پیشنهاد راهکار

سیاست‌گذار تکامل‌یافته پیامک

(PA-Evolved SMS Policy Enforcer)

مهر ۱۴۰۰

پیشنهاد راهکار: سیاست‌گذار تکامل‌یافته پیامک (PA-Evolved SMS Policy Enforcer)

شرکت پیام‌افزار پیک‌آسا

www.peykasa.ir

ایران، تهران، محله تیموری، خیابان شهید غیبعلی محمدزاده (هشتم)، کوچه اتکا، پلاک۷، برج فناوری بنتک

تلفن: ۰۲۱-۶۴۰۶۳۱۰۱

دورنگار: ۰۲۱-۶۶۰۰۷۷۷۰

فهرست

۱. مقدمه

راهکار سیاست‌گذار تکامل‌یافته پیامک شرکت پیک‌آسا، محصولی با فناوری نوین روز است که امکان مدیریت، پایش، فیلترینگ و اعمال سیاست بر روی ترافیک پیامک درون/بین اپراتوری را در اختیار متولیان امر قرار می‌دهد. این راهکار در نگاه کلان مشتمل بر دو زیرسیستم است که یکی از آن‌ها پس از یکپارچه شدن با مرکز پیام اپراتوری، در حوزه ترافیک پیامک درون اپراتوری به ایفای نقش می‌پردازد و دیگری با قرار گرفتن در لبه شبکه، به انجام عملیات بر روی ترافیک بین اپراتوری می‌پردازد.

زیرسیستم اول با حوزه عملکرد ترافیک درون اپراتوری که به اختصار کلیف خطاب می‌شود، نرم افزار جامع مبتنی بر وب است که با برقراری ارتباط با مراکز راه‌اندازی شده خدمات پیام کوتاه در شبکه، امکان کنترل و مدیریت متمرکز فیلترینگ و نظارت قانونی برخط و غیربرخط مراکز سرویس‌ها شرایطی را، جهت پیش‌گیری از هرگونه سوءاستفاده احتمالی، فراهم می‌آورد.

زیرسیستم دوم با حوزه عملکرد ترافیک بین اپراتوری که Home Router خطاب می‌شود، راه حلی برای نظارت و کنترل بر روی پیام‌های کوتاه ارسال‌شده از اپراتورهای دیگر به مشترکین خانگی اپراتور است. این زیرسیستم به عنوان بخشی از راه حل مسیریابی مجتمع پیام‌های کوتاه ورودی به اپراتور و نظارت و کنترل بر روی آنها و با رعایت توصیف فنی 3GPP TR 23.840 و نیازمندی‌های توصیف شده در مستندات GSMA (IR.71 و IR.82) طراحی و ساخته شده است. توضیح آنکه در توصیف اولیه استانداردهای 3GPP، پیام‌های کوتاه ارسال شده از اپراتورهای دیگر به مشترکین اپراتور خانگی در کنترل مرکز ارسال کننده پیام کوتاه قرار دارد و اپراتور مقصد نمی‌تواند کنترل یا نظارتی بر روی آنها داشته باشد. این وضعیت می‌تواند مشکلات فنی و امنیتی برای اپراتور مقصد به همراه داشته باشد. به عنوان مثالی از مشکلات فنی، در سناریوی رومینگ یعنی هنگامی که مشترک خانگی اپراتور از یک اپراتور دیگر (VPLMN) سرویس می‌گیرد، اگر اپراتور ارسال کننده پیام کوتاه با اپراتور سرویس دهنده (VPLMN) قرارداد تبادل پیام کوتاه نداشته باشد، عملا پیام‌های کوتاه ارسال شده به مشترک نمی‌تواند تحویل گردد و این در حالی است که اپراتور خانگی و اپراتور ارسال کننده قرارداد تبادل پیام کوتاه دارند. علاوه بر مشکلات فنی، با مطرح شدن مخاطرات، حملات و آسیب‌هایی که می‌تواند از درگاه تعبیه شده برای تحویل پیام‌های کوتاه ارسال شده توسط اپراتورهای دیگر به مشترکین خانگی به وجود بیاید (مستند GSMA IR.70)، نقش سیستم نظارت و کنترل بر روی این درگاه نیز پررنگ تر گردیده است. تمامی این نیازمندی‌ها توسط ماژول Home Router پیک‌آسا مرتفع می‌گردند.

مستند پیش رو به عنوان پیشنهاد راهکار سیاست‌گذار تکامل‌یافته پیامک جهت ارائه به شرکت ارتباطات آرین‌تل آماده گردیده است و شامل توصیفی سطح بالا از معماری و اجزای سیستم به همراه لیست قابلیت‌ها آن است که به همراه پیشنهاد بازرگانی مربوطه در قالب یک سند واحد تنظیم شده است.

۲. معرفی شرکت پیک‌آسا

شرکت پیک‌آسا با بیش از ۱۶ سال سابقه درخشان، یکی از پیشگامان ارائه خدمات نوین حوزه فناوری اطلاعات و ارتباطات در ایران است. دارا بودن بیش از ۵۰ سایت عملیاتی برای اپراتورهای مخابراتی نظیر اپراتور همراه اول (MCI)، شرکت مخابرات ایران (TCI)، شرکت ارتباطات زیرساخت (TIC)، ایرانسل(MTN)، رایتل، اپراتورهای مجازی و نیز ارائه خدمات متنوع به بیش از ۸۰ میلیون مشترک تلفن همراه و خط ثابت، پیک‌آسا را به یکی از بزرگ‌ترین شرکت‌های فعال در صنعت ایران بدل کرده است.

فعالیت‌های پیک‌آسا در حوزه راهکارها در سه حوزه ذیل قابل طبقه‌بندی است:

- **راهکارهای مخابراتی**: شرکت پیک‌آسا اولین و تنها تولیدکننده مرکز پیام کوتاه (SMSC) در ایران است که سال‌ها در شبکه اپراتور اول کشور مورد بهره‌برداری قرار می‌گرفت. متعاقبا در سال ۱۳۹۲، پیک‌آسا مراکز پرظرفیت SMSGW خود را به بازار ارائه نمود که تاکنون بخش بزرگی از ترافیک A2P موجود در شبکه همراه اول را تبادل نموده است. زیرساخت‌های پیامکی (SMS Center/Gateway، SMS Router و SMS Hub)، تجزیه‌وتحلیل سیگنالینگ، سرویس‌های مدیریت رومینگ، سرویس‌های مدیریت تماس، سیستم‌های مدیریت امنیت و جلوگیری از تقلب، زیرساخت اعمال قوانین بر ترافیک شبکه، زیرساخت سرویس‌های مبتنی بر مکان و پلتفرم‌های ارائه سرویس‌های ارزش‌افزوده از جمله راهکارها و محصولات شرکت پیک‌آسا در حوزه مخابراتی است.
- **راهکارهای هوشمندسازی**: راهکارهای هوشمندسازی شرکت پیک‌آسا به دنبال پاسخگویی به نیازهای نوظهور بازار و همگام بودن با روندی جهانی است که از آن با نام تحول دیجیتال یاد می‌کنند. دو روند فناورانه روز دنیا مشتمل بر راهکارهای کلان‌داده‌ای و اینترنت اشیاء در این حوزه طبقه‌بندی می‌شوند. واحد تولید راهکارهای پردازش کلان‌داده‌ها در فروردین سال ۱۳۹۳ و با هدف ارایهٔ خدمات و محصولات مبتنی بر دانش داده‌ها فعالیت خود را آغاز نمود. استفاده از نیروی انسانی متخصص و مجرب، بهره‌گیری از امکانات سخت‌افزاری و نرم‌افزاری به‌روز، برنامه‌ریزی منسجم و نیز، بهره‌گیری از بهترین رویه‌ها در حوزهٔ دانش داده‌کاوی و فناوری‌های کلان‌داده‌ای سبب شد تا این واحد به رشد و نمو مستمر خود ادامه دهد. هم‌اکنون واحد تولید راهکارهای پردازش کلان‌داده‌ها با توسعه پنج محصول مشخص و عرضه آن به صنعت کشور توانسته است به موفقیت‌های شگرفی دست یافته و خود را برای تامین نیازمندی‌های نوظهور مهیا سازد. در حوزه اینترنت اشیاء نیز پیک‌آسا

با ارائه ساختار ابری، پلتفرم M2M و همچنین سامانه تجمیع‌کننده آماده سرویس‌دهی به کسب-وکارهای مربوطه است. بر همین مبنا، پیک‌آسا خود نیز با ورود به لایه‌های عمودی، راهکارهای نوآورانه‌ای ذیل چتر خانه هوشمند، کشاورزی هوشمند و شهر هوشمند ارائه داده است. به عنوان نمونه، راهکار «مدیریت هوشمند موجودی شبکه ذخیره‌سازی غلات» که توسط این مجموعه توسعه یافته است، توسط معاونت علمی و فناوری ریاست جمهوری به عنوان طرح کلان ملی ثبت گردیده و در حال پیاده‌سازی در کل کشور است.

- **راهکارهای نوآوری کسب‌وکار**: راهکارهای نوآوری کسب‌وکار شرکت پیک‌آسا با اتخاذ رویکردی جامع، باعث بهبود تجربه کاربری مشتریان، ارتقای کیفیت سرویس و تعریف خدمات نوآورانه می-گردد. سیستم صدور یکپارچه صورت‌حساب، سیستم خدمات مشتریان، سیستم گزارش‌گیری هوشمند، سیستم مدیریت کاربران، سیستم مدیریت وفاداری، سیستم پاسخ‌دهی صوتی تعاملی، سیستم مدیریت خطا و کیف پول الکترونیکی از جمله محصولات موجود در سبد کاری پیک‌آسا در این حوزه هستند. این شرکت برای ارائه خدمات مخابراتی به منظور اندازه گیری رضایت مشتری در طول چرخه زندگی مشتری و ایجاد ، ارائه و نظارت بر خدمات مختلف بر اساس خواسته‌های آنها، چشم انداز پرنده‌ای را ارائه می‌دهد.

علاوه بر حوزه راهکارها، نام‌های تجاری زیر نیز ذیل مجموعه پیک‌آسا تعریف و در حال ارائه خدمت هستند:

- **آسانک**: پیک‌آسا به عنوان تامین‌کننده انحصاری پلتفرم ارائه سرویس از سوی مخابرات تهران، سرویس‌های ارزش افزوده تلفن ثابت و بازاریابی دیجیتال خود را تحت نام تجاری آسانک به بازار عرضه می‌نماید. پنل آسانک، سامانه‌ای تحت وب برای ارسال و دریافت پیامک از طریق اینترنت، با شماره تلفن ثابت و پیش‌شماره ۰۲۱و ۰۲۶ می‌باشد. متقاضی می‌تواند پس از ثبت نام در آسانک و فعال کردن شماره تلفن ثابت خود بر روی آن، به صورت انبوه، پیامک، ارسال و یا دریافت نماید. فعال‌سازی این سرویس و کاربری آن، هیچ ارتباطی به خط تلفن ثابت کاربر نداشته و در زمان استفاده از پنل، آن را اشغال نمی‌نماید.
- **پَکپی**: ارائه نوآوری‌های فناورانه در ارائه خدمات مالی یکی از خطوط مشی شرکت پیک‌آسا می‌باشد. نوآوری در خدمات مالی شامل انواع خدمات مختلفی از جمله خدمات پرداخت قبوض و انتقال پول، سرمایه‌گذاری، خدمات وام و بیمه می‌شود. این خدمات به خودی خود خدمات جدیدی نیستند

و همواره چنین خدماتی به شیوه‌های گوناگون ارائه می‌شدند. لیکن پیک‌آسا با به کارگیری فناوری روز و استفاده از زیرساخت‌های دیجیتالی باعث تسهیل و کارامد شدن فرآیندهای مربوطه شده‌اند. پس از سه سال تجربه در زمینه ارائه خدمات درگاه پرداخت به کسب و کارهای دیجیتال، پیک‌آسا فعالیت خود در حوزه فینتک را با نام تجاری پَکپِی (Packpay) تجاری‌سازی نموده است. پکپی درگاه متمرکز روش‌های مختلف پرداخت اعم از پیش‌پرداخت و پس‌پرداخت است که از طریق آن و تنها با عقد یک قرارداد می‌توانید درگاه‌های پرداخت بانکی، اپراتورهای تلفن همراه، و تلفن ثابت را همراه با یک کیف پول آماده را در اختیار داشته باشید. پیاده‌سازی در کوتاهترین زمان، یک قرارداد و تعامل با یک تیم پشتیبانی، سهولت و تنوع پرداخت برای کاربران، ترکیب مدل‌های نرخ‌گذاری و ابزارهای قدرتمند تحلیل فروش از جمله قابلیت‌هایی است که پکپی در اختیار می‌گذارد. لازم به ذکر است که پکپی پرداخت‌یار رسمی شاپرک و بانک مرکزی است.

- **آفرینک**: سرویس تماشای آنلاین فیلم، کارتون، و انیمیشن برای گروه کودک و نوجوان، با نام آفرینک و با شعار "می‌بینی، می‌خندی و سرگرم می‌شوی" مشغول به فعالیت است. این سرویس بر پایه پلتفرم ویدیوی مبتنی بر تقاضای توسعه یافته توسط شرکت پیک‌آسا بنا نهاده شده که بستری امن برای نگهداری محتوا و ارایه آن با کیفیت بالا به مشتریان نهایی است. پس از بارگذاری محتوا، پلتفرم آن را به صورت خدمات ابری یا سرورهای خصوصی برای نمایش در سطح اینترنت و گجت‌های مختلف عرضه می‌کند.

- **زیست‌بوم مجازی درسا**: زیست بوم مجازی درسا با ارائه محتوای مفید و جذاب در حوزه‌های مختلف از قبیل آموزش، تفریح و سرگرمی و سلامت، شرایط استفاده از فضای مجازی سالم را برای کودک و نوجوان مهیا می‌سازد. از سوی دیگر، والدین این امکان را پیدا می‌کنند تا با تعریف محدوده ارتباطی فرزندان، فضای امن و قابل اطمینانی را برای ارتباطات صوتی و پیامکی آن‌ها به ارمغان آورند. درسا بازار، دنیای درسا، اینترنت درسا، پرسا و خدمات ارزش افزوده از جمله سرویس‌های پشتیبانی‌شونده در این زیست بوم است.

با توجه به سوابق ذکر شده در بالا و همچنین استناد به آیین‌نامه رتبه‌بندی و احراز صلاحیت شرکت‌های انفورماتیکی، پیک‌آسا دارای گواهی معتبر انفورماتیک در رشته‌های زیر می‌باشد:

- مشاوره و نظارت بر اجرای طرح‌های انفورماتیک، فناوری‌های اطلاعات و ارتباطات: رتبه ۱

- سیستم‌های ویژه: رتبه ۱
- تولید و پشتیبانی نرم‌افزارهای سفارش مشتری: رتبه ۱
- خدمات پشتیبانی: رتبه ۱
- امنیت فضای تولید و تبادل اطلاعات: ۲
- شبکه داده‌های رایانه‌ای و مخابراتی: ۲
- ارائه و پشتیبانی نرم‌افزارهای پایه، سیستم و ابزارها: ٤
- ارائه و پشتیبانی بسته‌های نرم‌افزاری یا بسته‌های نرم‌افزاری حامل محتوا: ٥

در انتها لازم به ذکر است که تجربه ارزشمند سال‌ها فعالیت مرتبط، منجر به ایجاد شناخت دقیق پیک‌آسا از صنعت فناوری اطلاعات و ارتباطات در ایران شده است؛ شناختی که نتیجه آن انعطاف پذیری و دانش فنی لازم برای ارائه بهترین خدمات به مشتریان و شرکای تجاری بوده است. با عنایت به این پشتوانه بر این باوریم همکاری با آن مجموعه محترم، باعث هم‌افزایی متقابل و سرمنشاء اثرات مثبت در کسب‌وکار طرفین خواهد بود.

۳. زیرسیستم اول: کلیف

۳,۱ لیست سفید

اگرچه با توجه به روند رو به گسترش توسعه شبکه تلفن همراه در جامعه، و استفاده هرچه بیشتر از امکانات مختلف تبادل اطلاعات در شبکه تلفن همراه همچون ارسال پیام کوتاه، استفاده از سیستم‌های نظارتی چون نرم‌افزار کلیف مورد نیاز هر شبکه تلفن همراه می‌باشد، اما در میان مشترکین تلفن همراه مشترکینی هستند که بر اساس قوانین امنیتی موجود با توجه به ملاحظات امنیتی، قانون مصونیتی را برای اجرای سیاست-های نظارتی کنترل و نظارت و تهیه گزارش از تبادلات پیام کوتاه، برای این دست از مشترکین و رومرهای فعال در شبکه تعریف نموده است. شماره تلفن همراه این دسته از مشترکین در نرم افزار کلیف، با عنوان لیست سفید شناخته می‌شوند و هیچ یک از سیاست‌های مختلف نظارتی تعریف شده در نرم افزار کلیف همچون نظارت برخط و غیربرخط، فیلترینگ (ارسال/دریافت پیام) و ... آنها در شبکه بر روی این شماره‌ها اجرا نمی‌شوند.

أ. مدیریت لیست سفید

برای مدیریت لیست سفید و امکان بهره‌برداری از قابلیت مصون کردن برخی شماره‌های خاص از عملیات کنترلی و نظارتی، در بخش راهبری سیستم، زیر درخت مدیریت شماره‌های قرار گرفته در لیست سفید سیستم با عنوان لیست سفید در نظر گرفته شده است. مدیریت لیست سفید امکان تعریف و فعالسازی یک شماره سفید را به مدیر کلیف می‌دهد، تا از این طریق مدیر بتواند شماره‌های موردنظر خود را از کلیه عملیات نظارتی و کنترلی مصون بدارد. همچنین در صورت عدم نیاز به ادامه مصونیت شماره‌های خاص، غیرفعالسازی و حذف شماره سفید در بخش مدیریت لیست سفید، امکان پایان این فرایند را در اختیار مدیر قرار می‌دهد. مدیریت لیست سفید شامل موارد زیر است:

- مشاهده لیست سفید
- جستجو در لیست سفید
- تعریف شماره سفید
- فعال‌سازی شماره سفید
- غیرفعال‌سازی شماره سفید

- حذف شماره سفید
- ویرایش شماره سفید

ب.مشاهده لیست سفید

مدیر می‌تواند کلیه شماره‌های سفید تعریف شده در سیستم را مشاهده کند. اطلاعاتی که به ازای هر شماره سفید در این بخش نمایش داده می‌شود، در جدول زیر توصیف شده است:

جدول ۱- مشخصه‌های شماره سفید در لیست سفید

نام پارامتر	توصیف
Phone Number	شماره تلفن همراه شماره سفید موردنظر – این مورد به صورت لینک در اختیار کاربر قرار داده می‌شود که کاربر از طریق آن می‌تواند مشخصات کامل شماره سفید موردنظر را مشاهده نموده و در صورت نیاز تغییر دهد.
Description	برچسب موردنظر مدیر برای توصیف و شناسایی شماره سفید معرفی شده
Activation State	وضعیت کلی شماره سفید تعریف شده در نودها
Activate	لینک فعالسازی شماره سفید موردنظر
Deactivate	لینک غیرفعالسازی شماره سفید موردنظر
Activation Detail	لینک مشاهده جزئیات فعالسازی شماره سفید موردنظر به ازای هر یک از نمونه نودهای فعال تعریف شده در سیستم

ج. تعریف شماره سفید

تعریف شماره سفید در واقع به منزله هویت دادن و شناساندن سوژه موردنظر به سیستم است. کاربر باید مشخصات موردنیاز برای تعریف شماره سفید را مقداردهی کند. این مشخصات در جدول زیر توصیف شده است:

جدول ۲- مشخصه‌های تعریف شماره سفید

نام پارامتر	توصیف	نوع مقداردهی
Phone Number	شماره تلفن سفید موردنظر	اجباری
Label	برچسب موردنظر مدیر برای شناسایی شماره سفید	اختیاری

در صورت صحت اطلاعات و تکراری نبودن شماره در لیست سفید، شماره مذکور به لیست سفید افزوده می‌گردد. تعریف یک شماره سفید به منزله مصونیت آن از اعمال عملیات کنترل و نظارت در سیستم نیست. برای اعمال مصونیت، باید شماره سفید موردنظر را در سیستم فعال کرد.

د. فعال‌سازی/غیر فعال‌سازی شماره سفید

برای اعمال مصونیت یک شماره سفید از عملیات نظارت و کنترل، باید پس از تعریف شماره سفید، آن را در مراکز سرویس فعال کرد. همچنین برای خاتمه مصونیت شماره سفید، باید شماره سفید فعال موردنظر در سیستم غیرفعال شود. قابل توجه است که شماره سفید غیرفعال، در لیست سفید تعریف شده در سیستم باقی می‌ماند و در صورت نیاز، مدیر می‌تواند در آینده آن را دوباره فعال یا در صورت عدم نیاز حذف نماید. امکان فعالسازی/غیرفعالسازی شماره سفید به دو روش در اختیار مدیر قرار گذاشته شده است:

- فعال‌سازی/غیرفعال‌سازی گروهی لیست سفید
- فعال‌سازی/غیرفعال‌سازی موردی شماره سفید

۳,۲ لیست محدود

امکان مدیریت تعداد پیام‌های کوتاه از سوی مشترکین شبکه در یک بازه زمانی خاص یکی از سیاست‌های قابل استفاده در کلیف می‌باشد. در این حالت لیستی از شماره تلفن‌های مشترکین و رومرهای فعال در شبکه که دارای محدودیت ارسال پیام کوتاه در بازه زمانی مشخص هستند، قابل تعریف می‌باشند. برای هر شماره تلفن در این لیست، حداکثر تعداد پیام قابل ارسال توسط مشترک در بازه زمانی مشخص، تعیین می‌شود. سیستم به‌گونه‌ای طراحی شده است که مجموع تمام پیام‌های ارسال شده توسط فرستنده موردنظر در لیست محدود، شمارش می‌شود، تا از حد مجاز در بازه زمانی مشخص شده بیشتر نگردند. در صورت تجاوز تعداد پیام‌های اعضای لیست محدود از تعداد تعیین‌شده برای وی در لیست محدود، مرکز سرویس از ارسال این پیام‌های ارسالی جدید به گیرنده آن خودداری خواهد نمود.

أ. مدیریت لیست محدود

برای مدیریت لیست محدود و امکان بهره‌برداری از تعریف محدودیت برای شماره‌های خاص، در بخش راهبری سیستم زیر درخت مدیریت شماره‌های قرار گرفته در لیست محدود سیستم، با عنوان لیست محدود در نظر گرفته شده است. مدیریت لیست محدود امکان تعریف و فعالسازی محدودیت برای شماره‌های خاص را به مدیر کلیف می‌دهد. همچنین در صورت عدم نیاز به این محدودیت، غیرفعالسازی و حذف محدودیت در بخش مدیریت لیست محدود، امکان پایان این محدودیت را در اختیار مدیر قرار می‌دهد. مدیریت لیست محدود شامل موارد زیر است:

- مشاهده لیست محدود
- جستجو در لیست محدود
- تعریف محدودیت
- فعال‌سازی محدودیت
- غیرفعال‌سازی محدودیت
- حذف محدودیت
- ویرایش محدودیت

ب.مشاهده لیست محدود

مدیر می‌تواند کلیه محدودیت‌های تعریف شده در سیستم را مشاهده کند. اطلاعاتی که به ازای هر محدودیت در این بخش نمایش داده می‌شود، در جدول زیر توصیف شده است:

جدول ۳- مشخصه‌های محدودیت در لیست محدود

نام پارامتر	توصیف
Restricted Number	شماره تلفنی که محدودیت موردنظر باید روی آن اعمال شود – این مورد به عنوان شناسه محدودیت، به صورت لینکی در اختیار کاربر قرار داده می‌شود که کاربر از طریق آن می‌تواند مشخصات کامل محدودیت موردنظر را مشاهده نموده و در صورت نیاز تغییر دهد.
Activation State	وضعیت کلی محدودیت تعریف شده در نودها
Activate	لینک فعالسازی محدودیت موردنظر

Deactivate	لینک غیرفعالسازی محدودیت موردنظر
Activation Detail	لینک مشاهده جزئیات فعالسازی محدودیت موردنظر به ازای هر یک از نمونه نودهای فعال تعریف شده در سیستم

ج. تعریف محدودیت

تعریف محدودیت در واقع به منزله هویت دادن و شناساندن محدودیت موردنظر به ازای یک شماره خاص به سیستم است. کاربر باید مشخصات موردنیاز برای تعریف محدودیت را مقداردهی کند. این مشخصات در جدول زیر توصیف شده است:

جدول ٤– مشخصه‌های تعریف شماره محدودیت

نام پارامتر	توصیف	نوع مقداردهی
Restricted Number	شماره تلفنی که محدودیت موردنظر روی آن تعریف می‌شود.	اجباری
Description	توصیف محدودیت موردنیاز مدیر	اختیاری
Max SMS Count	حداکثر تعداد کوته‌پیامی که شماره موردنظر در یک روز می‌تواند ارسال کند.	اجباری
نوع مسدود شدن پیام کوتاه	در صورت تجاوز تعداد پیام‌های کوتاه ارسال شده توسط شماره موردنظر از تعداد تعیین شده، پیام‌های ارسالی بعدی مسدود خواهند شد. این پارامتر نحوه ارسال Ack به فرستنده پیام را در حالتی که پیام کوتاه موردنظر وی مسدود خواهد شد را مشخص می‌کند.	اجباری

در صورت صحت اطلاعات و تکراری نبودن شماره در لیست محدود، شماره مذکور به این لیست افزوده می‌گردد. اما تعریف یک محدودیت به منزله آغاز اعمال آن روی شماره تعیین شده نیست. برای اعمال محدودیت، باید محدودیت موردنظر را در سیستم فعال کرد.

د. فعال‌سازی/غیر فعال‌سازی محدودیت

برای اعمال محدودیت تعداد کوته‌پیام‌های قابل ارسال توسط یک شماره خاص، باید پس از تعریف محدودیت، آن را در مراکز سرویس فعال کرد. همچنین برای خاتمه اعمال این محدودیت، باید

محدودیت موردنظر در سیستم غیرفعال شود. قابل توجه است که محدودیت غیرفعال، در لیست محدود تعریف شده در سیستم باقی می‌ماند و در صورت نیاز مدیر می‌تواند در آینده آن را دوباره فعال یا در صورت عدم نیاز حذف نماید. امکان فعالسازی/غیرفعالسازی محدودیت به دو روش در اختیار مدیر قرار گذاشته شده است:

- فعال‌سازی/غیرفعال‌سازی گروهی لیست محدودیت
- فعال‌سازی/غیرفعال‌سازی موردی محدودیت

۳,۳ فیلترینگ پیام‌ها

نظارت بر پیام‌های کوتاه ارسالی در شبکه تلفن همراه و امکان انجام فیلترینگ روی پیام‌های مختلف بر اساس شرایط موردنظر، یکی از سیاست‌های مهم قابل اجرا در امر تبادل پیام کوتاه در شبکه تلفن همراه می‌باشد. فیلترینگ به عملی گفته می‌شود که طی آن کاربر مجاز سیستم می‌تواند با معرفی مشخصات پیام کوتاه غیرمجاز، از ارسال پیام‌های کوتاه تطبیق یافته در مراکز خدمات پیام کوتاه جلوگیری به عمل آورد. برای معرفی پیام‌های غیرمجاز و تعیین نحوه جلوگیری و مدیریت ارسال آنها، قوانین فیلترینگ در سیستم کلیف مورد استفاده قرار می‌گیرند. در تنظیم و تعریف قوانین فیلترینگ ویژگی‌های مختلف پیام کوتاه، شامل شماره فرستنده و گیرنده پیام کوتاه، محتوای پیام، اپراتور ارسال کننده و گیرنده، زمان ارسال پیام کوتاه و مکان حضور مشترک تلفن همراه در شبکه مورد استفاده قرار می‌گیرد؛ در صورت تطبیق شرایط قوانین فیلترینگ با پیام کوتاه ارسال شده، سرنوشت پیام کوتاه حالت‌های مختلفی چون بلوکه کردن، تغییر محتوای پیام، تأخیر و حتی جایگزینی آن با پیام کوتاه هشدار دهنده به گیرنده پیام کوتاه در قوانین فیلترینگ خواهد بود. امکان دریافت و مشاهده برخط پیام‌های کوتاه فیلتر شده، امکان دریافت اعلان هشدار فیلتر پیام به صورت صوتی و یا در قالب پیام کوتاه هشدار، امکان اطلاع یافتن مشترک فرستنده از فیلتر شدن پیام، طبقه‌بندی قوانین بنا به موضوع آنها و امکان مدیریت و جستجو آنها از جمله امکانات پیش‌بینی شده در نرم افزار کلیف می‌باشد.

أ. مدیریت قوانین فیلترینگ

برای مدیریت قوانین فیلترینگ و بهره‌برداری از قابلیت نظارت بر محتوا و مشخصات پیام‌های کوتاه در شبکه و ممانعت و تغییر مکانیزم ارسال پیام‌های کوتاه غیرمجاز، در بخش راهبری سیستم زیر درخت مدیریت قوانین فیلترینگ به عنوان یکی از بخش‌های زیردرخت فیلترینگ در نظر گرفته شده است. امکانات تعبیه شده در بخش مدیریت فیلترینگ امکان تعریف و فعال‌سازی قوانین فیلترینگ مختلف بر اساس محتوا، مشخصات زمانی و مکانی پیام کوتاه، دسته‌بندی قوانین مشابه و مرتبط به یکدیگر، استفاده از گروه شماره مشترکین و کلمات چند شکلی در تعریف قوانین و امکان مشاهده اعلان پیام کوتاه‌های تطبیق یافته در سیستم را برای مدیر کلیف فراهم نموده است، تا از این طریق مدیر بتواند بر جریان پیام‌های کوتاه ارسال شده در شبکه نظارت داشته باشد. همچنین در صورت عدم نیاز به هریک از قوانین فیلترینگ، غیرفعالسازی و حذف قوانین در این بخش، برای پایان اجرای قوانین فیلترینگ در اختیار مدیر قرار داده شده است. مدیریت قوانین فیلترینگ در سیستم شامل موارد زیر می‌باشد:

- مشاهده لیست قوانین
- جستجو در لیست قوانین
- تعریف قانون فیلترینگ
- فعال‌سازی قانون فیلترینگ
- غیرفعال‌سازی قانون فیلترینگ
- حذف قانون فیلترینگ
- ویرایش قانون فیلترینگ
- دسته بندی قوانین
- رصد و مانیتور اعلان‌های فیلترینگ
- مشاهده و جستجوی کلیه اعلان‌های فیلترینگ به صورت غیربرخط
- مشاهده حضور شماره‌های فرستنده و گیرنده در توصیف قوانین فیلترینگ

ب. مشاهده لیست قوانین

مدیر می‌تواند کلیه قوانین تعریف شده در سیستم را مشاهده کند. اطلاعاتی که به ازای هر قانون در این بخش نمایش داده می‌شود، در جدول زیر توصیف شده است:

جدول ۵- مشخصه‌های قانون در لیست قوانین فیلترینگ

نام پارامتر	توصیف
Clif Name	شناسه کلیفی **که قانون** فیلترینگ در آن تعریف شده است.
Name	نام تعیین شده به عنوان شناسه برای قانون فیلترینگ
Service Center Type	نوع مرکز سرویس که قانون فیلترینگ روی پیام‌های کوتاهی که از طریق آن دسته از مرکز سرویس مبادله می‌شوند، اعمال می‌شود.
Rules Count	تعداد قوانین منفردی که قانون فیلترینگ موردنظر شامل آنهاست.
Activation State	وضعیت کلی قانون فیلترینگ تعریف شده در نود(مراکز سرویس)ها (با توجه به نوع نود انتخاب شده در زمان تعریف قانون فیلترینگ)
Description	توصیف قانون فیلترینگ موردنظر
Location Base	مشخص کننده اینکه قانون فیلترینگ به مکان‌های شبکه حساس است یا نه. در واقع اینکه پیام‌ها بر اساس مکان فرستنده/گیرنده خود فیلتر می‌شوند یا نه.
Activation Detail	لینک مشاهده جزئیات فعالسازی قانون فیلترینگ موردنظر در هر یک از مراکز سرویس فعال و موجود از نوع مرکز سرویسی که قانون فیلترینگ روی آن تعریف شده است

ج. تعریف قانون فیلترینگ

تعریف قانون فیلترینگ در واقع به منزله هویت دادن و شناساندن قانون موردنظر به سیستم است. کاربر باید مشخصات موردنیاز برای تعریف قانون فیلترینگ را مقداردهی کند. مشخصه‌های موردنیاز برای تعریف یک قانون فیلترینگ به سه دسته تقسیم می‌شوند.

دسته اول شامل مشخصه‌های کلی قانون است. توصیف پارامترهای مربوط به این دسته در جدول زیر آمده است:

جدول ٦- مشخصه‌های عمومی تعریف قانون فیلترینگ

نام پارامتر	توصیف	وضعیت مقداردهی
Name	نام منحصربفرد قانون فیلترینگ	اجباری

Description	توصیف قانون فیلترینگ	اختیاری
Category	دسته‌ای که قانون فیلترینگ در آن قرار می‌گیرد. انتخاب دسته در واقع برای دسته‌بندی موضوعی قوانین مورد استفاده قرار می‌گیرد برای مقداردهی به این پارامتر یکی از دسته‌های موجود در سیستم باید انتخاب شود.	اختیاری
Service Center Type	نوع مرکز سرویس که قانون تعریف شده باید روی آن اعمال شود. می‌تواند یکی از مقادیر *SMSC*، *FSMS* یا *Inter PLMN Mediator* و یا *Intra* PLMN Mediator باشد	اجباری

دسته دوم مشخصه‌های قانون با عنوان "اگر" (IF) شناخته می‌شود. در این دسته در واقع شرایط مدنظر مدیر برای قانون توصیف می‌شود و در صورت رخداد شرایط در یک پیام، قانون فیلترینگ با آن متناظر می‌شود. پارامترهای مورد استفاده در این بخش، در رابطه AND با همدیگر قرار می‌گیرند. توصیف پارامترهای مربوط به این دسته در جدول زیر آمده است:

جدول ۷- مشخصه‌های IF قانون فیلترینگ

نام پارامتر	توصیف	وضعیت مقداردهی
Sender Address	آدرس فرستنده پیام- می‌تواند به یکی از روش‌های Exact یا "آدرس دقیق"، Prefix یا "پیشوندی" و Contain یا "در میانه عبارت" تعیین شود. محتوای این فیلد نیز می‌تواند به صورت دستی توسط مدیر مقداردهی شده یا از لیست گروه شماره تلفن-های تعریف شده در سیستم انتخاب شود.	اختیاری
Sender MSC	آدرس اپراتور ارسال کننده پیام- می‌تواند به یکی از روش‌های Exact یا "آدرس دقیق"، Prefix یا "پیشوندی" و Contain یا "در میانه عبارت" تعیین شود. در صورتی که مدیر Sender Location را به عنوان یکی از شرایط فیلترینگ انتخاب کرده باشد، نمی‌تواند آدرس اپراتور فرستنده را نیز مقدادهی کند.	اختیاری
Sender Location	مکان فرستنده پیام- در صورتی که مدیر Sender MSC را به عنوان یکی از شرایط فیلترینگ انتخاب کرده باشد، نمی‌تواند مکان فرستنده را نیز مقدادهی کند. مکان فرستنده با دو مقدار LAC و Cell ID شناخته می‌شود که کاربر می‌تواند به صورت آن را به صورت دستی مقداردهی کرده یا از بین مکان‌های تعریف شده در سیستم، انتخاب نماید. در صورت نیاز به انتخاب از بین	اختیاری

	مکان‌های تعریف شده در شبکه، باید ابتدا MSCای که مکان موردنظر در محدوده آن قرار دارد را انتخاب نماید و در مرحله بعد، امکان انتخاب LAC و سپس Cell ID مربوطه در اختیار وی قرار می‌گیرد.	
Reciever Address	آدرس گیرنده پیام- می‌تواند به یکی از روش‌های Exact یا "آدرس دقیق"، Prefix یا "پیشوندی" و Contain یا "در میانه عبارت" تعیین شود. محتوای این فیلد نیز می‌تواند به صورت دستی توسط مدیر مقدادهی شده یا از لیست گروه شماره تلفن-های تعریف شده در سیستم انتخاب شود.	اختیاری
Reciever MSC	آدرس اپراتور دریافت کننده پیام- می‌تواند به یکی از روش‌های Exact یا "آدرس دقیق"، Prefix یا "پیشوندی" و Contain یا "در میانه عبارت" تعیین شود. در صورتی که مدیر Reciever Location را به عنوان یکی از شرایط فیلترینگ انتخاب کرده باشد، نمی‌تواند آدرس اپراتور گیرنده را نیز مقدادهی کند.	اختیاری
Reciever Location	مکان گیرنده پیام- در صورتی که مدیر Reciever MSC را به عنوان یکی از شرایط فیلترینگ انتخاب کرده باشد، نمی‌تواند مکان گیرنده را نیز مقدادهی کند. مکان گیرنده با دو مقدار LAC و Cell ID شناخته می‌شود که کاربر می‌تواند به صورت آن را به صورت دستی مقداردهی کرده یااز بین مکان‌های تعریف شده در سیستم، انتخاب نماید. در صورت نیاز به انتخاب از بین مکان‌های تعریف شده در شبکه، باید ابتدا MSCای که مکان موردنظر در محدوده آن قرار دارد را انتخاب نماید و در مرحله بعد، امکان انتخاب LAC و سپس Cell ID مربوطه در اختیار وی قرار می-گیرد.	اختیاری
Content	مشخصات بدنه پیام کوتاه – محتوای این پارامتر می‌تواند از عباراتی شامل کلماتی به زبان فارسی و انگلیسی تشکیل شده باشد. ویژگیهای در نظر گرفته شده در این کادر عبارتند از: • وجود خط‌فاصله در میان کلمات به معنای رابطه AND محسوب می‌شود. • اصطلاحاتی که در داخل قرار "" بگیرند به صورت واحد در نظر گرفته می‌شوند. • هر کلمه موجود در لیست که با بخشی از کلمات موجود در پیام برابر شود، سیستم پیام مورد نظر را مورد فیلتر قرار می‌دهد. برای مثال در صورت تعریف ab در	اختیاری

	قانون فیلترینگ به عنوان محتوای فیلترینگ، تمام کلماتی که به صورت *ab* باشند با این تعریف مطابقت می‌کنند. در تعریف محتوای قانون فیلترینگ می‌توان از کلمات چندشکلی که قبلاً در سیستم تعریف شده‌اند، استفاده نمود.	

دسته سوم مشخصه‌های قانون با عنوان "آنگاه" (THEN) شناخته می‌شود که شامل عکس‌العمل تعریف شده به ازای پیام‌هایی است که بنا به بخش اگر، با قانون فیلترینگ متناظر و تطبیق داده شده‌اند. با مقداردهی پارامترهای این دسته، در واقع تصمیم‌گیری در خصوص وضعیت پیام‌های تطبیق یافته با قانون انجام می‌شود. اجزای این بخش شامل موارد زیر می‌باشد:

جدول ۸- مشخصه‌های THEN قانون فیلترینگ

نام پارامتر	توصیف	وضعیت مقداردهی
Action	پارامتر اصلی این بخش که رفتار کلیف در قبال پیام‌های منطبق شده با قانون را مشخص می‌کند و می‌تواند یکی از مقادیر زیر را داشته باشد: • Replace: جایگزین کردن پیام • Delay: ارسال با تأخیر • Mask: پنهان کردن بخش‌های تطبیق یافته از محتوای پیام • Block: توقف یا بلوکه کردن پیام	اجباری
Block Action	نحوه عمل توقف پیام کوتاه شبکه تلفن همراه- می‌تواند یکی از مقادیر زیر را داشته باشد: • Don't Send Ack: عدم ارسال پاسخ به فرستنده که به معنای عدم اطلاع فرستنده از متوقف شدن پیام است. در واقع فرستنده گمان می‌کند که پیام در حال ارسال به مرکز سرویس است. • Send Nack: ارسال پاسخ عدم تحویل پیام به مرکز سرویس، که به معنای عدم اطلاع فرستنده از توقف پیام بوده و این تصور پیش می‌آید که ارسال پیام به مرکز سرویس با مشکل مواجه شده و مرکز سرویس نتوانسته است پیام را دریافت کند. در واقع در این حالت فرستنده از عدم ارسال پیام با خبر می‌شود.	در صورت تعیین Block به عنوان Action، اجباری

	• Send Ack: ارسال پاسخ تحویل پیام به مرکز سرویس، در این حالت فرستنده متوجه دریافت پیام توسط مرکز سرویس می‌شود. در صورت انتخاب این گزینه باید در مورد نحوه ارسال گزارش تحویل (Delivery Report) از طریق پارامتر Ack Type تصمیم‌گیری کرد.	
Ack Type	نحوه ارسال گزارش تحویل – می‌تواند یکی از مقادیر زیر را داشته باشد: • Send FDR: فرستنده پیام عدم تحویل به گیرنده را دریافت می‌کند. • Send SDR: فرستنده پیام تحویل به گیرنده را دریافت می‌کند. (فیلترینگ کاملاً بدون اطلاع فرستنده) • Don't Send SDR: فرستنده هیچ پیام تحویل و یا عدم تحویلی دریافت نمی‌کند و در واقع از رسیدن پیام به گیرنده مطلع نمی‌شود.	در صورت تعیین Send Ack به عنوان Ack Type، اجباری
Delay	مدت زمان موردنیاز برای تأخیر ارسال پیام بر حسب ساعت	در صورت تعیین Delay به عنوان Action، اجباری
Send Notification	برای تعیین نیاز به تولید اعلان در صورت تطبیق پیام با قانون فیلترینگ. در این حالت غیر از اعلان تولید شده و قابل مدیریت در قالب Notifications، می‌توان اعلان‌های دیگری نیز دریافت کرد که در پارامتر Notification Type قابل تعیین است.	اختیاری
Notification Type	نحوه تولید اعلان در صورت تطبیق پیام با قانون فیلترینگ، به جز اعلان‌هایی که در قالب Notification قابل مدیریت هستند: • تولید اعلان صوتی (گزینه Play voice alarm): در صورت انتخاب این اعلان، به ازای تطبیق پیام‌های کوتاه با این قانون اعلان صوتی، به صورت پخش بوق انجام می‌شود. در صورت عدم نیاز به پخش این اعلان‌های صوتی امکان قطع اعلان‌های صوتی با انتخاب گزینه Mute در کادر پایین صفحه راهبری سیستم در دسترس می‌باشد. • ارسال پیام کوتاه (گزینه Send SMS): امکان آگاهی	در صورت انتخاب Send Notification، اختیاری

	مدیر سیستم از انطباق قوانین با پیام کوتاه‌های مختلف، به صورت پیام کوتاه با انتخاب گزینه Send SMS میسر می‌باشد. در این حالت با تنظیم گیرنده و زمان ارسال پیام کوتاه که در فایل پیکربندی سیستم انجام می‌شود، تعداد دفعات تطبیق قوانین فیلترینگ که ارسال این اعلان در آنها فعال شده است، با جریان پیام کوتاه ارسال شده در شبکه به تفکیک هر قانون به مدیر سیستم ارسال می‌شود. • ارسال پیام کوتاه هشدار (گزینه Send Warning SMS): امکان اعلام اخطار به فرستنده پیام کوتاه با ارسال پیام کوتاه در خصوص پیام کوتاه ارسالی او. در این حالت با تنظیم پیکربندیهای لازم در بازه زمانی مشخص پیام کوتاه اخطار به فرستنده پیام کوتاه‌های تطبیق یافته ارسال می‌شود.	

د. فعال‌سازی/غیر فعال‌سازی قانون

برای آغاز فیلترینگ پیام‌ها بر اساس قانون تعریف شده، باید پس از تعریف قانون، آن را در مراکز سرویس فعال کرد. همچنین برای پایان کار فیلترینگ پیام‌ها بر اساس یک قانون خاص، باید قانون فعال موردنظر در سیستم غیرفعال شود. قابل توجه است که قانون غیرفعال، در لیست قوانین تعریف شده در سیستم باقی می‌ماند و در صورت نیاز مدیر می‌تواند در آینده آن را دوباره فعال یا در صورت عدم نیاز حذف نماید. امکان فعالسازی/غیرفعالسازی قانون به دو روش در اختیار مدیر قرار گذاشته شده است:

- فعال‌سازی/غیرفعال‌سازی گروهی قوانین
- فعال‌سازی/غیرفعال‌سازی موردی قانون

ه. دسته‌بندی قوانین

به دلیل امکان تعریف قوانین فیلترینگ متعدد در سیستم، کلیف قابلیت دسته‌بندی قوانین را برای مدیر فراهم کرده است. با استفاده از این قابلیت مدیر می‌تواند دسته‌های مختلف قوانین را تعریف کرده و قوانین فیلترینگ موجود را به آنها اختصاص دهد. همچنین مدیر قادر است از این طریق،

وضعیت فعال بودن قوانین یک دسته را در حالت کلی مشاهده نماید. قابل توجه است که هر قانون تنها می‌تواند در یک دسته قرار داده شود.

مدیر کلیف برای استفاده از قابلیت دسته‌بندی قوانین ابتدا باید دسته موردنظر خود را تعریف کند. پس از تعریف یک دسته در کلیف، مدیر می‌تواند قوانین موردنیاز را به آن دسته اختصاص دهد. اختصاص قوانین به دسته‌ها به دو صورت امکان‌پذیر است:

- اختصاص قوانین موجود در سیستم به یک دسته
- اختصاص قانون به یک دسته ضمن تعریف آن قانون

علاوه بر امکان تعریف دسته‌ها امکان مشاهده لیست آنها در اختیار مدیر قرار می‌گیرد. اطلاعاتی که مدیر به ازای هر دسته می‌تواند مشاهده کند، در جدول زیر توصیف شده است:

جدول ۹- مشخصه‌های دسته در لیست دسته‌های فیلترینگ

نام پارامتر	توصیف
Clif Name	شناسه کلیفی که دسته فیلترینگ در آن تعریف شده است.
Name	نام تعیین شده به عنوان شناسه برای قانون فیلترینگ. این نام به صورت لینکی در اختیار مدیر قرار داده شده است، که از طریق آن مدیر امکان مشاهده جزئیات اطلاعات به ازای آن دسته و همچنین تغییر مشخصات آن را خواهد داشت.
Description	توصیف دسته موردنظر
FRS Count	تعداد قوانین فیلترینگ اختصاص داده شده به دسته موردنظر
Activation State	وضعیت کلی فعال بودن دسته فیلترینگ موردنظر که با توجه به وضعیت فعال بودن کلیه قوانین فیلترینگ مشمول در آن تعیین می‌شود.

و. رصد و مانیتور اعلان‌های فیلترینگ

با تعریف قوانین فیلترینگ مختلف و اعلان نیاز به دریافت اعلان‌های فیلترینگ و در نهایت فعال کردن آنها برای مراکز سرویس مختلف تعریف شده در سیستم، امکان دریافت اعلان انطباق و فیلتر شدن پیام‌ها به ازای آن قوانین فراهم می‌شود. در این صورت، امکان مشاهده اعلان‌های دریافت شده به صورت برخط در اختیار مدیر قرار می‌گیرد. در این بخش آخرین اطلاعات و اعلان‌های مربوط به اعمال قوانین روی پیام کوتاه‌های مبادله شده در شبکه، به محض تطبیق آنها با پیام و اعمال عمل

فیلترینگ موردنیاز، بر اساس مجموعه قوانین فعال در لیست قوانین فیلتر سیستم، نمایش داده می‌شود. در زمانی که آخرین اعلان‌های دریافت شده در اجرای جاری مورد نیاز نمی‌باشد، می‌توان برای رکوردهای فعلی موجود در صفحه نمایش اعلان‌ها را حذف نمود. در این حالت امکان تهیه گزارش از این اطلاعات دریافت شده در سیستم، از طریق مشاهده اعلان‌ها به صورت غیربرخط یا جستجوی این اعلان‌ها، در زمان‌های آینده وجود دارد. اما در صورت نیاز به حذف کامل اطلاعات مانیتورینگ دریافت شده قبلی، می‌توان به حذف کامل این اطلاعات از سیستم اقدام نمود. همچنین دسترسی مستقیم به آخرین اعلان اعمال قانون فعال شده بر روی پیام‌های کوتاه مختلف در صفحه نمایش مشخصات آن قانون و انتخاب سربرگ قابل انجام می‌باشد.

ز. مشاهده و جستجوی کلیه اعلان‌های فیلترینگ به صورت بر خط

تولید اعلان تطبیق پیام‌های مبادله شده در شبکه با قوانین فعال در سیستم، یکی دیگر از امکانات موجود در سیستم می‌باشد. قابل توجه است که برای دریافت چنین اعلان‌هایی باید در زمان تعریف قانون، درخواست مورنیاز را به سیستم اعلام کرد. در صورت اعلام نیاز، امکان مشاهده کلیه اعلان‌های دریافت شده به صورت غیربرخط، امکان‌پذیر است. در واقع در این حالت کلیه اعلان‌های موجود در سیستم که تا زمان ارائه درخواست مشاهده، توسط سیستم دریافت شده‌اند در اختیار مدیر قرار می‌گیرند.

همچنین بخش مجزایی برای تهیه گزارش‌های مختلف از اعلان‌های دریافت شده، در دسترس مدیر قرار می‌دهد. در این بخش مدیر قادر است بر اساس پارامترها و جزئیات موجود در محتوای اعلان‌ها، گزارش موردنیاز را خود از اعلانات دریافت شده از شبکه در بازه‌های زمانی مختلف تهیه نماید.

۳,٤ شماره‌های مشترکین

أ. مدیریت گروهی شماره‌های مشترکین

گروه‌های آدرس به عنوان امکانات جانبی بخش مدیریت فیلترینگ، و برای سهولت تعریف قوانین در بخش مدیریت قوانین فیلترینگ ارائه می‌شود. با استفاده از گروه شماره‌ها در واقع امکان دسته‌بندی الگوهای عددی شماره مشترکین مشابه و تسهیل استفاده از مشخصات آنها در تعریف قوانین فیلترینگ مختلف کلیف پیش‌بینی شده است. برای مدیریت گروهی شماره و آدرس مشترکین و رومرها و

امکان بهره‌برداری از آنها در تعریف قوانین فیلترینگ، این قابلیت در بخش راهبری سیستم در دسترس مدیر قرار داده شده است. مدیریت گروه شماره‌ها امکان تعریف، تغییر و یا حذف شماره‌های خاص را گروهی شماره‌ها در اختیار مدیر قرار می‌دهد. مدیریت گروه‌های شماره‌ها شامل موارد زیر است:

- مشاهده گروه شماره‌ها
- جستجو در لیست گروه‌های شماره‌ها
- تعریف گروه شماره‌ها
- حذف گروه شماره‌ها
- ویرایش گروه شماره‌ها

ب.مشاهده گروه‌های شماره

مدیر می‌تواند کلیه گروه‌های آدرس تعریف شده در سیستم را در صفحه "All Phone No Groups" مشاهده کند. اطلاعاتی که به ازای هر گروه آدرس در این بخش نمایش داده می‌شود، در جدول زیر توصیف شده است:

جدول ۱۰- مشخصه‌های یک گروه آدرس در لیست گروه‌های شماره مشترکین

نام پارامتر	توصیف
Clif Name	شناسه کلیفی که گروه آدرس موردنظر را تعریف کرده است
Name	نام گروه آدرس تعریف شده– این مورد به عنوان شناسه، به صورت لینکی در اختیار کاربر قرار داده می‌شود که کاربر از طریق آن می‌تواند مشخصات کامل گروه آدرس موردنظر را مشاهده نموده و در صورت نیاز تغییر دهد.
Number Of Members	تعداد آدرس‌های به کار برده شده در گروه آدرس تعریف شده

ج. تعریف گروه‌های شماره

تعریف یک گروه آدرس در واقع به منزله هویت دادن و شناساندن گروه موردنظر به سیستم است. کاربر باید مشخصات موردنیاز برای تعریف گروه را مقداردهی کند. این مشخصات در جدول زیر توصیف شده است:

جدول ۱۱- مشخصه‌های تعریف گروه گروه‌های شماره مشترکین

نام پارامتر	توصیف	نوع مقداردهی
Name	نام گروه آدرس موردنظر	اجباری
Phone Numbers	لیستی از شماره تلفن‌هایی که در قالب گروه آدرس موردنظر شناخته می‌شوند. شماره‌ها به صورت تک به تک به لیست اضافه شده و قابل حذف هستند.	اختیاری

در صورت صحت اطلاعات و تکراری نبودن نام گروه آدرس در لیست گروه‌های موجود، گروه مذکور به این لیست افزوده می‌گردد. پس از تعریف یک گروه آدرس، مدیر امکان استفاده از آن را در تعریف قوانین فیلترینگ مورد نیاز خود دارد.

۳,۵ کلمات چندریختی

أ. مدیریت کلمات چندریختی

کلمات چند ریختی به عنوان امکانات جانبی بخش مدیریت فیلترینگ، و برای سهولت تعریف قوانین در بخش مدیریت قوانین فیلترینگ ارائه می‌شود. افراد مختلف ممکن است کلمات یکسان را به شکل‌های مختلفی در متن پیام بنویسند. با استفاده از کلمات چند ریختی در واقع امکان تعریف حالت‌های مختلف نوشتاری یک کلمه خاص در قالب یک کلمه چندریختی، و استفاده از آن در تعریف قوانین فیلترینگ بر اساس محتوای پیام، در اختیار مدیر سیستم قرار می‌گیرد. برای مدیریت کلمات چند ریختی و امکان بهره‌برداری از آنها در تعریف قوانین فیلترینگ، این قابلیت در بخش راهبری سیستم، در دسترس مدیر قرار می‌گیرد. مدیریت کلمات چند ریختی امکان تعریف، تغییر و یا حذف کلمات چندریختی خاص را در اختیار مدیر قرار می‌دهد. مدیریت کلمات چند ریختی شامل موارد زیر است:

- مشاهده کلمات چند ریختی
- جستجو در لیست کلمات چند ریختی
- تعریف کلمه چند ریختی
- حذف کلمه چند ریختی
- ویرایش کلمه چند ریختی

ب.مشاهده کلمات چندریختی

مدیر می‌تواند کلیه کلمات چند ریختی تعریف شده در سیستم را مشاهده کند. اطلاعاتی که به ازای هر کلمه در این بخش نمایش داده می‌شود، در جدول زیر توصیف شده است:

جدول ۱۲- مشخصه‌های یک کلمه در لیست کلمات چند ریختی

نام پارامتر	توصیف
Clif Name	شناسه کلیفی که کلمه چندریختی موردنظر را تعریف کرده است
Name	نام کلمه چندریختی تعریف شده— این مورد به عنوان شناسه، به صورت لینکی در اختیار کاربر قرار داده می‌شود که کاربر از طریق آن می‌تواند مشخصات کامل کلمه چندریختی موردنظر را مشاهده نموده و در صورت نیاز تغییر دهد.
Number Of Members	تعداد عبارت‌های به کار برده شده در کلمه چندریختی تعریف شده یا به عبارتی تعداد حالت‌های مختلف کلمه چندریختی موردنظر

ج. تعریف کلمات چندریختی

تعریف یک کلمه چندریختی در واقع به منزله هویت دادن و شناساندن گروه موردنظر به سیستم است. کاربر باید مشخصات موردنیاز برای تعریف کلمه چندریختی را مقداردهی کند. این مشخصات در جدول زیر توصیف شده است:

جدول ۱۳- مشخصه‌های تعریف کلمه چندریختی

نام پارامتر	توصیف	نوع مقداردهی
Name	نام کلمه چندریختی موردنظر	اجباری
Members	لیستی از عبارت‌های به کار برده شده در کلمه چندریختی تعریف شده یا به عبارتی حالت‌های مختلف کلمه چندریختی موردنظر. عبارات به صورت تک به تک به لیست اضافه شده و قابل حذف هستند.	اختیاری

در صورت صحت اطلاعات و تکراری نبودن نام کلمه چندریختی در لیست کلمات، کلمه مذکور به این لیست افزوده می‌گردد. پس از تعریف یک کلمه چندریختی، مدیر امکان استفاده از آن را در تعریف قوانین فیلترینگ مورد نیاز خود دارد.

۳,٦ مکان‌های شبکه

أ. مدیریت مکان‌های شبکه

یکی از امکانات موجود در بخش فیلترینگ، قابلیت تعریف قانون فیلترینگ بر اساس مکان شبکه فرستنده یا گیرنده است. در واقع یکی از شرایطی که ممکن است باعث انطباق پیام با قانون فیلترینگ شود، موقعیت فرد ارسال کننده یا دریافت کننده پیام در شبکه است.

برای استفاده از مکان‌های شبکه در تعریف قانون در واقع باید موقعیت‌های مختلف موجود در شبکه در سیستم شناخته شده و قابل تشخیص و تعیین باشند. مکان‌های شبکه از طریق دو پارامتر اصلی LAC و Cell ID شناخته می‌شوند. این دو پارامتر در واقع مقادیری عددی هستند که در کنار یکدیگر مقدار منحصربفردی را تشکیل می‌دهند و متناظر با موقعیت خاصی در شبکه هستند. از آنجا که تعداد LAC و Cell ID های متناظر با موقعیت‌های مکانی کل شبکه بسیار زیاد است و شناسایی مکان‌ها و استفاده از آنها در تعریف قوانین، از طریق دانستن این مقادیر عددی دشوار است، کلیف امکان مدیریت حجم زیاد اطلاعات مکانی را با افزودن پارامترهای مختلفی که شناسایی این مکان‌ها را ساده‌تر می‌سازند، در اختیار مدیر قرار داده است. برای مدیریت مکان‌های شبکه و امکان بهره‌برداری از آنها در تعریف قوانین فیلترینگ، این قابلیت در بخش راهبری سیستم، در دسترس مدیر قرار می‌گیرد. مدیریت مکان‌های شبکه امکان تعریف مکان‌های مختلف بر اساس استان و مشاهده لیست مکان‌های تعریف شده در شبکه را در اختیار مدیر قرار می‌دهد. مدیریت مکان‌های شبکه شامل موارد زیر است:

- بارگزاری اطلاعات مکانی
- مشاهده لیست مکان‌های شبکه
- جستجو در لیست مکان‌های شبکه

ب.بارگزاری اطلاعات مکانی

از آنجا که تعداد LAC و Cell ID های متناظر با موقعیت‌های مکانی کل شبکه بسیار زیاد است، شناسایی مکان‌ها از طریق دانستن این مقادیر عددی دشوار خواهد بود. از این رو کلیف امکان تعریف مکان‌های مختلف را در سیستم، با استفاده از پارامترهای دیگری در کنار LAC و Cell ID متناظر با موقعیت مکانی، فراهم می‌کند. این پارامترها پس از انجام دسته‌بندی مکان‌ها، به مقادیر عددی LAC و Cell ID معنا و مفهوم می‌بخشند و از این طریق مدیریت مکان‌های شبکه را برای مدیر سیستم ساده‌تر می‌سازند. مشخصات این پارامترها عبارتند از:

- Description: توصیف متنی برای شناسایی بهتر موقعیت مکانی متناظر با LAC و Cell ID
- MSC: آدرس MSC در برگیرنده LAC و Cell ID موردنظر که در واقع دسته‌بندی اولیه‌ای برای موقعیت‌های مکانی ارائه می‌دهد.
- Province: استانی که LAC و Cell ID موردنظر در محدوده آن قرار می‌گیرند. هر استان در واقع شامل تعداد مشخصی MSC و هر MSC به نوبه خود شامل تعدادی LAC و Cell ID است. این پارامتر در واقع دسته‌بندی سطح بالاتری برای مکان‌های شبکه تحت مدیریت کلیف ارائه می‌دهد.

بنابراین کلیه مکان‌ها باید از طریق پارامترهای فوق در کنار LAC و Cell ID متناظر با آنها به سیستم ارائه شوند. کلیف برای مدیریت ساده‌تر مکان‌های شبکه و امکان تعریف حجم اطلاعات بیشتر در قالب یک عمل واحد، امکان بارگزاری مکان‌های شبکه از طریق فایل فراهم می‌کند. فایل موردنظر باید شامل کلیه پارامترهای توصیف شده فوق باشد. از طرفی برای دسته‌بندی بهتر اطلاعات مکانی و همچنین مدیریت مکان‌ها بر اساس استان، هر فایل باید شامل اطلاعات مکانی مختص یک استان باشد. بنابراین بارگزاری اطلاعات مکانی با ارائه اطلاعات زیر به سیستم انجام می‌شود:

جدول ١٤- مشخصه‌های موردنیاز برای بارگزاری اطلاعات مکانی

نام پارامتر	توصیف	نوع مقداردهی
Province	نام استان در بر گیرنده مکان‌های موردنظر	اجباری
File Location	آدرس فایل حاوی اطلاعات مکانی موردنظر	اختیاری

در صورت صحت اطلاعات مکان‌های موجود در فایل مذکور به این لیست افزوده می‌گردد. پس از تعریف مکان‌های جدید شبکه در سیستم، مدیر امکان استفاده از آنها را در تعریف قوانین فیلترینگ مورد نیاز خود دارد.

ج. مشاهده لیست مکان‌های شبکه

مدیر می‌تواند کلیه کلمات مکان‌های شبکه تعریف شده در سیستم را مشاهده کند. از آنجا که تعداد LAC و Cell ID های متناظر با موقعیت‌های مکانی کل شبکه بسیار زیاد است و شناسایی مکان‌ها از طریق دانستن این مقادیر عددی دشوار است، کلیف برای شناسایی هر موقعیت مکانی در سیستم، از پارامترهای دیگری نیز استفاده می‌کند. اطلاعاتی که به ازای هر مکان در این بخش نمایش داده می‌شود، در جدول زیر توصیف شده است:

جدول ۱۵- مشخصه‌های یک مکان در لیست مکان‌های شبکه

نام پارامتر	توصیف
MSC	آدرس MSC در برگیرنده LAC و Cell ID موردنظر
LAC	شماره LAC – این مقدار در کنار مقدار Cell ID متناظر با یک موقعیت منحصر بفرد شبکه است.
Cell ID	شماره Cell ID – این مقدار در کنار مقدار LAC متناظر با یک موقعیت منحصر بفرد شبکه است.
Description	توصیف متنی برای شناسایی بهتر موقعیت مکانی متناظر با LAC و Cell ID
Province	استانی که LAC و Cell ID موردنظر در محدوده آن قرار می‌گیرند.

۳,۷ مراکز سرویس

همانطور که پیشتر در بخش‌های قبلی اشاره گردید، اجرا و فعالسازی سیاست‌های مختلف در بخش-های مختلف، نیازمند حضور مراکز سرویس می‌باشد. با تعریف مراکز سرویس، مدیر سیستم قادر خواهد بود پس از تنظیم سیاست‌های مختلف در زمینه فیلترینگ پیام‌های کوتاه غیرمجاز، لیست سفید شماره‌ها و اپراتورها و لیست سوژه و ... نظارت آفلاین و آنلاین بر پیام‌های کوتاه در شبکه را محقق سازد. بدون حضور و فعالسازی مراکز سرویس استفاده از موارد رد سیستم امکان‌پذیر نمی‌باشد.

أ. مدیریت مراکز سرویس

برای مدیریت مراکز سرویس و امکان تعریف و نحوه فعالسازی آنها، در بخش راهبری سیستم زیر درخت مراکز سرویس سیستم با عنوان مدیریت مرکز پیام در نظر گرفته شده است. مدیریت مرکز پیام امکان تعریف و فعالسازی یک مرکز سرویس را به مدیر کلیف می‌دهد، تا از این طریق مدیر بتواند سیاست‌های نظارتی خود را در حوزه پیام کوتاه در دیگر بخش‌های سیستم کلیف فعال نماید. همچنین در صورت عدم نیاز به مرکز سرویس خاص، غیرفعالسازی و حذف مرکز سرویس در بخش مدیریت مرکز پیام امکان پایان این فرایند را در اختیار مدیر قرار می‌دهد. مدیریت مراکز سرویس شامل موارد زیر است:

- مشاهده لیست مراکز سرویس
- جستجو در مراکز سرویس
- تعریف مرکز سرویس
- فعال‌سازی مرکز سرویس
- غیرفعال‌سازی مرکز سرویس
- حذف مرکز سرویس
- ویرایش مرکز سرویس

ب.مشاهده لیست مراکز سرویس

مدیر می‌تواند کلیه مراکز سرویس تعریف شده در سیستم را در صفحه "All Messaging Centers" مشاهده کند. اطلاعاتی که به ازای هر مرکز سرویس در این بخش نمایش داده می‌شود، در جدول زیر توصیف شده است:

جدول ۱۶- مشخصه‌های مرکز سرویس

نام پارامتر	توصیف
Name	نام مرکز سرویس
Description	توضیحات یا برچسب توصیف کننده شرایط مرکز سرویس
Active/Deactive IP	مشخصات IP مرکز سرویس

Port	درگاه ورودی اتصال به مرکز سرویس
Type	نوع مرکز سرویس که پیام کوتاه از آن دسته مراکز سرویس دریافت شده اند و می‌تواند یکی از مقادیر *SMSC*، *FSMS* یا *Inter PLMN Mediator* و یا *Intra* PLMN Mediator
Status	وضعیت مرکز سرویس شامل دو حالت Active و Inactive

ج. تعریف مرکز سرویس

تعریف مرکز سرویس در واقع به منزله هویت دادن و شناساندن مرکز سرویس به سیستم می‌باشد. کاربر باید مشخصات موردنیاز برای تعریف مرکز سرویس را مقداردهی کند. این مشخصات در جدول زیر توصیف شده است:

جدول ۱۷- مشخصه‌های تعریف مرکز سرویس

نام پارامتر	توصیف	نوع مقداردهی
Name	نام مرکز سرویس از دید سیستم کلیف	اجباری
Description	توصیف مرکز سرویس جدید	اختیاری
Active/Deactive IP	مشخصات IP مرکز سرویس	اجباری
Port	درگاه ورودی مرکز سرویس	اجباری
Type	نوع مرکز سرویس که پیام کوتاه از آن دسته مراکز سرویس دریافت شده اند و می‌تواند یکی از مقادیر *SMSC*، *FSMS* یا *Inter PLMN Mediator* و یا *Intra* PLMN Mediator	اجباری

در صورت صحت اطلاعات و تکراری نبودن نام مرکز سرویس ، مرکز سرویس جدید به این لیست افزوده می‌گردد. قابل توجه است، تعریف یک مرکز سرویس به منزله آغاز استفاده از آن و آغاز اعمال سیاست‌های نظارتی نیست. برای حصول این امر، باید مرکز سرویس موردنظر در سیستم فعال شود.

د. فعال‌سازی/غیرفعال‌سازی مرکز سرویس

برای استفاده از مرکز سرویس در جریان تنظیم سیاست‌های نظارتی، باید پس از تعریف مرکز سرویس، نسبت به فعال‌سازی آن اقدام نمود. همچنین برای خاتمه اعمال قابل انجام بر روی مرکز سرویس، باید مرکز سرویس موردنظر در سیستم غیرفعال شود. قابل توجه است که مرکز سرویس غیرفعال، در سیستم باقی می‌ماند و در صورت نیاز مدیر می‌تواند در آینده آن را دوباره فعال یا در صورت عدم نیاز، حذف نماید.

۳,۸ گزارشات سیستمی

پس از اعمال سیاست‌های نظارتی مختلف بر روی پیام‌های کوتاه در شبکه تلفن همراه، امکان تهیه گزارشات مختلف از عملکرد بخش‌های مختلف، از ملزومات کار می‌باشد. گزارش‌های موردنیاز می‌توانند شامل موارد زیر باشند:

- گزارش اعلان‌های رصد غیرمحسوس مشترکین و رومرهای فعال در شبکه
- گزارش اعلان‌های فیلترینگ پیام‌های کوتاه که به صورت برخط و به لحظه قابل دریافت می‌باشد
- گزارش غیر برخط پیام‌های کوتاه مبادله شده در شبکه و وضعیت آنها
- گزارش‌های آماری از تعداد پیام کوتاه‌های تبادل شده در هر یک از مراکز سرویس

در کلیه گزارشات قابل تولید در سیستم، امکان صدور گزارش‌ها به فایل خروجی و تهیه نسخه‌های pdf، اکسل و یا csv از نتایج جستجو و همچنین تهیه چاپ کاغذی از جدول گزارش، قابلیتی است که مدیر سیستم می‌تواند در صورت نیاز، نسبت به تهیه آنها از نتایج گزارش اقدام نماید.

أ. گزارش آفلاین پیام‌های کوتاه ارسالی

امکان تهیه گزارش مشروح از پیام‌های کوتاه ارسالی در شبکه به شکل آفلاین و گزارش آماری از تعداد این پیام‌ها برای مدیر سیستم فراهم شده است. مدیر سیستم می‌تواند با توجه به مشخصات و جزئیات مختلف پیام کوتاه جستجوی خود را برای دریافت پیام‌های کوتاه به انجام رساند. اجزاء و

مشخصات پیام کوتاه برای انجام جستجو در سیستم شامل موارد مشخص شده در زیر می‌باشد. پارامترهای مورد استفاده در این بخش، در رابطه AND با همدیگر قرار می‌گیرند.

جدول ۱۸- مشخصه‌های جستجو پیام کوتاه در گزارشات آفلاین

نام پارامتر	توصیف	وضعیت مقداردهی
Sender Address	آدرس فرستنده پیام- می‌تواند به یکی از روش‌های Exact یا "آدرس دقیق"، Prefix یا "پیشوندی" و Contain یا "در میانه عبارت" تعیین شود. محتوای این فیلد نیز می‌تواند به صورت دستی توسط مدیر مقدادهی شده یا از لیست گروه شماره تلفن‌های تعریف شده در سیستم انتخاب شود.	اختیاری
Sender MSC	آدرس اپراتور ارسال کننده پیام- می‌تواند به یکی از روش‌های Exact یا "آدرس دقیق"، Prefix یا "پیشوندی" و Contain یا "در میانه عبارت" تعیین شود.	اختیاری
Reciever Address	آدرس گیرنده پیام- می‌تواند به یکی از روش‌های Exact یا "آدرس دقیق"، Prefix یا "پیشوندی" و Contain یا "در میانه عبارت" تعیین شود. محتوای این فیلد نیز می‌تواند به صورت دستی توسط مدیر مقدادهی شده یا از لیست گروه شماره تلفن‌های تعریف شده در سیستم انتخاب شود.	اختیاری
Reciever MSC	آدرس اپراتور دریافت کننده پیام- می‌تواند به یکی از روش‌های Exact یا "آدرس دقیق"، Prefix یا "پیشوندی" و Contain یا "در میانه عبارت" تعیین شود.	اختیاری
Content	مشخصات بدنه پیام کوتاه – محتوای این پارامتر می‌تواند از عباراتی شامل کلماتی به زبان فارسی و انگلیسی تشکیل شده باشد. ویژگی‌های در نظر گرفته شده در این کادر عبارتند از: • وجود خط‌فاصله در میان کلمات به معنای رابطه AND محسوب می‌شود. • اصطلاحاتی که در داخل قرار "" بگیرند به صورت واحد در نظر گرفته می‌شوند. • هر کلمه موجود در لیست که با بخشی از کلمات موجود در پیام برابر شود، سیستم پیام مورد نظر را مورد فیلتر قرار می‌دهد. برای مثال در صورت تعریف ab در قانون فیلترینگ به عنوان محتوای فیلترینگ، تمام کلماتی که به صورت *ab* باشند با این تعریف مطابقت می‌کنند.	اختیاری

	در جستجوی محتوای قانون فیلترینگ می‌توان از کلمات چندشکلی که قبلاً در سیستم تعریف شده‌اند، استفاده نمود.	
Final State	رفتار کلیف در قبال پیام‌های منطبق شده با قانون – می‌تواند یکی از مقادیر زیر را داشته باشد: • Replace: جایگزین کردن پیام • Delay: ارسال با تأخیر • Mask: پنهان کردن بخش‌های تطبیق یافته از محتوای پیام • Block: توقف یا بلوکه کردن پیام • Mask & Delayed: پنهان کردن بخش‌های تطبیق یافته از محتوای پیام و ارسال با تأخیر آن	اختیاری
Start Date & End Date	محدوده زمانی پیام کوتاه ارسال شده در شبکه	اختیاری
Service Center Type	نوع مرکز سرویس که پیام کوتاه از آن دسته مراکز سرویس دریافت شده اند – می‌تواند یکی از مقادیر *SMSC*، *FSMS* یا *Inter PLMN Mediator* و یا *Intra* PLMN Mediator باشد.	اختیاری
Center Name	نام مراکز سرویس متناظر با نوع مراکز انتخاب شده در Service Center Type	اختیاری
Sort By	امکان مرتب سازی نتایج جستجو بر شماره ارسال و یا دریافت کننده پیام و همچنین آدرس اپراتور دریافت کننده و یا ارسال کننده پیام و یا زمان ارسال پیام	اختیاری
Untrusted Operator	امکان جستجو و مشاهده پیام‌های کوتاه که به دلیل ارسال از اپراتورهای غیرمجاز، بلوکه شده‌اند	اختیاری
Restricted List	امکان جستجو مشاهده پیام‌های کوتاه که ارسال آنها از تعداد مجاز تعیین شده در لیست محدودیت عبور کرده و بلوکه شده اند.	اختیاری

ب. گزارش استفاده مفرط از پیام کوتاه

برای نظارت بر روی تعداد پیام‌های کوتاه ارسالی توسط ارسال کنندگان مختلف در شبکه تلفن، امکان اطلاع و مشاهده گزارش از تعداد پیام‌های ارسال شده توسط مشترکین و رومرهای فعال در شبکه با امکان انتخاب بازه‌های زمانی مختلف فراهم شده است.

ج. مشاهده و جستجوی کلیه اعلان‌های پیام‌های کوتاه هشدار فیلترینگ

همانطور که در بخش فیلترینگ پیام‌ها اشاره شد، یکی از روش‌های اعلام تطبیق قوانین فیلترینگ در سیستم، امکان تولید اعلان پیام کوتاه هشدار برای هریک از موارد تطبیق پیام‌های مبادله شده در شبکه، با قوانین فعال در سیستم می‌باشد. نوع ارسال این نوع پیام‌های کوتاه به دو صورت اخطار دهنده به فرستنده و هشدار دهنده به مدیر سیستم می‌باشد. برای دریافت چنین اعلان‌هایی باید در زمان تعریف قانون، درخواست مورنیاز را به سیستم اعلام کرد. در صورت اعلام نیاز، امکان مشاهده کلیه اعلان‌های مربوط به تطابق پیام‌های کوتاه با قوانین فیلترینگ امکان‌پذیر می‌باشد. در این حالت کلیه اعلان‌های موجود در سیستم که تا زمان ارائه درخواست مشاهده، توسط سیستم دریافت شده‌اند، در اختیار مدیر قرار می‌گیرند. در جدول زیر مشخصات لازم برای جستجو و تهیه گزارش از تولید اعلان پیام‌های کوتاه نمایش داده شده است.

جدول ۱۹- مشخصه‌های جستجو پیام کوتاه در گزارشات آفلاین

نام پارامتر	توصیف
Sender Number	شماره مشخص شده به عنوان ارسال کننده اعلان پیام کوتاه تولید شده
Receiver Number	شماره گیرنده دریافت کننده اعلان پیام کوتاه
Status	وضعیت نهایی ارسال اعلان پیام کوتاه که می‌تواند مقادیر Success: پاسخ از مرکز سرویس دریافت شده و عملیات درخواستی با موفقیت انجام شد. Failed: پاسخ مبنی بر عدم امکان انجام فعالیت درخواستی در مرکز سرویس دریافت شده است. Pending: هنوز پاسخی از مرکز سرویس دریافت نشده است. را اختیار نماید.
Type	نوع اعلان پیام کوتاه که شامل دو نوع Alarm یا Warning می‌باشد

د. گزارشات آماری پویا از سیاست‌های نظارتی

امکان تهیه گزارش‌های آماری از تأثیر سیاست‌های نظارتی مختلف چون قوانین فیلترینگ، لیست محدودیت، شماره مشترکین و رومرهای فعال در شبکه میسر می‌باشد. در این حالت، مدیر سیستم با وارد کردن پارامترهای مورد نیاز، از سیستم تقاضای نمایش گزارش آماری می‌کند. سیستم یک گزارش

پویا مطابق با پارامترهای گوناگون ورودی تولید کرده و نمایش می‌دهد. اجزاء مورد نیاز برای تولید این گزارش‌ها به صورت زیر می‌باشند:

جدول ۲۰- مشخصه‌های گزارش آماری پویا

نام پارامتر	توصیف
Service Center Type	نوع مرکز سرویس که پیام کوتاه از آن دسته مراکز سرویس دریافت شده اند و می‌تواند یکی از مقادیر SMSC، FSMS یا Inter PLMN Mediator و یا Intra PLMN Mediator و یا دو عبارت Any و All باشد. عبارت All به معنای همه گزینه‌های ممکن و عبارت Any به معنای هر یک از حالت‌های ممکن است.
Center Name	نام مراکز سرویس متناظر با نوع مراکز انتخاب شده در Service Center Type به همراه دو عبارت All و Any. عبارت All به معنای همه گزینه‌های ممکن و عبارت Any به معنای هر یک از حالت‌های ممکن است.
Category	دسته بندی کلی در نظر گرفته برای کلیه پیام‌های کوتاه دریافت شده در سیستم که به دو نوع Public شامل وضعیت عمومی پیام کوتاه و filter شامل حالت‌های مختلف فیلتر شدن پیام کوتاه تقسیم‌بندی می‌شود.
Counter	عنوان شمارنده وضعیت‌های مختلف پیش‌بینی شده بر اساس دسته‌بندی انتخاب شده در پارامتر – Category در صورت انتخاب عنوان public برای پارامتر Category، شامل عناوین زیر می‌باشد: • Input_Message: تعداد کل پیام‌های کوتاه دریافت شده از مراکز سرویس انتخاب شده در Service Center Type و Center Name • Filtered: تعداد پیام‌های کوتاه تغییر وضعیت داده شده • White_list_member: تعداد پیام‌های کوتاه تطبیق شده که در لیست سفید سیستم قرار گرفته بوده‌اند. • Passed: تعداد پیام‌های کوتاه که از سیاست‌های نظارتی تعریف شده در سیستم تخطی نکرده و به حالت طبیعی عبور داده شده‌اند. و در صورت انتخاب عنوان filter برای پارامتر Category، شامل عناوین زیر می‌باشد: • Block_SendAck_SendSDR: تعداد پیام‌های کوتاه بلوکه شده که از دید فرستنده پیام ارسال آن کامل شده و پاسخ Delivery Report مبنی بر ارسال موفق برای آنها به فرستنده ارسال شده است. • Block_SendAck_SendSDR: تعداد پیام‌های کوتاه بلوکه شده که از دید فرستنده پیام، ارسال آن کامل شده و اما پاسخ Delivery Report مبنی بر ارسال ناموفق برای آنها به فرستنده ارسال شده است. • Block_SendAck_SendSDR: تعداد پیام‌های کوتاه بلوکه شده که از دید فرستنده

	پیام ارسال آن کامل شده و اما هیچ پاسخ Delivery Report برای فرستنده ارسال نشده است. • Block_SendNAck: تعداد پیام‌های کوتاه بلوکه شده که از دید فرستنده پیام، ارسال آن ناموفق می‌باشد و پاسخ ارسال ناموفق دریافت نموده است. • Block_DSendAck: تعداد پیام‌های کوتاه بلوکه شده که از دید فرستنده پیام، ارسال آن ناموفق می‌باشد و هیچ پاسخی مبنی بر اعلام موفقیت یا عدم موفقیت ارسال پیام کوتاه به فرستنده آن ارسال نمی‌شود. • Replace: تعداد پیام‌های کوتاهی که متن آن به عبارتی پیش فرض جایگزین شده است • Mask: تعداد پیام‌های کوتاه که بخشی از متن پیام با کاراکترهای خاصی مخفی شده اند
Start Date & End Date	برای تعیین محدوده زمانی (بر حسب تاریخ و ساعت و دقیقه) پیام‌های کوتاه ارسال شده در شبکه
Time Unit	واحد زمانی گزارش شامل مقادیری چون ۵ دقیقه، ربع‌ساعت، ساعت، روز، هفته، ماه، هیچکدام، سایر که با انتخاب "سایر" مدیر می‌تواند یک مقدار از ۵ دقیقه تا یک هفته را بر اساس دقیقه که مضربی از ۵ دقیقه باشد را وارد نماید. در این حالت موارد مشخص شده بر اساس واحد زمانی انتخاب شده شمارش می‌شوند. در صورتی که مقدار "هیچکدام" انتخاب شود، یعنی لازم نیست شمارش‌های انتخاب شده در قسمت‌های قبلی در واحد زمانی جداگانه محاسبه شوند. به طور کلی مقدار انتخاب شده در این بخش در تعداد رکوردهای موجود گزارش تولید شده مؤثر خواهد بود.

در تولید گزارش آماری امکان تولید و نمایش ترکیب‌های چندگانه از انتخاب ٤ آیتم Service Center Type، Center Name، Category و Counter در سیستم پیش‌بینی شده است. بدین منظور ضروری است پس از انتخاب پارامترهای ترکیب حضور آنها به عنوان یکی از حالت‌های مورد درخواست به/از لیست نهایی گزارش اضافه/کم شوند. امکان استفاده از دو عبارت All و Any در دو آیتم Service Center Type و Center Name نیز وجود دارد.

ه. گزارش آماری از اثر قوانین فیلترینگ

تهیه گزارش از اثر قوانین فیلترینگ فعال در سیستم یکی دیگر قابلیت‌های سیستم می‌باشد. در این بخش گزارش تعدادی از پیام‌های کوتاه تطبیق یافته با قوانین فیلترینگ سیستم بر حسب مراکز سرویس مختلف فعال در سیستم و بازه‌های زمانی قابل تنظیم نمایش داده می‌شود. برای نمایش نتایج، امکان استفاده از واحدهای زمانی مختلف در نظر گرفته شده است. برای تفکیک اطلاعات و تسهیل در استفاده از نتایج نمایش داده شده از رنگ‌های مختلف برای نمایش تعداد پیام‌های تطبیق

یافته در مراکز سرویس مختلف استفاده شده است. در حالت خاصی که اطلاعات تعدادی دریافت شده از تطبیق قوانین برای قوانین فیلترینگ تعریف نشده در سیستم در این گزارش نمایش داده شود، از رنگ قرمز در سیستم استفاده می‌شود. اجزا و پارامترهای مورد نیاز برای تولید این گزارش به صورت زیر می‌باشند:

جدول ۲۱- مشخصه‌های لازم برای تولید گزارش تعدادی قوانین فیلترینگ

نام پارامتر	توصیف
Service Center Type	نوع مرکز سرویس که پیام کوتاه از آن دسته مراکز سرویس دریافت شده‌اند و می‌تواند یکی از مقادیر *SMSC*، *FSMS* یا *Inter PLMN Mediator* و یا *Intra* PLMN Mediator
Center Name	نام مراکز سرویس متناظر با نوع مراکز انتخاب شده در Service Center Type
Start Date & End Date	برای تعیین محدوده زمانی (بر حسب تاریخ و ساعت و دقیقه) پیام‌های کوتاه ارسال شده در شبکه
Time Unit	واحد زمانی گزارش شامل مقادیری چون ۵ دقیقه، ربع‌ساعت، ساعت، روز، هفته، ماه، هیچکدام، سایر که با انتخاب "سایر" مدیر می تواند یک مقدار از ۵ دقیقه تا یک هفته را بر اساس دقیقه که مضربی از ۵ دقیقه باشد را وارد نماید. در این حالت موارد مشخص شده بر اساس واحد زمانی انتخاب شده شمارش می‌شوند. در صورتی که مقدار "هیچکدام" انتخاب شود، یعنی لازم نیست شمارش‌های انتخاب شده در قسمت‌های قبلی در واحد زمانی جداگانه محاسبه شوند. به طور کلی مقدار انتخاب شده در این بخش در تعداد رکوردهای موجود گزارش تولید شده مؤثرخواهد بود.

۳,۹ مدیریت اطلاعات رومر

در بخش‌های مختلف سیستم کلیف که در بخش‌های گذشته شرح جزئیات آن ارائه گردید، اعمال سیاست‌های نظارتی مختلف بر روی پیام‌های کوتاه ارسال شده بر روی انواع مختلف مراکز سرویس امکان‌پذیر است. در برخی از این مراکز سرویس امکان سرویس‌دهی و دسترسی به اطلاعاتی بیش از پیام‌های کوتاه ارسالی فراهم شده است. این موضوع در خصوص مراکز سرویس نوع Inter PLMN Mediator شامل اطلاعات حاوی اعلام حضور مشترکین مهمان و رومرهای وارد شده به شبکه تلفن همراه و اطلاعات مشترکین خارج شده از شبکه تلفن همراه خواهد بود. با دسترسی به این نوع اطلاعات در این نوع مراکز سرویس، امکان نظارت بر حضور رومرها به تفکیک شماره VLR آنها و

تهیه گزارش‌های مربوطه از آنها برای مدیر سیستم کلیف فراهم شده است. همچنین امکان اختصاص برچسب به شماره‌های مختلف VLR در شبکه و امکان جستجو و تهیه گزارش ورود و خروج مشترکین و رومرهای فعال در شبکه فراهم شده است.

أ. گزارش ورود/خروج مشترکین به/از شبکه

امکان آگاهی از آخرین اطلاعات ورود و خروج مشترکین و رومرهای فعال در شبکه در اختیار مدیر سیستم قرار گرفته است. مدیر قادر است بر اساس پارامترهایی چون شناسه IMSI، MSISDN و شماره VLR و یا برچسب توصیف کننده شناسه VLR گزارش موردنیاز را خود از ورود و خروج افراد از شبکه و ورود به شبکه‌های بین المللی تلفن همراه و بالعکس را در بازه‌های زمانی مختلف تهیه نماید. مشخصات لازم برای ثبت این داده در جدول زیر توصیف شده است:

جدول ۲۲- مشخصه‌های توصیف کننده شناسه VLR در شبکه

نام پارامتر	توصیف	نوع مقداردهی
VLR Id	شناسه آدرس شبکه اپراتور تلفن همراه	اجباری
Name	برچسب و عبارت توصیف کننده شناسه VLR Id	اجباری

جدول زیر مشخصات لازم را برای جستجو و تهیه گزارش نظارت بر ورود و خروج رومرها در شبکه تلفن همراه را نمایش داده است:

جدول ۲۳- مشخصه‌های نظارت و جستجوی اطلاعات ورود و خروج رومرها

نام پارامتر	توصیف
MSISDN	شماره مشترک و یا رومر تلفن همراه
VLR Id	شناسه آدرس شبکه اپراتور تلفن همراه
Start Date & End Date	برای تعیین محدوده زمانی (بر حسب تاریخ و ساعت و دقیقه) اطلاعات ورود و خروج رومرها در سیستم

۳,۱۰ مدیریت و راهبری سیستم

احراز شرایط امنیتی لازم برای استفاده از سیستم، مدیریت تعداد کاربران مجاز و تنظیم میزان دسترسی هریک از کاربران به بخش‌های مختلف سیستم و پیکربندی عمومی سیستم یکی از نیازمندی‌های عمومی اکثر سیستم‌های نرم افزاری می‌باشد. این قابلیت در کلیف به گونه‌ای طراحی شده است که علاوه بر انجام این موضوع، امکان کنترل عملکرد کاربران و تهیه گزارش از جزئیات عملکرد آنها در هریک از بخش‌های سیستم در اختیار مدیر سیستم قرار گیرد. در ادامه دو بخش مدیریت امنیت و پیکربندی عمومی سیستم ارائه می‌شود.

أ. مدیریت امنیت سیستم

برای مدیریت امنیت سیستم و امکان بهره‌برداری توسط کاربران مختلف و تنظیم دسترسی آنها، قابلیت‌های لازم در بخش راهبری سیستم در نظر گرفته شده است. در این بخش امکان تعریف و فعال‌سازی کاربران مختلف به مدیر کلیف داده شده است. برای تنظیم دسترسی‌های مختلف به کاربران در سیستم، مفهوم نقش (Role) در سیستم در نظر گرفته شده است. به هر یک از کاربران بر حسب وظیفه تعریف شده برای آنها، نقشی اختصاص داده می‌شود. هر نقش شامل تعدادی از عملیات شناخته شده در سیستم است که با عنوان Action شناخته می‌شوند. اختصاص یک Role شامل تعدادی Action به یک کاربر، بدین معناست که کاربر به تمامی Action های موجود در آن Role دسترسی خواهد داشت. در حالت کلی یک Role را می‌توان به چند کاربر اختصاص داد. کاربران بر اساس وظایف و نقشی که در سیستم برای آنها در نظر گرفته شده است، دسترسی‌های مناسب در حیطه کاری و در رابطه با نقش و وظایف تعیین شده خود بدست می‌آورند. در هر لحظه در صورت عدم نیاز به دسترسی خاص به کاربران مختلف، امکان تغییر نقش و یا حذف و غیرفعال‌سازی کاربر در بخش مدیریت امنیتی سیستم، در اختیار مدیر قرار داده شده است. مدیریت امنیتی سیستم شامل موارد زیر است:

- مشاهده لیست کاربران
- تعریف و فعال‌سازی کاربران
- جستجو در لیست کاربران
- مشاهده لیست نقش‌ها

- تعریف نقش‌ها
- ویرایش کاربرها
- انتصاب نقش‌ها
- جستجو در لیست نقش‌ها
- حذف/غیرفعال‌سازی کاربران
- ویرایش نقش‌ها
- تهیه گزارش از عملکرد کاربران در سیستم
- پیکربندی عمومی سیستم

ب. مشاهده لیست کاربران

مدیر می‌تواند کلیه کاربران تعریف شده در سیستم را مشاهده کند. اطلاعاتی که به ازای هر کاربر در این بخش نمایش داده می‌شود، در جدول زیر توصیف شده است:

جدول ٢٤- مشخصه‌های محدودیت در لیست محدود

نام پارامتر	توصیف
User Name	نام کاربری مورد استفاده در سیستم
Contact Name	نام و نام خانوادگی کاربر
Status	وضعیت فعالیت کاربر
Role Manager	لینک مشاهده جزئیات قابل تغییر نقش کاربر در سیستم

ج. تعریف کاربر

تعریف کاربر در واقع به منزله هویت دادن و شناساندن کاربر موردنظر در سیستم می‌باشد. لازم است مشخصات زیر برای تعریف کاربر مقداردهی شوند:

جدول ٢٥- مشخصه‌های تعریف کاربر جدید

نام پارامتر	توصیف	نوع مقداردهی
First Name	نام کاربر	اجباری

Last Name	نام خانوادگی کاربر	اجباری
Password	رمز عبور	اجباری
User Name	عنوانی برای شناسایی نام کاربری	اجباری
Status	وضعیت کاربر در سیستم، مقدار پیش فرض این پارامتر مقدار Active می‌باشد.	اجباری

در صورت صحت اطلاعات و تکراری نبودن نام کاربری در لیست کاربران، مشخصات مذکور به لیست کاربران سیستم افزوده می‌گردد. اما تعریف یک کاربر به منزله امکان فعالیت کاربر جدید در سیستم نمی‌باشد. برای ایجاد امکان استفاده کاربر جدید از سیستم، باید نقش و حیطه کاری کاربر در سیستم تعریف و به آن نسبت داده شود.

د. مشاهده لیست نقش‌ها

مدیر می‌تواند کلیه کاربران تعریف شده در سیستم را مشاهده کند. اطلاعاتی که به ازای هر نقش در این بخش نمایش داده می‌شود، در جدول زیر توصیف شده است:

جدول ۲۶- مشخصه‌های نقش کاربران سیستم

نام پارامتر	توصیف
ID	شناسه مورد استفاده در سیستم
Name	نام نقش
Description	برچسب موردنظر مدیر برای توصیف و شناسایی نقش تعریف شده

ه. تعریف نقش

تعریف نقش که در واقع توصیف حیطه دسترسی یک کاربر در سیستم می‌باشد. در صفحه تعریف نقش جدید کاربر باید مشخصات موردنیاز برای تعریف نقش مقداردهی کند. این مشخصات در جدول زیر توصیف شده‌اند:

جدول ۲۷- مشخصه‌های لازم تعریف نقش در سیستم

نام پارامتر	توصیف	نوع مقداردهی

Name	نام نقش	اجباری
Description	برچسب موردنظر مدیر برای توصیف و شناسایی نقش یا کاربران استفاده کننده	اختیاری
Action	لیست عملیات مختلف که نقش موردنظر شکل می‌دهد. این پارامتر به صورت درختی و در ساختاری که با استفاده از عناوین بخش‌های مختلف سیستم شکل گرفته است، نمایش داده شده و قابل انتخاب است.	اجباری

در صورت صحت اطلاعات و تکراری نبودن نام نقش در لیست نقش‌های سیستم، مشخصات مذکور به لیست نقش‌ها افزوده می‌گردد.

و. حذف کاربران

برای قطع فعالیت کاربران سیستم به صورت موقت و دایم، امکان غیرفعال‌سازی و حذف کاربر از سیستم پیش‌بینی شده است. انجام این امر برای کاربران به جهت نیاز به نگهداری سوابق کاربر با انجام تغییراتی صورت می‌گیرد. در این حالت کاربر مشخصات کاربر و شناسه آن از سیستم حذف نمی‌شود و تنها وضعیت آن به حالت حذف شده تغییر می‌یابد. برای انجام این کار مدیر سیستم می‌تواند با انجام فرایند تغییر مشخصات کاربر وضعیت کاربر به حالت Deleted تغییر دهد.

ز. گزارش رویداد نگاری از عملیات کاربران

پس از تعریف و فعال‌سازی کاربران، مدیر سیستم می‌تواند گزارش تراکنش‌های انجام شده کاربران در بخش‌های مختلف سیستم را دریافت نماید. برای هریک از کاربران عملیات مختلف ورود و خروج از سیستم همراه با اطلاع از شناسه IP محل ارسال درخواست، درخواست‌های مختلف مدیریت و تغییرات داده شامل اضافه، حذف، تغییر، مشاهده صفحات و جزئیات آن، مشاهده گزارش و ارسال به فایل در کلیه بخش‌های سیستم بر حسب زمان قابل ردیابی خواهند بود. اجزا و آیتم‌های مورد نیاز برای تولید این گزارش به صورت زیر می‌باشند:

جدول ۲۸– مشخصه‌های لازم برای تهیه گزارش رویدادنگاری کاربران

نام پارامتر	توصیف
Start Date & End Date	برای تعیین محدوده زمانی (بر حسب تاریخ و ساعت و دقیقه) تراکنش و عملیات انجام شده در

	سیستم
Category	دسته بندی عملیات درخواست شده به دو دسته کلی ۱) عملیات ورود/خروج از سیستم (Login/logout) ۲) مدیریت داده‌ها در بخش‌های مختلف سیستم (Data Managemtent)
User Name	نام کاربری
Type	یکی از حالات: ۱) Login: ورود به سیستم ۲) Logout: خروج از سیستم ۳) View List: مشاهده قوانین فیلترینگ و مشخصات لیست‌ها در بخش‌های مختلف سیستم مانند لیست سفید، لیست محدود و ... ٤) View Detail Info: مشاهده بخش مشخصات جزئی اعضای لیست‌ها در بخش‌های مختلف سیستم ٥) Delete: حذف اجزای لیست‌ها در بخش‌های مختلف سیستم ٦) Add: افزودن عضو جدید به لیست‌ها در بخش‌های مختلف سیستم ۷) Update: ویرایش لیست‌ها در بخش‌های مختلف سیستم ۸) Activate Rule: فعالسازی قانون فیلترینگ ۹) Deactivate Rule: غیرفعالسازی قانون فیلترینگ ۱۰) Search: جستجو در لیست‌های تعریف شده ۱۱) Print: صدور چاپ از گزارش نمایش داده شده ۱۲) Monitor: مشاهده مانیتورینگ اعلانات قوانین فیلترینگ و یا شنود آنلاین ۱۳) Export: صدور گزارش به فایل خارجی
Entity Name	یکی از موجودیت‌های بخش‌های مختلف سیستم: ۱) Polymorphic Word ۲) Phone No Group ۳) White List ٤) Filtering Rule ٥) Category ٦) Filtering Notification ۷) LI Target ۸) LI Notification ۹) Offline Log ۱۰) Offline Log Counter ۱۱) System User ۱۲) System Role ۱۳) Login ۱٤) Logout ۱٥) Operator White List ۱٦) Filtrered Number ۱۷) Restricted List ۱۸) Get SMS Overuse ۱۹) ...

Service Center Type	نوع مرکز سرویس که پیام کوتاه از آن دسته مراکز سرویس دریافت شده اند و می‌تواند یکی از مقادیر SMSC، FSMS یا Inter PLMN Mediator و یا Intra PLMN Mediator باشد.
Center Name	نام مراکز سرویس متناظر با نوع مراکز انتخاب شده در Service Center Type
Result	نتیجه تراکنش به صورت : موفق (Ok) و ناموفق (Fail)

ح. پیکربندی عمومی سیستم

در جریان تعریف قوانین فیلترینگ پیام کوتاه در سیستم برای اجرای سیاست‌های تنظیم شده در این قوانین، همانند اجرای ارسال اعلانات صوتی و یا پیام کوتاه و اجرای دستور Replce و یا Mask برای پیام‌های غیرمجاز، مشاهده آخرین اعلانات پیام‌ها در صفحه مانیتورینگ اعلانات برخی پیکربندی‌ها برای تکمیل اجرای آنها مورد نیاز می‌باشد. مدیر سیستم می‌تواند نسبت به تغییر و تنظیم پارامترهای لازم برای اجرای کامل آنها اقدام نماید. پارامترهای قابل تنظیم در این صفحه به صورت زیر می‌باشند:

جدول ۲۹– مشخصات گزینه‌های قابل تنظیم در بخش پیکربندی عمومی سیستم

نام پارامتر	توضیحات
بخش Send Alarm SMS Setting	
Don’t Send Alarm SMS Older Than	حداکثر زمان اعتبار برای ارسال پیام کوتاه اعلان به مدیر سیستم را مشخص می‌کند. مقدار این فیلد به دقیقه بیان می‌شود. فقط پیام کوتاه‌هایی که زمان وقوع آنها کمتر و یا مساوی مقدار این فیلد باشد، شامل ارسال پیام کوتاه اعلان مدیر می‌شوند.
Start Time of Sending Alarm SMS	زمان شروع بازه زمانی مجاز ارسال پیام کوتاه اعلان برای مدیر سیستم در طول ۲٤ ساعت شبانه روز بر حسب ساعت و دقیقه
End Time of Sending Alarm SMS	زمان پایان بازه زمانی مجاز ارسال پیام کوتاه اعلان برای مدیر سیستم در طول ۲٤ ساعت شبانه روز بر حسب ساعت و دقیقه
Receivers Address of Alarm SMS	لیستی از شماره تلفن‌ها که پیام کوتاه اعلان برای آنها ارسال می‌شود، دنباله‌ای از اعداد (شماره تلفن) که با – از هم جدا می شوند
Life Time Of Alarm SMS	مدت زمان انقضای پیام کوتاه‌های اعلان بر حسب ساعت؛ بعد از این مدت ارسال پیام کوتاه منقضی می‌شود.

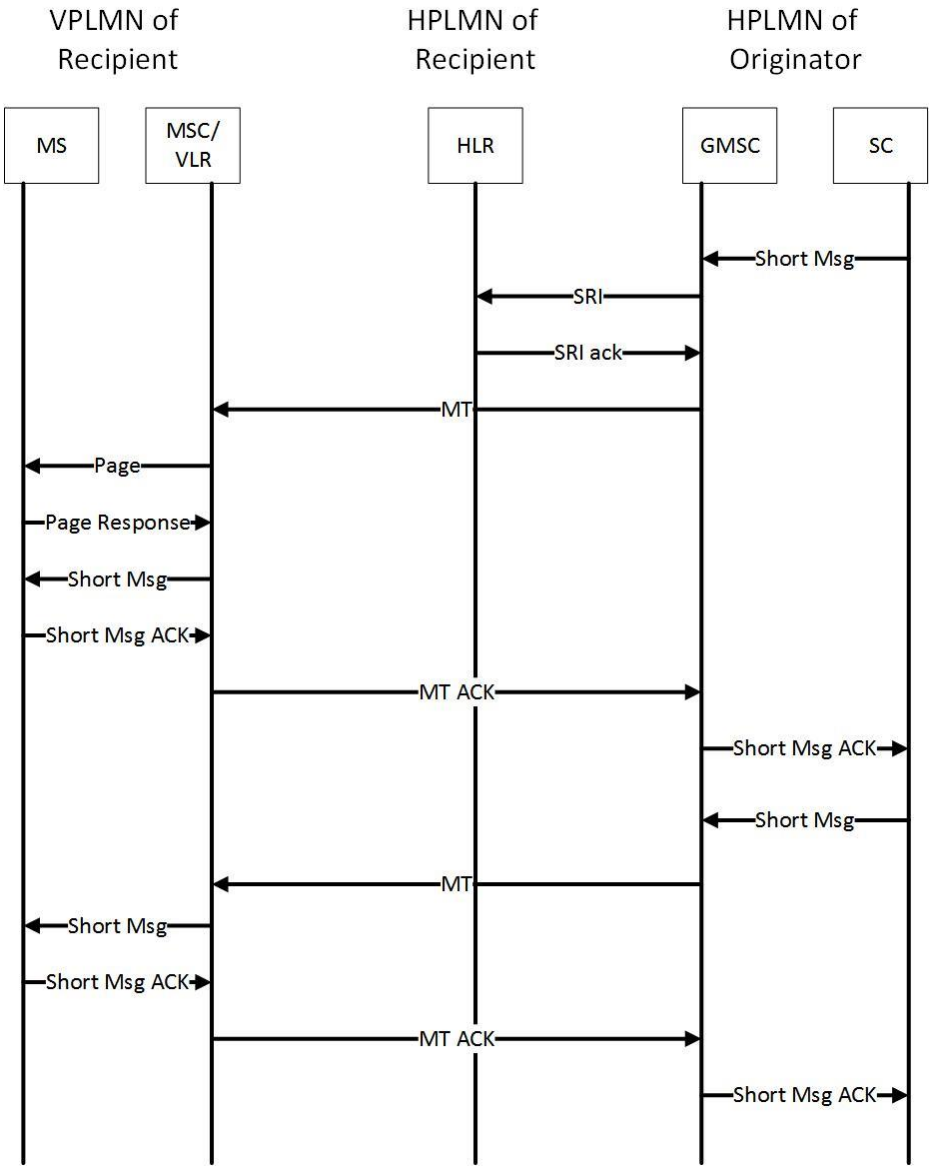
بخش Send Warning SMS Setting	
Don’t Send Alarm SMS Older Than	حداکثر زمان اعتبار برای ارسال کوته پیام اخطار به فرستنده را مشخص می‌کند. مقدار این فیلد به دقیقه بیان می‌شود. فقط پیام کوتاه‌هایی که زمان وقوع آنها کمتر و یا مساوی مقدار این فیلد باشد، شامل ارسال پیام کوتاه اخطار به فرستنده می‌شوند.
Sending Warning SMS	برای فعال و غیر فعال کردن ارسال پیام کوتاه اخطار برای فرستنده استفاده می‌شود.
Warning SMS Content	متن پیام کوتاه اخطار برای فرستنده – متنی حداکثر به اندازه یک پیام کوتاه.
Warning SMS origin Address	آدرس فرستنده پیام کوتاه اخطار برای فرستنده.
Life Time Of Warning SMS	مدت زمان انقضای پیام کوتاه‌های اخطار برای فرستنده بر حسب ساعت، بعد از این مدت ارسال پیام کوتاه منقضی می شود.
بخش SMS Center Setting	
IP	مشخص کننده IP مرکز SMS ی که برای ارسال پیام کوتاه از آن استفاده می‌شود.
Port	مشخص کننده Port مرکز SMS ی که برای ارسال پیام کوتاه از آن استفاده می‌شود.
Id	مشخص کننده ID مرکز SMS ی که برای ارسال پیام کوتاه از آن استفاده می‌شود.
Password	مشخص کننده password مرکز SMS ی که برای ارسال پیام کوتاه از آن استفاده می‌شود.
System Type	مشخص کننده sysType مرکز SMS ی که برای ارسال پیام کوتاه از آن استفاده می‌شود.
Delivery	مشخص کننده وضعیت گزارش تحویل موردنیاز.
Language	مشخص کننده زبان پیام کوتاه.
بخش Scheduler Setting	
Expiry time of Online Notifications	حداکثر مدت زمان مجاز برای نگهداری رکوردهای آخرین اجرای شنود برخط (بر مبنای روز)
بخش Page Refresh Time	

Refresh Time of Filtering Notifications Page	مدت زمان refresh شدن خودکار صفحه مانیتورینگ اعلان‌های فیلترینگ (بر مبنای ثانیه)
Refresh Time of Online Monitoring Notifications Page	مدت زمان refresh شدن خودکار صفحه مانیتورینگ شنود بر خط (بر مبنای ثانیه)
بخش Rules Setting	
Message in Replacement Rule	متن جایگزین پیام فیلتر شده در تعریف یک قانون فیلترینگ در زمانی که از عمل جایگزینی برای برخورد با پیام کوتاه‌های غیرمجاز استفاده شود.
Character in Mask Rule	تعیین کاراکتر جایگزین کلمات فیلتر شده در تعریف یک قانون فیلترینگ، در زمانی که از عمل Mask برای برخورد با پیام‌های کوتاه غیرمجاز استفاده شود.
Language	کد زبان متن جایگزین پیام فیلتر شده در تعریف یک قانون فیلترینگ
بخش Sound Alarm Setting	
Sound Alarm Path	مسیر فایل آلارم صوتی، که باید به ازای اعلان‌های تولید شده توسط قوانین فیلترینگ پخش شود. این مسیر باید نسبت به آدرس نرم افزار کلیف نسبت شده داده شود.
Life Time of Sound Alarm	حداکثر زمان اعتبار اعلان‌های پخش آلارم صوتی فیلترینگ پیام‌ها را مشخص می‌کند. مقدار این فیلد به دقیقه بیان می‌شود. فقط اعلان‌های فیلترینگی که زمان وقوع آنها کمتر و یا مساوی مقدار این فیلد باشد، آلارم صوتی برایشان پخش خواهد شد.

٤. زیرسیستم دوم: Home Router

٤,١ سیگنالینگ ارسال پیام کوتاه

در شکل ۱ سناریوی ارسال یک یا چند پیام کوتاه بدون وجود Home Router ترسیم شده است.



شکل ۱: سناریوی ارسال پیام کوتاه بدون حضور Home Router

همانطور که در شکل ۱ مشاهده می‌شود، جهت ارسال یک پیام از GMSC فرستنده یک پیام SRI به HLR مربوط به اپراتور سیمکارت ارسال می‌گردد و HLR شماره IMSI و همچنین شماره MSC که در حال حاضر

کاربر به آن متصل می‌باشد را بر میگرداند و GSMC به صورت مستقیم پیام را برای MSC مقصد ارسال می‌نماید.

در این روش محدودیت‌ها و مشکلات زیر وجود دارد:

- در صورتی که مسیری بین اپراتور ارسال کننده پیام به اپراتوری که کاربر در حال حاضر در آن به شبکه متصل است، وجود نداشته باشد پیام به مقصد تحویل داده نمی‌شود.
- در صورتی که مشترک به اپراتور دیگری، ترابرد کرده باشد که اپراتور فرستنده پیام با آن اپراتور ارتباطی نداشته باشد ارسال پیام به مقصد تحویل داده نمی‌شود.
- امکان ارسال و دریافت هرزنامه به مشترکین خانگی وجود دارد و نمی‌توان روی آن کنترلی داشت.
- در صورتی که اپراتور اصلی مشترک بخواهد سرویس‌های ارزش افزوده‌ای در حوزه ی پیام‌های دریافت شده از اپراتورهای دیگر اجرا کند (مثلا پیام‌های دریافتی را به یک نرم افزار دریافت پیام تحویل دهد)، این امکان وجود نخواهد داشت.
- به علت عدم وجود کنترل بر روی پیام‌های ورودی، اپراتور نمی‌تواند کنترل مالی لازم بر روی این فرآیند را داشته باشد (فرآیند محاسبه صورتحساب برای اپراتورهای دیگر، پیچیده و زمان بر است و می‌بایست از طریق پردازش فایل‌های CDR تولید شده در تمامی سوییچ‌های شبکه انجام شود)

برای حل این مشکلات، راه حل Home Routing یعنی دریافت متمرکز تمامی پیام‌های ورودی در اپراتور خانگی و مسیریابی مجدد آن به سمت مشترک مقصد در استاندارد 3GPP TR 23.840 ارائه گردیده است. در این استاندارد، دو روش پیاده سازی برای این راه حل ارائه گردیده است:

- Transparent Mode
- Non Transparent Mode

در هر دو روش ذکر شده، یک نود جدید با عنوان Home Router پس از HLR قرار گرفته و HLR تمامی SRI4SM های دریافت شده از اپراتورهای دیگر (یا بخشی از آن را که براساس ترجیح و پیکربندی اپراتور انتخاب می‌شود) را به سمت آن ارسال می‌نماید (مسیریابی SRI4SM به سمت Home Router می‌تواند توسط Signaling GW یا SPS نیز انجام شود). این نود، مجددا SRI4SM را به HLR ارسال نموده و IMSI واقعی مشترک و آدرس MSC سرویس دهنده به وی را استخراج می‌نماید و پس از آن به SRI4SM اصلی دریافت شده از اپراتور دیگر پاسخ می‌دهد. در پاسخ ارسال شده، برای پنهان ماندن هویت IMSI مشترک از

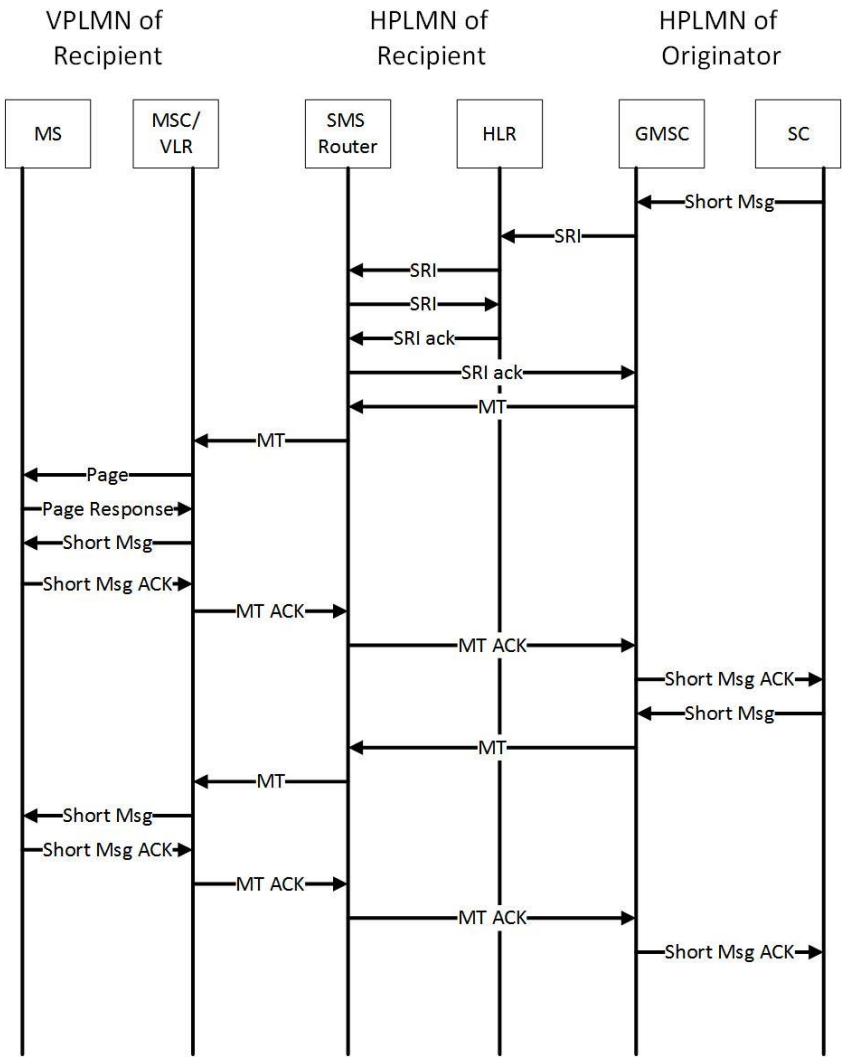
یک IMSI غیر واقعی استفاده می‌شود و برای دریافت پیام MT، به جای آدرس MSC واقعی سرویس دهنده، آدرس Home Router قرار داده می‌شود. در این صورت پیام‌های MT قبل از ارسال به مشترک مقصد، به Home Router تحویل شده و سپس در صورت احراز شرایط مدنظر اپراتور، به مشترک مقصد تحویل داده می‌شود.

در محصول پیشنهاد شده، علاوه بر دو سناریوی استاندارد مطرح شده، سناریوی دیگری نیز پوشش داده شده است. در سناریوی سوم، مشترک مقصد، یک نرم افزار دریافت پیام است که از طریق پروتکل SMPP به مرکز پیام کوتاه (SMSC) اپراتور متصل شده است. بنابراین پیام دریافتی توسط سیستم Home Router، بجای ارسال مجدد به شبکه، به مرکز پیام کوتاه اپراتور تحویل داده می‌شود.

در ادامه، فرآیند سیگنالینگ هر ۳ حالت اشاره شده، توضیح داده شده است.

أ. Transparent Mode

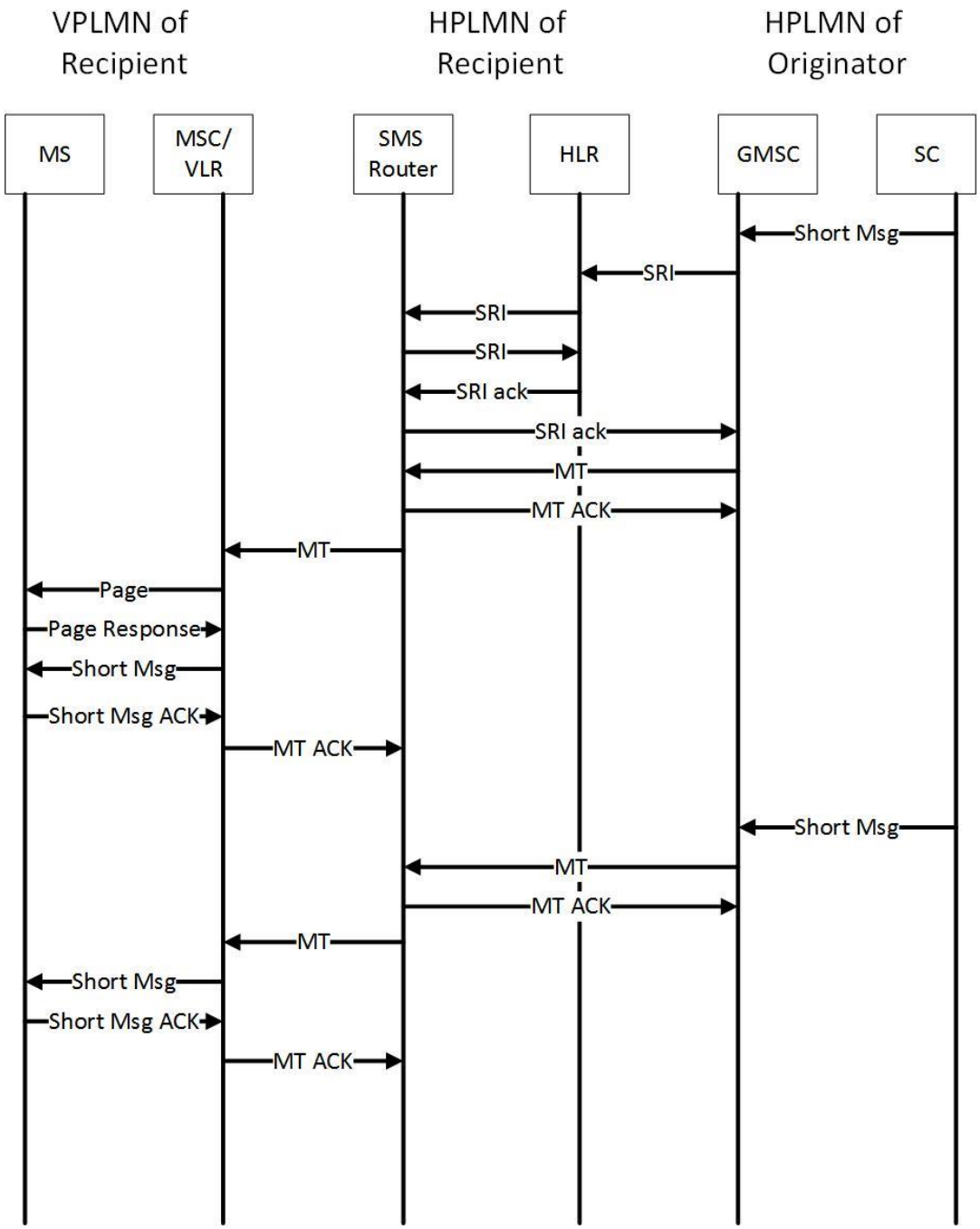
در این حالت پاسخ ACK یا NACK مربوط به پیام‌ها زمانی به اپراتور فرستنده پیام ارسال می‌شود که Home Router پاسخ را دریافت کرده باشد. در شکل ۲ روش ارسال پیام در روش Transparent نشان داده شده است.



شکل ۲: سناریوی ارسال پیام کوتاه در حضور Home Router (حالت Transparent)

ب. Non Transparent Mode

در این حالت Home Router پس از دریافت MT از اپراتور فرستنده پیام، ابتدا و قبل از ارسال MT به مشترک مقصد، یک پیام Ack به سمت ارسال کننده پیام می‌فرستد و سپس پیام را برای اپراتور گیرنده ارسال می‌نماید.

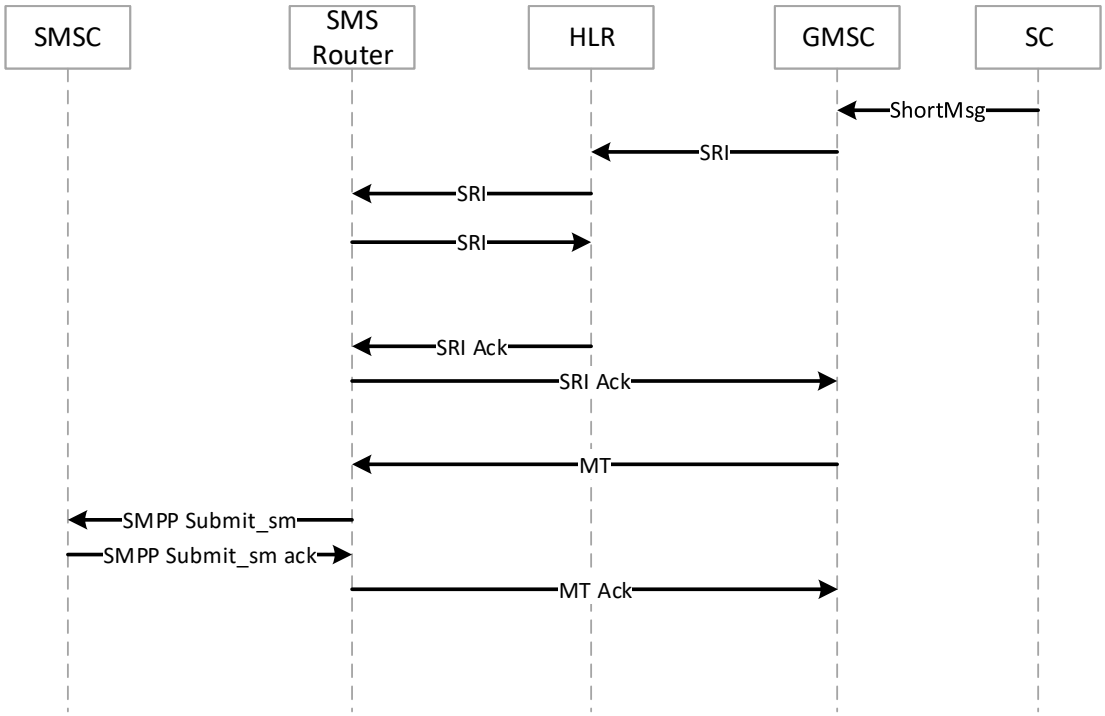


شکل ۳: سناریوی ارسال پیام کوتاه در حضور Home Router (حالت Non-Transparent)

ج. تحویل پیام به نرم افزار تحویل گیرنده با استفاده از پروتکل SMPP

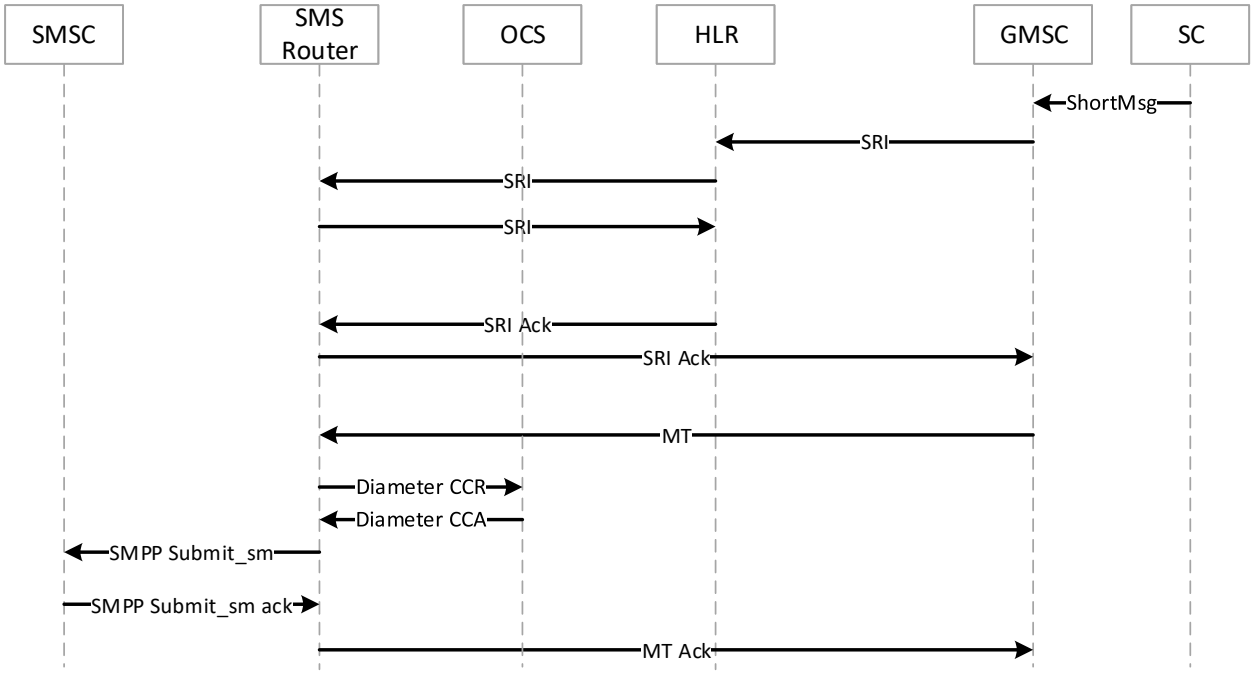
در این حالت، پیام‌های ارسال شده توسط مشترکین اپراتورهای دیگر باید به یک نرم افزار ارسال پیام کوتاه (که عموما به SMSC اپراتور خانگی متصل است) ارسال شود. در واقع، در این حالت، مقصد پیام، یک نرم افزار دریافت کننده پیام است و نه یکی از مشترکین تلفن همراه اپراتور خانگی.

از آنجا که شماره یا سرشماره‌های متعلق به نرم افزارهای ارسال پیام، در HSS اپراتور خانگی تعریف نشده اند، در این حالت و برخلاف دو حالت قبلی، Home Router پس از دریافت پیام SRI4SM، این پیام را به سمت HSS ارسال نمی‌کند و پاسخ SRI4SM را از روی پیکربندی‌های انجام شده توسط اپراتور آماده کرده و به ارسال کننده می‌فرستد. پس از آن، Home Router پیام MT را دریافت نموده و آن را از طریق پروتکل SMPP (در قالب پیام Submit_sm) به SMSC اپراتور خانگی تحویل می‌دهد. پس از دریافت پاسخ از SMSC، پاسخ بسته MT را به ارسال کننده می‌فرستد. در شکل ٤، سیگنالینگ در این حالت نشان داده شده است.



شکل ٤: تحویل پیام به نرم افزار تحویل گیرنده با استفاده از پروتکل SMPP

در حالت اخیر، امکان شارژ مشترک مقصد (نرم افزار دریافت کننده پیام) نیز وجود دارد. با توجه به نیازمندی اپراتور، در حال حاضر از پروتکل Diameter برای بررسی و شارژ مشترک مقصد استفاده می‌شود. در شکل ۵، سیگنالینگ مربوط به بررسی شارژ نیز به فرآیند تحویل افزوده شده است.



شکل ۵: تحویل پیام به نرم افزار تحویل گیرنده و شارژ با استفاده از پروتکل Diameter

٤,٢ معماری کلان نرم افزاری

سامانه Home Router از تعدادی مؤلفه نرم‌افزاری تشکیل شده است که این مؤلفه‌ها طبق طراحی مشخصی بر روی تعدادی ماشین مجازی نصب می‌شوند. در ادامه به صورت مختصر این معماری معرفی می‌شود و به تفصیل در بخش‌های بعدی، هر مؤلفه، بررسی خواهد شد.

ارتباطات این سامانه با سایر اجزا شبکه شامل موارد زیر است:

- رابطه سامانه با شبکه SS7/SIGTRAN، لینک‌های M3UA هستند که بسته‌های ورودی از این طریق وارد سامانه می‌شوند. بسته‌های مجاز برای این سامانه، SRI و پاسخ آن و MTForwardSM

و پاسخ آن است. هر بسته دیگری، نامرتبط خواهد بود. بسته‌های خروجی به سمت شبکه SS7/SIGTRAN از طریق همین رابط وارد شبکه SS7 می‌شوند.

- رابطه سامانه با مرکز پیام کوتاه (SMSC): بسته‌هایی که باید به نرم افزارهای دریافت پیام تحویل داده شوند، از طریق واسط پروتکلی SMPP به مرکز پیام کوتاه تحویل داده می‌شوند.
- رابطه سامانه با مرکز OCS اپراتور: در صورت پیکربندی اپراتور، نرم افزار دریافت کننده پیام، قبل از دریافت پیام شارژ می‌گردد. فرآیند شارژ توسط سیستم Home Router و با استفاده از پروتکل Diameter انجام می‌شود.
- رابط کاربری گرافیکی: که به صورت یک واسط تحت وب است که کاربر می‌تواند از طریق آن گزارشات مختلف سیستم را مشاهده کند و همین‌طور، قوانین را به دلخواه خود تغییر دهد (واسط تحت وب نیازی به اتصال به اینترنت ندارد)
- Zabbix: سیستم مدیریت رخدادها که از طریق آن وضعیت نرم افزارها، منابع و سرویس پایش می‌شود. تریگرهای از پیش تعریف شده در این سیستم، رخدادهای مهم و حیاتی سیستم را در قالب یک واسط تحت وب در اختیار کاربر قرار می‌دهد. امکان تعریف تریگرهای موردنیاز آتی و اتصال آن به Zabbix مرکزی اپراتور نیز وجود دارد.
- OMC: سیستم مدیریت شمارنده‌ها، KPI ها و پیکربندی‌های سیستم است که از طریق آن می‌توان به شمارنده‌های مؤلفه‌ها و همچنین برخی از تنظیمات، دسترسی پیدا کرد.

ارتباطات داخلی اجزا به صورت خلاصه به شرح زیر است:

بسته‌های سیگنالینگی از طریق لینک‌های SIGTRAN/M3UA وارد ماژول سیگنالینگ می‌شوند. این ماژول، مدیریت لینک‌های سیگنالینگ، مسیردهی بسته‌ها و ترجمه بسته‌های پروتکل MAP به پروتکل‌های داخلی سیستم را بر عهده دارد. علاوه بر آن، ارسال پیام‌ها به مرکز پیام (SMSC) که از طریق پروتکل SMPP انجام می‌شود نیز از طریق همین ماژول انجام می‌شود.

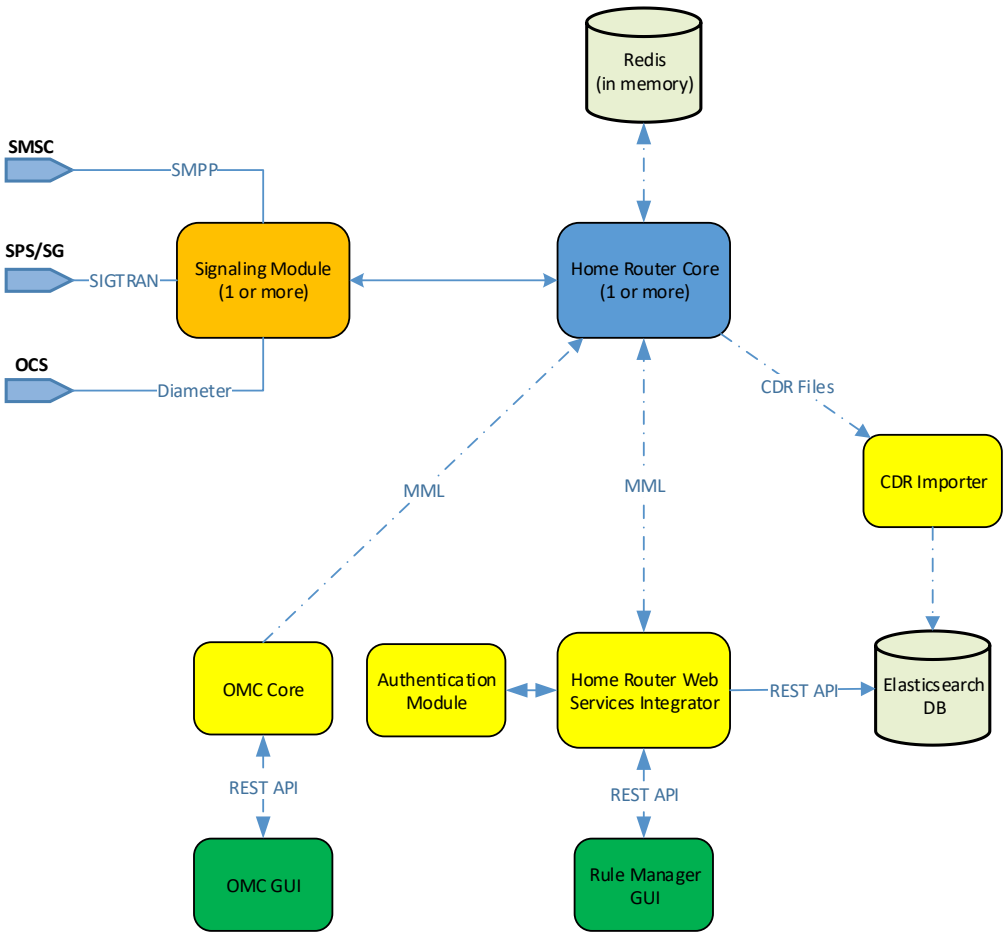
قلب سامانه، مؤلفه Home Router Core است که عملیات پردازش بسته‌های ورودی و تعامل با شبکه SS7 را بر عهده دارد. از این مؤلفه می‌توان به صورت کلاستر شده و به تعداد لازم برای ظرفیت‌های بیشتر استفاده کرد.

قوانین تعریف شده توسط اپراتور توسط این ماژول بر روی پیام‌ها و جریان‌های عبوری اعمال می‌شوند. این مؤلفه پاسخ‌های مناسب با توجه به قوانین خود، برای درخواست‌های شبکه فراهم می‌کند و جزئیات مورد نیاز را در قالب فایل‌های CDR ذخیره می‌کند. گزارش‌گیری با استفاده از این فایل‌های CDR انجام می‌شود.

مؤلفه CDR Importer فایل‌های CDR که توسط مؤلفه‌های Home Router Core تهیه شده‌اند را در قالب رکوردهای json وارد پایگاه داده Elasticsearch می‌کند.

مولفه Home Router Web Services Integrator به عنوان یک وب سرور، امکان دسترسی به سرویس-های مختلف مولفه‌های مختلف را برای GUI فراهم می‌نماید. واسط گرافیکی (GUI) از طریق این مولفه، امکان تغییر قوانین در حین اجرا و همین‌طور مشاهده گزارشات مختلف را برای کاربران فراهم می‌سازد.

در شکل ٦، نمایی کلی از معماری نرم افزاری این سامانه نشان داده شده است.



شکل ٦: نمایی کلی از مولفه‌ها و طراحی Home Router پیک‌آسا

٤,٣ ماژول سیگنالینگ

زیرسیستم سیگنالینگ ماژولی نرم افزاری برای برقراری ارتباط SIGTRAN/M3UA با شبکه SS7 و ارتباط SMPP با مرکز پیام کوتاه است. این زیرسیستم دارای وظایف و قابلیت‌های زیر می‌باشد:

- ایجاد لینک‌های سیگنالینگی مابین سیستم و نودهای خارجی مانند Signaling Gateway ها (M3UA)
- ایجاد لینک‌های SMPP ورژن ٣,٤ با مرکز پیام کوتاه (در نقش کلاینت)
- ایجاد لینک Diameter با مرکز OCS (در نقش کلاینت)
- مسیریابی براساس نوع پروتکل
- مسیریابی براساس SubSystemNumber، GlobalTitle و Destination PointCode (مربوط به پیام‌های SCCP)
- مسیریابی براساس شماره ارسال کننده و دریافت کننده (مربوط به پیام‌های SMPP)
- انطباق کامل با پروتکل‌های SCTP، M3UA، SCCP، TCAP و MAP مبتنی بر استانداردهای 3GPP.
- انطباق کامل با پروتکل SMPP v3.4
- انطباق با توصیف 3GPP TS 32.299 (شارژینگ Diameter)
- مدیریت جریان بار ورودی و خروجی (Flow Control)
- توزیع بار ورودی بر روی کلاسترهای مختلف مبتنی بر شماهای مختلف و قابل پیکربندی (براساس شماره‌های ارسال کننده و دریافت کننده، نوع پیام‌های دریافتی، میزان بار و ...)
- معماری Fault Tolerant توزیع شده

Home Router Core ۴,۴

این مؤلفه هسته اصلی Home Router است و تمامی قابلیت‌ها و عملکردهای مرتبط با Home Routing را پیاده سازی می‌نماید. ساز و کار اصلی این نرم افزار با استفاده از قوانین قابل تعریف و تنظیم توسط کاربر سیستم کنترل می‌شود. این قوانین توسط کاربر هم قبل از اجرای برنامه و هم در حین اجرای برنامه قابل تغییر هستند و به گونه‌ای طراحی شده‌اند که آزادی عمل بسیار زیادی برای تعریف قوانین متنوع وجود داشته باشد.

در ادامه قابلیت‌های مهم به کار گرفته شده در این نرم افزار شرح داده شده است.

أ. پیاده سازی سناریوی استاندارد Home Routing

سناریوی استاندارد Home Routing به این شرح است: یک پیام SRI4SM در شبکه اپراتور خانگی دریافت می‌شود. به صلاحدید اپراتور و براساس شروط دلخواه، این پیام می‌تواند به مرکز Home Router ارسال شود. مرکز Home Router پیام SRI4SM را مجددا به شبکه بازگردانده و از آنجا که پیام جدید توسط یک مرکز معتبر (Home Router خانگی اپراتور) ارسال شده است، با پاسخ همراه خواهد شد. در پاسخ SRI4SM دریافت شده، شماره IMSI کاربر و شماره GT سوییچ سرویس دهنده به مشترک، برگردانده می‌شود. در این مرحله، Home Router پاسخ بسته SRI4SM اولیه را ارسال می‌کند. در این پاسخ، آدرس سوییچ سرویس دهنده به مشترک، با آدرس Home Router جایگزین می‌شود تا پیام MT به دست Home Router برسد. پس از دریافت پیام MT، سیستم Home Router پیام را به مقصد سوییچ اصلی سرویس دهنده به مشترک ارسال نموده و پاسخ دریافتی را برای مرکز پیام کوتاه ارسال کننده باز می‌فرستد.

ب.مسیریابی پیام‌ها به مقصد نرم افزار

نرم افزار Home Router Core می‌تواند براساس طرح مسیریابی تنظیم شده توسط اپراتور، پیام‌های ارسال شده به برخی شماره‌ها را به یک نرم افزار دریافت کننده پیام تحویل دهد (به عبارت دیگر، مشترک مقصد در این حالت مشترک تلفن همراه نیست). در این حالت، Home Router Core براساس طرح مسیریابی، پیام SRI4SM دریافت شده را بدون استعلام از HSS پاسخ می‌دهد (IMSI مشترک را به دلخواه قرار می‌دهد). پس از دریافت پیام MT، این پیام را در قالب بسته Submit_sm در پروتکل SMPP به مرکز پیام کوتاه تحویل می‌دهد.

ج. شارژ نرم افزار دریافت کننده پیام

نرم افزار Home Router Core می‌تواند براساس طرح تنظیم شده توسط اپراتور، نرم افزار دریافت کننده پیام را با استفاده از پروتکل Diameter و از طریق OCS اپراتور شارژ نماید. در این حالت و پس از دریافت پیام MT، ابتدا یک پیام Diameter CCR به سامانه OCS ارسال می‌گردد. در صورت تایید سامانه OCS، پیام از طریق پروتکل SMPP به مرکز پیام کوتاه تحویل داده می‌شود و در غیر این صورت، کدخطای از پیش تعریف شده توسط اپراتور بازگردانده می‌شود.

در طرح شارژینگ نرم افزار، عنصری در سیستم با نام CP تعریف می‌گردد. این عنصر، متناظر با پروفایلی است که نرم افزار گیرنده پیام در سامانه OCS اپراتور دارد. هر CP می‌تواند دارای لیستی از شماره/سرشماره-ها باشد. هنگام بررسی شارژ یک شماره/سرشماره، المان CP شارژ شود. به عبارت دیگر مالک مجموعه‌ای از سرشماره‌ها به صورت یکجا شارژ می‌شود و نه براساس سرشماره‌های مجزایی که متعلق به آنهاست.

د. پنهان سازی اطلاعات کاربر و شبکه

در سناریوی Home Routing، تمام یا بخشی از پیام‌های SRI4SM مورد نظر اپراتور به سامانه Home Router فرستاده می‌شوند تا توسط این سامانه پاسخ داده شوند. سامانه Home Router، در پاسخ پیام‌های SRI4SM دو پارامتر مهم را تغییر می‌دهد:

اول: آدرس سوییچ سرویس دهنده به مشترک را با آدرس Home Router جایگزین می‌نماید. با این جایگزینی، در وهله اول پیام MT توسط Home Router دریافت شده و امکان اعمال سیاست‌های مختلف بر روی آن فراهم می‌شود و در وهله دوم آدرس سوییچ‌های شبکه به بیرون از اپراتور ارسال نمی‌شود.

دوم: آدرس IMSI مشترک با یک آدرس رندم جایگزین می‌شود. این آدرس به صورت رندم ایجاد می‌شود و تنها برای یک دقیقه معتبر هستند. آدرس رندم ایجاد شده در محدوده IMSI های اپراتور خانگی ساخته می‌شود اما تناظر یک به یک با IMSI مشترکین ندارد. به عبارت دیگر، در هر بار ارسال SRI4SM برای یک مشترک، یک عدد رندم جدید به عنوان IMSI مشترک ارسال می‌شود. با این تغییر، شناسه منحصر به فرد و مهم مشترک (آدرس IMSI) از دید شبکه بیرون اپراتور پنهان خواهد ماند و امکان سواستفاده از آن کاهش خواهد یافت.

۵. قوانین کنترلی

نرم افزار Home Router Core امکان تعریف طیف وسیعی از قوانین کنترلی و نظارتی را فراهم می‌سازد. در این نرم افزار و براساس پارامترهای زیر می‌توان فیلتر تعریف نمود:

۱: آدرس Global Title ارسال کننده بسته SRI4SM

۲: آدرس ارسال کننده پیام SRI (مقدار پارامتر ServiceCenterAddress در لایه MAP)

۳: آدرس MSC واقعی مشترک (دریافت شده در پاسخ بسته ی SRI)

٤: آدرس IMSI واقعی مشترک مقصد (دریافت شده در پاسخ بسته ی SRI)

۵: آدرس SMSC ارسال کننده پیام MT (مقدار پارامتر sm-RP-OA)

٦: آدرس Global Title ارسال کننده پیام MT

۷: آدرس MSISDN ارسال کننده پیام (مقدار پارامتر TP-Originating-Address)

۸: آدرس MSISDN مشترک مقصد (دریافت شده در بسته SRI)

۹: مقدار پارامتر TP-DCS در بسته MT

پس از اعمال فیلتر بر روی بسته‌های ورودی، امکان اعمال چندین اقدام روی آنها وجود دارد:

۱- بلوکه سازی: در این اقدام بسته دریافت شده بلوکه شده و مبتنی بر تنظیم کاربر، برای ارسال کننده پاسخ موفق یا ناموفق (با کدخطای قابل پیکربندی به ازای هر قانون) ارسال می‌شود.

۲- عبور: در این اقدام بسته دریافت شده با توجه به سناریوی اصلی Home Routing برای مقصد ارسال می‌شود.

۳- رله: در این اقدام که برای بسته‌های SRI4SM قابل تعریف است، Home Router آدرس سوییچ سرویس دهنده و IMSI واقعی مشترک را در بسته SRI4SM برای ارسال کننده ارسال می‌کند. در این حالت، پیام MT مستقیم به سوییچ سرویس دهنده رله می‌شود و توسط Home Router روی آن کنترلی انجام نمی‌شود.

به طور معمول، قانون پیش فرض Home Router یک قانون بلوکه کننده است. بنابراین اپراتور می‌بایست قانون‌هایی جهت مجاز نمودن عبور پیام‌ها در سیستم تعریف نماید (بخشی زیادی از این قوانین به صورت پیش فرض در سیستم تعریف گردیده و قابل ویرایش هستند)

مهمترین قانون هایی که به طور معمول موردنیاز اپراتور بوده و در سیستم Home Router قابل تعریف است به شرح زیر است:

۱- تعریف لیست سیاه شماره یا پیش شماره‌های ارسال کننده

۲- تعریف لیست سفید شماره یا پیش شماره‌های ارسال کننده

۳- تعریف لیست سفید شماره یا پیش شماره‌های ارسال کننده از یک یا چند آدرس GT ارسال کننده خاص

٤- تعریف لیست سفید شماره یا پیش شماره‌های ارسال کننده به تفکیک اپراتورهای مختلف

٥- تعریف لیست مجاز مقدار DCS پیام‌های عبوری به تفکیک سرشماره/اپراتور ارسال کننده

٦- تعریف لیست سیاه شماره‌های دریافت کننده

۷- تعریف لیست سیاه سوییچ‌های مقصد

۸- تعریف لیست سیاه اپراتورهای مقصد (وضعیت رومینگ مشترک مقصد)

علاوه بر موارد فوق، تمام ترکیب‌های ممکن از حالت‌های مختلف در سیستم منعطف مدیریت قانون در Home Router قابل تعریف است.

و. بلوکه سازی پیام MT بدون پیام SRI4SM متناظر

در صورتی که یک پیام MT بدون دریافت یک پیام SRI4SM متناظر با آن توسط Home Router دریافت شود، پیام بلوکه شده و پاسخ ناموفق برای ارسال کننده فرستاده می‌شود.

ز. توسعه پذیری بالا

با توجه به Stateless بودن نرم افزار Home Router Core، با اختصاص منابع لازم و اجرای نسخه‌های بیشتر، می‌توان ظرفیت سیستم Home Router را افزایش داد.

ح. ثبت فایل جزییات پیام‌ها (CDR)

هر رکورد CDR در یک خط ذخیره می‌شود و اطلاعات آن با استفاده از "," از هم جدا می‌شوند. اطلاعات مختلف موجود در CDR، از پارامترهای بسته‌های مختلف موجود در یک سناریو (SRI، MTForward ها و پاسخ‌های آنها) استخراج می‌شوند.

اطلاعاتی که از بسته‌های SRI، پاسخ آن و عملیات انجام شده بر روی آنها استخراج می‌شوند به شرح زیر است:

- زمان رسیدن بسته SRI4SM
- آدرس SCCP ارسال کننده SRI4SM (Calling GT)
- مقدار پارامتر MSISDN (شماره گیرنده پیام)
- آدرس SCCP ارسال کننده SRI4SM (MAP-SC)
- مقدار پارامتر sm-RP-PRI
- زمان ارسال SRI4SM به HLR توسط HR
- زمان دریافت پاسخ SRI4SM از HLR
- IMSI واقعی گیرنده پیام
- آدرس MSC واقعی دریافت کننده پیام
- نتیجه پاسخ SRI4SM (کد خطا یا ۰ برای وضعیت موفق)
- نتیجه پاسخ SRI4SM ارسال شده توسط HR (کد خطا یا ۰ برای وضعیت موفق)
- آدرس MSC ارسال شده در پاسخ SRI4SM (آدرس HR)
- IMSI غیرواقعی تولید شده توسط HR
- زمان ارسال پاسخ SRI4SM

اطلاعاتی که از بسته‌های MTForward، پاسخ آن و عملیات انجام شده بر روی آنها استخراج می‌شوند به شرح زیر است:

- زمان دریافت بسته MT
- شماره MSISDN ارسال کننده پیام

- آدرس SCCP ارسال کننده پیام MT (Calling GT)
- آدرس SMSC ارسال کننده پیام (پارامتر sm-RP-OA)
- طول پیام
- مقدار پارامتر TP-PID
- مقدار پارامتر TP-DCS
- تعداد بخش‌های MT مربوط به یک flow
- شماره بخش MT
- متن پیام دریافتی (در صورت بلوکه شدن پیام و فعال سازی در بخش قوانین)
- زمان ارسال بسته MT
- زمان دریافت پاسخ MT
- نتیجه پاسخ MT (کد خطا یا ۰ برای وضعیت موفق)
- نتیجه پاسخ MT ارسال شده توسط HR (کد خطا یا ۰ برای وضعیت موفق)
- زمان ارسال پاسخ MT

اطلاعاتی که از وضعیت نهایی Flow استخراج می‌شوند به شرح زیر است:

جدول ۳۰- اطلاعات قابل استخراج از وضعیت نهایی Flow

شناسه یکتای Flow (ایجاد شده توسط HR)	Id
شناسه یکتای مقصد پیام (SS7 یا یکی از اتصالات SMPP)	DestinationRoute

FlowSummary	وضعیت نهایی Flow که شامل مقادیر است: Delivered MT_Blocked SRI_Blocked MT_Nack SRI_Nack MT_Timeout MT_Resp_Timeout SRI_Timeout SRI_Without_MT MT_Without_SRI Out_of_order Server_Busy State_Not_Found
LoggedTimeStamp	زمان ثبت CDR (با فرمت timestamp)
LoggedTimeLocal	زمان ثبت CDR (با فرمت تاریخ)

٤,٥ دیتابیس‌ها

در سیستم Home Router و برای کاربردهای مختلف، از چند دیتابیس متفاوت استفاده شده است.

أ. دیتابیس Redis

از آنجا که پیام‌های SRI4SM و MT دریافت شده برای هر پیام کوتاه، مستقل از هم ارسال می‌شوند، نرم افزار Home Router Core باید مقدار IMSI واقعی و آدرس MSC سرویس دهنده به مشترک را که در پاسخ پیام SRI4SM دریافت می‌نماید را تا رسیدن پیام MT نگهداری نماید. از آنجا که ذخیره سازی و واکشی مجدد این مقادیر باید با سرعت بالا انجام گیرد، از دیتابیس Redis استفاده شده است. این دیتابیس یک دیتابیس درون حافظه‌ای (In-memory Database) است که برای تراکنش‌های با تعداد و سرعت بالا توصیه گردیده است.

ب.دیتابیس MySQL

واسط مدیریتی سامانه Home Router داده‌هایی مانند پیکربندی‌های سیستمی، نام کاربران، رمزهای عبور و ... را در دیتابیس MySQL نگهداری می‌نماید.

ج. دیتابیس Elasticsearch

دیتابیس Elasticsearch یک دیتابیس NoSQL است که می‌توان داده‌های مختلف با مشخصات متفاوت را در آن ذخیره سازی نمود. در سیستم Home Router، از این دیتابیس برای ذخیره سازی تمامی رکوردهای CDR، جزییات عملکرد کاربران در واسط مدیریتی و تمامی لاگ‌های سیستم استفاده می‌شود. دیتابیس Elasticsearch دارای ویژگی‌های مهمی است که بهره گیری از آن در سیستم Home Router را توجیه می‌نماید. از مهمترین ویژگی‌های این دیتابیس می‌توان به موارد زیر اشاره نمود:

- پشتیبانی از توزیع شدگی و توسعه (با افزایش داده‌ها و منابع در اختیار و بدون راه اندازی مجدد یا از بین رفتن داده‌های قبلی، امکان توزیع و توسعه دیتابیس وجود دارد)

- ذخیره سازی داده‌ها بدون شمای از پیش تعریف شده (تغییر شمای داده‌ها مثلا اضافه یا کم شدن فیلدهایی به رکوردهای CDR نیازمند تغییر در دیتابیس نیست)

- پردازش و ایندکس گذاری متنی (روی فیلدهای زیادی از دیتابیس می‌توان عملیات جستجو و تجمیع را با سرعت بالا انجام داد. به عبارت دیگر، لازم نیست فیلدهای شرکت کننده در عملیات جستجو و تجمیع از ابتدای طراحی مشخص و محدود باشند)

- واسط‌های گزارش‌گیری ساده و شبیه به SQL (در صورت نیاز به دسترسی مستقیم به دیتابیس، واسط‌های آن برای اپراتور و کاربران احتمالی، ساده و قابل فهم است)

OMC ۴,۶

ماژول OMC که شامل یک نرم افزار هسته و یک پوسته تحت وب است، وظیفه جمع آوری شمارنده‌های سیستم، فراهم سازی امکان گزارش‌گیری‌های آماری و فراهم‌سازی امکان مشاهده و تغییر برخی از پیکربندی‌های سیستمی را فراهم می‌سازد. مهمترین قابلیت‌های این ماژول به شرح زیر است:

۱- امکان تعریف KPI

۲- امکان گزارش‌گیری‌های تجمیعی برحسب زمان از شمارنده و KPI ها (ساعت به ساعت، روزانه، ماهانه)

۳- امکان تعریف گراف روی شمارنده یا KPI ها

٤- امکان مشاهده پیکربندی‌های سیستمی و تغییر آنلاین پیکربندی‌های مجاز

مجموعه شمارنده‌های موجود در سیستم Home Router به شرح زیر است:

أ. شمارنده‌های عمومی

- Total_received: تعداد بسته‌هایی که توسط نرم افزار دریافت شده است، اعم از SRI، MT و پاسخ‌های آنها
- Received_HLR_QUERY: تعداد بسته‌های SRI دریافت شده
- Received_HLR_QUERY_ACK: تعداد بسته‌های پاسخ SRI که حاوی نتیجه موفق باشند
- Received_HLR_QUERY_NACK: تعداد بسته‌های پاسخ SRI که حاوی کدخطا باشند (ناموفق)
- Received_MT_FORWARD: تعداد بسته‌های MT دریافت شده
- Received_ACK_DELIVER_REPORT: تعداد بسته‌های پاسخ MT که حاوی نتیجه موفق باشند
- Received_ERROR_DELIVER_REPORT: تعداد بسته‌های پاسخ MT که حاوی کدخطا باشند (ناموفق)
- Decode_Failed: تعداد بسته‌هایی که دیکد آنها با مشکل مواجه شده است (به دلیل ناقص بودن، نامرتبط بودن یا وجود نقصی در پارامترهای بسته دریافتی)

- Received_Invalid_MSU: تعداد بسته‌های دریافتی که نامرتبط هستند (SRI، MT یا پاسخ آنها نباشند. این تعداد در متغیر Decode_Failed هم شمرده می‌شوند)
- timeout_HLR: هنگامی که یک درخواست SRI به سمت HLR ارسال شود و پاسخی در مدت زمان معین دریافت نشود، این متغیر شمرده می‌شود.
- timeout_HLR_Resp: هنگامی که پاسخ یک درخواست SRI ارسال شود و در مدت زمان معین بسته MT متناظر با آن دریافت نشود، این متغیر شمرده می‌شود.
- timeout_MT: هنگامی که یک درخواست MT به سمت سوییچ مقصد ارسال شود و پاسخی در مدت زمان معین دریافت نشود، این متغیر شمرده می‌شود.
- timeout_MT_Resp: هنگامی که پاسخ یک درخواست MT ارسال شود و بسته MT بعدی که حاوی بخش بعدی از پیام کوتاه است در مدت زمان معین دریافت نشود، این متغیر شمرده می‌شود (اگر MT پاسخ داده شده آخرین بسته در دیالوگ TCAP باشد این متغیر شمرده نخواهد شد)
- Pre_State_Not_Found: هنگامی که بسته‌ای غیر از SRI به سیستم می‌رسد و سیستم به دلایلی، نمی‌تواند State ذخیره شده برای Flow مربوط به آن بسته را بیابد (مثلا به دلیل بروز اختلال در پایگاه داده Redis یا منقضی شدن Flow قبل از رسیدن بسته اخیر) این متغیر شمرده می‌شود.
- Succeeded_Flows: اگر Flow کامل شود و پیامک به صورت صحیح و کامل به دست کاربر برسد، این متغیر شمرده می‌شود. وقتی Flow بلوکه می‌شود شمرده شدن یا نشدن این متغیر مکانیزم دیگری دارد که در بخش مربوط به بلوکه شدن به طور کامل توضیح داده شده است.
- Failed_Flows: اگر Flow به هر دلیل اعم از بلوکه شدن توسط بخش مدیریت قوانین، ناقص بماند و یا با خطا توسط HLR یا سوییچ مقصد، مواجه شود و پیام کوتاه در نهایت به دست کاربر نرسد این متغیر شمرده خواهد شد (در نظر گرفته شود که در یک Flow ممکن است بیش از یک پیام وجود داشته باشد و یک پیام هم ممکن است به وسیله بیش از یک Flow ارسال شود، این متغیر و متغیر قبلی، تعداد Flow ها را می‌شمارد نه پیام‌های کوتاه را).
- Server_Busy: اگر ترافیک ورودی از آستانه تحمل تعریف شده بیشتر شود، این متغیر شمرده می‌شود.
- Out_Of_Order: اگر بسته‌ای دریافت شود که با توجه به وضعیت Flow مورد انتظار نباشد (مثلا قبل از دریافت پاسخ بسته MT ارسال شده، پیام MT دیگری دریافت شود) این متغیر شمرده می‌شود.

- ActiveJobs: تعداد job های فعال را نمایش می‌دهد. مقدار این شمارنده می‌تواند نمودی از میزان ترافیک ورودی باشد. اگر تعداد job های فعال از حد آستانه بیشتر شود، وضعیت سیستم به server_busy تغییر خواهد کرد.
- AverageRespTime_us: میانگین زمان پاسخ برای ٦٥٥٣٦ بسته دریافتی قبلی
- MaxRespTime_us: حداکثر زمان پاسخ برای ٦٥٥٣٦ بسته دریافتی قبلی

ب.شمارنده‌های مربوط به پاسخ‌ها به تفکیک کد خطا

خطاهای مربوط به پاسخ بسته‌های SRI

- No_Error: تعداد پاسخ‌های موفق دریافت شده
- System_Failure: تعداد پاسخ‌های ناموفق با کد خطای ٣٤
- Data_Missing: تعداد پاسخ‌های ناموفق با کدخطای ٣٥
- Unexpected_Data_Value: تعداد پاسخ‌های ناموفق با کدخطای ٣٦
- Facility_Not_Supported: تعداد پاسخ‌های ناموفق با کدخطای ٢١
- Unknown_Subscriber: تعداد پاسخ‌های ناموفق با کدخطای ١
- Teleservice_Not_Provisioned: تعداد پاسخ‌های ناموفق با کدخطای ١١
- Call_Barred: تعداد پاسخ‌های ناموفق با کدخطای ١٣
- Absent_Subscriber_Sm: تعداد پاسخ‌های ناموفق با کدخطای ٢٧
- GGW_Timeout: تعداد پاسخ‌های ناموفق با کدخطای ٢٠٣ (کدخطای داخلی به معنای عدم دریافت پاسخ توسط ماژول سیگنالینگ)
- Other: تعداد پاسخ‌های ناموفق با کدخطایی غیر از کدخطاهای شمارش شده در سایر شمارنده‌ها

خطاهای مربوط به پاسخ بسته‌های MT

- No_Error: تعداد پاسخ‌های موفق دریافت شده
- System_Failure: تعداد پاسخ‌های ناموفق با کد خطای ٣٤
- Data_Missing: تعداد پاسخ‌های ناموفق با کد خطای ٣٥
- Unexpected_Data_Value: تعداد پاسخ‌های ناموفق با کد خطای ٣٦

- Facility_Not_Supported: تعداد پاسخ‌های ناموفق با کد خطای ۲۱
- Unidentified_Subscriber: تعداد پاسخ‌های ناموفق با کد خطای ۵
- illegal_Subscriber: تعداد پاسخ‌های ناموفق با کد خطای ۹
- illegal_Equipment: تعداد پاسخ‌های ناموفق با کد خطای ۱۲
- Subscriber_Busy_For_Mt_Sms: تعداد پاسخ‌های ناموفق با کد خطای ۳۱
- SM_Delivery_Failure: تعداد پاسخ‌های ناموفق با کد خطای ۳۲
- Absent_Subscriber_Sm: تعداد پاسخ‌های ناموفق با کد خطای ۲۷
- GGW_Timeout: تعداد پاسخ‌های ناموفق با کدخطای ۲۰۳ (کدخطای داخلی به معنای عدم دریافت پاسخ توسط ماژول سیگنالینگ)
- Other: تعداد پاسخ‌های ناموفق با کدخطایی غیر از کدخطاهای شمارش شده در سایر شمارنده‌ها

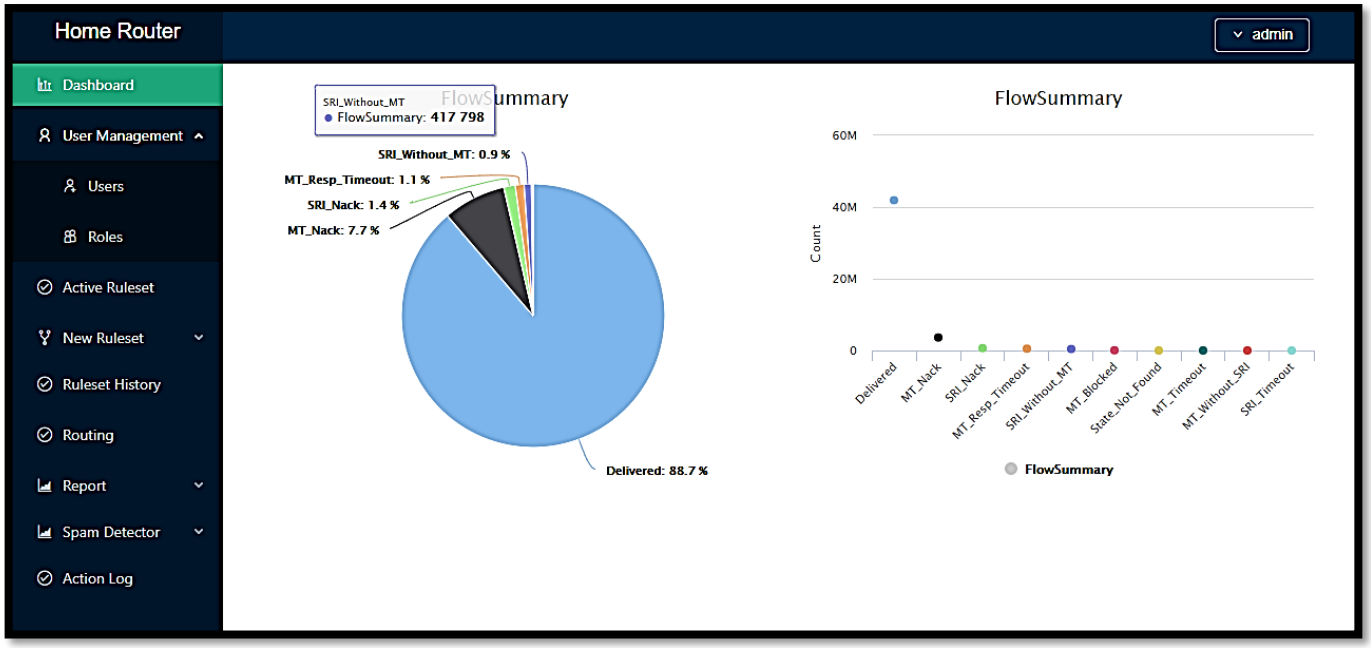
ج. شمارنده‌های مربوط به قوانین تعریف شده

به ازای هر قانون تعریف شده در بخش مدیریت قوانین، لیستی از شمارنده‌ها به شرح زیر وجود دارد:

- Applied: تعداد دفعاتی که قانون اعمال شده است
- ApplicationFailed: تعداد دفعاتی که حین اجرای عملیاتِ قانون مورد نظر خطا رخ داده است.
- Sent_HLR_Query: تعداد بسته‌های SRI که در نتیجه عملیاتِ قانون مورد نظر، ارسال شده است.
- Sent_HLR_Query_Ack: تعداد پاسخ‌های موفق بسته‌های SRI، که در نتیجه عملیاتِ قانون مورد نظر، ارسال شده است.
- Sent_HLR_Query_Nack: تعداد پاسخ‌های ناموفق بسته‌های SRI، که در نتیجه عملیاتِ قانون مورد نظر، ارسال شده است.
- Sent_MT_FORWARD: تعداد بسته‌های MT که در نتیجه عملیاتِ قانون مورد نظر، ارسال شده است.
- Sent_ACK_DELIVER_REPORT: تعداد پاسخ‌های موفق بسته‌های MT، که در نتیجه عملیاتِ قانون مورد نظر، ارسال شده است.
- Sent_ERROR_DELIVER_REPORT: تعداد پاسخ‌های ناموفق بسته‌های MT، که در نتیجه عملیاتِ قانون مورد نظر، ارسال شده است.

٤,٧ واسط گرافیکی مدیریتی

شکل ۷ نمایی از واسط گرافیکی مدیریتی سیستم Home Router را نشان می‌دهد.



شکل ۷: نمایی از واسط گرافیکی مدیریتی سیستم Home Router

قابلیت‌های واسط گرافیکی مدیریتی سیستم Home Router به شرح است:

- مدیریت کاربران (User Management)

در این بخش، امکان تعریف کاربر و اعطای مجوزهای دسترسی بخش‌های مختلف به آنها وجود دارد.

- مشاهده قوانین تعریف شده (Active Ruleset)

در این بخش، قوانین تعریف شده در سیستم و اجزا آن قابل مشاهده است. همچنین امکان ذخیره سازی و بازیابی مجدد قوانین آن در این بخش تعبیه شده است.

- تغییر قوانین تعریف شده (New Ruleset)

در این بخش، امکان تغییر قوانین و اجزای آن فراهم شده است. کاربر می‌تواند تمامی تغییرات موردنظر خود را انجام داده و سپس به صورت یکباره روی سیستم اعمال نماید.

- مشاهده تاریخچه تغییرات قوانین (Ruleset History)

در این بخش، امکان مشاهده تاریخچه تغییرات قوانین توسط کاربران مختلف وجود دارد. کاربرانی که به این بخش دسترسی دارند، می‌توانند مشاهده کنند که چه کاربری، در چه زمانی قوانین را تغییر داده است و این تغییرات چه بوده اند.

- تعریف مسیر یابی (Routing)

در این بخش، امکان تعریف، ویرایش و حذف مسیریابی (Routing) فراهم گردیده است. کاربر در این بخش می‌تواند مقصد مجموعه‌ای از شماره/سرشماره‌ها را مشخص نماید. مقصد پیام‌های دریافتی می‌تواند شبکه SS7 یا یکی از اتصالات SMPP سیستم با مراکز پیام کوتاه (SMSC) اپراتور باشد.

- گزارش‌گیری (Report)

در این بخش، کاربر می‌تواند گزارش‌های مختلفی از رکوردهای CDR تولید شده در سیستم Home Router اخذ نماید. جستجو و مشاهده جزییات رکوردها، گزارش‌های آماری و تجمیعی وگزارش‌های نموداری از امکانات فعلی این بخش هستند. علاوه بر این، کاربر می‌تواند شرایط و فیلترهایی که برای اخذ گزارش استفاده نموده است را ذخیره نموده و هر بار از آن استفاده نماید.

- مشاهده تاریخچه عملیات انجام شده (Action Log)

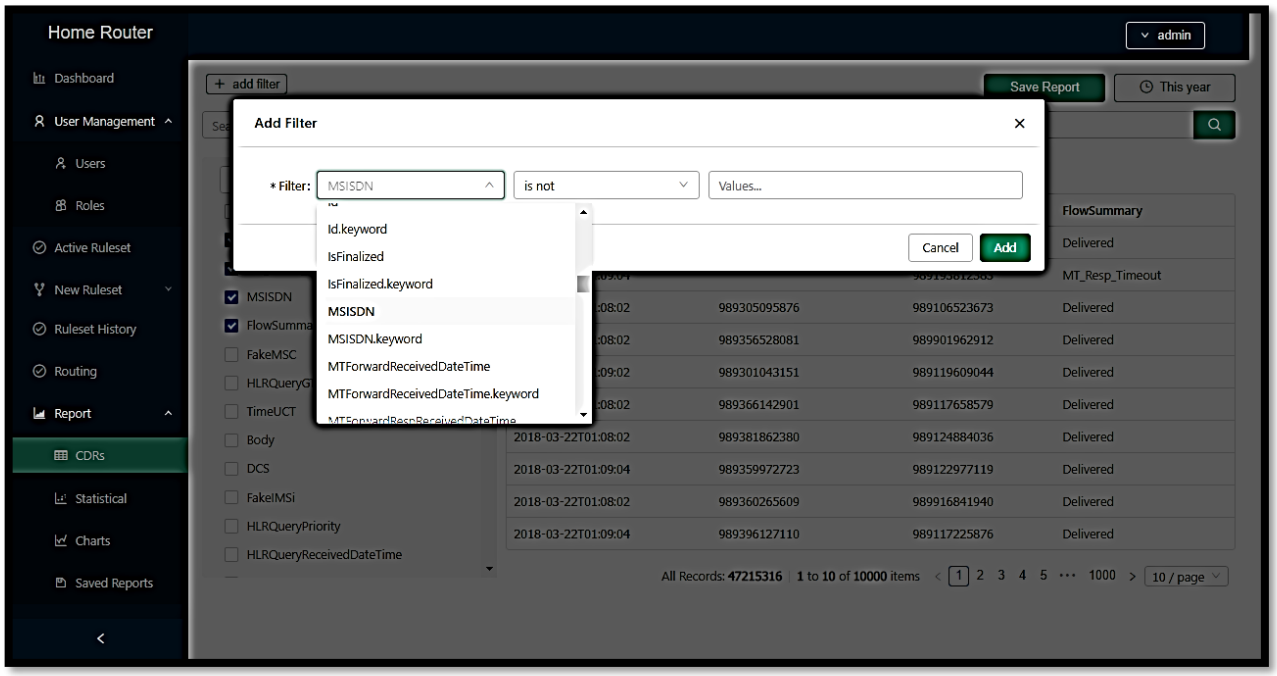
علاوه بر تاریخچه تغییرات قوانین، سایر عملیات انجام شده توسط کابران از جمله تعریف و حذف کاربران یا سطوح دسترسی آنها، گزارش‌های اخذ شده از سیستم، ورود و خروج به سیستم و ... در بخش مشاهده تاریخچه عملیات انجام شده قابل مشاهده است.

أ. قابلیت‌های گزارش‌گیری

قابلیت‌های بخش گزارش‌گیری واسط گرافیکی مدیریتی سیستم Home Router به شرح زیر است:

۱- سربرگ CDRs: در این سربرگ امکان جستجو و مشاهده ریز اطلاعات موجود در CDR ها فراهم شده است. در این بخش می‌توان با استفاده از عبارت‌های منطقی روی تمامی فیلدهای موجود در رکوردهای CDR، رکوردهای موجود در دیتابیس را فیلتر کرده و در یک فایل با فرمت CSV نیز ذخیره نمود. شکل ۸ نمایی از این سربرگ را نشان می‌دهد. همانطور که مشاهده می‌شود، امکان تعریف فیلترهای مختلف بر روی تمامی فیلدهای موجود در فایل‌های CDR و همچنین انتخاب فیلدهای مطلوب در خروجی گزارش نیز وجود دارد.

علاوه بر این، امکان ذخیره سازی قالب گزارش نیز وجود دارد (دکمه Save Report). کاربر با استفاده از این قابلیت می‌تواند گزارش جاری را به عنوان یک قالب ذخیره سازی نماید و پس از آن صرفا با انتخاب بازه زمانی مدنظر، گزارش مطلوب را دریافت نماید.

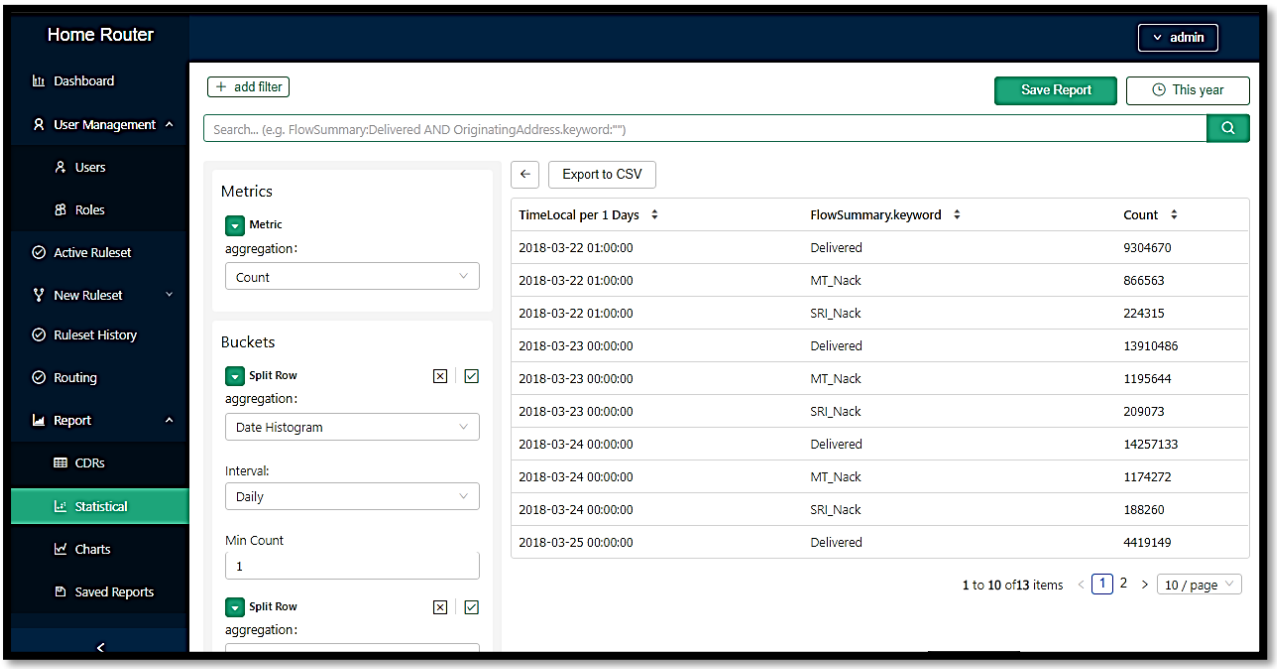


شکل ۸: نمایی از سربرگ CDRs

۲- سربرگ Statistical: در این سربرگ امکان گزارش‌گیری آماری و تجمعی فراهم گردیده است. در این بخش، می‌توان همانند بخش CDRs، فیلترهای منطقی بر روی تمامی فیلدهای موجود در CDR تعریف نمود. علاوه بر آن می‌توان تا ٤ سطح رکوردهای خروجی را دسته بندی نموده و آمار به تفکیک دسته بندی‌های مختلف را مشاهده نمود. به عنوان مثال می‌توان گزارش‌هایی مانند تعداد پیام‌های دریافتی از یک اپراتور خاص به تفکیک آدرس GT های ارسال کننده، به تفکیک کدخطا و به تفکیک ساعت در یک روز خاص را در این بخش از واسط گرافیکی اخذ نمود.

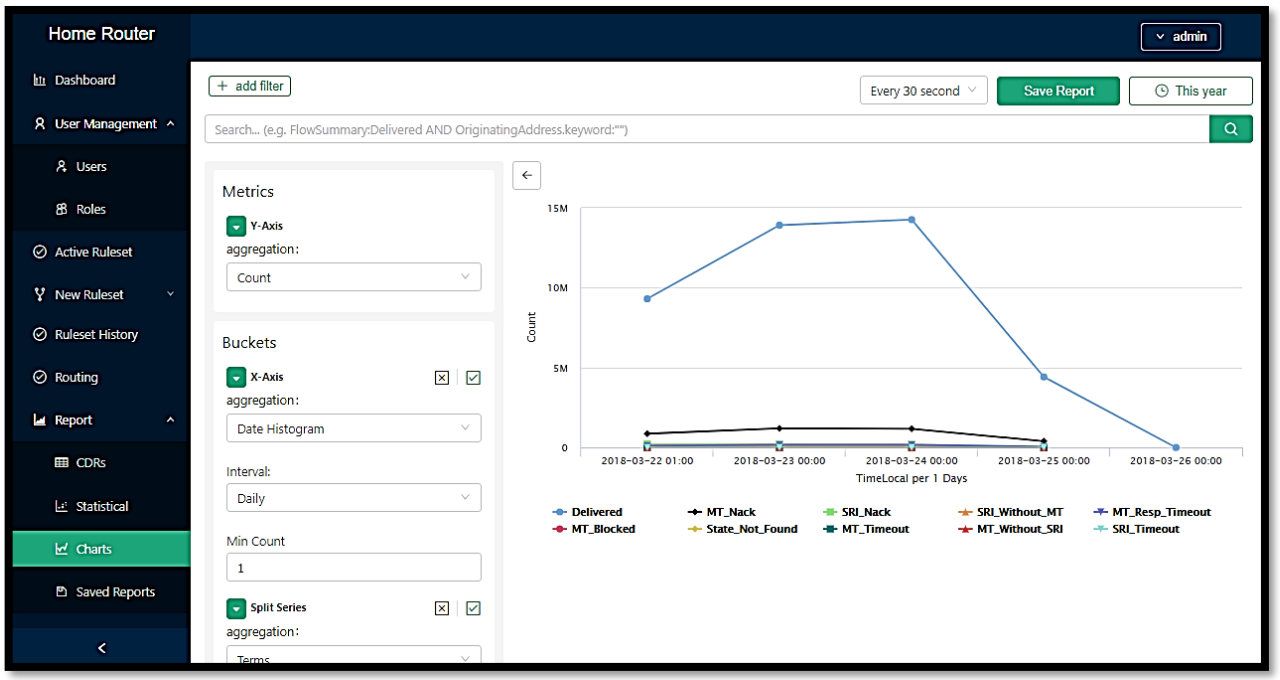
شکل ۹، نمایی از این سربرگ را نشان می‌دهد. در این مثال، مجموعه پیام‌های دریافت شده بر حسب وضعیت نهایی آنها (فیلد FlowSummary در رکوردهای CDR) و به صورت روز به روز تجمیع گردیده اند.

همانند بخش CDRs، امکان ذخیره سازی خروجی و همچنین امکان ذخیره سازی قالب گزارش نیز وجود دارد.



شکل ۹: نمایی از سربرگ Statistical

۳- سربرگ Charts: در این سربرگ امکان مشاهده گزارش‌های آماری و تجمیعی به صورت نمودار فراهم گردیده است. امکانات این بخش دقیقا مشابه با سربرگ Statistical است با این تفاوت که نتیجه به صورت نمودار نمایش داده می‌شود.

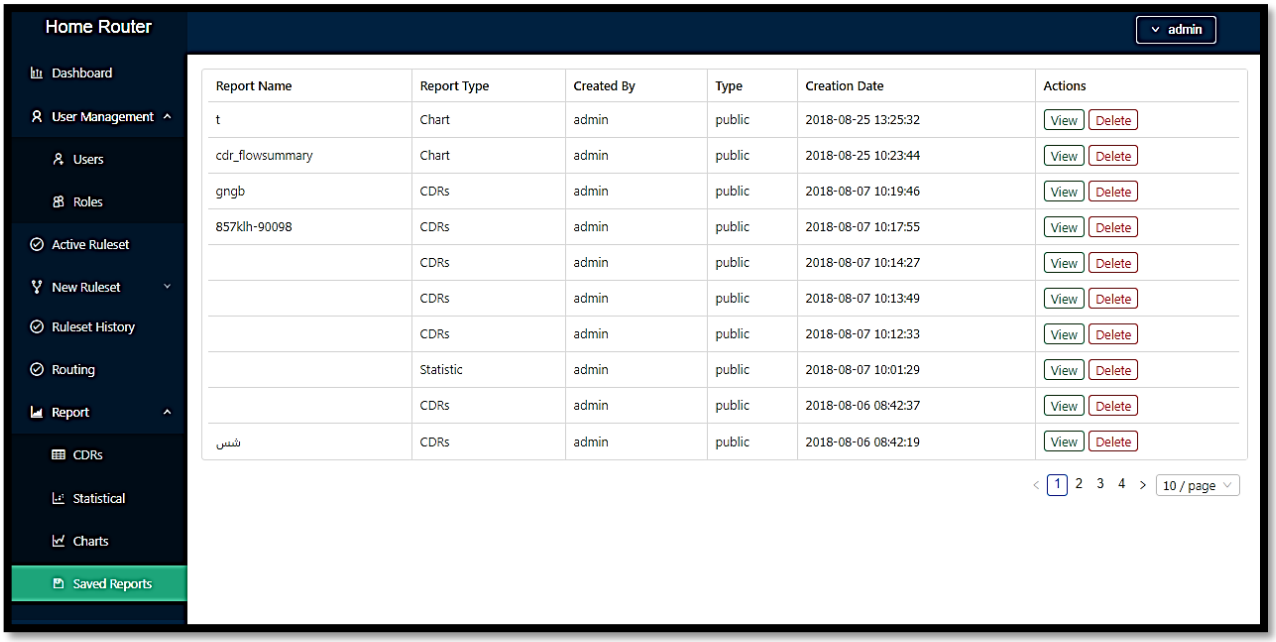


شکل ۱۰: نمایی از سربرگ Charts

شکل ۱۰، نمایی از این سربرگ را نشان می‌دهد. در این مثال همانند مثال مطرح شده در سربرگ Statistical، مجموعه پیام‌های دریافت شده بر حسب وضعیت نهایی آنها (فیلد FlowSummary در رکوردهای CDR) و به صورت روز به روز تجمیع و به صورت نمودار ترسیم گردیده اند.

همانند دو بخش قبل، امکان ذخیره سازی قالب گزارش نیز وجود دارد.

٤- سربرگ Saved Reports: در تمامی سربرگ‌های گزارش‌گیری ذکر شده امکان ذخیره سازی قالب گزارش‌گیری شامل فیلترها، فیلدهای تجمیع و تنظیمات خروجی وجود دارد. به عبارت دیگر، کاربر می‌تواند گزارش‌های پر تکرار خود را یک بار ایجاد و به صورت یک قالب (Template) ذخیره نموده و در دفعات بعد تنها با تغییر بازه زمانی موردنظرش، خروجی را اخذ کند. در سربرگ Saved Reports، گزارش‌های ذخیره شده‌ای که کاربر به آنها دسترسی دارد، نمایش داده می‌شود و امکان گزارش‌گیری براساس آنها فراهم است (شکل ۱۱)



شکل ۱۱: نمایی از سربرگ Saved Reports

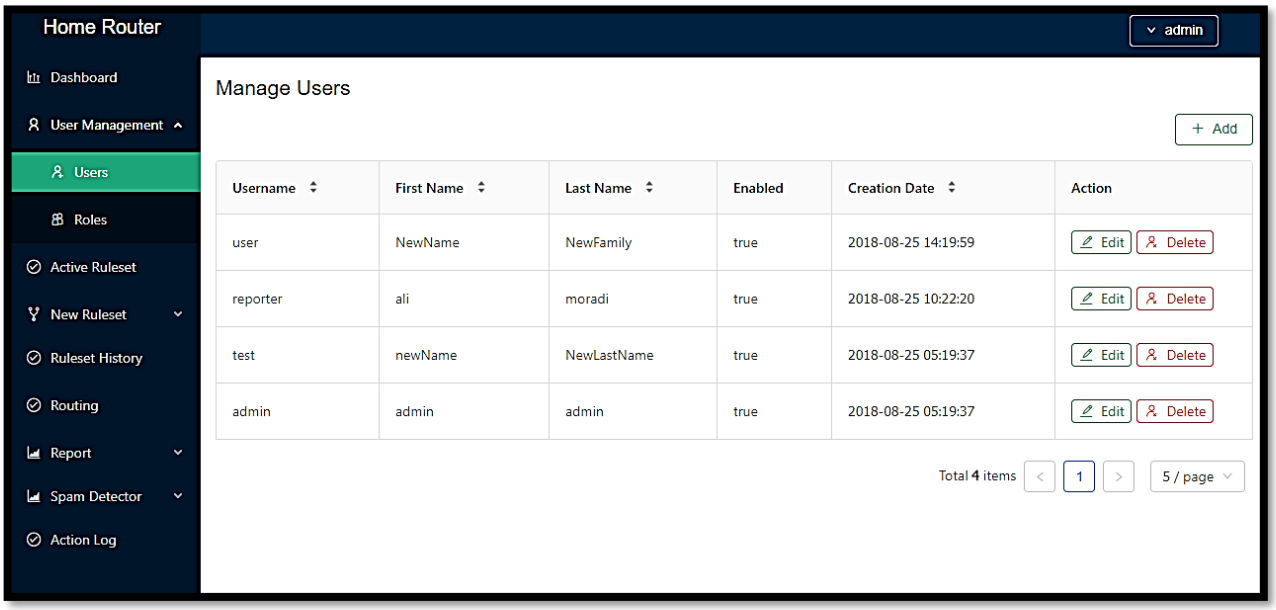
ب. قابلیت‌های مدیریت کاربران

مهمترین ویژگی‌ها و قابلیت‌هایی که در بخش مدیریت کاربران واسط مدیریتی وجود دارد به شرح زیر است:

- قابلیت تعریف/ویرایش/حذف نام کاربری و رمز عبور جدید
- قابلیت فعال/غیر فعال سازی نام کاربری
- قابلیت تعریف شرایط لازم برای رمزهای عبور (مثلا حداقل طول، کاراکترهای مجاز، کاراکترهای لازم و ...)
- قابلیت تنظیم میزان زمان معتبر بودن رمزهای عبور (پس از آن کاربران باید رمز عبور خود را تغییر دهند)
- قابلیت بلوکه سازی محدود نام کاربری در صورت ورود اشتباه رمز عبور (تعداد دفعات قابل پیکربندی)
- قابلیت اعطای زیر مجموعه‌ای از مجموعه مجوزهای موجود به یک کاربر

در بخش مدیریت کاربران ۲ سربرگ Users و Roles وجود دارد.

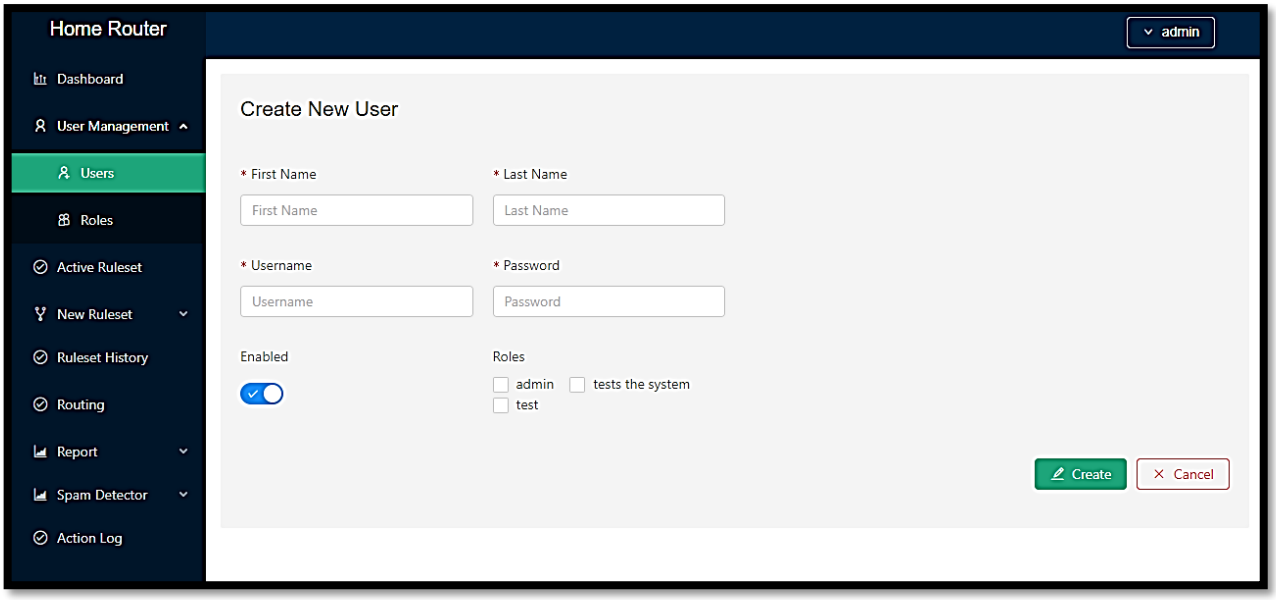
۱- سربرگ Users: در این بخش کاربر می‌تواند لیست کاربران موجود و مشخصات جزیی آنها را مشاهده نماید (شکل ۱۲)



شکل ۱۲: نمایی از سربرگ Users

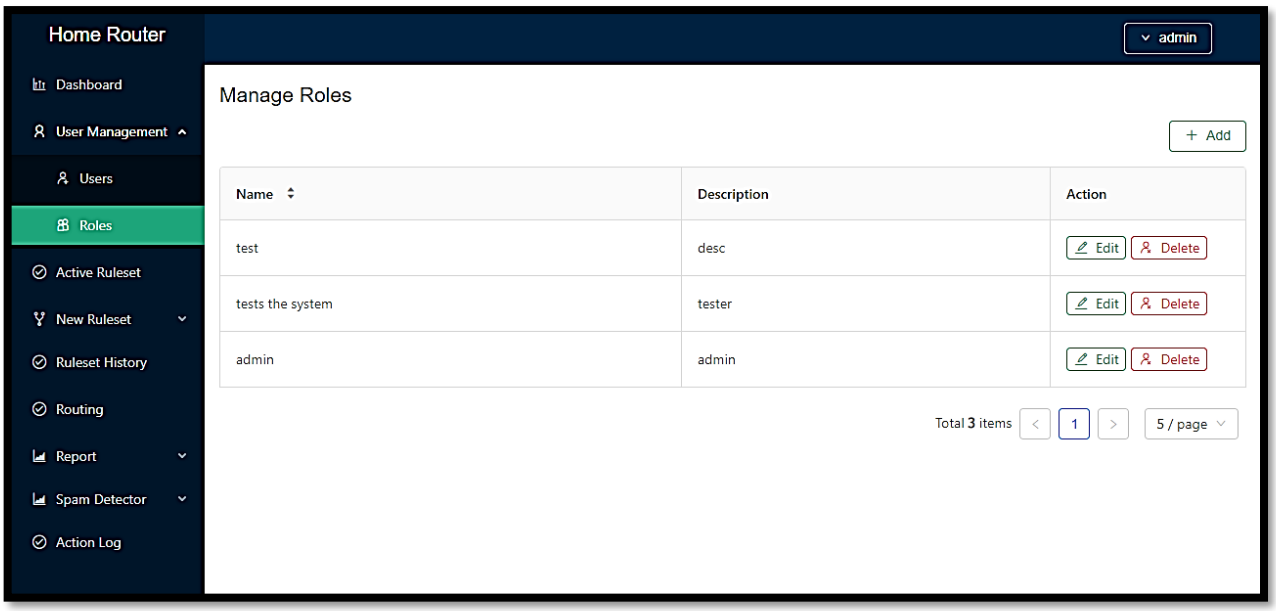
در این سربرگ همانطور که در شکل ۱۲ مشاهده می‌شود، امکان تعریف نام کاربری جدید نیز فراهم گردیده است (شکل ۱۳)

همانطور که در شکل ۱۳ مشاهده می‌شود، در زمان تعریف هر کاربر، علاوه بر مشخصات، نام کاربری و رمز عبور، امکان اعطای مجوزهای مختلف به آن نیز وجود دارد. این مجوزها می‌بایست قبل از تعریف کاربر و در سربرگ Roles تعریف شده باشند.



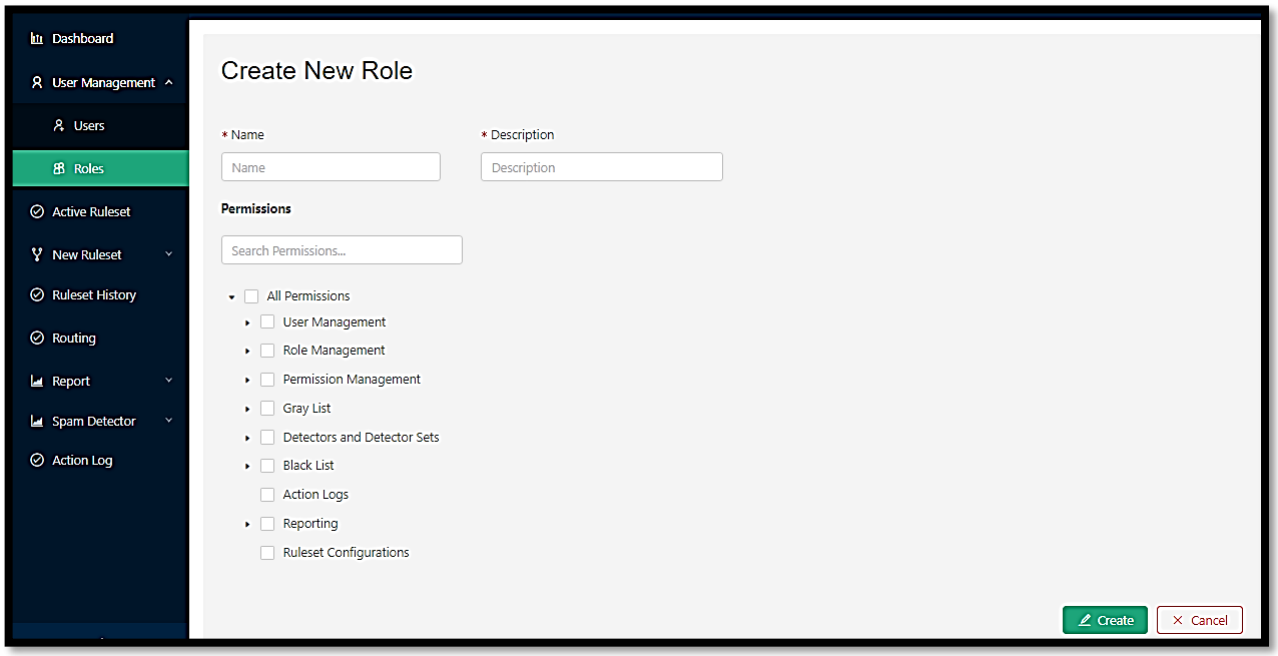
شکل ۱۳: تعریف کاربر جدید

۱- سربرگ Roles: کاربر در این بخش می‌تواند لیست مجوزهای تعریف شده به همراه مشخصات جزیی آنها را مشاهده نماید (شکل ۱٤)



شکل ۱٤: نمایی از سربرگ Roles

در این سربرگ همانطور که در شکل ۱۴ مشاهده می‌شود، امکان تعریف مجوز جدید نیز فراهم گردیده است (شکل ۱۵)



شکل ۱۵: تعریف مجوز (Role) جدید

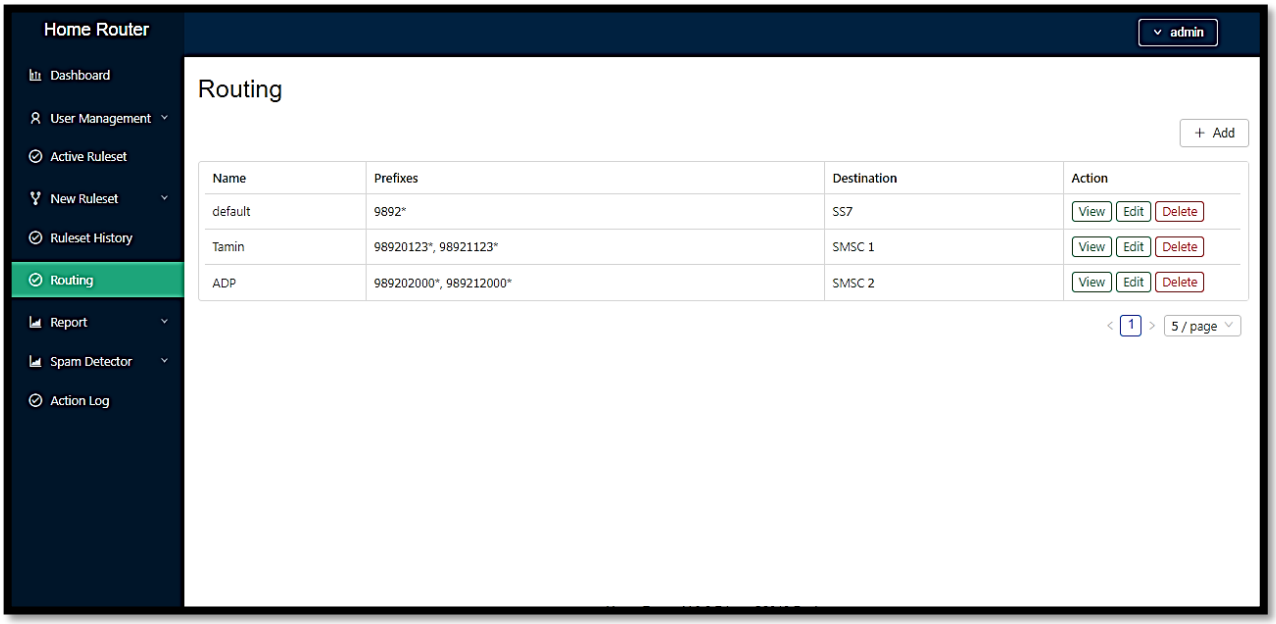
در این بخش، می‌توان مجوزهای مختلفی برای دسترسی به واسط کاربری تعریف نمود. مجوزهایی که می‌توان زیرمجموعه‌ای از آنها را به هر کاربر تعریف شده در سیستم اعطا نمود، به شرح زیر است:

- مجوز ایجاد کاربر جدید (User Create)
- مجوز مشاهده لیست کاربران (View Users)
- مجوز بروزرسانی تعاریف یک کاربر (Update User)
- مجوز حذف یک کاربر (Delete User)
- مجوز ایجاد نقش جدید (Create Role)
- مجوز مشاهده لیست نقش‌ها (View Roles)
- مجوز بروزرسانی تعاریف یک نقش (Update Role)
- مجوز حذف یک نقش (Delete Role)
- مجوز مشاهده لیست مجوزها (View Permissions)
- مجوز مشاهده و تغییر قوانین (Ruleset Configurations)

- مجوز مشاهده گزارش‌ها (View Reports)
- مجوز ذخیره سازی گزارش (Create Report)
- مجوز حذف گزارش (Delete Report)
- مجوز تعریف مسیریابی جدید (Create Route)
- مجوز بروزرسانی مسیریابی موجود (Update Route)
- مجوز حذف یک مسیریابی موجود (Delete Route)

ج. قابلیت‌های تعریف مسیریابی (Routing)

در این بخش، لیست مسیریابی (Routing) های تعریف شده در سیستم قابل مشاهده می‌شود (شکل ۱۶)

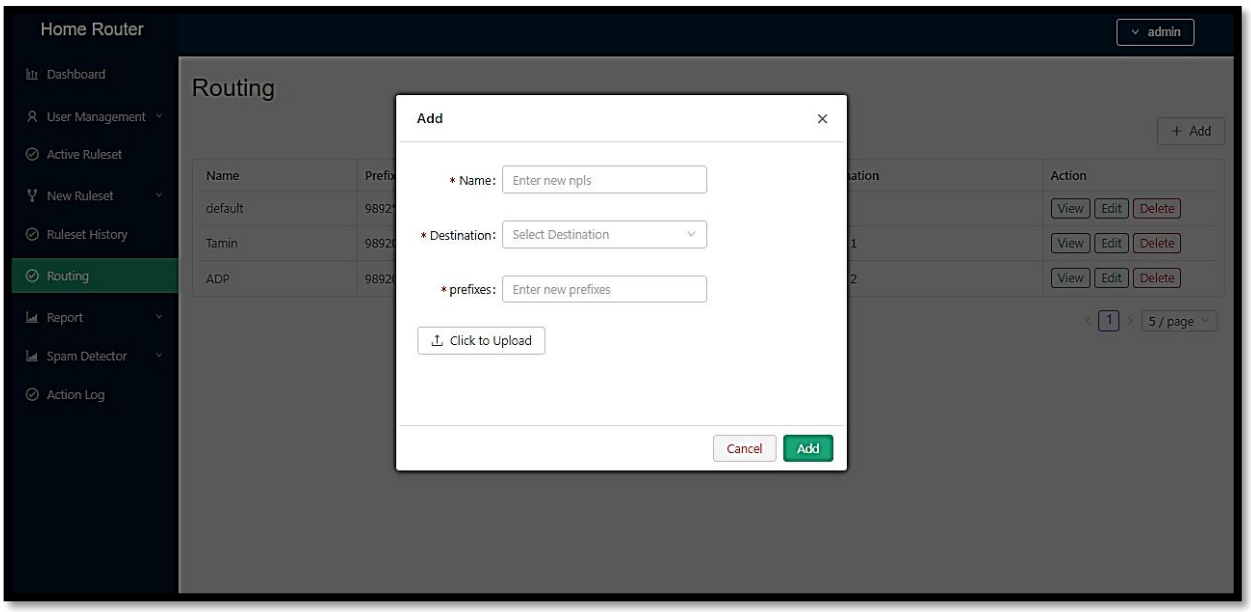


شکل ۱۶: نمایی از سربرگ Routing

در این بخش علاوه بر مشاهده لیست مسیریابی‌های موجود، می‌توان یک مسیریابی جدید تعریف نمود یا یک مسیر یابی موجود را ویرایش یا حذف نمود.

کاربر برای تعریف مسیریابی جدید (شکل ۱۷) باید یک نام منحصر به فرد به آن اختصاص دهد. لیستی از شماره‌ها/پیش شماره‌ها (عدد یا حروف) را تعریف نماید (علاوه بر امکان تایپ شماره‌ها در صفحه تعریف Routing جدید، امکان بارگذاری آنها از طریق فایل CSV نیز وجود دارد) و در نهایت مقصد نهایی پیام‌ها را

تعیین نماید. مقصد نهایی پیام‌ها می‌تواند شبکه SS7 یا یکی از اتصالات SMPP برقرار شده با مرکز پیام کوتاه اپراتور باشد. کاربر می‌تواند یکی از آیتم‌های موجود در لیست مقاصد مجاز (شامل SS7 و شناسه اتصالات SMPP موجود) را انتخاب نماید.

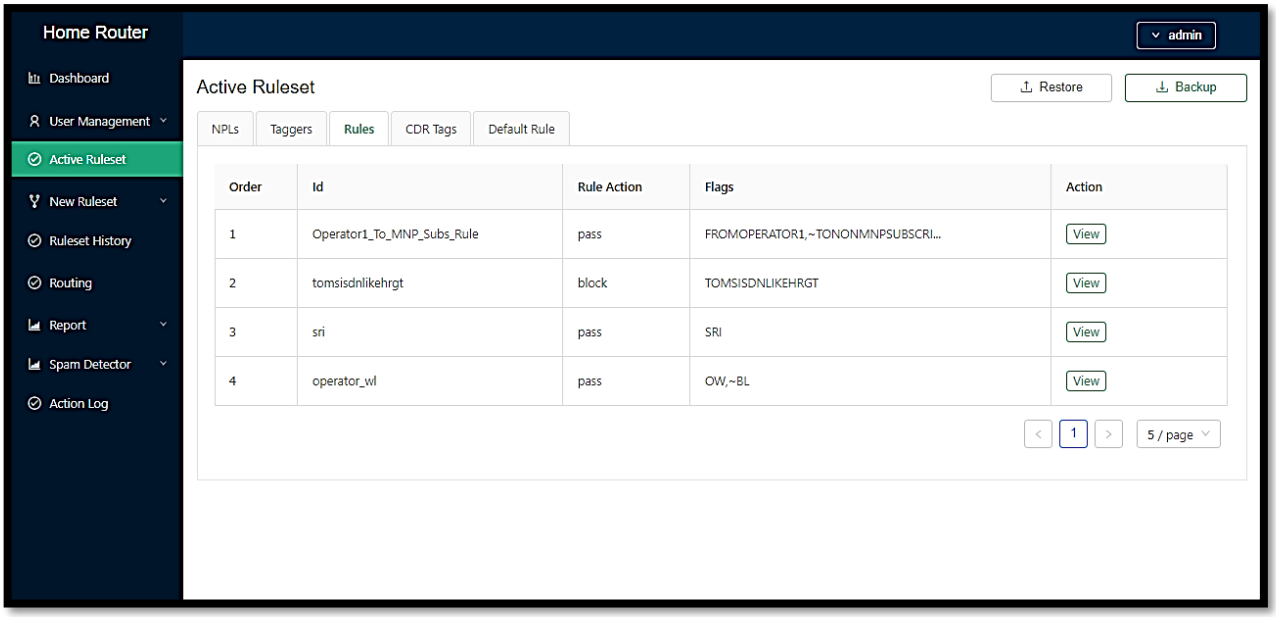


شکل ۱۷: تعریف Routing جدید

د. قابلیت‌های بخش مدیریت قوانین

در واسط مدیریتی، دو سربرگ جهت دسترسی به بخش مدیریت قوانین تعبیه گردیده است.

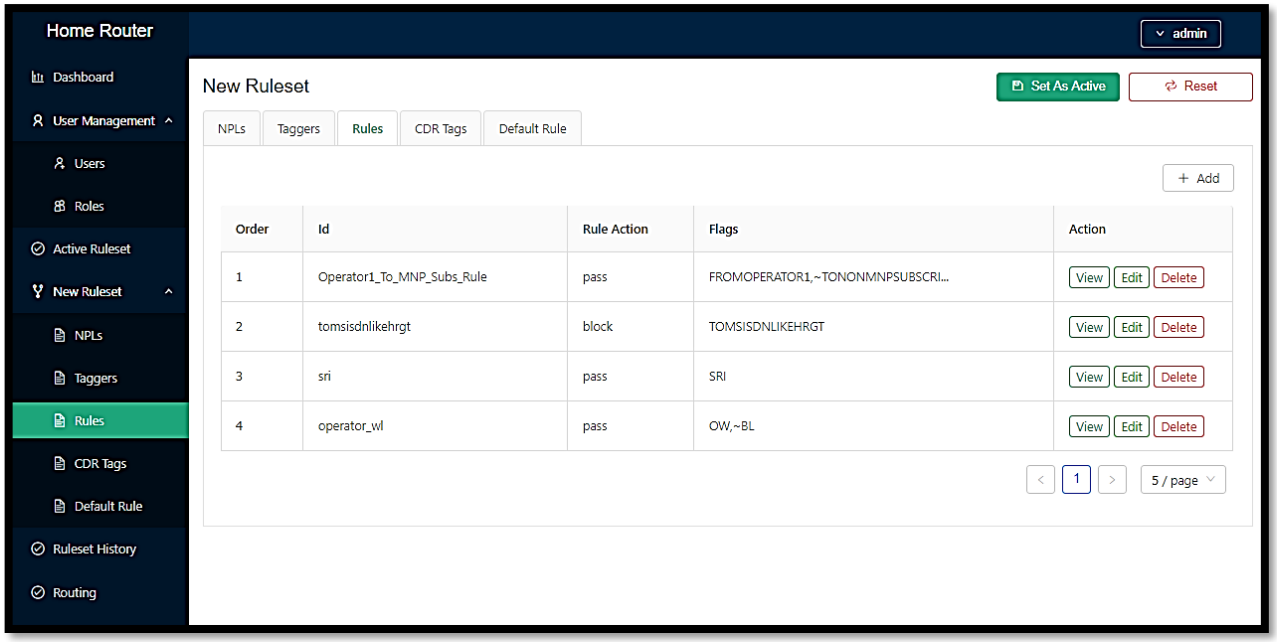
۱- سربرگ Active Ruleset: که حاوی وضعیت جاری سیستم و قوانین تعریف شده و فعال آن است (شکل ۱۸)



شکل ۱۸: نمایی از سربرگ Active Ruleset

در این بخش، امکان ویرایش قوانین وجود ندارد و صرفا برای مشاهده قوانین تعبیه گردیده است. علاوه بر این، همانطور که در شکل ۱۸ مشاهده می‌شود، امکان پشتیبان گیری و بازیابی مجدد مجموعه تمامی قوانین به همراه تمامی جزییات آن‌ها در این سربرگ فراهم گردیده است.

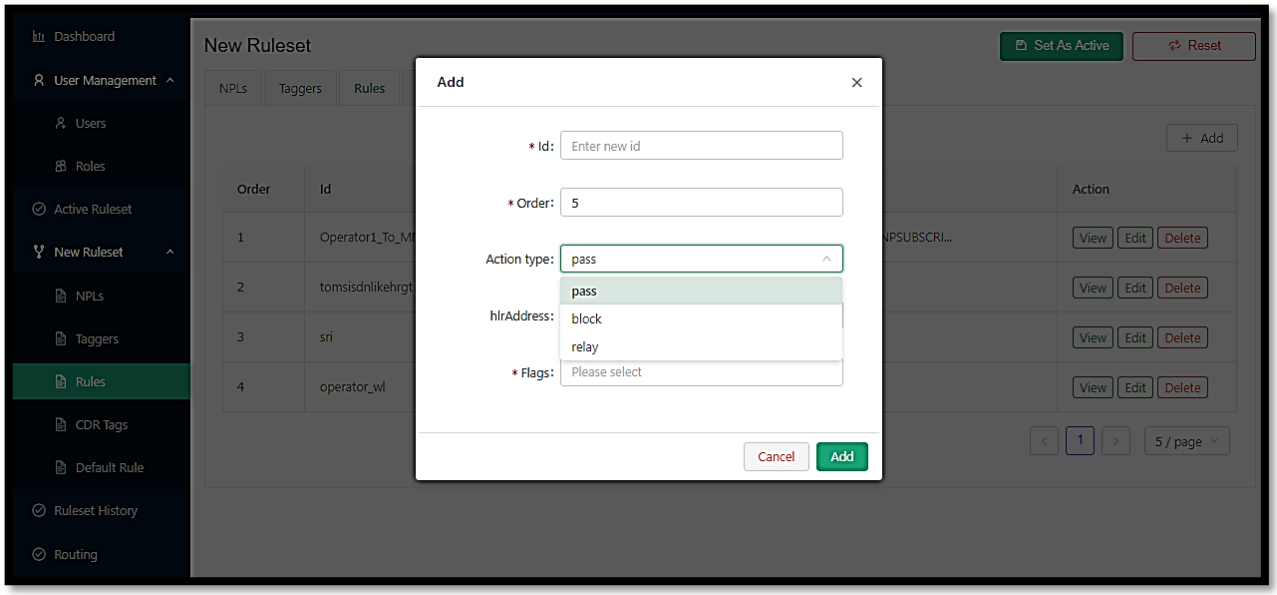
۲- سربرگ New Ruleset: این سربرگ دقیقا مشابه با سربرگ Active Ruleset است با این تفاوت که امکان اضافه/ویرایش/حذف قوانین در آن فراهم شده است (شکل ۱۹). کاربر در این بخش می‌تواند تمامی تغییرات موردنظر خود را اعمال نماید، از صحت آنها مطمئن شده و سپس آنها را به صورت یکجا روی سیستم اعمال نماید.



شکل ۱۹: نمایی از سربرگ New Ruleset

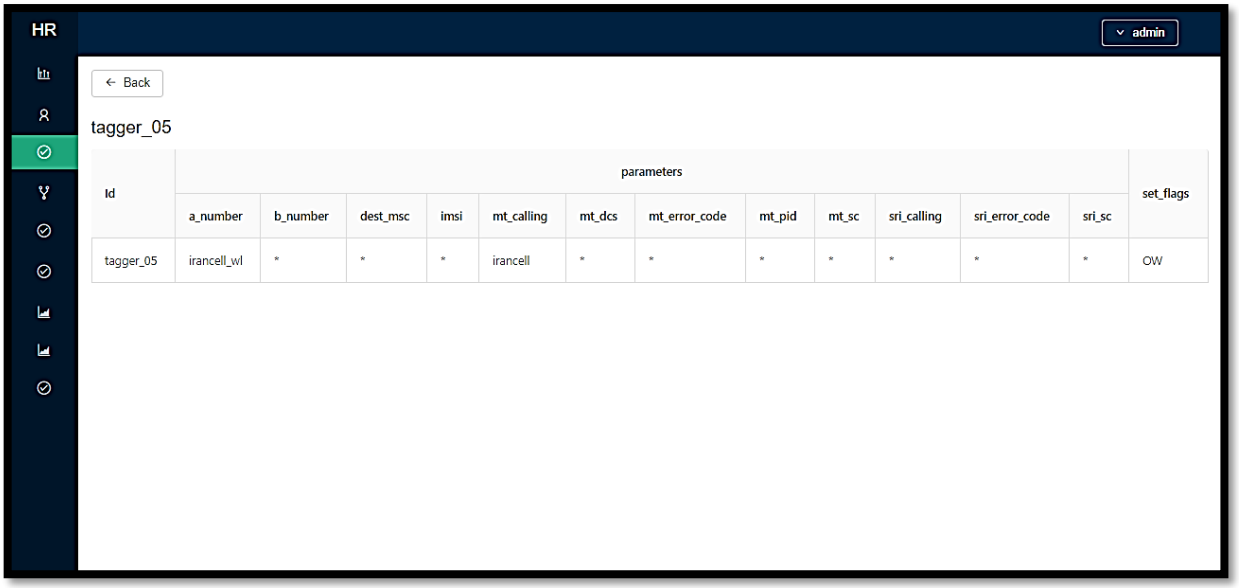
در بخش New Ruleset، سربرگ‌های مختلفی وجود دارد. مهمترین سربرگ در این بخش، سربرگ Rules است که حاوی لیست قوانین موجود و امکان تعریف قوانین جدید است (شکل ۲۰)

همانطور که در شکل ۲۰ مشاهده می‌شود، برای تعریف هر قانون جدید می‌بایست یک شناسه (نام منحصر به فرد)، اولویت، نوع عملیات (عبور، بلوکه، رله) و لااقل یک Flag وارد شود.



شکل ۲۰: تعریف Rule جدید

در بخش مدیریت قوانین سیستم Home Router، جهت جلوگیری از تعریف قوانین مشابه یا تکراری، مکانیزم Tag گذاری روی پیام ورودی پیاده سازی گردیده است. به این ترتیب، در ابتدا مشخصات هر پیام ورودی با مجموعه‌ای از شروط تعریف شده توسط کاربر مقایسه می‌شود و در صورتی که پیام با یک یا چند شرط سازگار باشد، Tag های تعریف شده توسط کاربران روی پیام نوشته می‌شود (همانطور که در توضیحات ماژول Home Router Core توضیح داده شد، ۹ مشخصه از مشخصات پیام‌های ورودی می‌توانند به عنوان پارامترهای شروط در نظر گرفته شوند). برای مشاهده لیست شروط و تعریف شرط‌های جدید از سربرگ Tagger در بخش New Ruleset استفاده می‌شود. شکل ۲۱ نمونه‌ای از آن را نشان می‌دهد.



شکل ۲۱: مشخصات یک شرط (Tagger) نمونه

شرط یا Tagger نمایش داده شده در شکل ۲۱، به این معنی است که اگر پیام ورودی از یکی از شماره/پیش شماره‌های موجود در لیست irancell_wl ارسال شده باشد (A Number)، آدرس GT ارسال کننده پیام MT نیز در لیست irancell باشد (MT Calling)، آنگاه روی این پیام تگ OW نوشته شود (تمامی لیست‌های حاوی شماره/پیش شماره (عدد یا حروف) در سربرگ NPLS تعریف می‌شوند. این روش جهت جلوگیری از تکرار شماره‌ها به ازای هر شرط انتخاب شده است). تگ‌ها رشته‌های دلخواهی هستند که توسط کاربر تعریف می‌شوند.

با این توضیحات، پارامتر Flag در تعریف قانون جدید (شکل ۲۰)، یک یا چند تگ تعریف شده در شروط هستند. به این ترتیب، قانون جدید و نوع عملیات آن، روی تمامی پیام‌هایی که تگ‌های انتخاب شده روی

آنها نوشته شده است، اعمال می‌گردد (امکان انتخاب نقیض تگ‌ها نیز وجود دارد. یعنی اگر روی پیام تگ موردنظر نوشته نشده باشد، آنگاه قانون مورد نظر اعمال شود)

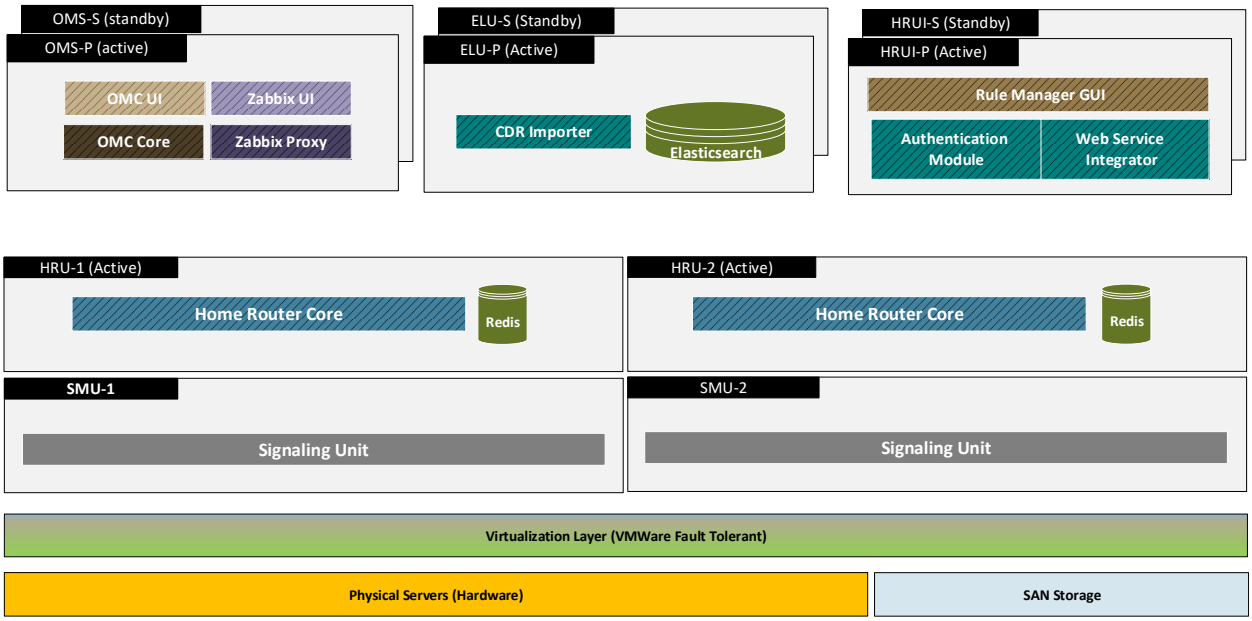
۴,۸ مدیریت رخدادها (Zabbix)

در سامانه Home Router پیک‌آسا برای مدیریت رخدادها و پایش وضعیت نرم افزار، سخت افزار و سرویس، از فریم ورک Zabbix استفاده شده است. از جمله قابلیت‌های این فریم ورک که در سامانه Home Router مورد استفاده قرار گرفته است می‌توان به موارد زیر اشاره کرد:

- مشاهده توپولوژی نرم افزاری/سخت افزاری
- پایش وضعیت لینک‌های سیگنالینگی (M3UA)
- پایش وضعیت اتصالات SMPP
- مشاهدله آنلاین تعداد بسته‌های رد و بدل شده به تفکیک هر لینک سیگنالینگی
- پایش وضعیت عملکرد نرم افزارها به تفکیک ماژول‌ها (از جمله میزان مصرف منابع، سرعت پردازش و ...)
- پایش وضعیت سرویس به تفکیک شاخص‌ها (از جمله درصد موفقیت پیام‌های متفاوت، تغییر الگوی ترافیک، تغییر الگوی دریافت کدخطاهای رایج از شبکه و ...)
- امکان تعریف تریگرهای مختلف با سطوح اهمیت دلخواه
- امکان تعریف الگوی تغییر سطح اهمیت رخدادها براساس میزان یا زمان تکرار آنها
- امکان تعریف سطوح مختلف دسترسی
- امکان اتصال به Zabbix مرکزی اپراتور
- امکان ارسال آلارم‌ها از طریق SMS، Email یا سایر پیام‌رسان‌های دارای API

٤,٩ معماری سخت افزاری

معماری سخت افزاری سامانه Home Router و جانمایی نرم افزارها بر روی آن مطابق شکل شماره ۲۲ است.



شکل ۲۲: معماری سخت افزاری سیستم Home Router

معماری سخت افزاری Home Router مبتنی بر مجازی سازی است و برای پیاده سازی آن در مجموع به ۱۰ ماشین مجازی با مشخصات ذکر شده در بخش بعد نیاز است. با توجه به اینکه تامین سرورهای سخت افزاری برعهده اپراتور است، موارد مربوط به امنیت و دسترس پذیری آن در این مستند مطرح نشده است.

۱- ماژول سیگنالینگ در دو نسخه و روی دو ماشین مجازی با نام SMU و به صورت فعال/فعال نصب می‌گردد. نیمی از لینک‌های سیگنالینگ به هر یک از ماژول‌ها متصل می‌گردد. در صورتی که یکی از ماشین‌ها یا ماژول‌ها از مدار خارج شوند (به علت خرابی یا بروزرسانی)، ماشین یا ماژول دیگر تمامی بار ورودی/خروجی را تحمل نموده و سرویس دچار اختلال نمی‌شود.

۲- ماژول Home Router Core نیز در دو نسخه و روی دو ماشین مجازی با نام HRU و به صورت فعال/فعال نصب می‌شود. این طرح علاوه بر بالا بردن قابلیت اطمینان و تحمل خرابی، امکان بروزرسانی سیستم بدون تاثیر روی سرویس را فراهم می‌نماید.

۳- سایر نرم افزارها با توجه به طرح جانمایی (شکل شماره ۲۲) در دو نسخه و روی دو ماشین مجازی به صورت فعال/غیر فعال نصب و راه اندازی می‌شوند. مکانیزم داخلی مبتنی بر Zabbix تمامی نرم افزارها، ماشین‌ها و سرویس‌ها را پایش نموده و در صورت لزوم ماشین فعال را با ماشین دوم جایگزین می‌نماید. در زمان بروزرسانی، ماشین غیرفعال در ابتدا بروز شده و سپس جایگزین سیستم فعال می‌شود. بروزرسانی سیستم فعال و بازگشت آن به مدار، پس از آن انجام می‌گردد.

٤- هارددیسک‌های مورد نیاز دیتابیس Elasticsearch که حاوی تمامی داده‌های CDR جهت گزارش-گیری از سیستم است، به طور معمول روی SAN Storage قرار داده می‌شوند و بنابراین نیازی به تکثیر (Replicate) داده‌های موجود در دیتابیس وجود ندارد. با این حال، تمامی فایل‌های خام CDR در یک منبع دیگر جهت آرشیو ذخیره می‌گردند. در صورتی که به هر دلیل داده‌های موجود در دیتابیس از دست برود، می‌توان از روی فایل‌های خام موجود در آرشیو، دیتابیس را مجددا بازیابی نمود (برای بازیابی دیتابیس حاوی ۹۰ روز داده از روی فایل‌های خام CDR، حدود ٤٨ ساعت زمان لازم است)

٤,۱۰ ملاحظات امنیتی

در سامانه Home Router ملاحظات مرتبط با حوزه امنیت در تمامی فازهای تحلیل، طراحی، تولید و پیاده سازی در نظر گرفته شده است. برخی از ملاحظات قابل ذکر در این حوزه به شرح زیر است:

۱- تمامی واسط‌های بین نرم افزاری به صورت کد شده پیاده سازی گردیده اند. علاوه بر این، این واسط‌ها با نام کاربری و رمز عبور نیز محدود شده اند (هم واسط‌های داخلی و هم واسط‌های خارجی سیستم)

۲- سایر واسط‌های وب سرویسی با نام کاربری و رمز عبور محدوده شده اند و روی وب سرورهای HTTPS راه اندازی می‌گردند.

۳- تمامی دیتابیس‌های موجود در سیستم دارای نام کاربری و رمز عبور هستند و تنها نرم افزارهای سامانه اجازه اتصال مستقیم به آنها را دارند. عملیات ممکن روی دیتابیس‌ها در سایر اتصالات، محدود شده اند.

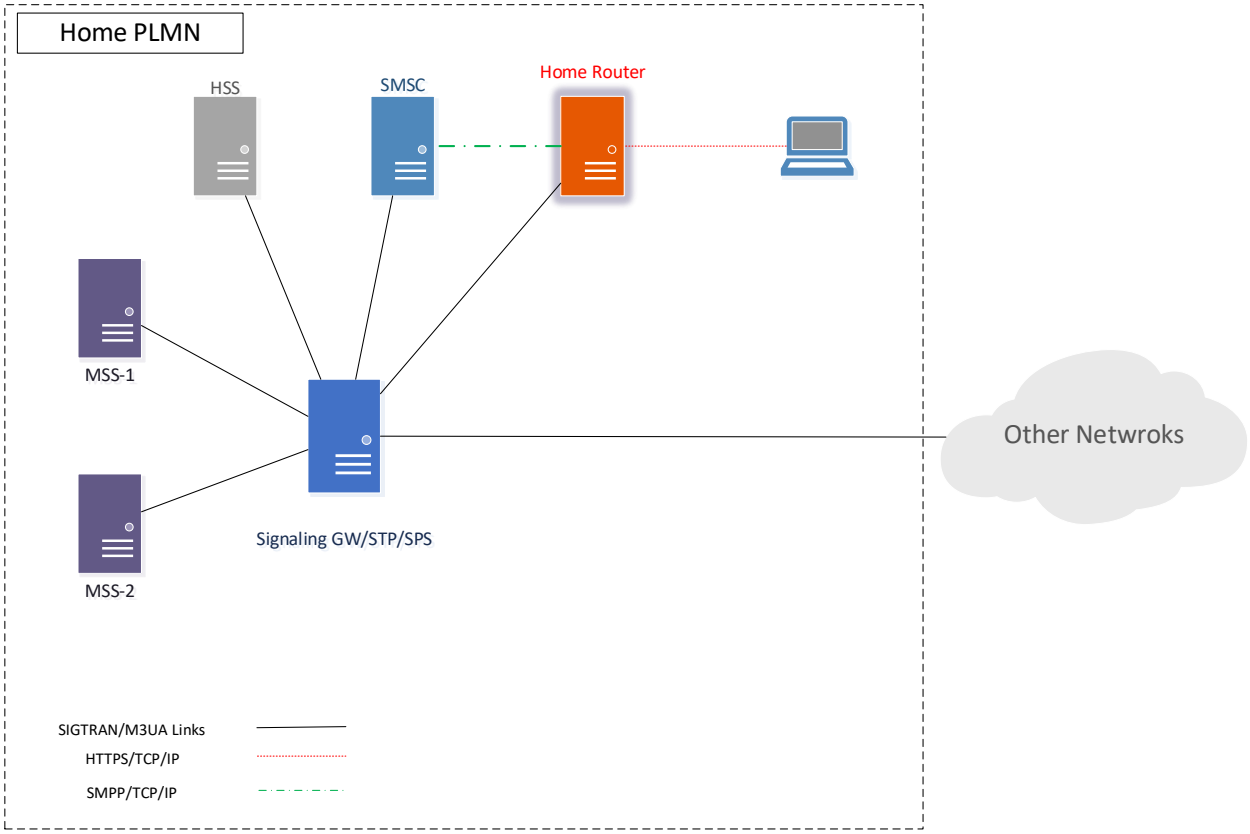
٤- تمامی ماشین‌های مجازی موجود در سامانه دارای فایروال نرم افزاری هستند.

۵- دسترسی به ماشین‌های مجازی موجود با مکانیزم استاندارد سطوح دسترسی در سیستم عامل لینوکس محدود شده است. سایر عملیات کاربران متصل شده به سیستم، ثبت و آرشیو می‌شود.

٦- تست‌های امنیتی مربوط به واسط‌های گرافیکی (hijacking) روی تمامی واسط‌های گرافیکی با موفقیت انجام شده است.

٤,١١ توپولوژی استقرار

توپولوژی استقرار سامانه Home Router در شبکه خانگی اپراتور مطابق شکل شماره ۲۳ است.



شکل ۲۳: توپولوژی استقرار سیستم Home Router

۵. شکست کار

طرح اولیه شکست کار پروژه به شرح زیر است. در این طرح، طول مدت پروژه (٤ ماه) در دوره‌های دوهفته‌ای برنامه‌ریزی گردیده است. بدیهی است این طرح صرفاً یک طرح اولیه است و طرح نهایی برنامه‌ریزی و شکست کار، پس از شروع پروژه و تحلیل نهایی نیازمندی‌های آن قابل حصول خواهد بود.

فاز	توصیف	دو هفته							
		۱	۲	۳	٤	٥	٦	۷	۸
اول (شناخت و طراحی)	آشنایی تیم توسعه با پروژه و نیازمندی‌ها	■							
	مطالعه سیستم‌های مشابه و پیش‌نیازها	■							
	نهایی سازی طراحی اولیه		■						
دوم (پیاده-سازی)	راه‌اندازی محیط توسعه و CI/CD			■					
	پیاده‌سازی و آزمون زیرسیستم کلیف				■	■	■		
	پیاده‌سازی و آزمون زیرسیستم Home Router				■	■	■		
سوم (یکپارچه-سازی)	آزمون‌های یکپارچگی مولفه‌ها و رفع نواقص							■	
	نصب و راه‌اندازی آزمایشی نسخه نهایی در محیط مشتری							■	■
	یکپارچه‌سازی با نودهای شبکه میزبان								■
	تحویل و آموزش								■

٦. طرح آزمون

آزمون‌های کارکردی و غیرکارکردی سامانه پس از تحلیل نهایی نیازمندی‌ها و طراحی سامانه و در طی فازهای عملیاتی پروژه طراحی خواهد شد و به صورت دوره‌ای در قالب مستندات طرح آزمون ارائه خواهد شد.

۷. پیشنهاد دوره آموزشی

پیشنهاد اولیه دوره آموزشی به شرح زیر است. با توجه به اینکه راهکار مذکور می‌بایست طی یک دوره زمانی مشخص تحلیل، طراحی و تولید گردد و ممکن است تغییراتی در شرح نیازمندی‌ها یا طراحی اولیه پیشنهادی اتفاق بیفتد، محتوای آموزشی پیشنهادشده در این بخش نیز ممکن است تحت تأثیر قرار گرفته و در ادامه پروژه بروزرسانی گردد.

دوره آموزشی پیشنهادی با هدف آموزش تمامی ابعاد راهکار سیاست‌گذار تکامل‌یافته پیامک شامل طراحی نرم‌افزاری، چگونگی عملکرد سیستم، نحوه کار با واسطهای آن و سایر مفاهیم و ابزارهای استفاده‌شده در طراحی و عملکرد سامانه برنامه‌ریزی خواهد شد.

عنوان جلسه	سرفصل‌ها	مدت
آشنایی با مفاهیم Container Platform و Docker	○ آشنایی با داکر و معماری آن ○ مدیریت و چرخه حیات Containerها ○ معرفی اجزای اصلی داکر ○ معرفی ابزارهای جانبی داکر ○ آشنایی با Kubernetes و معماری آن	۲ ساعت
تشریح طراحی و معماری نرم‌افزار	○ معماری سرویس‌ها و ماژول‌ها، قابلیت‌ها و نحوه عملکرد سیستم ○ توپولوژی استقرار و ارتباطات مابین مؤلفه‌ها ○ تشریح دیتابیس‌ها و فرمت داده‌های ذخیره‌شده	۲ ساعت
آموزش پرتال تحت وب	○ مدیریت کاربران و سطوح دسترسی ○ مدیریت سرویس‌ها ○ توصیف گزارش‌های سیستم و کاربرد آن‌ها ○ تشریح ورودی‌ها و خروجی‌های گزارش‌های سیستم	۱,۵ ساعت
آموزش نصب و راه‌اندازی سامانه	○ ملاحظات و پیش‌نیازهای نصب و راه‌اندازی تمامی ماژول‌ها	۲ ساعت

آموزش Zabbix و آلارم‌های سیستم	○ مروری بر معماری سرور و عامل‌های Zabbix ○ پیکربندی شامل نحوه تعریف host، آیتم‌ها و trigger ها ○ تشریح تمامی آیتم‌ها و trigger های سامانه	۱,۵ ساعت
آموزش واسط مدیریت کارایی و پیکربندی	○ مروری بر معماری واسط مدیریت کارایی و پیکربندی ○ توصیف شمارنده‌های و شاخص‌های حیاتی سیستم ○ توصیف گزارش‌های سیستم و کاربرد آن‌ها ○ تشریح ورودی‌ها و خروجی‌های گزارش‌های سیستم ○ توصیف پارامترهای پیکربندی سیستم و نحوه مقداردهی آن‌ها	۲ ساعت
نحوه برخورد با مشکلات احتمالی	○ مشکلات مربوط به نرم‌افزارهای هسته سامانه ○ مشکلات مربوط به واسط‌های وب ○ مشکلات مربوط به سرویس‌های داخلی و خارجی سامانه	۱ ساعت
پرسش و پاسخ		۱ ساعت
آزمون		۲ ساعت

۸. پیشنهاد قیمت

با توجه به توضیحات ارائه‌شده در این مستند، لیست قیمت‌ها به شرح مندرج در جدول زیر می‌باشد. بدیهی با توجه به اینکه راهکار مذکور می‌بایست طی یک دوره زمانی مشخص تحلیل، طراحی و تولید گردد و ممکن است تغییراتی در شرح نیازمندی‌ها یا طراحی اولیه پیشنهادی اتفاق بیفتد، لیست قیمت‌های پیشنهادشده در این بخش نیز ممکن است تحت تأثیر قرار گرفته و در ادامه پروژه بروزرسانی گردد.

ردیف	شرح کالا	تعداد/واحد	قیمت واحد (ریال)	قیمت کل (ریال)
۱	نرم‌افزار مربوط به زیرسیستم کلیف با ظرفیت ۵۰۰ پیامک بر ثانیه	۱	۵,۵۲۰,۰۰۰,۰۰۰	۵,۵۲۰,۰۰۰,۰۰۰
۲	نرم‌افزار مربوط به زیرسیستم Home Router با ظرفیت ۵۰۰ پیامک بر ثانیه	۱	۱۳,۸٤۰,۰۰۰,۰۰۰	۱۳,۸٤۰,۰۰۰,۰۰۰
۳	خدمات نصب، راه‌اندازی و یکپارچه-سازی	۱	۲,٦٤۰,۰۰۰,۰۰۰	۲,٦٤۰,۰۰۰,۰۰۰
٤	خدمات آموزش	۱۵ نفر-روز	رایگان	رایگان
۵	پشتیبانی سامانه	۱۲ ماه	به توضیحات مراجعه شود	
مجموع قیمت خالص (به عدد)			۲۲,۰۰۰,۰۰۰,۰۰۰	
تخفیف			٤,٤۰۰,۰۰۰,۰۰۰	
قیمت نهایی (به عدد)			۱۷,٦۰۰,۰۰۰,۰۰۰	
مجموع قیمت خالص (به حروف): هفده میلیارد و ششصد میلیون ریال				

- پینوشت ۱: هزینه پشتیبانی سامانه پس از دریافت SLA قابل محاسبه خواهد بود.
- پینوشت ۲: پیشنهاد قیمت بالا به مدت ۱ ماه از تبادل این مستند معتبر است و پس از آن لازم است پیشنهاد قیمت مجددا اخذ گردد.
- پینوشت ۳: میزان تخفیف اعمال شده بر روی پیشنهاد قیمت، صرفا در حالت خرید هر دو زیرسیستم معتبر بوده و در صورت تمایل خریدار به خرید یک زیرسیستم، میزان تخفیف صفر خواهد بود.