidor de correo en algún lugar:
   - Permitir TCP 143 (IMAP) desde la subred LAN a cualquier lugar.
8. Permitir conexiones remotas a un servidor Windows externo para administración remota:
   - Permitir TCP/UDP 3389 (Terminal server) desde la subred LAN a la dirección IP del servidor remoto.
9. Permitir que la LAN acceda a recursos compartidos de Windows en la DMZ, a través de NETBIOS/Microsoft-DS:
   - Permitir TCP/UDP 137 desde la subred LAN (NETBIOS) a la subred DMZ.
   - Permitir TCP/UDP 138 desde la subred LAN (NETBIOS) a la subred DMZ.
   - Permitir TCP/UDP 139 desde la subred LAN (NETBIOS) a la subred DMZ.
   - Permitir TCP 445 desde la subred LAN (NETBIOS) a la subred DMZ.

DMZ SALIENTE

Por defecto, no hay reglas en las interfaces DMZ.

1. Permitir que los servidores utilicen Windows Update o naveguen por la WAN:
   - Permitir TCP 80 desde la subred DMZ (HTTP) a cualquier lugar.
   - Permitir TCP 443 desde la subred DMZ (HTTP) a cualquier lugar.
2. Permitir a los usuarios conectarse a un servidor DNS externo:
   - Permitir TCP/UDP 53 desde la subred DMZ (DNS) a la dirección IP del servidor o servidores DNS ascendentes.
3. Permitir que los servidores utilicen un servidor horario remoto:
   - Si se utiliza un servidor horario remoto ascendente:
     - Permitir UDP 123 desde la subred DMZ (NTP) a la dirección IP del servidor de hora remoto.
   - En caso contrario:
     - Permitir UDP 123 desde la subred DMZ (NTP) a cualquiera.

CONFIGURACIÓN QUE AÍSLA LA LAN Y LA DMZ, CADA UNA CON ACCESO ILIMITADO A INTERNET

La siguiente configuración puede utilizarse en su lugar si el acceso saliente es más indulgente, pero sigue estando controlado entre las interfaces locales. Esto supone que todas las redes locales están numeradas de forma privada y que ya se han configurado las interfaces.

Cree un alias, Firewall > Aliases en el menú principal, llamado RFC1918 que contenga 192.168.0.0/16, 172.16.0.0/12, y 10.0.0.0/8.

CONFIGURACIÓN LAN

1. Para DNS desde el cortafuegos:
   - Permitir TCP/UDP desde la subred LAN al puerto 53 de la dirección LAN.
2. Para acceder a la GUI:
   - Permita TCP desde la subred LAN al puerto 443 de la dirección LAN.
3. Para hacer ping al cortafuegos desde la LAN:
   - Permitir ICMP desde la subred LAN a la dirección LAN.
4. Si se requiere tráfico desde la LAN a la DMZ:
   - Permita cualquier tráfico requerido desde LAN a DMZ.
5. No permita que la LAN alcance la DMZ u otras redes privadas:
   - Rechazar cualquiera desde la subred LAN a RFC1918.
6. Para acceso a Internet:
   - Permitir Cualquiera desde la subred LAN a cualquiera.

CONFIGURACIÓN DMZ

1. Para DNS desde el cortafuegos:
   - Permitir TCP/UDP desde la subred DMZ al puerto 53 de la dirección DMZ.
2. Para acceder a la GUI (opcional):
   - Permitir TCP desde la subred DMZ al puerto 443 de la dirección DMZ.
3. Para hacer ping al cortafuegos desde la DMZ:
   - Permitir ICMP desde la subred DMZ a la dirección DMZ.
4. Si se requiere tráfico desde la DMZ a la LAN:
   - Permita cualquier tráfico requerido desde DMZ a LAN.
5. No permita que la DMZ alcance la LAN u otras redes privadas:
   - Rechazar cualquiera desde la subred DMZ a RFC1918.
6. Para acceso a Internet:

- Permitir Cualquiera desde la subred DMZ a cualquiera.

INTERFACES ADICIONALES

Repita el patrón anterior según sea necesario.