الزامات امنیتی نصب و راه‌اندازی دستگاه Yeastar MyPBX

ساعیان ارتباط

علاوه بر امکانات و قابلیت‌هایی تلفنی که دستگاه‌های MyPBX فراهم می‌کنند، این محصول دارای امکانات امنیتی مناسبی می‌باشد، که سیستم تلفنی شما را تا در برابر بسیاری از حملات و سوء استفاده‌های رایج، محافظ می‌کند. در جدول زیر نحوه بکارگیری این امکانات امنیتی، لیست شده است.

ردیف	الزام امنیتی	توضیحات
۱	تغییر رمز عبور پیش‌فرض واسط کاربری	رمز عبور پیش‌فرض برای کاربر Admin، password می‌باشد و لازم است در بخش System->System Preferences -> Password Settings، با یک رمز عبور قوی، جایگزین شود.
۲	غیرفعال کردن SSH	در صورتی که نیاز به دسترسی به دستگاه از طریق پروتکل SSH ندارید، لازم است تا از طریق System->Lan Settings ، این پروتکل را غیرفعال نمایید.
۳	تغییر پورت پیش‌فرض SSH	در صورتی که نیاز اساسی به دسترسی از طریق پروتکل SSH دارید، توصیه می‌شود تا پورت پیش‌فرض آن را از طریق System->Lan Settings تغییر دهید.
۴	تغییر رمز عبور پیش‌فرض SSH	رمز عبور پیش‌فرض SSH برای کاربر root، ys123456 می‌باشد و لازم است تا از طریق SSH به دستگاه و اجرای دستور passwd، رمز عبور کاربر root را تغییر دهید.
۵	تغییر پورت پیش‌فرض واسط وب (HTTP)	در صورتی که لازم است تا به GUI دستگاه از خارج شبکه محلی، متصل شوید، لازم است تا پورت پیش‌فرض HTTP را از طریق PBX->Basic Settings->General Preferences->HTTP Bind Port تغییر دهید.
۶	تغییر پورت پیش‌فرض پروتکل SIP	برای در امان ماندن دستگاه از حملات امنیتی بر روی پورت پیش‌فرض ۵۰۶۰ پروتکل SIP، لازم است تا از طریق PBX->Advanced Settings->SIP Settings->General->UDP Port این مقدار را تغییر دهید.
۷	غیر فعال کردن ارتباط تلفنی غیر مجاز	برای در امان ماندن دستگاه از حملات امنیتی و برقراری تماس‌های غیرمجاز، لازم است تا از طریق PBX->Advanced Settings->SIP Settings->Advanced Settings ، مقدار Allow Guest را به No تغییر دهید.
۸	تغییر رمز عبور داخلی های پیش‌فرض	لازم است تا رمز عبور داخلی‌های SIP که به صورت پیش‌فرض بر روی این دستگاه تعریف شده‌اند، با مقادیری که از لحاظ امنیتی، ترکیب قدرتمندی داشته باشند، جایگزین گردد. این مهم باید برای داخلی‌های جدیدی که تعریف می‌شوند نیز اعمال گردد.

۹	غیر فعال کردن مجوز رجیستر از راه‌دور	در صورتی که کاربران راه‌دور (Remote) ندارید، لازم است تا گزینه Register Remotely را در تنظیمات داخلی، غیر فعال نمایید.
۱۰	فعال سازی تنظیمات IP Restriction	به جهت محدود کردن دسترسی داخلی‌ها، می‌توان گزینه IP Restriction را برای هر داخلی فعال کرد و آدرس مجاز را برای آن‌ها، تعریف کرد.
۱۱	فعال سازی Firewall	به جهت محدود کردن هر گونه دسترسی غیر مجاز به دستگاه MyPBX و سوء استفاده از ارتباطات تلفنی، فعال سازی Firewall و تعریف رول‌های صحیح در آن، الزامی است. از طریق بخش System->Security Settings->Firewall Rules->Enable Firewall می‌توان Firewall داخلی دستگاه را فعال ساخت. پس از فعال سازی، لازم است تا حداقل رول‌های زیر تعریف شوند: ۱- رول دسترسی به پروتکل SIP برای شبکه داخلی ۲- رول دسترسی به GUI ۳- رول دسترسی به SSH (در صورت نیاز) در صورت نیاز به سایر دسترسی‌ها، باید رول مربوط به آن تعریف شود. توصیه می‌شود، گزینه Drop All را فعال نمایید تا از ورود تمامی ترافیک‌های غیرمجاز، جلوگیری شود.
۱۲	فعال سازی IP Blacklist	توصیه می‌شود تا به منظور افزایش بیشتر امنیت دستگاه، گزینه IP BlackList را از طریق System->Security Settings->IP Blacklist فعال نموده و رول‌های مورد نیاز را تعریف نمایید. این قابلیت با بررسی تعداد درخواست‌های دریافتی، در صورتی که میزان آن‌ها از حد مجاز بالاتر رود، آدرس IP ارسال کننده درخواست را، در لیست سیاه قرار می‌دهد.

رعایت موارد امنیتی فوق، تا حد قابل توجهی امنیت دستگاه‌های IP-PBX را در برابر حملات امنیتی، تامین کرده و هرگونه سوء استفاده از آن‌ها را کاهش می‌دهد؛ اما جهت برقراری سطح بالایی از امنیت، در شرایطی که این دستگاه در محیط اینترنت، در دسترس قرار داده می‌شود و ارتباط با نقاط دیگر و یا کاربران، از طریق یک بستر عمومی همچون اینترنت، صورت می‌پذیرد، پیشنهاد می‌گردد که تجهیزاتی با عنوان Session Border Controller (SBC)، که در نقش فایروال شبکه VoIP عمل می‌کنند، بکار گرفته شود.