کاوا ارتباطات هوشمند

Asterisk & Elastix Security

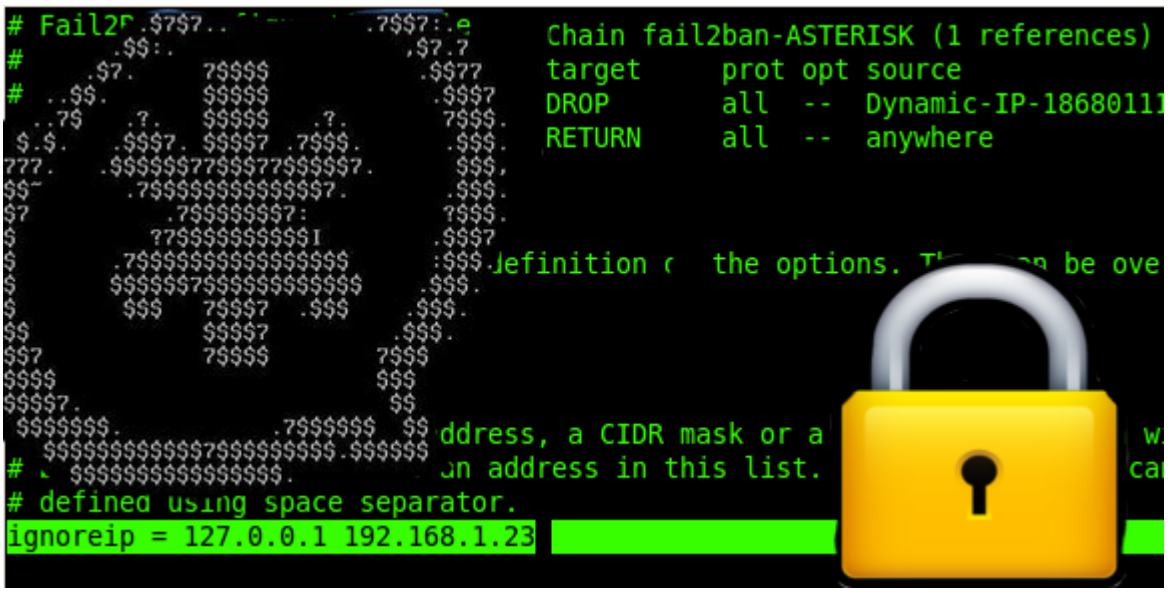
کاوا ارتباطات هوشمند

ارتباطات یکپارچه صوت ، تصویر ، دیتا

www.KavaTelecom.com

www.voipshop.ir

فهرست مطالب



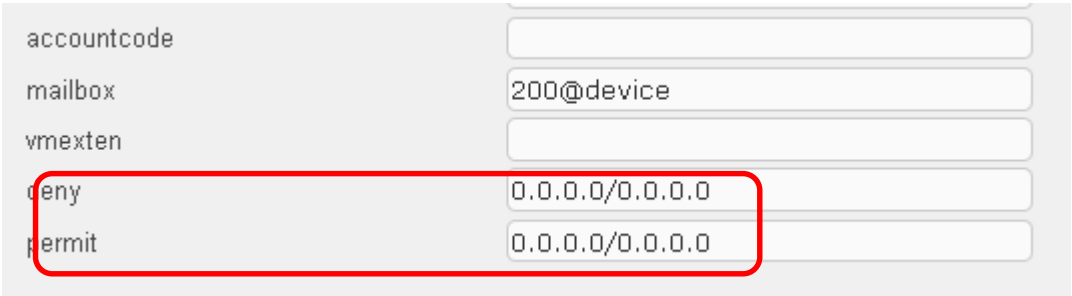
امنیت در استریسک و الستیکس

برای اینکه امنیت بیشتری را برای سیستم تلفنی سازمان خود فراهم کنید بهتر است نکات زیر را مد نظر قرار دهید.

۱ – عدم پذیرش درخواست Authentication از همه IP ها

با استفاده از "Permit=" و "Deny=" در Sip.conf تنها به زیر مجموعه ای از آی پی های مجاز در شبکه خود اجازه دسترسی دهید.

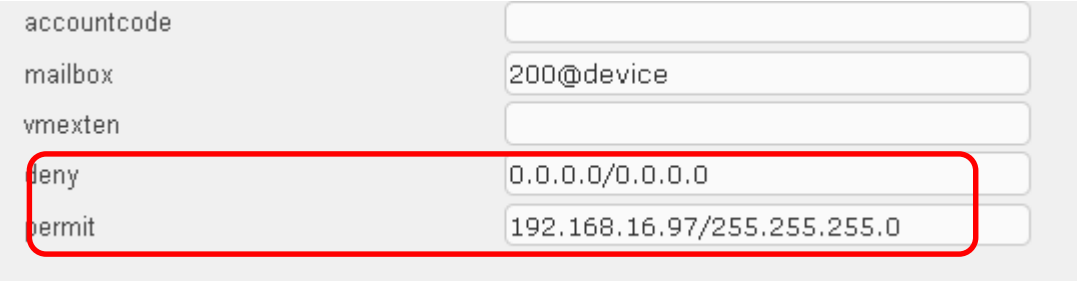
در الستیکس این مقادیر را در بخش extensions می توانید تنظیم کنید.



در صورتی که تنظیمات به صورت بالا باشد همه آی پی ها امکان رجیستر کردن این داخلی را دارند.

برای اینکه محدود کنید چه آی پی هایی امکان رجیستر کردن این داخلی را داشته باشند به صورت زیر تنظیم کنید.

Deny=0.0.0.0/0.0.0.0 همه آی پی ها را رد می کند و permit تنها این آی پی را مورد پذیرش قرار می دهد.



۲- "alwaysauthreject" در sip.conf

مقدار پیش فرض این متغیر no است. با قرار دادن این متغیر برابر با yes درخواست های bad authentication با username صحیح همانند usernameهای اشتباه reject می شوند.(attacker متوجه نخواهد شد username اشتباه است یا رمزعبور)

در الستیکس این مقدار را می توانید در بخش unembeded Freepbx و در Asterisk SIP setting به صورت زیر تنظیم کنید:

۳- تعریف رمز عبورهای قوی برای اکانتهای SIP

برای تعریف رمز عبور برای داخلی های کاربران از رمز عبورهای complex استفاده کنید. به طوری که toolهایی که برای کشف رمز عبور هستند نتوانند به سادگی رمز را بدست آورند.

٤- بلاک پورت های AMI Manager

متغییر های "permit= " و "deny= " را در manager.conf فقط برای IP هایی که نیاز به استفاده ازین پورت ها دارند باز کنید. پسورد AMI را نیز به صورت complex انتخاب کنید.

٥- تفکیک شماره داخلی و sip username

در صورتی که شماره داخلی ۱۲۳۴ را برای کاربری انتخاب کرده اید SIP user را برای مثال به صورت ترکیبی از آدرس MAC تلفن کاربر+ شماره داخلی انتخاب کنید.

٦- امنیت context [default]

به تماس گیرندگانی که unauthenticated هستند اجازه دسترسی به هیچ context ای را ندهید. تنها به تعداد معدودی از کاربران اجازه دسترسی به کانتکست default را بدهید. با تنظیم متغییر "allowguest =no" در بخش [general] در sip.conf اجازه دسترسی را محدود کنید.

در الستیکس این بخش را می توانید در asterisk SIP setting به صورت زیر تنظیم کنید:

تنظیمات فایروال

پس از پیاده سازی کامل سرور تلفنی الستیکس فراهم نمودن امنیت برای سرور تلفنی یکی از گام های مهم در توسعه سیستم های تلفنی است.

برای محدود کردن دسترسی ها به سیستم تلفنی پیشنهاد می شود دسترسی به پورت های SSH و SIP و HTTP و HTTPS را تنها برای آدرس های آی پی که مجاز می دانید باز بگذارید.

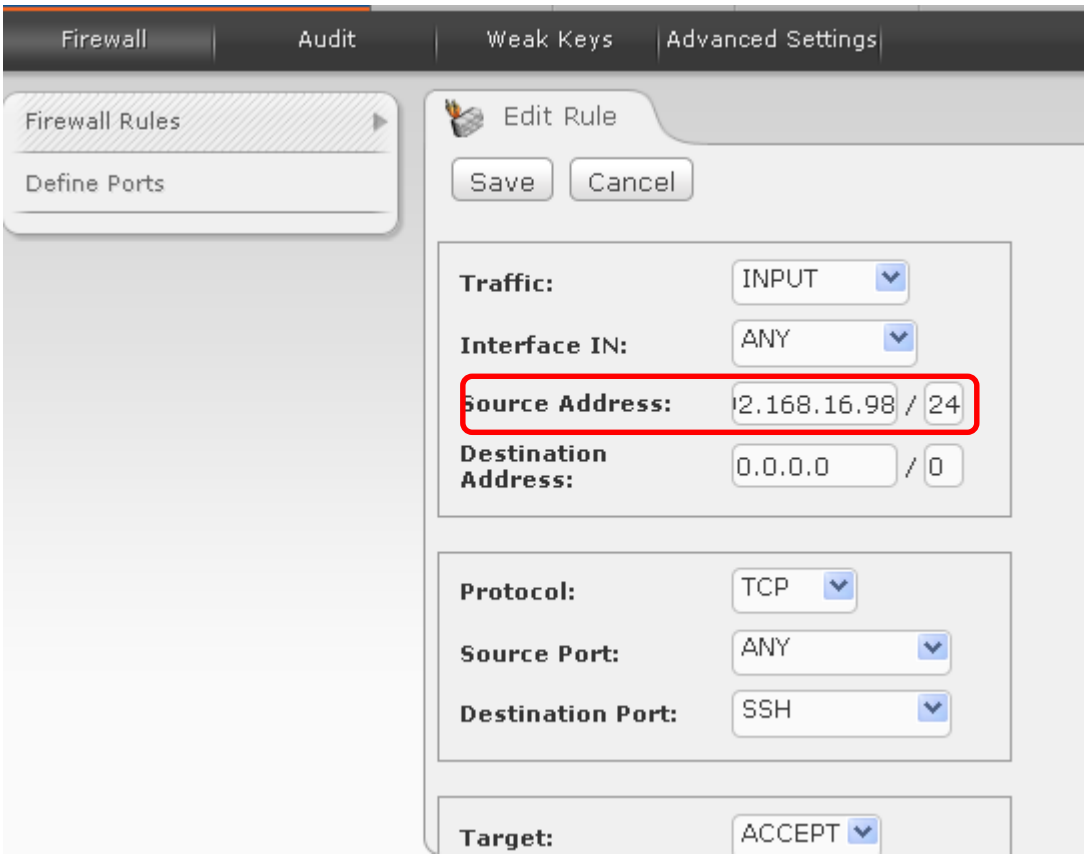
1. پورت SSH

برای اینکه تعیین کنید کدام یک از آدرس های آی پی امکان دسترسی به SSH به سرور شما را داشته باشند باید مراحل زیر را دنبال کنید:

وارد بخش security در الستیکس شوید. در بخش firewall میتوانید Rule های مختلف را مشاهده کنید. یکی از این قوانین مربوط به پورت SSH است.

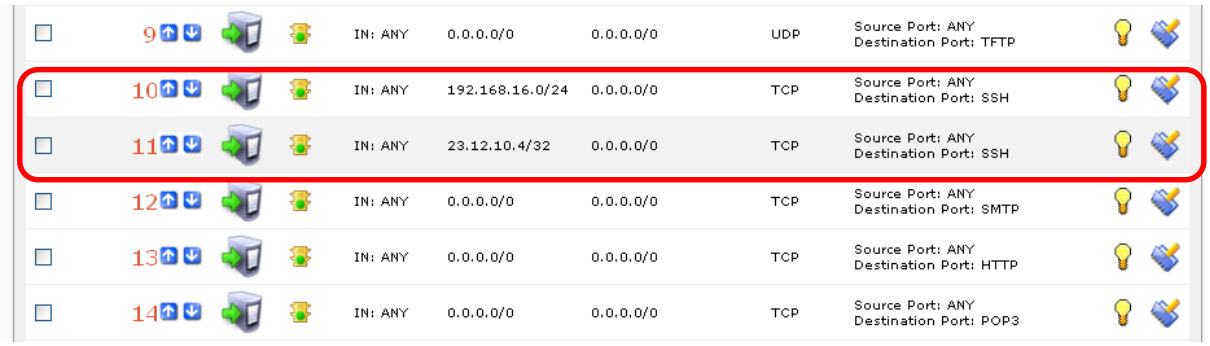
☐	4		IN: ANY	0.0.0.0/0	0.0.0.0/0	UDP	Source Port: ANY Destination Port: IAX	
☐	5		IN: ANY	0.0.0.0/0	0.0.0.0/0	UDP	Source Port: ANY Destination Port: IAX1	
☐	6		IN: ANY	0.0.0.0/0	0.0.0.0/0	UDP	Source Port: ANY Destination Port: SIP	
☐	7		IN: ANY	0.0.0.0/0	0.0.0.0/0	UDP	Source Port: ANY Destination Port: 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	

با edit کردن این بخش می توانید دسترسی به پورت SSH را تنها به یک آی پی و یا رنج آی پی های دلخواه خود بدهید.



مشاهده می کنید که در این مثال به رنج آی پی 192.168.16.xxx امکان دسترسی به پورت SSH داده شده است.

در صورتی که بخواهید دو رنج آی پی external و Internal برای دسترسی به پورتSSH تعیین کنید باید یک Rule جدید ایجاد کنید:

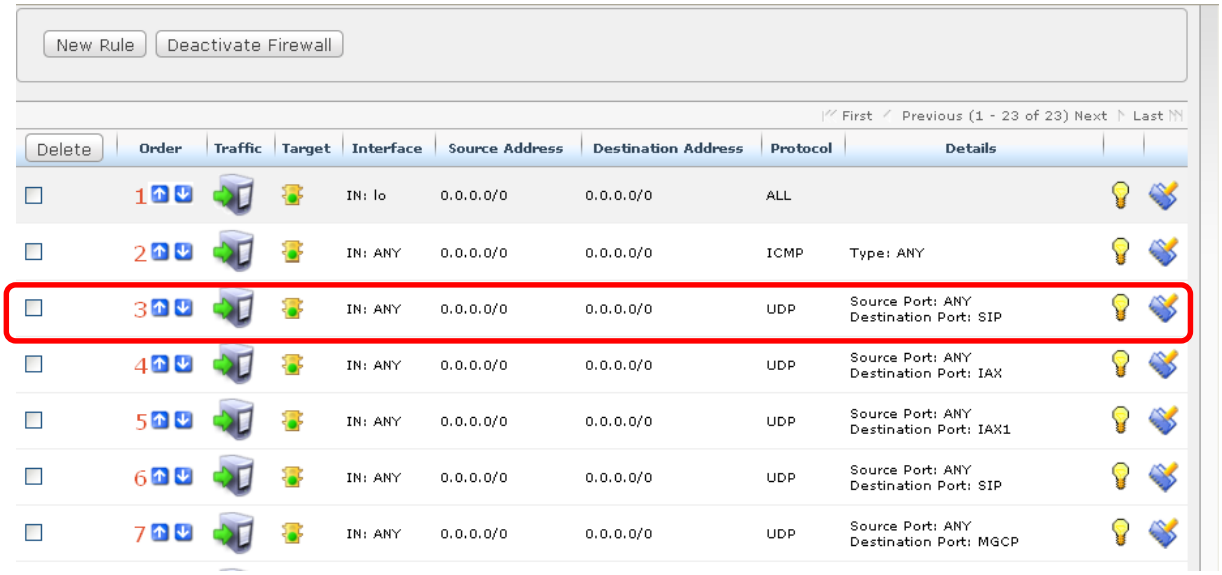


در نمونه بالا مشاهده می کنید که رنج آی پی اینترنال 192.168.16.xxx و آی پی اکسترنال 23.12.10.4 به پورت SSH دسترسی خواهند داشت.

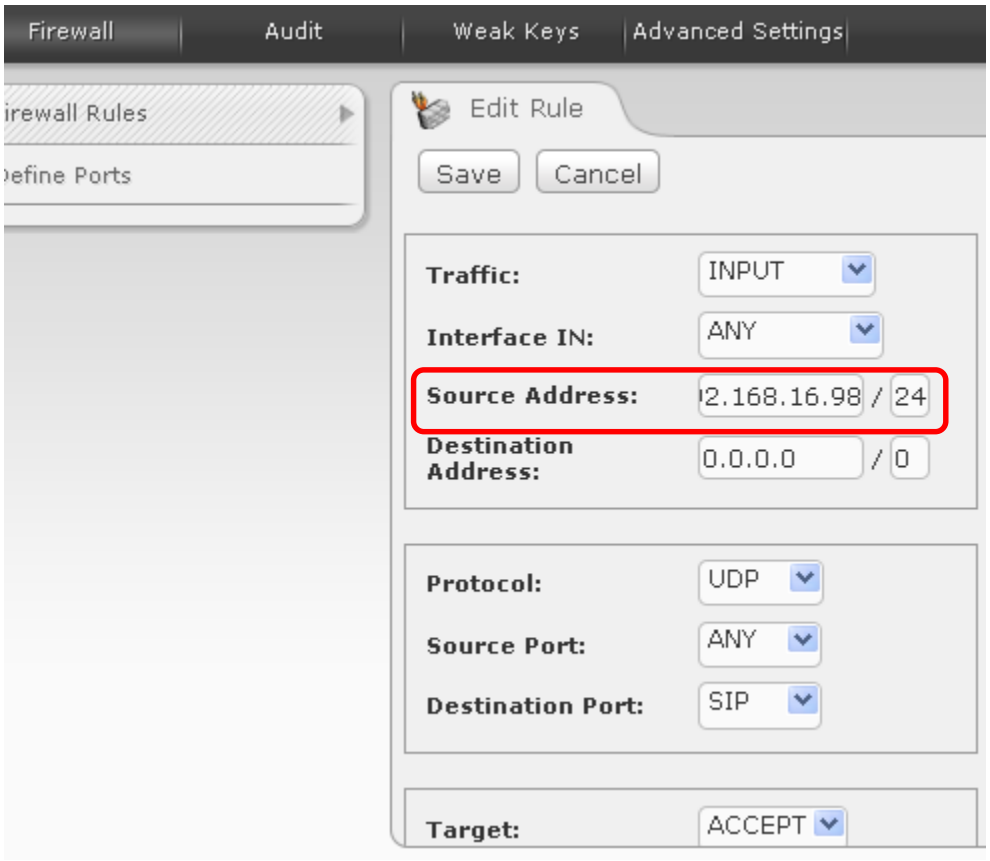
2. پورت SIP

گام بعدی محدود کردن پروتکل SIP است. چرا که با انجام این کار امکان رجیستر شدن دیوایس های آی را پی در سیستم تلفنی خود کنترل خواهید کرد.

در Rule های موجود قانونی که مربوط به SIP است را بیابید تا آن را edit کنید:



در این مورد نیز مانند مثال قبل می توانید دسترسی به پورت SIP را به رنج آی پی های دلخواه خود محدود کنید.در این مثال دسترسی به پورت SIP را تنها به آدرس های آی پی رنج 192.168.16.xxx داده ایم.



3. پورت HTTPS

در صورتی که می خواهید دسترسی به صفحه وب سیستم تلفنی الستیکس را محدود به یک آدرس آی پی کنید باید قانون مربوط به پورت https را تنظیم کنید.

در مثال زیر تنها آدرس آی پی 192.168.16.98 به صفحه وب سرور دسترسی خواهد داشت.