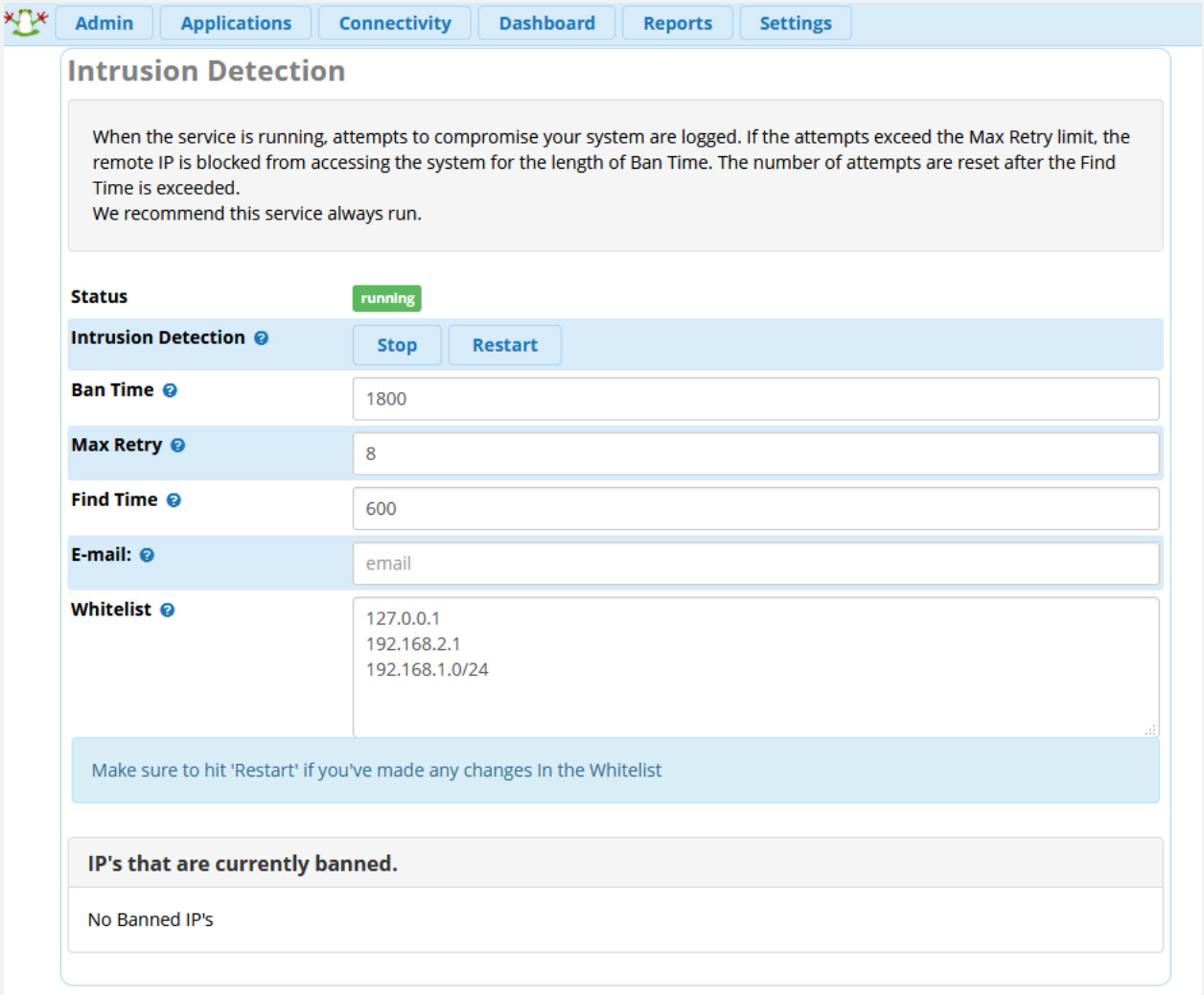
Intrusion Detection در FreePBX

یکی از مواردی که پس از نصب فری‌پی‌بی‌ایکس (FreePBX) برای کاربران بوجود می‌آید این است که ارتباط تجهیزاتی مانند گیت‌وی با استریسک، پس از دقایقی قطع می‌شود. در ادامه ابتدا به بررسی علت این مسئله و راهکار آن می‌پردازیم.

نحوه کار قابلیت Intrusion Detection

این قابلیت که بخشی از ماژول System Admin، محسوب می‌شود به سیستم شما قابلیت پیشگیری در برابر آسیب پذیری‌های امنیتی را می‌دهد. زمانی که سرویس Intrusion Detection فعال باشد، تمامی تلاش‌ها برای برقراری ارتباط با سیستم FreePBX ذخیره می‌شوند، اگر تعداد این تلاش‌ها به حداکثر محدودیت تعیین شده (Max Retry) برسد، دسترسی آن آدرس IP برای بازه‌ی زمانی تعیین شده‌ای که Ban Time نام دارد به حالت Blocked در می‌آید و پس از سپری‌شدن این زمان، دسترسی برای آن آی‌پی ریست شده و مجدد همین چرخه ادامه پیدا می‌کند.



فیلدهایی که در این بخش وجود دارند عبارتند از:

Status: وضعیت فعال/غیر فعال‌بودن سرویس را نمایش می‌دهد.

Intrusion Detection: در اینجا می‌توان سرویس را Stop و یا Restart کرد.

Ban Time: طول مدت زمانی (ثانیه) که یک آی‌پی بلاک می‌ماند، قبل از اینکه ریست شود.

Max Retry: تعداد دفعاتی که یک آی‌پی می‌تواند برای برقراری ارتباط تلاش کند. (در بازه‌ی زمانی Find Time)

Find Time: طول بازه‌ی زمانی (ثانیه) که پس از سپری شدن آن، لاگ ها برای آن IP ریست می‌شوند.

** در تصویر بالا تعیین شده است که اگر یک آی پی در بازه‌ی زمانی ۶۰۰ ثانیه، بیش تر از ۸ بار تلاش برای برقراری ارتباط با سیستم داشته باشد، برای مدت زمان ۱۸۰۰ ثانیه در حالت Banned قرار می‌گیرد.*

E-mail: در این قسمت می‌توان آدرس پست الکترونیکی مدیر سیستم را وارد کرد تا Notificationهای این سرویس برای او ایمیل شود.

Whitelist: آدرس تک آی‌پی/رنج آی‌پی‌هایی که در این بخش وارد شوند در لیست سفید قرار گرفته و محدودیت‌های این سرویس برایشان غیر فعال می‌گردد.

** نکته: پس از انجام هر گونه تغییرات در بخش Whitelist حتما یک بار سرویس را Restart کنید.*

برای این کار می‌توان بالای همین صفحه روی Restart کلیک کرد یا در محیط CLI برنامه دستور زیر را وارد نمود:

Service fail2ban restart

یا

Systemctl restart fail2ban

IP's that are currently banned: در این بخش لیست آی‌پی‌هایی که در حال حاضر Banned شده‌اند نمایش داده خواهد شد.

برای برخی کاربران که از ورژن‌های قدیمی‌تر FreePBX استفاده می‌کنند یا ماژول‌های خود را آپدیت نکرده اند، ممکن است پیش بیاید که با اینکه آی‌پی یا رنج آی‌پی موردنظر خود را در بخش Whitelist وارد کرده‌اند اما مجدداً برقراری ارتباط با برنامه قطع می‌شود. برای بررسی این مورد ابتدا فایل زیر را باز نمایید:

Vim/etc/fail2ban/jail.local

و سپس با بررسی قسمت ignoreip، اگر آی‌پی یا رنج آی‌پی‌های بخش Whitelist در اینجا وجود نداشت آن‌ها را به ترتیب وارد کرده و ذخیره کنید؛ سپس سرویس fail2ban را با دستوری که پیش‌تر گفته شد، ری‌استارت نمایید.

```
# Configuration automatically generated via the Sysadmin Module
# This file will be overwritten by Sysadmin on startup. If you modify
# this file, your changes will be lost. DO NOT MODIFY THIS FILE!
# generated: Thu, 12 Apr 2018 11:47:29 +0000

[DEFAULT]
ignoreip = 127.0.0.1 192.168.2.1 192.168.1.0/24
bantime = 1800
findtime = 600
maxretry = 8
backend = auto

[asterisk-iptables]
enabled = true
filter = asterisk
action = iptables-allports[name=SIP, protocol=all]
logpath = /var/log/asterisk/fail2ban

[pbx-gui]
enabled = true
filter = freepbx
action = iptables-allports[name=SIP, protocol=all]
logpath = /var/log/asterisk/freepbx_security.log
```

همانطور که در تصویر بالا مشاهده می‌شود لیست آی‌پی‌های قسمت Whitelist در این قسمت قرار گرفته و آی‌پی‌ها با استفاده از فاصله (Space) از یکدیگر جدا شده‌اند.