Voip-iran.com

امنیت در الاستیکس

نوشته : امین نجفی

به نام خالق

سود هنگامی است که شما یک گوشی تلفن دارید.

تجمل زمانی است که شما دو تلفن دارید.

توانگری و قدرت آن هنگام است که شما سه تلفن دارید.

و بهشت جایی است که هیچ تلفنی وجود ندارد.

داگ لارسون

مقدمه 3

فصل اول .....

امن کردن ساده Elastix 7

تعویض elastix admin account password پیش فرض 8

تعویض freePBX account password پیش فرض 9

امنیت قوی در extension ها 12

امن کردن sip account ها 13

Permit/Deny options 14

ابزار پیش بینی 15

Elastix default accounts 16

فصل دوم 17

Advanced Security Measures 17

Perimeter Firewall / Router 18

Elastix Firewall 20

Fail2ban 21

تغییر پورت پیش فرض SSH 22

VPN 22

Monitoring 22

راهنمای استفاده از sip و تعامل با firewall/router 24

فصل سوم .....

اشنایی با نصب و راه اندازی Elastix Firewall 25

Elastix Firewall 26

یافتن ELastix Firewall 26

نگاهی به elastix firewall 27

تنظیمات پورت 27

تعریف Rule 31

چگونه با Firewall Rule رفتار کنیم: 34

محدود سازی Firewall..... 36

نکاتی درباره ی ip table:..... 38

سوال و جواب 38

فصل چهارم .....

دیگر feature های ایمن سازی elastix 39

نصب Fail2Ban 40

نصب apf..... 42

نصب bfd 46

نصب و راهنمای Csf 47

حرف اخر 59

مقدمه

سال ها پیش اگر مقدمه ای برای این موضوع می نوشتم به احتمال قوی پر یاس و ناامیدی بود؛یا این طور می نوشتم:

"در طول سال‌های گذشته مطالب زیادی راجع به نقاط ضعف امنیت VoIP گفته شده است و به ما اخطارهای زیادی درباره شنود مکالمات، اسپم‌های صوتی، سیادی، نرم‌افزارهای جاسوسی و حملات (Denial of Service DoS)داده شده است. متأسفانه اکثر این مشکلات تحت تأثیر دیواره آتش وcarrier ها است که حاضر به طراحی امنیت برای VoIP نیستند و این مسائل را تصوری غیرواقعی می‌پندارند".

ولی در حال حاضر، مشاوران امنیتی و تولیدکنندگان دیواره آتش و کنترل‌کننده‌های مرزهای تماس(SBC) ، کارشان را برای فناوری جدیدتر برای دیوارهای آتش ادامه می‌دهند. به طوری که در واقع نسل موجود دیواره‌های آتش برای حفاظت از شبکه‌های مجزای VoIP مناسبند. زمانی‌که ما به شبکه VoIP متصل می‌شویم، تعدادی استاندارد، ارتباط ما را در مقابل محدودیت‌هایی که باعث جاسوسی ما می‌شوند، محافظت می‌کنند.

حال بدون این‌که از SBC یا دیوار آتش استفاده شود. در حقیقت این دستگاه‌ها عملاً امنیت کلی را با مخلوط شدن با مکانیزم‌های جدید امنیتی، افزایش می‌دهند .

هزینه‌ها

متهم کردن و اطلاعات غلط درباره امنیت VoIP محدود به ناشران نمی‌شود.

CSIA (Cyber Security Industry Alliance)یکی از متخلفان برجسته در ارائه اطلاعات غلط است. در حالی که اطلاعاتشان در این زمینه بسیار کم است، گزارش‌های آن‌ها بسیار عصبانی کننده و فریبنده است. به طوری که آن‌ها ادعا می‌کنند VoIP مانند تخم‌مرغ شکننده است CSIA و بقیه مکرراً باعث افزایش توهم نسبت به شنود در VoIPشده‌اند. با این حال، این امر عملاً مشکلی نیست که خیلی‌ها انتظار دارند. شنود در شبکه تلفن سنتی نیز آسان است، مهاجمان تنها به دسترسی به یک خط فیزیکی و تجهیزات ارزانقیمت نیاز دارند. در مقام

مقایسه، شنود در VoIP در یک شبکه مبتنی بر IP به دسترسی در سطح مدیر به سوییچ و ایجاد پل به سوییچ یا پورت مانیتورینگ به منظور جمع‌آوری پکت‌ها از پورت یک سوییچ دیگر نیاز دارد.

استفاده از یک شبکه بی‌سیم با VPN یا لایه دوم رمزنگاری شده مثل (Wi-Fi Protected Access) WAP امنیت خوبی را به وجود می‌آورد. خیلی از مقاله‌ها درباره امنیت VoIP اشاره به حملات DoS می‌کنند. در حقیقت حمله‌های DoS روی سوییچ‌های PSTN در اواخر دهه ۱۹۸۰ و اوایل دهه ۱۹۹۰ بسیار معمول بود. کلید کاهش تأثیر حمله‌هایDoS ، داشتن پهنای باند کافی است؛ چرا که در این صورت برنامه واقعی‌ای که باید اجرا شود، می‌تواند کارش را تا زمانی‌که حمله‌کننده مسدود شود، ادامه دهد. اینترنت از نظر بزرگی بسیار بزرگ‌تر از PSTNاست که آن را توانمندتر می‌کند. به عنوان مثال، در یازدهم سپتامبر شبکه تلفن در East coast به شدت دچار مشکل شد، ولی ایمیل، IMو تلفن‌های IP کارشان را ادامه دادند .

سرویس‌دهندگان اینترنت حملات DoS را با پهنای باند زیاد خود دفع می‌کنند. همچنین سعی می‌کنند حملات DoSرا هر چه نزدیک‌تر به هسته اینترنت مسدود کنند. اینگونه حملات که به طور نادر اتفاق می‌افتد، مشکل‌تر از حمله به شبکه‌های PSTN است .

همیشه نگرانی درباره استفاده از نرم‌افزارهای جاسوسی مخصوص VoIP که تماس‌ها را کنترل می‌کنند وجود دارد و آن‌ها وقتی واردsoftphone ها می‌شوند، در حقیقت فقط درsoftphone ها باقی نمی‌مانند و باعث به وجود آمدن دو تهدید می‌شوند؛ یکی این‌که VoIP باعث اضافه شدن یک مسیر برای وارد شدن نرم‌افزارهای مخرب می‌شود و دیگر این‌که یک ویروس می‌تواند باعث ایجاد خسارت به یک کامپیوترِ به خطر افتاده شود که قبلاً این کار امکان‌پذیر نبود .

به هر حال برخلاف HTML و javascript که توسط مرورگرهای وب و برنامه‌های ایمیل استفاده می‌شود، پروتکل‌های SIPفقط اطلاعاتی را به کاربر می‌دهند که از نوع اطلاعاتی باشد که ارسال شده باشد .

در حال حاضرsoftphone هایی که از SIP استفاده می‌کنند به کاربر اجازه نمی‌دهند یک درخواست SIP به کامپیوتر مقصد ارسال کنند تا یک برنامه را که کاربر مهیا کرده است روی آن اجرا کند. همه ویروس‌ها برای تکثیر شدن به چنین روش‌هایی نیاز دارند. تا این زمانsoftphone هایی که از SIP استفاده می‌کنند، از اسکریپت‌های زبان‌ها دوری کرده‌اند؛ چرا که آن‌ها باعث گسترش ویروس می‌شوند. وقتی که یک کامپیوتر آلوده می‌شود، یک هکر می‌تواند هر برنامه دلخواهی را روی آن کامپیوتر اجرا کند. برای یک هکر یک کامپیوتر آلوده برای به دست آوردن اطلاعات شخصی (معمولاً اطلاعات آدرس‌های ایمیل و اطلاعات ارسالی)، ارسال هرزنامه یا اجرای حملات DoS بسیار مفید است .

در حال حاضر هرزنامه، تلفن‌ها و فکس‌های ناخواسته، به عنوان یک مشکل در شبکه‌های PSTN هستند. تقریباً همه شبکه‌های VoIP ارتباطاتی را که گیرنده نامشخص باشد و از شبکه PSTN استفاده می‌کند، مسدود می‌کنند؛ چرا که در این صورت آن‌ها مثل خطوط معمولی PSTN آسیب‌پذیر می‌شوند .

اسپم و سیادی روی دو مشخصه تکیه دارند؛ اول این‌که، اکثر کاربران نمی‌توانند پیش‌بینی کنند که با چه کسی تماس برقرار خواهند کرد. بنابراین آن‌ها به هر کسی اجازه ارتباط می‌دهند. دومین مشخصه استفاده از فیلتر است که در صورتی‌که از یک برنامه قوی قابل اطمینان استفاده شود که بتواند تعیین کند چه چیزی فیلتر شود، مؤثر خواهد بود .

گروه کاری IETF که روی SIP کار می‌کنند، یک سری مسائل اصلی امنیت را به طور جامع توسعه داده‌اند تا از SIPدر مقابل شنود، سرقت جلسه، حمله‌های فعال و همچنین درستی هویت کاربر، محافظت کنند. این کار با استفاده از

Secure Real-Time Transport Protocol) SRTP)برای حفاظت مدیا و HTTPS برای امنیت تنظیمات انجام می‌شود و این‌ها یک سطح امنیت مناسب را مهیا می‌کنند و می‌توانند قسمت به قسمت توسعه داده شوند و اغلب برای قابلیت کار با کامپیوترها با یکدیگر در دوره توسعه، توسط SIPIT مورد آزمایش قرار می‌گیرند .

SIPمثلHTTP ، هم می‌تواند توسط Transport Layer Security) TLS) حمل شود .SIP توسطTLS ،

رمزنگاری و درستی پیام‌ها را برای کانال ارتباطی مهیا می‌کند و سرور بعدی را نیز شناسایی می‌نماید. برخلاف HTTPدرخواست SIP قبل از این‌که به مقصد نهایی برسد، می‌تواند از چند hop عبور کند. ویژگی SIP یک رویه خاص را تعریف می‌کند که مشابه HTTPS است. برنامه SIP طوری طراحی شده است تا اطمینان دهد که هر hopاز TLS استفاده می‌کند و هر سرور، سرور بعدی را شناسایی می‌کند .

چندین راه‌حل برای اجرای SIP روی TSL وجود دارد.که تا همینجا هم مقدمه زیاد شده و خسته کننده.

به هیچ عنوان اینجانب مسولیتی در قبال درست انجام شدن و یا نشدن دستورات ندارم. و مسولیت ان با خود شماست.

فصل اول

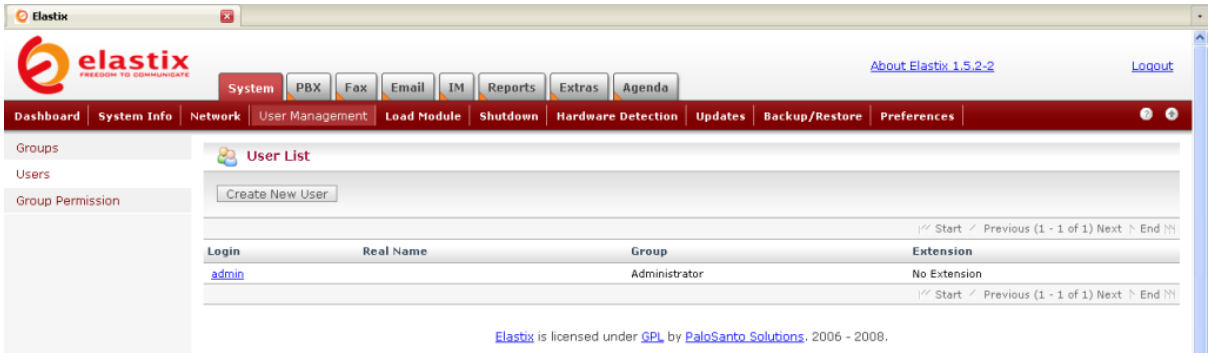
امن کردن ساده Elastix

در این فصل خواهیم خواند:

- تعویض elastix admin account password پیش فرض
- تعویض freePBX account password پیش فرض
- امنیت قوی در extension ها
- امن کردن sip account ها
- ابزار پیش بینی
- Elastix default accounts

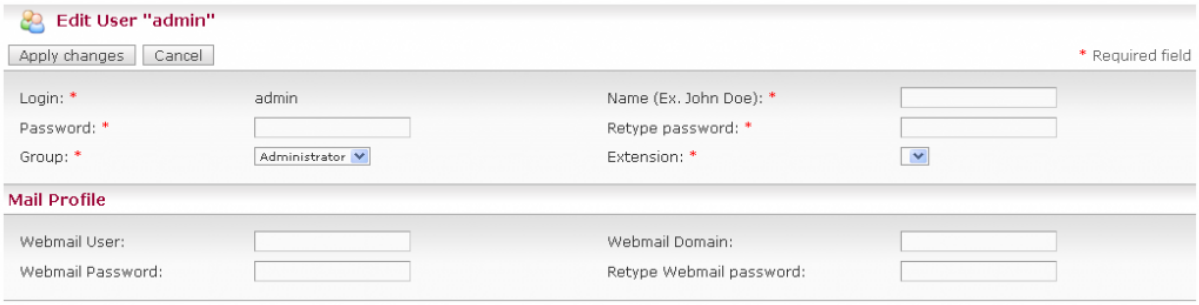
تعویض elastix admin account password پیش فرض

در مرحله اول نیاز به تغییر رمز حساب کاربری پیش فرض داریم. به appliance الاستیکس توسط browser وصل شوید.به مسیر *System->User Management* و سپس *Users* از پنل سمت چپ انتخاب کنید.



کاربر admin را انتخاب کرده.

بروی Edit کلیک کنید.



در قسمت password یک رمز قوی درج کنید و همان را در retype تکرار کنید.

منظور از رمز قوی:

- ترکیب کلمات بزرگ و کوچک.
- اعداد.
- سمبل ها (!"£$%^&*()_=+_-<>;:'@#~/?).
- دو یا سه space در وسط رمز

در فیلد name نام مدیر شبکه را وارد کنید.

و در اخر Apply changes را برای اعمال تغییرات بزنید. بعد از این کار نیاز به login کردن دوباره دارید.

به هیچ عنوان کلمه رمز را فراموش نکنید.

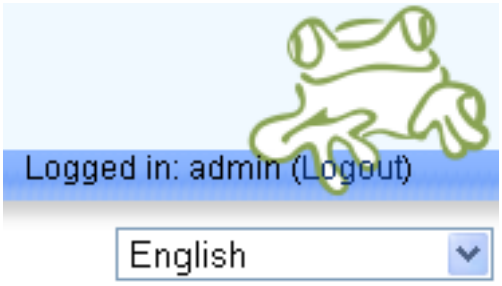
تعویض freePBX account password پیش فرض

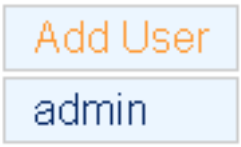
freePBX و elastix بسیار به هم وابسته اند،به طوری که elastix را اینترفیسی برای freePBX می دانند.

freePBX ، username و password پیش فرض admin/admin را داراست.برای تغییر این پیش فرض ها به محیط freePBX وارد شده.

سپس تب admin را انتخاب کرده.و از بالا سمت چپ تب setup را.و در انتها Administrators را انتخاب کنید.

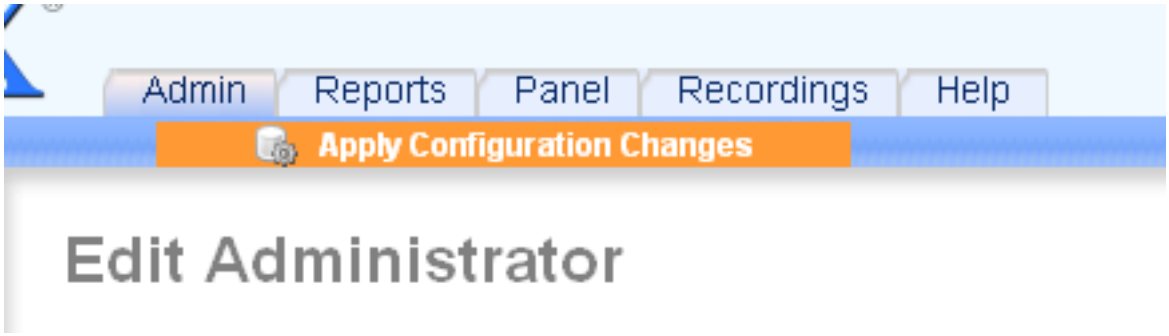
از لیست سمت راست admin user را انتخاب کرده:



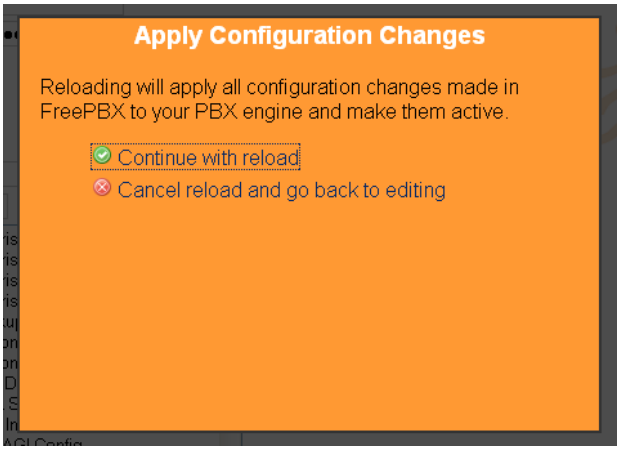


مشخصات این حساب کاربری نمایش داده خواهد شد:

مانند بخش قبل رمز عبور قوی انتخاب کنید. و در انتها Submit Changes را فشار دهید. برای تایید این تغییرات Apply Configuration Changes که در بالا صفحه به نمایش در امده را فشار دهید.



بعد از این کار freePBX از شما یک confirm می خواهد:



Continue with reload to apply را بزنید. تغییرات اعمال می شود.

امنیت قوی در extension ها

Extension ها ریسک بزرگ اما الزامی سیستم شما هستند،نه به دلیل اینکه به سرور دسترسی دارند بلکه به این دلیل که ان ها اجازهی برقراری تماس و استفاده پهنا ی باند شما را دارند.داشتن رمز عبور قوی به معنی دعوت نامه " لطفا از سیستم من استفاده کنید" برای دیگران است.هر داخلی که یک بار register شده باشد میتوانند تماس برقرار کند،نوع تماس بسته به چگونه راه اندازی شبکه توسط شماست.

هر داخلی که به شبکه وصل شود نیاز به یک secret دارد که قبلا توسط شما تعریف شده.شما می توانید از FreePBX استفاده کنید تا توسط Weak Passwords ماژول رمز های ضعیف را شناسایی کند ، اما با این کار تنها اولویت های سطح پایین را انجام دادید،پس انچنان هم به ما کمک نمی کند و همچنین شما نیاز دارید وارد محیط freePBX شوید.تجربه نشان داده خیلی از Admin ها تمایل استفاده از freePBX را ندارند.پس بهترین راه حل پیشگیری.یعنی از همان ابتدا رمز قوی انتخاب کنید.

پیشنهاد میکنم حداقل از 8 کارکتر استفاده کنید.و از ترکیب حروف بزرگ،کوچک،اعداد و نشانه ها استفاده کنید.به هیچ عنوان از تبدیل کلمات عادی به قوی استفاده نکنید: مانند mypassword ----> MyP4$$w0rd که بر خلاف ظاهر به راحتی قابل تشخیص اند.

به محدودیت توجه کنید، اغلب phone ها توانایی درج حرف را ندارند و تنها میتوان از digit استفاده کرد. شاید به ذهن بعضی از شرکت ها رسیده که از تعداد بیشتر digit استفاده کنند.اما 10 الی 12 دیجیت کافیست.بسیاری از متخصصان پیشنهاد میکنند در یک بازه زمانی (سه ماه) رمز ها عوض شود.

از این لینک برای ایجاد رمز استفاده کنید

http://automation.binarysage.net/?page_id=554

امن کردن sip account ها

SIP Account مهم ترین نقطه نفوظ محسوب می شوند،مخصوصا زمانی که یک SIP Account داشته باشیم که همواره به بیرون از شبکه ارتباط دارد. بعلاوه ابزار های زیادی برای هک این سیگنالینگ تولید شده.

در زیر چند روش که در *Elastix forum* و *VOIP Tech* برای این امر ذکر شده را نقل قل می کنم:

- محدود کردن ip source Addresses

اگر میتوانید SIP connection در تمام ip address ها محدود کنید. در فایل sip_general_custom.conf از deny و permit استفاده کنید.

(Elastix->PBX->Tools->FileEditor).

تذکر:درصورتی که از roaming استفاده می کنید و هر area ادرس ip جدایی دارد به هیچ عنوان از این امر استفاده نکنید.

- جلوگیری از افشای اطلاعات sip extension

از نسخه 1.2 دراستریسکاین امکان به وجود امد تا بتوان از افشای این اطلاعات جلوگیری کرد.

برای جلوگیری این امر در elastix:

alwaysauthreject=yes به فایل sip_general_custom.conf اضافه کنید..(Elastix->PBX->Tools->FileEditor)

- از رمز عبور قوی استفاده کنید

- در local subnet ها پورت نرم افزار های AMI[1] manager را بلوکه کنید.

[1] Asterisk Management Interface

به صورت پیش فرض "deny=0.0.0.0/0.0.0.0" و"permit=127.0.0.1/255.255.255.0" در الاستیکس در فایل manager.conf فعال است. دقت کنید این دستور را در این فایل یا "manager_additional.conf" "manager_custom.conf" override نکنید.

- Anonymous inbound sip call

Elastix توانایی قبول کردن تماس anonymous inbound SIP را از ترانک دارد. تنظیمات 'Allow anonymous inbound SIP calls' در هر زمانی NO بگذارید. واگر برای تست inbound SIP call در ترانک استفاده می کنید فراموش نکنید که حتما به NO برگردانید.

تنظیمات ان را در پایین این ادرس میتوانید پیدا کنید(PBX->PBX Configuration->Allow anonymous inbound SIP calls).

Anonymous SIP یک چالش بزرگ نیست اما مثل یک قطعه شن در کفش شماست،چقدر ازار دهنده است!

تذکر: در صورتی که این امر yes باشد، به تمام تماس هایی که از sip امده اجازه عبور داده ایدا در بهترین حالت annoying است و در بدترین حالت DISA .

Permit/Deny options

همانطور که اشاره شد freepbx این امکان را به ما میدهد. به شکل زیر دقت کنید:

Device Options

This device uses sip technology.

secret	d882ueUee92e2
dtmfmode	rfc2833
canreinvite	no
context	from-internal
host	dynamic
type	friend
nat	yes
port	5060
qualify	yes
callgroup	
pickupgroup	
disallow	
allow	
dial	SIP/201
accountcode	
mailbox	201@device
deny	0.0.0.0/0.0.0.0
permit	172.22.22.0/255.255.255.0

در این شکل به کاربر اجازه داده شده به تمام ip در بازه 172.22.22.0/24 دسترسی داشته باشد(تماس برقرار کند) که ip شبکه شما درpermit قرار می گیرد. و در deny تمام شبکه را با quad zero بلاک کرده ایم.(0.0.0.0/0.0.0.0).

در AMI که در بالا گفتیم، چنین کاری انجام می شد با این تفاوت که در این قسمت برای extension هاست و در AMI ،ادرسی که اجازه ی دسترسی به AMI interface را دارد.

ابزار پیش بینی

در فصل بعدی کامل توضیح داده شده.

Elastix default accounts

- **Main username and password in linux:**

Username: root
Password: palosanto

- **Main username and password in web interface:**

Username: admin
Password: palosanto

- **Sugar CRM:**

Username: admin
Password: password

- ***A2bill:***

Username: admin
Password: mypassword

or

Username: root
Password: myroot

- ***Operator Flash Panel (from 0.6 version):***

Password: eLaStIx.2oo7

- ***Freepbx:***

Username: admin
Password: admin

- ***vtigerCRM:***

Username: admin
Password: admin

- ***MySQl :***

Username: root
Password: eLaStIx.2oo7

فصل دوم

Advanced Security Measures

در این فصل خواهیم خواند:

- Perimeter Firewall / Router
- Elastix Firewall
- Fail2ban
- SSH
- VPN
- Monitoring
- تعامل sip و فایروال

این روش ها تنها ایده ای برای monitoring شبکه اند.که متاسفانه در ایران نادیده گرفته می شود؛اما شما که هم اکنون این مقاله را می خوانید حتما به فکر امن کردن شبکه ی خود هستید.

به این نکته توجه کنید که که تمام ابزار تست نفوذ به شبکه شما که توسط شرکت های مختلف ارایه میشود هم از نظر کاربرد وهم نفوذ نسبت به انچه که یک هکر تولید می کند ضعیف تر است.

نفوذگران به هیچ عنوان به روش هایی که شناخته شده وارد سیستم شما نمی شوند.در خوشبینانه ترین حالت از طریق سیستم دیگری وارد شبکه شما شده و از تماس های client ها استفاده می کنند.

Perimeter Firewall / Router

بسیاری از router ها و firewall ها با یکدیگر سازگاری ندارند.برخی از افراد از firewall الاستیکس استفاده میکنند اما در انتها مجبور به لغو دیواره اتش خود می شوند.اما این امر reliable از بین می برد؛پس چه کنیم؟

برای اینکه سیستم شما reliable تعریف شود؛ باید پورت هایی که تمام افراد به ان نیاز دارند را باز بگذاریم.به طور خاص در sip پورت 5060.

به طور کل اگر در سرور elastix خود مشکلی با NAT پیدا کنید؛ پیشنهاد می شود پورت های 5060 الی 5084 (sip-udp) و 10000 الی 20000 (Rtp-UDP) را forward کنید. اما شما تنها نیاز به پورت 5060 برای sip (در سرور الاستیکس) دارید، پورت های 10000–20000 RTP استاندارد Asterisk که بسته به تعداد تمای است که شما در لحظه دریافت می کنید که توسط خود شما هم قابل تغییر است؛ اما برای حفظ reliable بودن سیستم، شما این پورت را باز بگذارید تا تماسی را از ئست ندهید.و سعی به امن کردن این پورت ها کنید.

شما خوب می دانید Voip با NAT سازگار نیست ، NAT به خودی خود هیچ Packet Filterring ندارد و تنها Header را برای یافتن شماره پورت بررسی می کند و اگر قوانین NAT برقرار باشد طبق دستور تعریف شده ان بسته را به ادرس مورد نظر شما NAT می کند.

Firewall مناسب firewall است که برای NAT هم راهکاری داشته باشد یا به کل بتواند پورت ها،ادرس مبدا، ادرس مقصد و نوع ip (tcp/udp) را در ورود و خروج بسته بررسی کند.Firewall/Router این امکان Firewalling را به می دهد.

اطلاعات Public IP که توسط VSP[2] برای سرورSip شما استفاده شده را پیدا کنید.به این توجه کنید که شما تنها به Sip address نیاز ندارید، بلکه یک VSP – قابل قبول – از چندین سرور و چندین DNS به صورت Redundancy و یا Balace استفاده می کند. بدین ترتیب شما به فایروال خود اعلام خواهید کرد که تنها از این ادرس ها بسته های SIP و RTP را دریافت کند و اگر ادرس دیگری درخواست این پورت را داشت، پورت را Close کنند.

اگر شما قادر به استفاده از Firewall نیستید از Elastix نسخه 2.04 به بالاتر استفاده کنید، که بر اساس ip table طراحی شده اند.

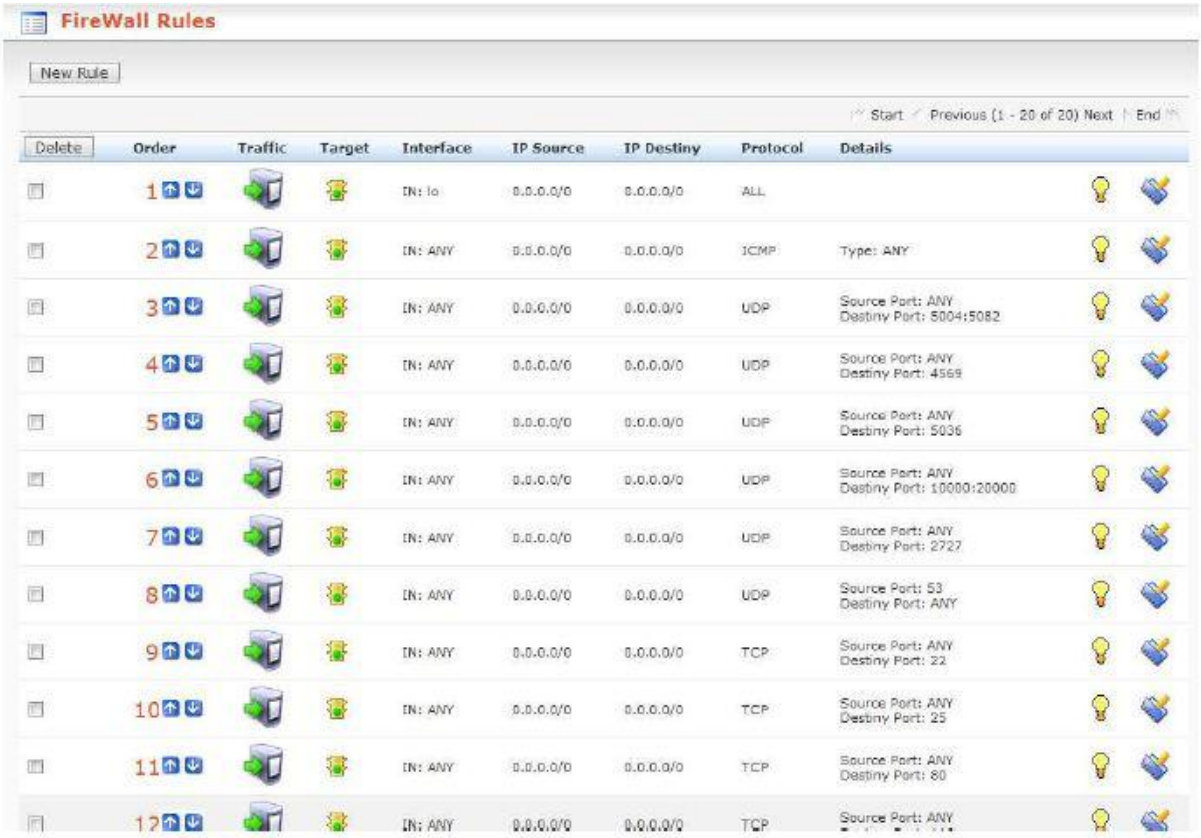
[2] Voip Service Provider

Elastix Firewall

Elastix firewall یک محیط گرافیکی از ip table می باشد . بسیاری از شرکت ها، Firewall های مختلفی برای اجرا و استفاده از iptable تولید کرده اند که elastix firewall نیز یکی از این GUI محسوب می شود.

در هر صورت من استفاده بیرونی از یک فایروال را توصیه می کنم ، اما به دلیل محدودیت و یا هر دلیل دیگری این امکان در الاستیکس نیز موجود است.

در زیر نمایی از این GUI است که Elastix یک سری از قوانین پیش فرض را در ان قرار داده.توجه کنید که در نسخه های بتای Elastix تعدادی bug در GUI و قوانین ان وجود دارد، یکی از قانون های ان اجازه ی update کردن yum و freepbx را نمی دهد.



شما میتوانید قانون (rule) های جدیدی به Elastix اضافه کنید؛ اگر چگونگی اجرا ی Iptable را می دانید این روش یک راهکار ساده یا میانبر برای شما محسوب می شود.

اگر شما امکان استفاده از این فایروال را ندارید میتوانید از iptable و یا هر نرم افزار دیگری استفاده کنید.

Fail2ban

یک نرم افزار یا Tool بسیار فوق العاده برای جلوگیری از حملات Brute-force و تلاش برای Script kiddie break-in[3] است که به صورت اتوماتیک Rule هایی را برای جلوگیری از این نوع حملات به کار می برد که نیاز به مانیتورینگ دایم شما ندارد.

Fail2ban این نوع حملات را هم بلوک و هم مانیتور مکند: تعداد دفعات Fail شدن یک ip را بررسی کرده، اگر تعداد دفعات این fail بیش تر از حد مجاز باشد ان ادرس را به مدت زمان تعیین شده بلوک می کند. که این امر باعث می شود هکر تلاش کند از سیستم دیگری وارد شبکه شود.

Fail2ban مستقیم با ip table کار می کند، پس نیاز به تنظیمات ip table هم داریم که می توانیم حتی از elastix gui برای تنظیم ip table استفاده کنیم.

[3] امکان دسترسی به Event های داخل سیستم شما که توسط گروهی از هکرها جمع اوری می شود و در اختیار دیگران قرار می گیرد(script kiddies).

تغییر پورت پیش فرض SSH

بیش ترین تعداد به elastix از طریق پورت 22 انجام می گیرد.عده ای فکر می کنند نیازی به این پورت ندارند و عده ای دیگر توسط این پورت Remote access می کنند. به شخصه این پورت را باز نمی گذارم، اما اگر می خواهید از این پورت استفاده کنید از حالت استاندارد ان را خارج کنید.

- در مثال زیر پورت SSH را از 22 به 6222 تغییر داده ام:

خط زیر را به فایل /etc/ssh/sshd.config اضافه کنید:

Port 6222

و سپس توسط دستور زیر ان را reload کنید:

Service ssh reload

VPN

بسیاری از Firewall/Router ها توانایی اجرای Vpn endpoint را دارند که به معنی امن نگه داشتن نقاط پایانی در شبکه است.در طرفی PBX و در طرفی ip phone ها قرار دارند.

به طور خاص برای این امر باید OpenVpn را بروی سرور الاستیکس خود اجرا و از ip phone ها یی که Open Vpn Client هستند استفاده کنید(مانند Yea star T28).

Monitoring

بسیاری از کاربران elastix باور دارند که وقتی از firewall و یا دیگر امکانات security استفاده می کنند ، شبکه امنی خواهند داشت و ممکن است حتی یک روز کامل شبکه را مانیتور کنند تا از صحت امنیت مطمین شوند ، اما دیگر تا زمانی که مشکلی در شبکه پیش نیاید سراغ مانیتورینگ نمی روند. و یا شاید یک صبح حوصله کار دیگری ندارند و سراغ مانیتورینگ می روند.

مانند Backup ، شما به درستی کار تا زمانی که از ان استفاده کنید مطمین نیستید.

Monitoring روند ساده ای برای بررسی log ها دارد ، زمان زیادی هم تحلیل ان طول نمی کشداما باید مستمر انجام شود.

یکی از این log ها در ادرس زیر امده:

- /var/log/secure

که ادرس ip ها یی را نشان می دهد که توسط SSH به سیستم شما حمله کرده اند.

- /var/log/audit/audit.log

Login های موفق و یا نا موفق را نشان می دهد.دنبال username های نا متعارف باشید که این امر نشان می دهد شما مورد حمله قرار گرفته اید یا خیر.

راهنمای استفاده از sip و تعامل با firewall/router

در ابتدا باید به مفهوم NAT در Firewall/Router الاستیکس که مجبور به استفاده از Sip هستند بپردازیم، چرا که این اولین Application (در بسیاری از موارد) است که اگر نتوانیم از Dynamic NAT استفاده کنیم ان را به کار می بریم. منظور از Dynamic NAT زمانی است که روتر درک کند که بسته ای از داخل شبکه شما تصمیم به ورود به شبکه دیگر را دارد و پورت خروجی را برای ان اختصاص دهد تا ترافیک برگشتی نیز با ان پورت ارتباط برقرار کند.(به Dynamic NAT ؛ PAT نیز می گویند).

دلیل اینکه Sip با NAT مشکل دارد این است که ip table هایی که از Sip استفاده میکنند تنها از یک پورت استفاده نمی کنند و بسیاری از Firewall/Router توانایی تشخیص بسته های Sip را ندارند تا پورت هایی را به صورت پویا به ان اختصاص دهند !

دلیل دیگری که sip از NAT نمی تواند استفاده کند ؛ NAT Session به دلیل کمبود ترافیک Sip در هنگام مکالمه کاملا از بین می رود (collapsing) که زمان ان بسته به نوع روتر دارد. در بسیاری از موارد در انجمن Voip-iran اتفاق افتاده که اعضا از قطع شدن مکالمه بعد از 3 دقیقه یا 10 دقیقه شکایت دارند، اغلب این امر به دلیل Collasp کردن NAT session هایی است که به صورت dynamic ساخته شده اند(در Router).

چرا روتر این نوع Session را می بندد؟ به دلیل اینکه ترافیک زیادی در پورت sip قابل دریافت نیست و به همین دلیل از RTP برای عبور ترافیک استفاده می کنیم.

به دلیلی که گفته شد، نیاز به استفاده از Static NAT داریم تا router بداند مکالمه را به کدام پورت بفرستد.

به تازگی برای رفع این مشکل از Stun Server استفاده می کنند که یک Feature رایگان است به طوری که بسته ها به این سرور ارسال می شود و این سرور قابلیت تشخیص پورت ها را داراست. اما به دلیل رایگان بودن تنها در موارد ضروری و برای تعداد مشتریان کم تر از 50 تن استفاده خواهد شد.

فصل سوم

اشنایی با نصب و راه اندازی Elastix Firewall

در این فصل خواهیم خواند:

- Elastix Firewall
- نگاهی به elastix firewall
- تنظیمات پورت
- تعریف Rule
- محدود سازی Firewall

Elastix Firewall

از Elastix 2.2 امکان جدیدی به نام Firewall/Router به این سرور اضافه شد که ip table با قدمت 12 سال در لینوکس را به صورت GUI به کاربر ارایه می دهد.

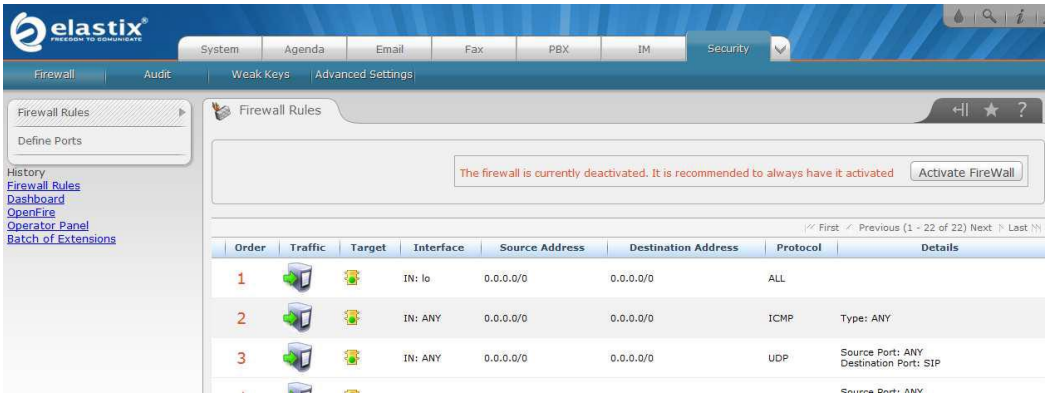
پس شما برای اجرای Firewalling در Elastix یا باید از Ip table استفاده کنید یا از Palosanto ‘s Firewall و نمی توان از هر دو همزمان استفاده کرد؛ پیشنهاد من همیشه این است که از هر شرکتی که خرید می کنید از همان شرکت هم توصیه امنیتی قبول کنید پس برای الاستیکس از Palosanto ‘s Firewall استفاده کنید.

اگر توانایی خرید فایروال دیگری دارید حتما این کار انجام دهید؛ چرا که Firewall نباید در خود سرور باشد و باید در Device دیگری قرار گیرد و این اولین نکته برای شماست. و در غیر این صورت از Palosanto ‘s Firewall استفاده کنید(اجرای Elastix firewall بهتر از نبودن Firewall است).

یافتن ELastix Firewall

بسته به اینکه از کدام Elastix GUI Theme استفاده می کنید؛ Elastix Firewall جزیی از Security TAB در Elastix است.

وقتی Security را کلیک کردید، تصویر مشابهه زیر را خواهید دید.



اکنون شما در محیط Firewall هستید ؛ متن قرمزی به شما هشدار می دهد که Firewall اکنون فعال نیست.

Palosanto تعدادی rule پیش فرض را که برای تمام برنامه هیی که به صورت پیش فرض در Elastix نصب می شود ضروری باشد را در خود جای داده.

با فعال کردن Firewall تمام ترافیک غیر از ترافیک هایی که rule های انان وجود دارد، Stop می شوند.

نگاهی به elastix firewall

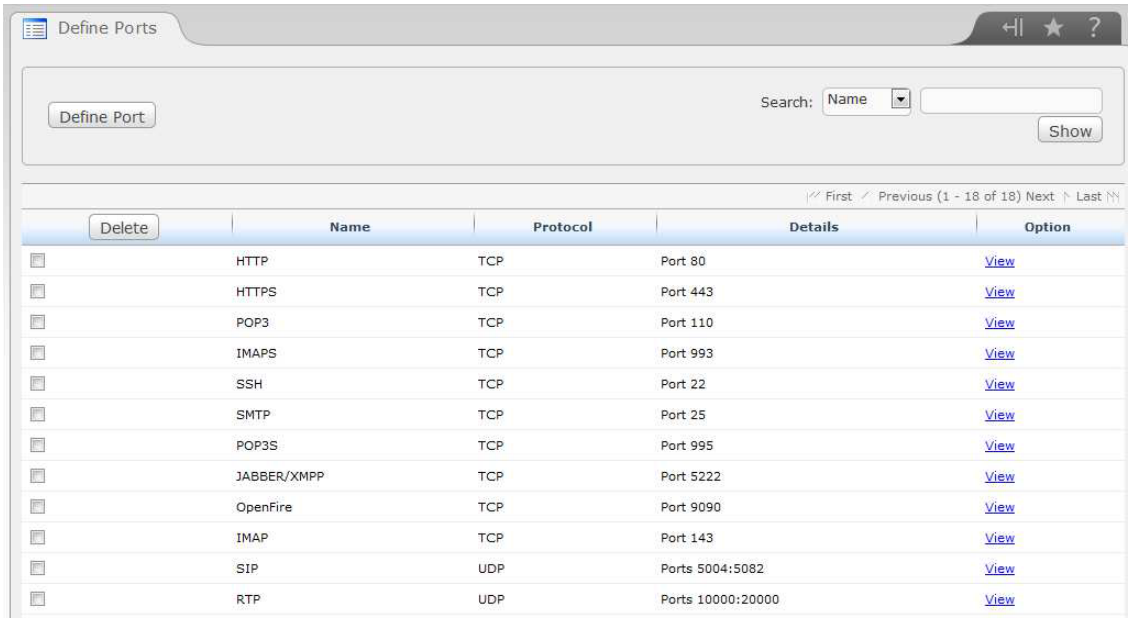
در سمت چپ شما یک Basic Menu خواهید داشت که شامل:

1) Firewall rules
2) Define ports

این دو منو در تمام firewall ها وجود دارد.در هر فایروال شما باید بتوانید rule وارد کنید و پورت های مورد نظر خود را تعریف کنید.

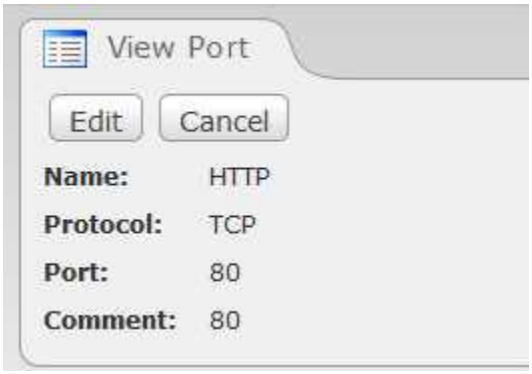
تنظیمات پورت

قبل از اینکه به قسمت rule ها برویم ، نگاهی به Port Defination میکنیم.پس Define ports را انتخاب کنید:

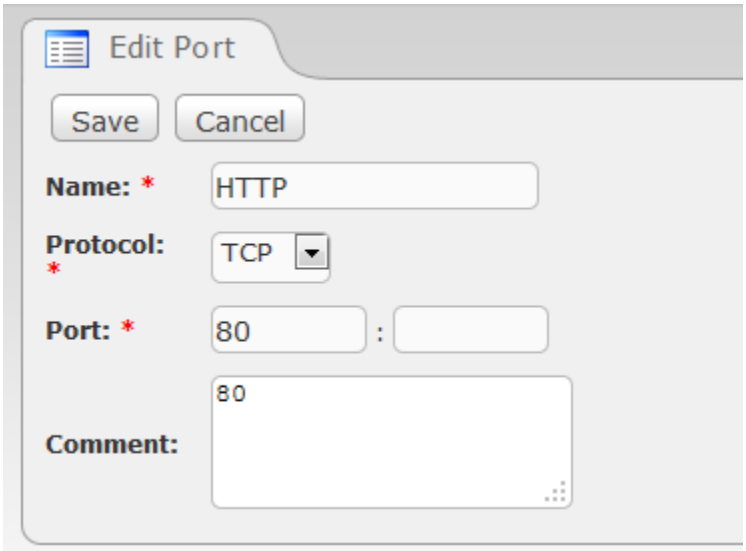


Polasanto تعداد پورت هایی که به صورت پیش فرض در Elastix وجود دارد را نمایش می دهد.

بیاییم به دو پورت موجود نگاهی کنیم: در خطی که به Http اشاره شده در قسمت option بروی View کلیک کنید:

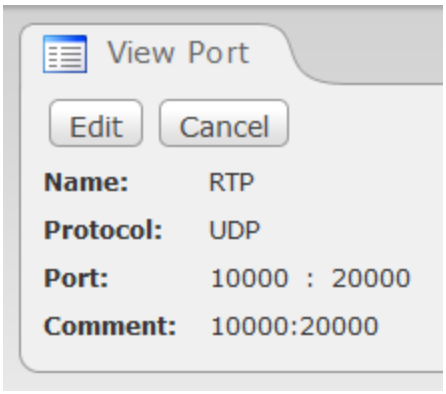


شما اطلاعاتی را درباره این پورت دریافت می کنید. و همه ی ما می دانیم پورت 80 مربوط به Http است. بروی EDIT کلیک کنید.

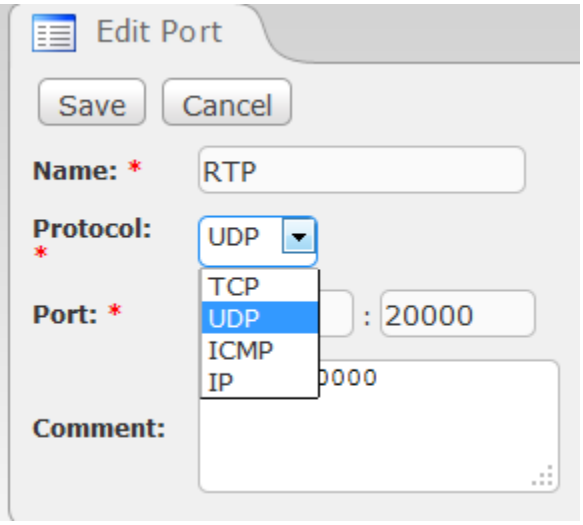


حال می توانیم تغییراتی در این پورت دهیم ، هر تغییری در این قسمت و زدن Save حساس و باید با دانش انجام گیرد(تمام فیلد های ضروری با ستاره ی قرمز (رنگ مشخص شده).

در این زمان Cancel را تا به پورت دیگری نگاه کنیم. پورت RTP را انتخاب کنید:



حتما فرق این پورت را خواهید یافت؛ بازه ی پورتی که دارد. پورت 10000:20000 به همین دلیل است که در اجرای firewall rule پورت هایی از 10000 تا 20000 را اجازه عبور می دهیم. فرق دیگر Protocol ان است ، که بروی UDP است.



حال که بحث protocol پیش امد چند پروتکل موجود در این بخش را بررسی می کنیم:

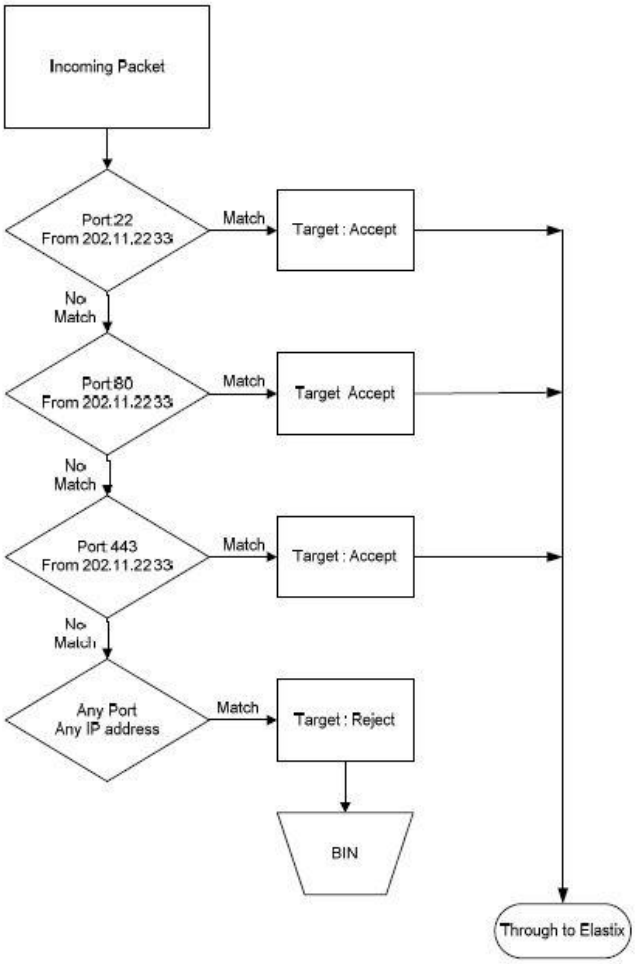
- TCP: پورت هایی که با این پروتکل کار می کنند(مانند Http/Https).
- UDP: همانند TCP با این تفاوت که پورت ها با بسته های UDP کار می کنند (مانند RTP/Sip).
- ICMP: internet control message protocol .که ممکن است برنامه هایی همچون Traceroute و Ping از ان استفاده کنند.این بسته ها هیچ اطلاعاتی را حمل نمی کنند؛ اما حاوی information درباره شبکه اند.
- Ip: زمانی که نمی دانیم چه port مربوط به کدام پروتکل است از ip استفاده می کنیم.

برای اضافه کردن یک پورت جدید تنها کا فی است بروی Define ports کلیک کرده و مشابه انچه در بالا گفتیم عمل کنید.

پیشنهاد می کنم همیشه port های خود را چک کنید و سپس به سراغ rule بروید؛ زیرا rule ها برای پورت ه نوشته می شوند.

تعریف Rule

به دیاگرام زیر نگاه کنید؛ این دیاگرام چگونه کار کردن Rule ها را نمایش می دهد:



این دیاگرام نشان می دهد که Rule ها از بالا به پایین چک می شوند (همانند Sequence # های Cisco)، پس در قرار گیری Rule ها دقت کنید.

توضیح شکل: اگر بسته ای امد به اولین Rule نگاه کن ، اولین Rule در این سکل پورت 22 (SSH) است اگر بسته درخواست این پورت را دارد و از ادرس ip 202.11.22.33 اجازه عبور به ان توسط Elastix داده شود.

اگر این Rule مد نظر نباشد به Rule بعدی می رود تا زمانی که با یک Rule ، match شود.

در انتها جدول Rule ها یک Rule وجود دارد که اعلام میکند اگر بسته ای غیر از ip مورد نظر و پورت های تعریف شده باشد Reject شود.

مطلب دیگری که لازم می دانم درباره ی ان توضیح دهم؛ مفهوم Local Loop Back است:

این interface با "LO" نمایش داده می شود. در محیط لینوکس دستور ifconfig را درج کنید.بعد از interface اترنت شما، اینترفیس Lo قرار دارد.

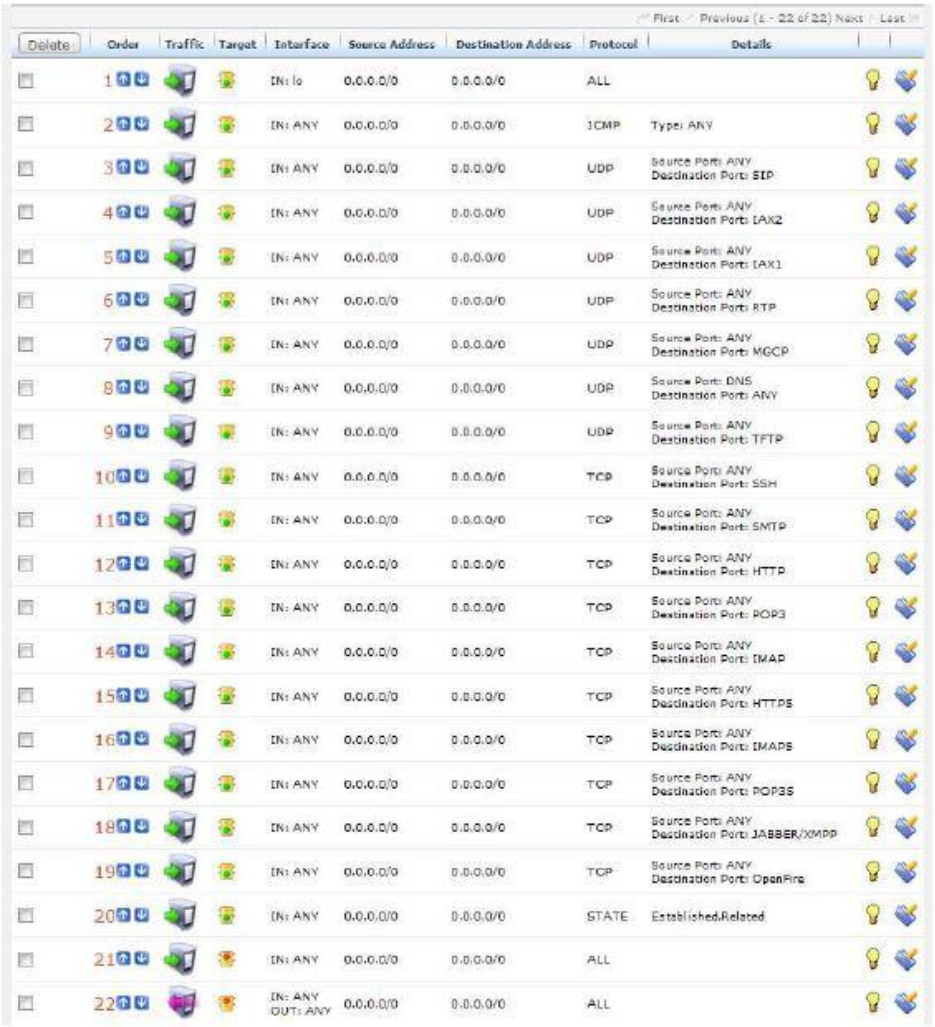
```
[root@elastix22 ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:13:20:B5:5E:4F
          inet addr:172.22.22.15  Bcast:172.22.22.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:802437 errors:0 dropped:0 overruns:0 frame:0
          TX packets:536271 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:420280965 (400.8 MiB)  TX bytes:188364845 (179.6 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:392938 errors:0 dropped:0 overruns:0 frame:0
          TX packets:392938 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:45042821 (42.9 MiB)  TX bytes:45042821 (42.9 MiB)
```

هر Application در داخل سیستم عامل شما با اینترفیس LO در ارتباط است.

همانطور که در شکل بالا می بینید LO ترافیکی را handle می کند پس نیاز است در Firewall Rule به صورت دایم حضور داشته باشد. بعلاوه از اینترفیس LO برای Virtual adaptor (که نیازی به Hardware ندارد) نیز استفاده می شود. زمانی که شما Elastix را بدون هیچ کارت شبکه و Driver نصب می کنید این interface در ان وجود دارد، به معنی ان است که هر برنامه ای که با ip stack کار کند در سیستم شما قابل اجرا ست.

به تصویر زیر دقت کنید:

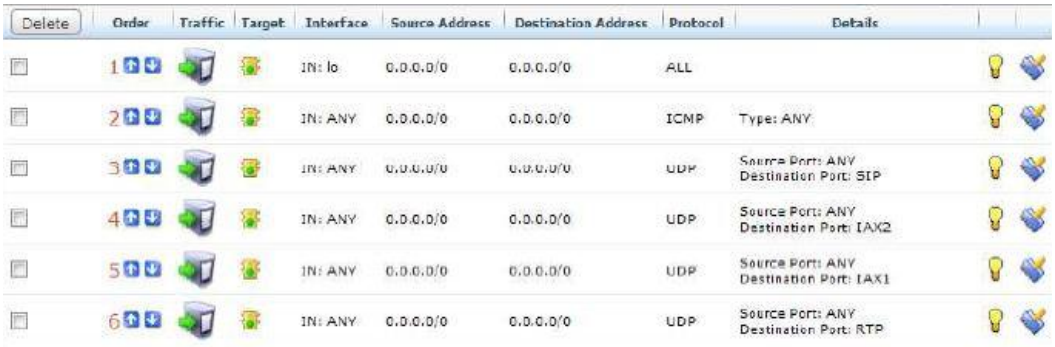


Delete	Order	Traffic	Target	Interface	Source Address	Destination Address	Protocol	Details
	1			IN: lo	0.0.0.0/0	0.0.0.0/0	ALL	
	2			IN: ANY	0.0.0.0/0	0.0.0.0/0	ICMP	Type: ANY
	3			IN: ANY	0.0.0.0/0	0.0.0.0/0	UDP	Source Port: ANY Destination Port: SIP
	4			IN: ANY	0.0.0.0/0	0.0.0.0/0	UDP	Source Port: ANY Destination Port: IAX2
	5			IN: ANY	0.0.0.0/0	0.0.0.0/0	UDP	Source Port: ANY Destination Port: IAX1
	6			IN: ANY	0.0.0.0/0	0.0.0.0/0	UDP	Source Port: ANY Destination Port: RTP
	7			IN: ANY	0.0.0.0/0	0.0.0.0/0	UDP	Source Port: ANY Destination Port: MGCP
	8			IN: ANY	0.0.0.0/0	0.0.0.0/0	UDP	Source Port: DNS Destination Port: ANY
	9			IN: ANY	0.0.0.0/0	0.0.0.0/0	UDP	Source Port: ANY Destination Port: TFTP
	10			IN: ANY	0.0.0.0/0	0.0.0.0/0	TCP	Source Port: ANY Destination Port: SSH
	11			IN: ANY	0.0.0.0/0	0.0.0.0/0	TCP	Source Port: ANY Destination Port: SMTP
	12			IN: ANY	0.0.0.0/0	0.0.0.0/0	TCP	Source Port: ANY Destination Port: HTTP
	13			IN: ANY	0.0.0.0/0	0.0.0.0/0	TCP	Source Port: ANY Destination Port: POP3
	14			IN: ANY	0.0.0.0/0	0.0.0.0/0	TCP	Source Port: ANY Destination Port: IMAP
	15			IN: ANY	0.0.0.0/0	0.0.0.0/0	TCP	Source Port: ANY Destination Port: HTTPS
	16			IN: ANY	0.0.0.0/0	0.0.0.0/0	TCP	Source Port: ANY Destination Port: IMAPS
	17			IN: ANY	0.0.0.0/0	0.0.0.0/0	TCP	Source Port: ANY Destination Port: POP3S
	18			IN: ANY	0.0.0.0/0	0.0.0.0/0	TCP	Source Port: ANY Destination Port: JABBER/XMPP
	19			IN: ANY	0.0.0.0/0	0.0.0.0/0	TCP	Source Port: ANY Destination Port: OpenFire
	20			IN: ANY	0.0.0.0/0	0.0.0.0/0	STATE	Established,Related
	21			IN: ANY	0.0.0.0/0	0.0.0.0/0	ALL	
	22			IN: ANY OUT: ANY	0.0.0.0/0	0.0.0.0/0	ALL	

دستورات بالا، دستورات پیش فرض هستند که در Elastix وجود دارند. اگر Rule جدیدی اضافه کرده اید که با Rule های قدیمی مشابهه اند ، Rule قدیمی را باید پاک کنید.

اگر تصویر بالا با انچه شما در سیستم خود می بینید مغایر است، به این دلیل که شما هنوز Firewall را فعال نکرده اید و تا زمانی که firewall فعال نکنید اجازه ی Edit و یا move کردن Rule ها را ندارید.

بیا ییم نگاهی به چند Rule کنیم:



Delete	Order	Traffic	Target	Interface	Source Address	Destination Address	Protocol	Details
	1			IN: lo	0.0.0.0/0	0.0.0.0/0	ALL	
	2			IN: ANY	0.0.0.0/0	0.0.0.0/0	ICMP	Type: ANY
	3			IN: ANY	0.0.0.0/0	0.0.0.0/0	UDP	Source Port: ANY Destination Port: SIP
	4			IN: ANY	0.0.0.0/0	0.0.0.0/0	UDP	Source Port: ANY Destination Port: IAX2
	5			IN: ANY	0.0.0.0/0	0.0.0.0/0	UDP	Source Port: ANY Destination Port: IAX1
	6			IN: ANY	0.0.0.0/0	0.0.0.0/0	UDP	Source Port: ANY Destination Port: RTP

- Arrow ابی رنگ به ما اجازه حرکت یک Rule به بالا یا پایین را می دهد.
- Arrow سبز رنگی که به سمت کامپیوتر کشیده شده اند، نشان دهنده ی ترافیک ورودی به firewall است.برای کارکرد درست باید بروی input قرار گیرد تا packet ها به سمت سیستم وارد شوند. هم چنین برای Forward می توان بگذاریم(packet هایی که توسط elastix مسیر یابی می شوند) و output که نشان دهنده ی بسته هایی است که از سیستم خارج می شوند.
- اگر چراغ راهنمایی سبز باشد نشان دهنده ی Accept بودن این Rule است.
- Interface : اینترفیس های انتخاب شده را نشان می دهد.
- Source address: همانطور که می بینید به صورت پیش فرض 0.0.0.0/0 (any) تعریف می شود در این قسمت می توانیم ادرس ip ورودی به elastix را محدود کنیم.
- Destination address: برای ادرس ip خروجی استفاده می شود که به صورت پیش فرض 0.0.0.0/0 تعریف گردیده.
- Detail : پروتکل و اطلاعات پورت که در defined ports تعریف کرده ایم در این قسمت می اید.
- Light bulb : لامپی که نشان دهنده ی فعال یا غیر فعال بودن Rule است.
- و در اخر icon مربوط به ویرایش قرار دارد.

چگونه با Firewall Rule رفتار کنیم:

تعدادی Rule پیش فرض وجود دارد:

1. Rule مربوط به LO را بدون تغییر رها کنید. و بگذارید در بالای جدول باقی بماند.
2. در مورد تغییر Http و https دقت کنید، تغییر و حذف این Rule باعث مشکلات بعدی خواهد شد. به طوری که شما دیگر نمی توانید به GUI دسترسی داشته باشید. (اگر چنین مشکلی برایتان پیش امده به اخر این بخش مرا جعه کند).

3. Rule 3 در اخر این جدول وجود دارد، بگذارید این 3 قانون در جای خود به طور پیش فرض باقی بمانند.

این Rule 3 :

- Rule20 : قانونی است که اجازه می دهد ترافیک که از elastix خارج شده ، برگردد (با همان پورت ارسالی). برای مثال اگر Elastix سرویس خارجی را از طریق پورت 1678 درخواست کند در پاسخ ترافیک برگشتی در صورتی که جواب به همین پورت و همان ادرس ip باشد اجازه ورود به elastix را خواهد داشت.
- Rule21: deny برای تمام Rule ها است.بنابر این اگر ترافیکی با هیچ match Rule نشد تا به این Rule برسد Reject می شود.
- Rule22: این قانون نیز Deny برای تمام Rule ها است اما برای ترافیک هایی که Forward شده اند.

نکته اخر این که اگر شما Rule جدیدی تعریف کنید، در پایین Rule22 قرار می گیرد و عملا elastix ، Rule شما را چک نمی کند، تا زمانی که شما Rule را به بالا جدول هدایت کنید(بالاتر از 3 قانون انتهایی).

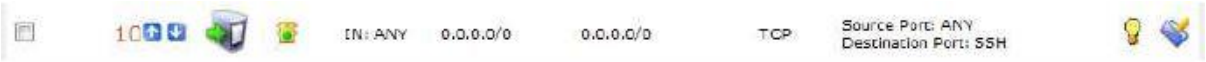
برای اطلاعات بیش تر نسبت به Rule20 در google کلمه زیر را جستجو کنید:

Ip Tables Connection Tracking

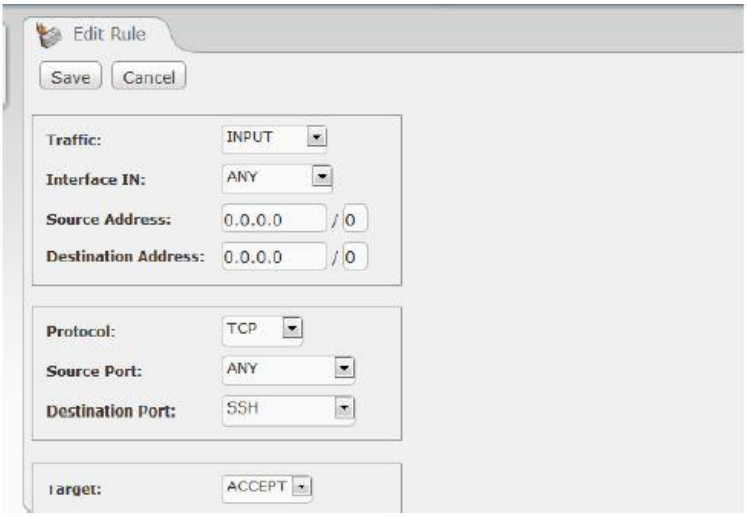
محدود سازی Firewall

شاید شما بخواهید Rule برای SSH تعریف کنید و ادرس ip ان را محدود سازید.

به Rule10 بروید:



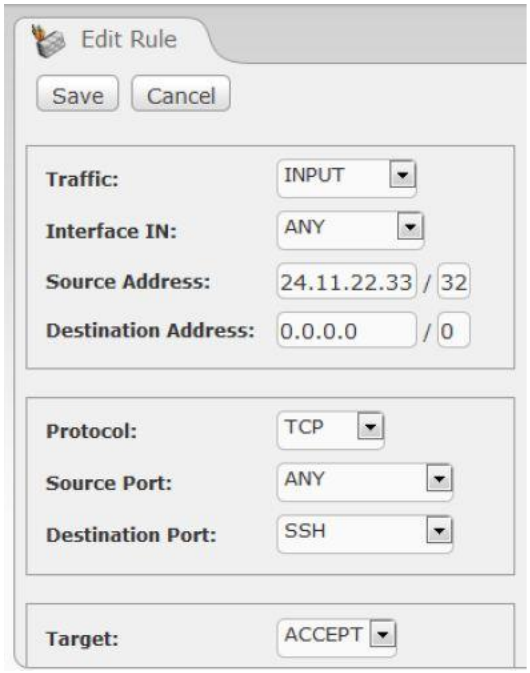
EDIT کلیک کنید:



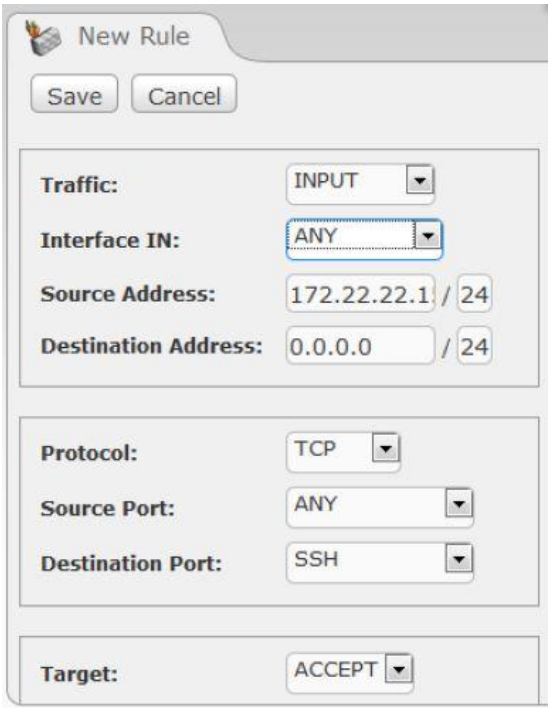
در این قسمت شما Source port/Destination port می بینید که دربارهی ان مطلبی نگفته ام.

Inbound Rule در Destination port قرار میگیرد(پورتی که اجازه ی ورود ترافیک به Elastix را دارد).

به صورت استاندارد شما نباید SSH port خود را محدود کنید و برای اعلام این محدودیت تنها اجازه ی ورود ادرس ip خاص را در source address دارید.در این مثال ادرس 24.11.22.23/32 ip را قرار داده ام. Subnet mask 32 را به دلیل انتخاب این ip به عنوان تنها host منظور کرده ام، پس فقط 24.11.22.23 می تواند درخواست SSH کند. اگر شما یک host ip ندارید، میتوانید بازه ای از شبکه خود را درج کنید (مانند 24.11.22.0/24) و سپس Save کنید.



با اعمال این تغییرات فقط یک ip یل رنجی از ip می توانند از بیرون شبکه به سرور شما SSH بزنند، اما شبکه lan خودمان چطور؟ باید Rule جدیدی برای شبکه خودمان تعریف کنیم.New Rule را بزنید:



Source address همان شبکه lan است (172.22.22.1/24).Save کنید و rule را به مکان مناسب ببرید. به شکل زیر دقت کنید:

همانطور که مشاهده می کنید دو rule برای ssh سا ختە ایم، اولی برای شبکه های external و دومی برای internal. شاید بگویید که این کار در firewall های دیگر اسان تر است اما ip table لینوکسی چنین فرایندی دارد.

- در تمرین بعدی شما sip rule را تغییر دهید.اما به این نکته توجه کنید که اگر sip را به یک ادرس external محدود کنید، امادگی cancel شدن تمام تماس های خود را داشته باشید پس مطمئن شوید که یک internal rule هم ساخته اید(برای RTP هم همین روال را پیش بروید).

نکاتی درباره ی ip table:

1. Ip table از قبل بروی سرور شما نصب بوده.
2. نیازی به command line برای save یا flush کردن table ندارد (نیاز به restart شدن ip table نیست).
3. بعد از اینکه در GUI ، rule های خود را اعمال کردید می توانید در CLi هم ان ها را با تایپ دستور زیر ببینید:

   Iptable –L
4. نیازی به start ، ip table ندارد.

سوال و جواب

- به طور اتفاقی HTTPS را بلاک کردم و حالا نمی توانم به Elastix GUI دسترسی داشته باشم، چه کنم؟
- اگر هنوز SSH می توانید بزنید به elastix وصل شوید و در linux prompt دستور زیر را بزنید:

  /etc/init.d/iptables stop

حالا به GUI وصل شوید به قسمت firewall رفته و مشکل را حل کنید و بعد از ان save کنید. نیازی به کار دیگری نیست اما پیشنهاد میکنم یک بار reboot کنید.

فصل چهارم

دیگر feature های ایمن سازی elastix

در این فصل خواهیم خواند:

- نصب Fail2Ban
- نصب apf
- نصب bfd
- نصب و راهنمای Csf

نصب Fail2Ban

فایل fail2ban-0.8.4.tar.bz2:

http://sourceforge.net/projects/elifetech.u/files/security/fail2ban-0.8.4.tar.bz2/download

1-نحوه نصب:

```
tar -jxf fail2ban-0.8.4.tar.bz2
cd fail2ban-0.8.4
python setup.py install
/usr/src/fail2ban-0.8.4/files/redhat-initd /etc/init.d/fail2ban cp
chmod 755 /etc/init.d/fail2ban
cd /etc/fail2ban/filter.d
touch asterisk.conf
```

2- محتوا `asterisk.conf`

دریافتasterisk.conf

http://sourceforge.net/projects/elifetech.u/files/security/asterisk.conf/download

این دو متغیر در این فایل توجه کنید:

maxretry = 5

bantime = 600

3-

asterisk-iptables را به /etc/fail2ban/jail.conf file

اضافه کنید:

```
# /etc/fail2ban/jail.conf
#====================

[asterisk-iptables]
enabled = true
filter = asterisk
action = iptables-allports[name=ASTERISK, protocol=all]
sendmail-whois[name=ASTERISK,
dest=youremailaddress@somewhere.com,
sender=fail2ban@somewhere.com]
logpath = /var/log/asterisk/full
maxretry = 5
```

```
bantime = 600
#====================
```

4-

و در این مسیر /etc/fail2ban/jail.conf

شبکه ip خودرا به عنوان شبکه امن معرفی کنید:

```
ignoreip = 127.0.0.1 192.168.1.0/24
```

(یعنی این شبکه ها رو مورد باز خواست قرار ندهد.)

5-

[general] را به فایل /etc/asterisk/logger.conf **اضافه کنید.**

```
#====================
[general]
dateformat=%F %T
#====================
```

6-سپس

asterisk -rx "module reload logger"

chkconfig fail2ban on

/etc/init.d/fail2ban start

iptables -L –v

با اجرای دستور اخر باید fail2ban-ASTERISK **در** ip-table **شما قرار بگیرد.**

نصب apf

Advanced Policy Firewall(APF):

وظیفه کنترل iptable در سرور و باز و بسته کردن پورت را دارد.

با BFD توسط reactive address block(RAB) ارتباط برقرار میکند.

Brute force Detection(BFD):

برای کنترل fail login و بلوک کردن ip.. مثل fail2ban.

نصب:

در صورتی که به اینترنت سرور شما دسترسی دارد:

دریا فت فایل sh:

http://sourceforge.net/projects/najafi/files/voip/apf_bfd/install_apf_bfd.sh/download

و نمود نصب:

```
chmod 755 install_apf_bfd.sh
./install_apf_bfd.sh
```

نصب به صورت manual:

دریافت فایل ها:

http://sourceforge.net/projects/najafi/files/voip/apf_bfd/apf-current.tar.gz/download

http://sourceforge.net/projects/najafi/files/voip/apf_bfd/bfd-current.tar.gz/download

```
tar -xvf apf-current.tar.gz

cd apf-9.7-2
```

```
chmod 755 install.sh
./install.sh
```

```
tar -xvf bfd-current.tar.gz

cd bfd-1.5

chmod 755 install_apf_bfd.sh
./install_apf_bfd.sh
```

APF

تنظیمات اسانی دارد..و فایل config ان در مسیر */etc/apf/* قرار دارد.

اسم این فایل config.apf است.

در صورت نداشتن چنین فایلی شما هنوز این نرم افزار نصب نکرده اید.

حال باید conf.apf را تنظیم کنیم.(توجه کنید شما فقط این فایلرا edit می کنید.)

شما اگر از چند network interface استفاده میکنید،حتما باید IFACE_IN وIFACE_out برای اینترفیس تعریف کنید.

اینترفیس که به اینترنت دسترسی دارند untrust هستند و اینترفیس که internal استفاده میشه trust، که با IFACE_TRUSTED این دستور به سیستم اعلام میشه.

1- با nano /etc/apf/conf.apf و یا winscp شروع به ویرایش می کنیم.

در این فایل untrusted ها را مشخص مکنیم.

SET_TRIM را صفر میگذاریم تا این دستور مقدار deny rule را در کنار trust بگذارد.که برای حفظ ram و زمان نیازی به این قسمت نداریم.

2- Apf توانایی ارایه QOS برای بسته ها هم دارد.

برای sip و IAX در conf.apf مقدار tos زیر را بدهید.

TOS_8="21,20,80,4569,5060,10000_20000"

3- اگر پورت ssh تغییر داده اید.در این فایل هم این تغییر باید ذکر گردد.

HELPER_SSH_PORT="2222"

4- اگر از IAX برای ترانک بین سرور داخلی استفاده کردید و نمی خواهید از بیرون شبکه پورت ها رو باز ببینند:

IG_TCP_CPORTS="2222,69,80,5060,6600,10000_20000"
IG_UDP_CPORTS="69,5060,10000_20000"

5- Egress filtering:

می توانیم outbound را فیلتر کنیم.

"EGF="0

Disable میکنیم.

6- تنظیمات apf تمام شد.

حال شروع به راه اندازی میکنیم.. نگران نباشید اگر خطایی انجام دادید یا apf به درستی اجرا نشد بعد از 5 دقیقه به طور اتوماتیک از process خارج می شود.(" DEVEL_MODE="1 در فایل conf.apf چک کنید)

7- فایل save کنید

8- دستور apf بدون هیچ flag بزنید.

به فلگ ها توجه کنید. سپس:

apf -s

9- apf راه افتاد.

10- می توانید rule مختلف از سایت *dshield.org* یا *spamhaus.org* بگیرید.

11- حال به سرور ssh بزنید..اگه از شبکه داخلی نتوانستید ssh بزنید بعد از 5 دقیقه apf خاموش می شود.

اما اگر به راحتی ssh زدید "DEVEL_MODE="0 کنید تا به شما develop ندهد.(با نرم افزار puTTy می توانید SSH بزنید).

به فایل های deny_hosts.rules و allow_hosts.rules حتما توجه کنید. حاوی اصلاعات مهمی هستند.

نکاتی درباره ی Apf:

-اگر میخواهیم یک ip به تمام پورت های سرور دسترسی داشته باشد(مثلا سرور دومی که از IAX استفاده می کند) از دستور زیر استفاده میکنیم:

```
apf -a 192.168.1.216
```

که هر `ip` می تواند باشد.

پس اگر سرور دوم هم `apf` اجرا کردید، برای `ip` سرور اول همین کار را تکرار کنید.

-برای بلاک کردن یک `subnet` ویا `host`:

```
apf -d 202.86.128.0/24
apf -d 202.86.128.200
```

نصب bfd

Brute Force Detection همانطور که قبلا گفته ام برای چک کردن login اشباه به سرور است.

- فایل configان در مسیر in/usr/local/bfd قرار دارد.(conf.bfd)
- همچنین اگه بخواهیم ip را بلاک کنیم از فایل زیر استفاده می کنیم.

/usr/local/bfd/ignore.hosts

1-فایل conf.bfd برای ویرایش باز کنید.

TRIG را پیدا کنید.مقداری که جلوی ان درج می کنیم تعداد دفعات مجاز برای failed attempts البته قبل از ban شدن.مقدار پیش فرض 15 مناسب است.اما بسته به حساسیت خودشما ان را کم تر کنید.

2-bfd امکان ارسال alert به ایمیل شما را هم دارد..یعنی وقتی مورد حمله قرار گرفت ایمیلی به شما ارسال می کند.

EMAIL_ALERTS را مقدار 1 بدهید.تا فعال شود.

در EMAIL_ADRESS ادرس ایمیل خود را درج کنید.

3-bfd در **/etc/cron.d و هر 3 دقیقه اجرا می شود. با دستور BFD می توانید روند کار و ip را نگاه کنید.**

bfd -a با این دستور هم لیستی از ip برای شما نمایش داده می شود.

bfd -s برای شروع به کار bfd به کار می رود.

نصب و راهنمای Csf

Config Server Security & Firewall

این بخش راهنمای کامل درباره ی Csf نیست اما برای امن سازی سیستم کافی است.

در ابتدا نیاز به نصب Webmin دارید، زیرا Csf توسط این کنسول اجرا می شود.

از ادرس زیر webmin دریافت و نصب کنید:

```
wget http://prdownloads.sourceforge.net/webadmin/webmin-1.580-1.noarch.rpm
rpm -U webmin-1.580-1.noarch.rpm
```

حال نوبت به نصب csf رسیده:

```
wget http://www.configserver.com/free/csf.tgz
tar zxf csf.tgz
cd csf
sh install.sh
```

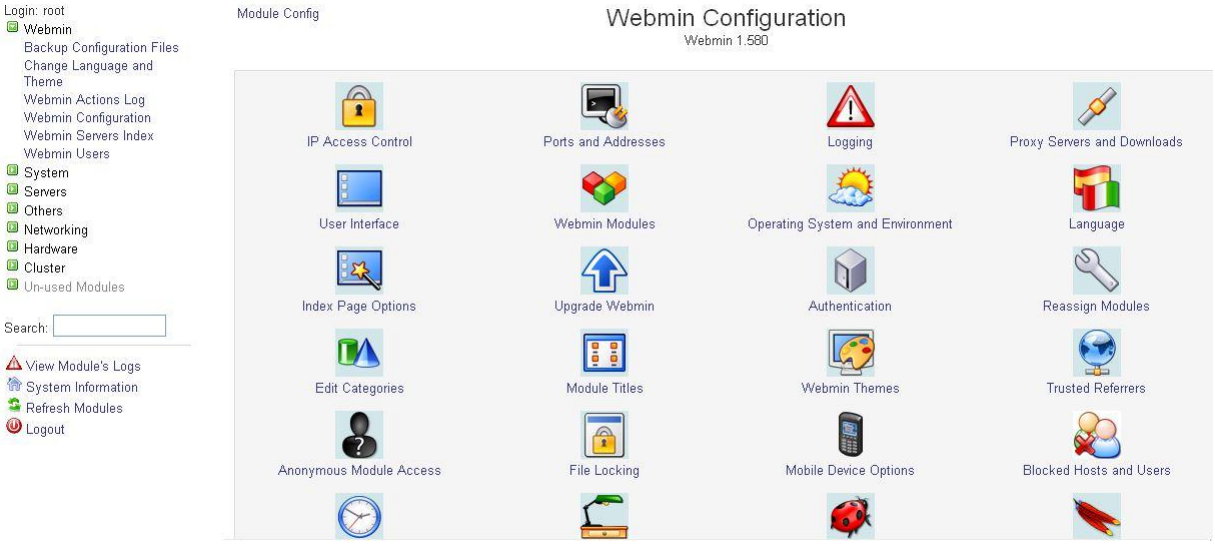
سپس به webmin وارد شوید:

https://your server ip:10000/

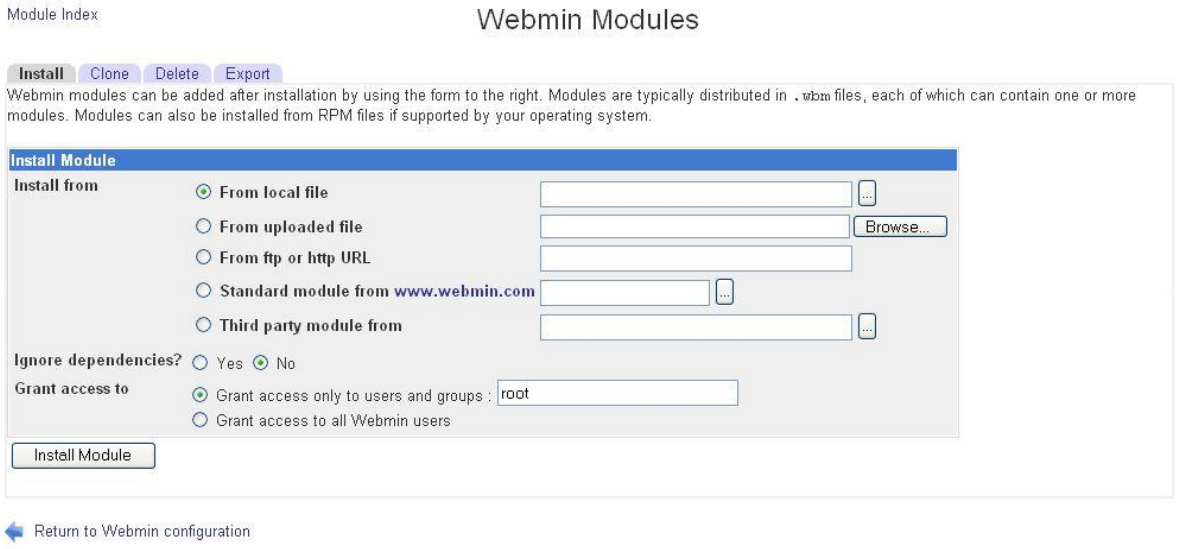
با root و root password که برای elastix تعیین کرده اید وارد کنسول شوید.

Webmin را مانند شکل انتخاب کنید:

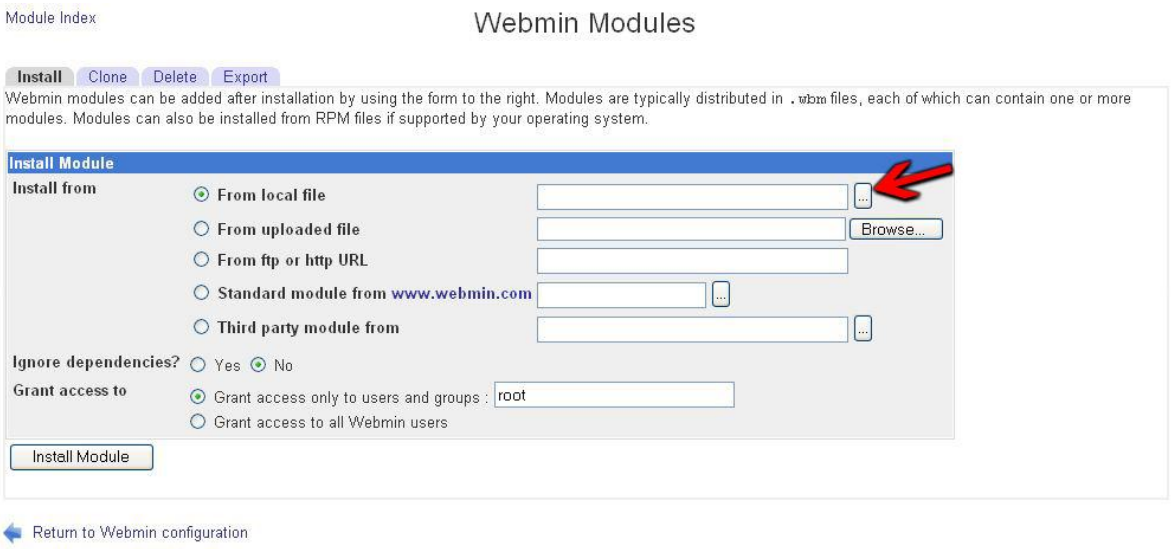
و سپس webmin configuration را بزنید:



سپس webmin module را زده:

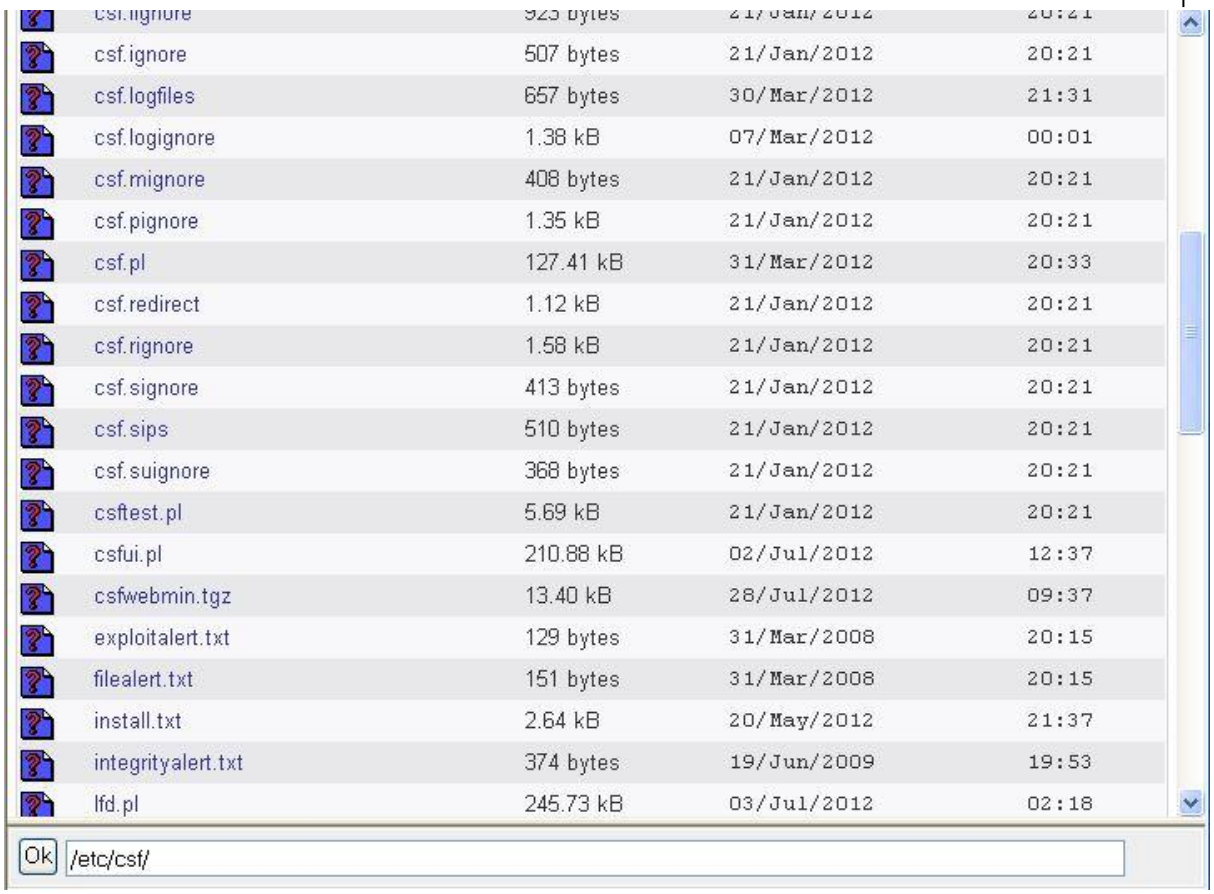


گزینه From local file بر روی browse کلیک کنید:



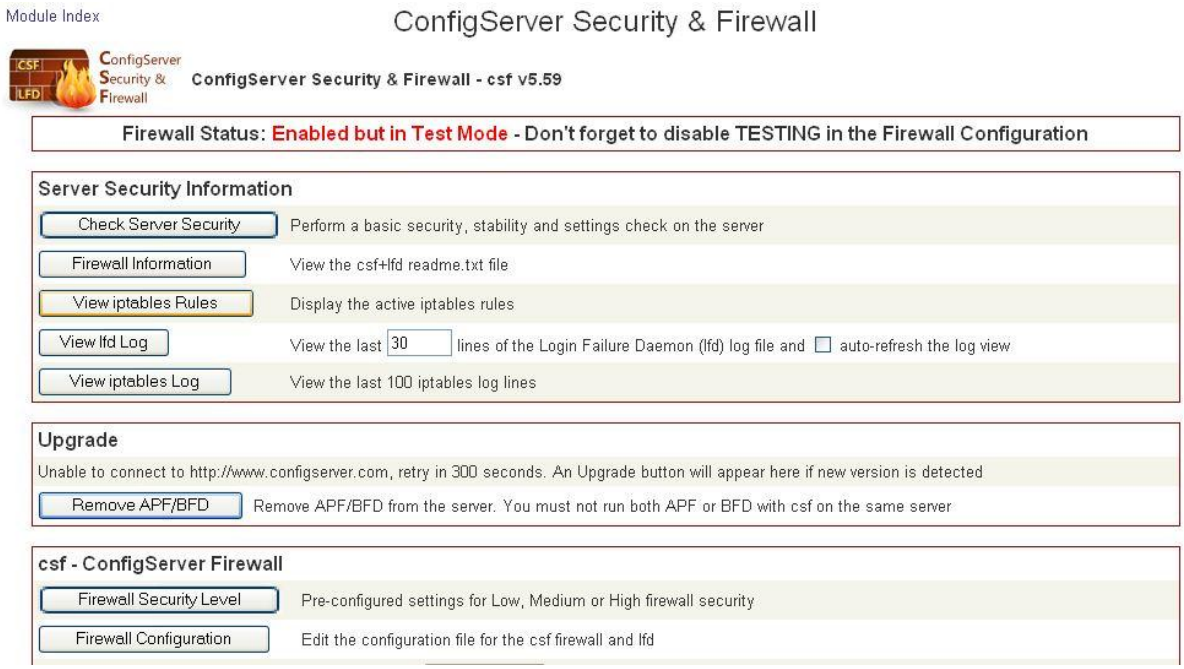
و به ادرس زیر بروید:

/etc/csf/csfwebmin.tgz

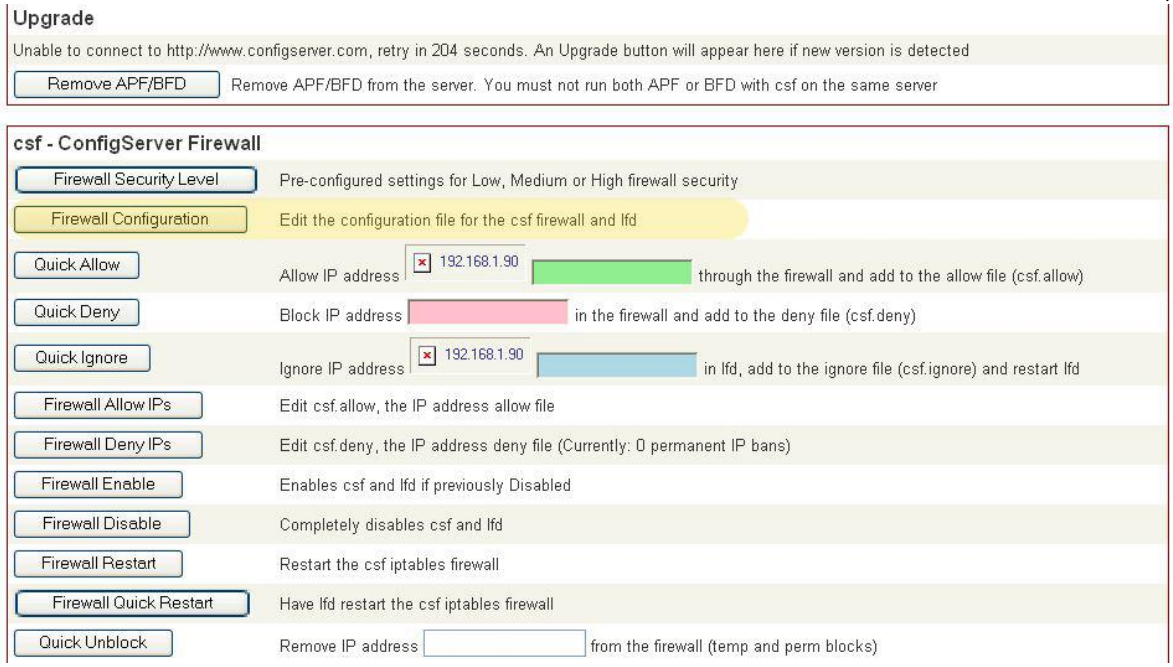


حال بروی install module کلیک کنید و همه موارد را به صورت default رها کنید. پس از تکمیل این فرایند به زیر مجموعه system یک قسمت جدید به نام config server security & firewall اضافه خواهد شد.

بروی ان کلیک کنید.

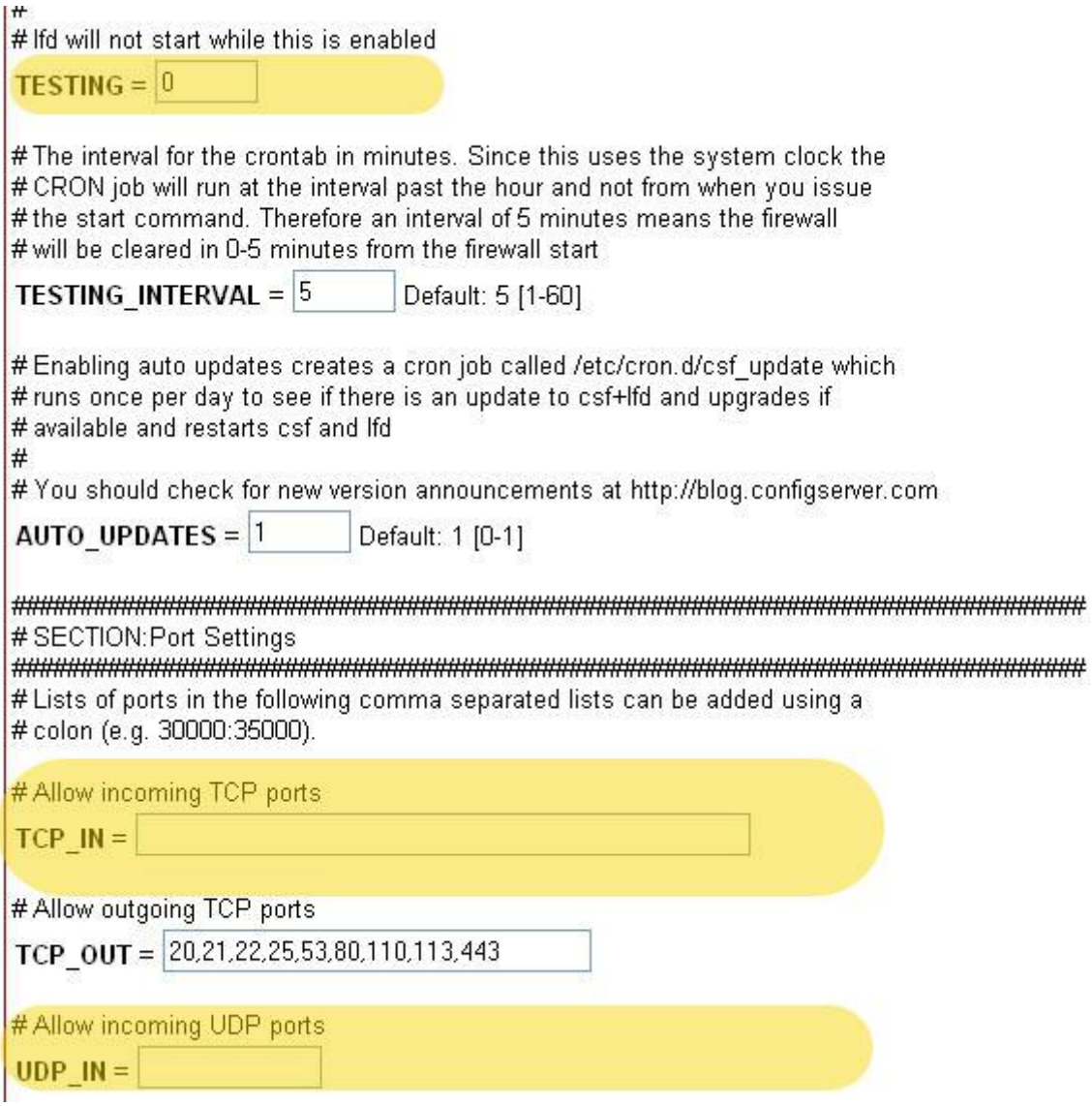


قسمت Firewall configuration را پیدا کنید، در این قسمت می خواهیم تنظیمات مربوط به firewall ان را انجام دهیم:

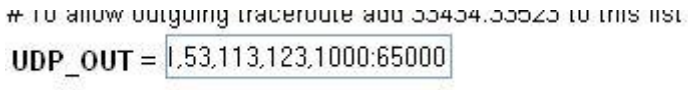


قسمت testing را برابر صفر می گذاریم؛ تا firewall از حالت test به حالت اجرایی ببریم.

UDP-in و TCP-in را پاک کرده تا همه ی کاربران را در حالت عادی از ورود به سیستم منع کنیم تا زمانی که ip مورد قبول ما را داشته باشند:



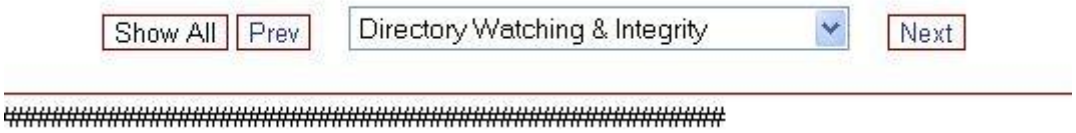
در قسمت UDP-out پورت های 10000:65000 را اضافه می کنیم، البته نگران نباشید تا زمانی که شما اجازه ندهید این پورت ها بسته اند.



اگر از dynDNS برای Remote extension با ip داینامیک استفاده می کنید بخش Dyndns را روی 300 تنظیم کنید، این امر باعث می شود تا تغییرات ادرس توسط firewall چک شود.

همچنین DynDNS-IGNORE=1 قرار دهید؛ اگر نمی خواهید تنظیمات اضافی بروی DNS انجام دهید با قرار دادن 1 در این بخش به ان می رسید:

به بخش directory watching integrity بروید:



تمام option های این بخش را disable کنید (صفر بگذارید) تا به ازای هر alert به شما email فرستاده نشود(در صورت فعال بودن، ایمل های بیشماری به شما ارسال می شود).

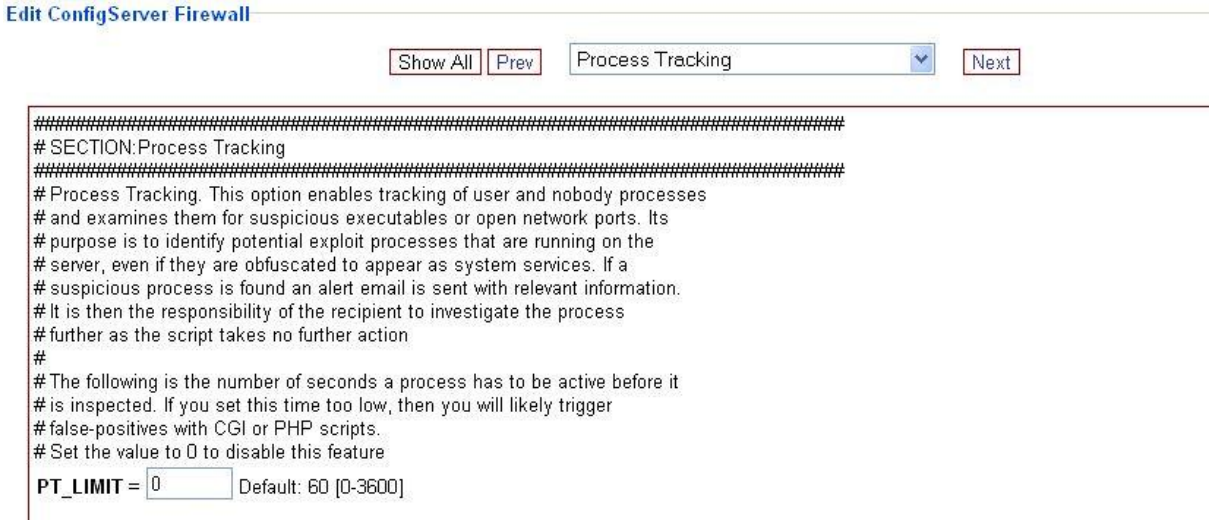
LF_DIRWATCH = 0 Default: 300 [0 or 30-86400]

# To remove any suspicious files found during directory watching, enable the
# following. These files will be appended to a tarball in
# /etc/csf/suspicious.tar
LF_DIRWATCH_DISABLE = 0 Default: 0 [0-1]

This option allows you to have lfd watch a particular file or directory for
changes and should they change and email alert using watchalert.txt is sent
#
To enable this feature set the following to the checking interval in seconds
(a value of 60 would seem sensible) and add your entries to csf.dirwatch
#
# Set to disable set to "0"
LF_DIRWATCH_FILE = 0 Default: 0 [0 or 30-86400]

System Integrity Checking. This enables lfd to compare md5sums of the
servers OS binary application files from the time when lfd starts. If the
md5sum of a monitored file changes an alert is sent. This option is intended
as an IDS (Intrusion Detection System) and is the last line of detection for
a possible root compromise.
#
There will be constant false-positives as the servers OS is updated or
monitored application binaries are updated. However, unexpected changes
should be carefully inspected.
#
Modified files will only be reported via email once.
#
To enable this feature set the following to the checking interval in seconds
(a value of 3600 would seem sensible). This option may increase server I/O
load onto the server as it checks system binaries.
#
# To disable set to "0"
LF_INTEGRITY = 0 Default: 3600 [0 or 120-86400]

در قسمت process tracking ؛ PT-limit را صفر بگذارید:



در اخر change را در پایین صفحه فشار دهید و سپس restart csf+lfd را:

```
LOCALINPUT  all opt -- in !lo out *  0.0.0.0/0  -> 0.0.0.0/0

...Done.

Restarting lfd...

Stopping lfd:[FAILED]
[  OK  ]
Starting lfd:[  OK  ]

...Done.
```

حال تمام ارتباطات با سرور شما قطع شده.

برای برقراری ارتباط:

روش 1):

از کنسول لینوکس خود به مسیر /etc/csf/csf.allow رفته و ip شبکه خو را در ان تایپ کنید:

```
###############################################################################
# Copyright 2006-2012, Way to the Web Limited
# URL: http://www.configserver.com
# Email: sales@waytotheweb.com
###############################################################################
# The following IP addresses will be allowed through iptables.
# One IP address per line.
# CIDR addressing allowed with a quaded IP (e.g. 192.168.254.0/24).
# Only list IP addresses, not domain names (they will be ignored)
#
# Advanced port+ip filtering allowed with the following format
# tcp/udp|in/out|s/d=port|s/d=ip
# See readme.txt for more information
#
# Note: IP addressess listed in this file will NOT be ignored by lfd, so they
# can still be blocked. If you do not want lfd to block an IP address you must
# add it to csf.ignore
192.168.1.0/24
_


^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

و سپس به csf.ignore رفته و شبکه خود را در ان قرار دهید، تا این ip را چک نکند:

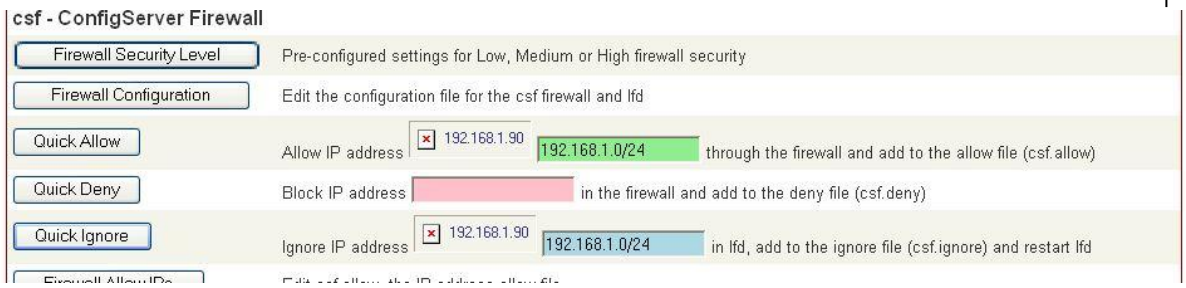
```
###############################################################################
# Copyright 2006-2012, Way to the Web Limited
# URL: http://www.configserver.com
# Email: sales@waytotheweb.com
###############################################################################
# The following IP addresses will be ignored by all lfd checks
# One IP address per line
# CIDR addressing allowed with a quaded IP (e.g. 192.168.254.0/24)
# Only list IP addresses, not domain names (they will be ignored)
#

127.0.0.1
192.168.1.0/24
```

روش2)

در همان اولین مرحله در config server security & Firewall بخش Allow ip address را پیدا کنید و شبکه خود را در ان قرار دهید.

ودر بخش ignore ip address نیز همین طور:



تنظیمات دیگر هم در csf وجود دارد که در مقاله ای دیگر به ان میپردازیم.

حرف اخر

امنیت الزام یک شبکه است. اما همیشه این جمله را فراموش نکنید؛ امنیت همانند خمیر نان است به اندازه در مشت شما باید فشرده شود ، اگر محکم تر این خمیر را بگیرید از هم متلاشی می شود ((نقل قول از استاد حسین شاملو)).

بسیاری از روش هایی که در این مقاله گفته شد تکرار روش قبلی بوده ، پس به چند روش بسنده کنید.

اگر عمری بود ؛ مقاله ای درباره ی VPN و CSF به طور کامل تر و اجرایی تری می نویسم.

امید است این نوشته مورد توجه شما قرار گیرد.

موفق و پیروز باشید

امین نجفی

تابستان 91

Najafi.L.Amin@gmail.com