Example basic configuration

From PFSenseDocs

This article is part of the **How-To** series.

Contents

- 1 Summary
- 2 Caveats
- 3 Example of a basic lock down of the LAN and DMZ out going rules
  - 3.1 Outbound LAN
  - 3.2 Outbound DMZ
- 4 Example setup isolating LAN and DMZ but each with unrestricted Internet access
  - 4.1 Prerequisites/Assumptions
  - 4.2 LAN Configuration
  - 4.3 DMZ Configuration
  - 4.4 Additional Interfaces

Summary

This article is designed to describe how pfSense performs rule matching and a basic strict set of rules.

Caveats

- **Always** remember that rules on Interface tabs are matched on the **INCOMING Interface**.
- The approach described in this document is not the most secure, but will help understand how rules are setup.
- Read the Aliases article as it will make management of rules easier.

Example of a basic lock down of the LAN and DMZ out going rules

Outbound LAN

- Make sure the “Default LAN > any” rule is either disabled or removed.
- Allow DNS access - if pfSense is the DNS server, use LAN address, if using outside DNS create rule to allow TCP/UDP 53 to anywhere
  - Allow TCP/UDP 53 (DNS) from LAN subnet to LAN Address, -or-
  - Allow TCP/UDP 53 (DNS) from LAN subnet to Upstream DNS Servers, -or-
  - Allow TCP/UDP 53 (DNS) from LAN subnet to anywhere
- Allow all users to browse web pages anywhere.
  - Allow TCP 80 (HTTP) from LAN subnet to anywhere
- Allow users to browse secure web pages anywhere.
  - Allow TCP 443 (HTTPS) from LAN subnet to anywhere
- Allow users to access FTP sites anywhere.
  - Allow TCP 21 (FTP) from LAN subnet to anywhere
- Allow users to access SMTP on a mail server somewhere.
  - Allow TCP 25 (SMTP) from LAN subnet to anywhere
- Allow users to access POP3 on a mail server somewhere.
  - Allow TCP 110 (POP3) from LAN subnet to anywhere
- Allow users to access IMAP on a mail server somewhere.

    - Allow TCP 143 (IMAP) from LAN subnet to anywhere
- To allow remote connections to an outside windows server, configure a rule for Remote administration.
    - Allow TCP/UDP 3389 (Terminal server) from LAN subnet to **IP address of remote server**
- To allow LAN to access windows shares on the DMZ, allow NETBIOS/Microsoft-DS from the LAN to the DMZ
    - 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.
- To allow 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
- If an external DNS server is used, allow the computers to leave the network to connect to a DNS server.
    - Allow TCP/UDP 53 from DMZ subnet (DNS) to **IP address of the upstream DNS server (s)**
- To allow servers to use a remote time server open UDP port 123
    - Allow UDP 123 from DMZ subnet (NTP) to **IP address of remote time server** -or-
    - Allow UDP 123 from DMZ subnet (NTP) to any

Example setup isolating LAN and DMZ but each with unrestricted Internet access

The strict approach above may not be necessary if outbound access should be more lenient, but still controlled between local interfaces. The following setup can be used instead.

Prerequisites/Assumptions

This assumes all local networks are privately numbered, and that interfaces have already been configured.

Create an alias (**Firewall > Aliases**) called *RFC1918* containing *192.168.0.0/16*, *172.16.0.0/12*, and *10.0.0.0/8*

LAN Configuration

- Allow TCP/UDP from LAN subnet to LAN Address port 53 for DNS from the firewall
- Allow TCP from LAN subnet to LAN address port 443 for accessing the GUI
- Allow ICMP from LAN subnet to LAN address to ping the firewall from the LAN
- Allow any traffic required from LAN to DMZ (if any)
- Reject Any from LAN subnet to RFC1918 -- Do not allow LAN to reach DMZ or other private networks
- Allow Any from LAN subnet to any -- Internet access rule

DMZ Configuration

- Allow TCP/UDP from DMZ subnet to DMZ Address port 53 for DNS from the firewall
- Allow TCP from DMZ subnet to DMZ address port 443 for accessing the GUI (optional)
- Allow ICMP from DMZ subnet to DMZ address to ping the firewall from the DMZ
- Allow any traffic required from DMZ to LAN (if any)
- Reject Any from DMZ subnet to RFC1918 -- Do not allow DMZ to reach LAN or other private

networks
- Allow Any from DMZ subnet to any -- Internet access rule

Additional Interfaces

Repeat the above pattern as needed.

Retrieved from "https://doc.pfsense.org/index.php?title=Example_basic_configuration&oldid=6184"

Category: Howto

- This page was last modified on 19 November 2014, at 12:48.