Basic Firewall Configuration Example

Basic Firewall Configuration Example

This article is designed to describe how pfSense® software performs rule matching and a basic strict set of rules. The approach described in this document is not the most secure, but will help show how rules are setup.

Rules on the **Interface** tabs are matched on the **incoming** interface.

See also

Read the Aliases article as it will make management of rules easier.

Basic lock down of the LAN and DMZ outgoing rules

Outbound LAN

Make sure the **Default LAN > any** rule is either disabled or removed.

1. Allowing DNS access:
   - If pfSense is the DNS server:
     - Allow **TCP/UDP 53** (DNS) from LAN subnet to **LAN Address**.
   - If using Upstream DNS Servers:

        - Allow **TCP/UDP 53** (DNS) from LAN subnet to **Upstream DNS Servers**.
    - Otherwise:
        - Allow **TCP/UDP 53** (DNS) from LAN subnet to **anywhere**.
2. Allowing all users to browse web pages anywhere:
    - Allow **TCP 80** (HTTP) from LAN subnet to **anywhere**.
3. Allowing users to browse secure web pages anywhere:
    - Allow **TCP 443** (HTTPS) from LAN subnet to **anywhere**.
4. Allowing users to access FTP sites anywhere:
    - Allow **TCP 21** (FTP) from LAN subnet to **anywhere**.
5. Allowing users to access SMTP on a mail server somewhere:
    - Allow **TCP 25** (SMTP) from LAN subnet to **anywhere**.
6. Allowing users to access POP3 on a mail server somewhere:
    - Allow **TCP 110** (POP3) from LAN subnet to **anywhere**.
7. Allowing users to access IMAP on a mail server somewhere:
    - Allow **TCP 143** (IMAP) from LAN subnet to **anywhere**.
8. Allowing remote connections to an outside windows server for remote administration:
    - Allow **TCP/UDP 3389** (Terminal server) from LAN subnet to **IP address of remote server**.
9. Allowing LAN to access windows shares on the DMZ, via NETBIOS/Microsoft-DS:
    - Allow **TCP/UDP 137** from LAN subnet (NETBIOS) to **DMZ subnet**.
    - Allow **TCP/UDP 138** from LAN subnet (NETBIOS) to **DMZ subnet**.
    - Allow **TCP/UDP 139** from LAN subnet (NETBIOS) to **DMZ subnet**.
    - Allow **TCP 445** from LAN subnet (NETBIOS) to **DMZ subnet**.

Outbound DMZ

By default, there are no rules on **OPT** interfaces.

1. Allowing servers to use Windows update or browse the **WAN**:
    - Allow **TCP 80** from DMZ subnet (HTTP) to **anywhere**.
    - Allow **TCP 443** from DMZ subnet (HTTP) to **anywhere**.
2. Allow users to connect to an external DNS server:
    - Allow **TCP/UDP 53** from DMZ subnet (DNS) to **IP address of the upstream DNS server(s)**
3. Allowing servers to use a remote time server:
    - If using an upstream remote time server:
        - Allow **UDP 123** from DMZ subnet (NTP) to **IP address of remote time server**.
    - Otherwise:
        - Allow **UDP 123** from DMZ subnet (NTP) to **any**.

Setup isolating LAN and DMZ, each with unrestricted Internet access

The following setup can be used instead if outbound access is more lenient, but still controlled between local interfaces. This assumes all local networks are privately numbered, and that interfaces have already been configured.

Create an alias, **Firewall > Aliases** from the main menu, called `RFC1918` containing `192.168.0.0/16`, `172.16.0.0/12`, and `10.0.0.0/8`.

LAN Configuration

1. For DNS from the firewall:
   - Allow **TCP/UDP** from LAN subnet to **LAN Address port 53**.
2. For accessing the GUI:
   - Allow **TCP** from LAN subnet to **LAN address port 443**.
3. To ping the firewall from the LAN:
   - Allow **ICMP** from LAN subnet to **LAN address**.
4. If there is any traffic required from LAN to DMZ:
   - Allow any traffic required from **LAN** to **DMZ**.
5. Do not allow LAN to reach DMZ or other private networks:
   - Reject **Any** from LAN subnet to **RFC1918**.
6. For internet access:
   - Allow **Any** from LAN subnet to **any**.

DMZ Configuration

1. For DNS from the firewall:
   - Allow **TCP/UDP** from DMZ subnet to **DMZ Address port 53**.
2. For accessing the GUI (optional):
   - Allow **TCP** from DMZ subnet to **DMZ address port 443**.
3. To ping the firewall from the DMZ:
   - Allow **ICMP** from DMZ subnet to **DMZ address**.
4. If there is any traffic required from DMZ to LAN:
   - Allow any traffic required from **DMZ** to **LAN**.
5. Do not allow DMZ to reach LAN or other private networks:
   - Reject **Any** from DMZ subnet to **RFC1918**.

6. For Internet access:
    - Allow **Any** from DMZ subnet to **any**.

Additional Interfaces

Repeat the above pattern as needed.

Revision #1
Created 29 December 2023 04:31:06 by ColtM
Updated 29 December 2023 04:31:37 by ColtM