Firewall

FreePBX Firewall is a tightly integrated, low level firewall, that removes the complexity of configuring a firewall on your VoIP server.

This project was started due to the lack of a common, comprehensive, firewall, in the VoIP server community. Various attempts had been made previously, but they all suffered from a lack of understanding of the challenges involved, or a lack of flexibility which caused most users to disable IPtables on the PBX.

FreePBX Firewall was designed and written by security professionals, with a thorough understanding of the issues and limitations of trying to secure a VoIP service but still leave it open enough to keep users from disabling the Firewall.

Its aim is to provide a simple way to secure the 'average' VoIP server installation, the 95%. In more complex setups, it is always wise to discuss your security requirements with someone with experience in this arena.

Firewall is under *active development*, and community engagement is **strongly encouraged**! Please read and comment on the forum thread, with feature requests, or questions!

Requirements

FreePBX

Firewall is only compatible with FreePBX 13 and higher.

Operating System Requirements

Firewall requires a Linux machine, and requires iptables 1.4.7 or higher, and the ipt_recent, or xt_recent kernel modules (if you wish to enable the Responsive Firewall component).

Package Requirements

'sysadmin-rpm'

This is a RPM package that allows secure privilege escalation in limited circumstances. Firewall requires this to alter the system iptables rules. This RPM is installed on most modern RPM-based distros. Currently there is no method for privilege escalation without this package. Support for non-rpm-based operating systems is on hold until this issue is resolved.

Licence

The Firewall module is a 100% Free Open Source Module, licenced under the AGPL v3. The code is hosted on git.freepbx.org with a mirror on GitHub for your convenience. Pull requests are welcome!

Getting Started

When you enable the module, **no firewall rules** are enabled. Please read the Getting Started Guide for more information on how to do a simple setup.

FAQs

- Do I need to configure each Trunk or Peer in the firewall?
  No! The firewall **automatically** interrogates the FreePBX installation, discovers all known peers or trunks, and accepts traffic from that peer on their defined protocol. This means that if you have a trunk to an IAX peer, and that peer is compromised, that peer **can not** send chan_sip or pjsip signalling through. It can only send IAX traffic to the server, because it is only registered for IAX.
- Does Firewall support IPv6?
  Yes. Firewall has full support for IPv6.
- What is the Responsive Firewall?
  It lets you expose your SIP/IAX ports to the internet, with an intelligent monitoring of connections that will automatically block hack attempts, but will also allow valid clients through. For more information, see the Responsive Firewall Page.
- How do I add a Trusted Network or Host?
  Through the 'Networks' tab on the 'Main' page. More information is in Firewall Permissions
- Can I allow a client with DDNS through?
  Yes. Simply add their DDNS hostname to the 'Networks' tab on the 'Main' page, and assign them to a zone.
- How do I assign individual privileges to clients?
  Upcoming feature: You will be able to provide access to different services via Userman. This is unimplemented at the moment.

- How do I reject traffic?
  All traffic that isn't explicitly allowed is **already** rejected. This firewall implements a 'deny by default' rule. More information is on the Firewall Zones page. In addition there is a blacklist which can be populated with hosts, see the 'Blacklist' tab on the 'Services' page.
- How do I define RTP ports?
  All interfaces explicitly allow RTP traffic, as it is configured in Asterisk SIP Settings. There is no need to configure this through the Firewall module. Note that if you set your RTP ports to be an extremely unusual range (such as less than 1024), the Firewall module will refuse to honour that setting, as it could potentially expose other attack surfaces.
  It is **not recommended** to change your RTP range.
- Can I get locked out of my machine?
  Not while Safe Mode is available. When this is available, if you reboot your server twice within 5 minutes, the firewall rules will be delayed for the first five minutes the machine is up. This will give you enough time to get into the machine, and add any missing rule that locked you out. There will also be a large warning at the top of the Firewall screen warning you of this. The firewall rules will be applied automatically after 5 minutes, or, if you disable Safe Mode in the Firewall.
- I can't disable the firewall, I can see 'Firewall can not be disabled' instead of 'Disable'
  This is because your system administrator has **explicitly decided** that the firewall should not be disabled, and has created a lock file.
  For information how to remove this lock file, see the 'Firewall can not be disabled' page.

Overview

Zones

All network connections coming in to your VoIP server are deemed to be part of a zone. Every network interface has a default Zone, and data arriving at that interface is treated as belonging to that Zone, **unless** it is a known network, which overrides the default Zone. Services are individually granted to each Zone. The default zones are:

- Reject
  Any incoming network packets are rejected. Note that this zone still accepts RTP traffic, but no other ports are listening by default. **You rarely want to use this**. All connections, by default, are rejected. This is here only as a fallback. Traffic in this zone may be processed by the Responsive Firewall, if enabled.
- Internet (formerly called External)
  Traffic classified as 'Internet' means you do not automatically trust the other computers on networks to not harm your computer. This, by default, only allows https connections to the management interface, and access to the UCP port, if defined. Traffic in this zone may be processed by the Responsive Firewall, if enabled.
- Other
  Provided for advanced users, intended for use on trusted external networks, or other well known networks (such as a DMZ, or OpenVPN network). This, by default, allows access to UCP, and provides unfiltered SIP and IAX access.
- Local (formerly called Internal)
  For use on internal networks that do not have traffic from non-trusted hosts. You mostly trust the other computers on the networks to not harm your computer. This, by default, allows access to most services.
- Trusted
  All network connections are accepted. **No firewalling is done on this interface, all incoming traffic from a trusted zone is permitted.** This is the default setting for newly discovered interfaces. Any **network interface** that is associated with this zone is treated as a configuration error, and alerts will be raised. All interfaces must be assigned to a non-default zone. As discussed in the Firewall Getting Started guide, you assign networks or hosts to the Trusted zone, you should never assign an interface to that zone.

Network Overrides

You can define an endpoint in 'Networks' (which aren't *just* networks), which allows you to override traffic arriving at your machine. This can be a single host (203.0.113.10), a network definition (203.0.113.0/24), a hostname (client.example.com), or a DDNS client (name.ddns.org). Each entry is then assigned to a zone, and traffic arriving from that endpoint is treated as being from that Zone.

- Firewall Blacklist
- Firewall can not be disabled error
- Firewall Command Line
- Firewall Custom Rules
- Firewall Getting Started Guide
- Firewall Permissions
- Firewall Technical Details
- Firewall Zones
- Responsive Firewall
- Safe Mode