



محصولات حوزه امنیت ایمیل رایان نیک تجهیز



رایان نیک تجهیز



Email Edge
(ESA Cisco)



**Email Load
Balancing**



URL Protect



رایان نیک تجهیز



رایان نیک تجهیز

OTP

احراز هویت دو عاملی



Mail Server



Email
Encryption



ZIX Email Encryption

روکا رمز

EM



رایان نیک تجهیز

www.rayan-net.com

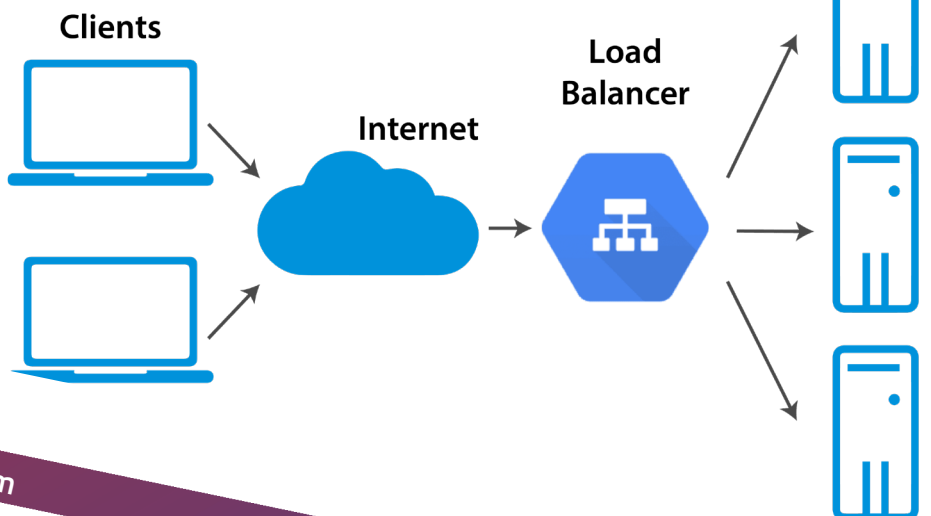
شرکت رایان نیک تجهیز قادر به ارائه انواع میل سرورهای سازمانی از جمله میل سرور Microsoft Exchange می باشد. Microsoft Exchange به دلیل پایداری و گسترش پذیری بالا برای سازمان های متوسط و بزرگ مناسب می باشد و تمامی ویژگی های آن قابل ارائه بر روی سرورهای Graphical و یا Core نیز می باشد. لازم به ذکر است در صورت درخواست کارفرما میل سرور های دیگر از جمله سرورهای لینوکسی نیز قابل ارائه و پیاده سازی می باشد.

میل سرور Microsoft Exchange



رایان نیک تجهیز

www.rayan-net.com



سرویس Load Balancing حجم بار ترافیک ورودی را بین سرورهای مختلف تقسیم می کند تا از کارافتادن سیستم جلوگیری کند و سیستم در ترافیک بالا به فعالیت خود ادامه دهد. سرویس Load Balancing را به دو صورت سخت افزاری و نرم افزاری می توان نصب کرد که سرویس سخت افزاری شامل Load Balancing و Web Application Firewall (WAF) می باشد و سرویس نرم افزاری آن نیز مناسب سازمان های متوسط و کوچک می باشد.

Load Balancing



رایان نیک تجهیز

www.rayan-net.com

برای اینکه جلوی حملات فیشینگ ناشی از لینک های آلوده در ایمیل ها را بگیرید می توانید از تکنولوژی URL Protection استفاده کنید.

مزایای استفاده از URL Protection برای سازمان ها:

- محافظت فوری در برابر حملات هدفمند
- فیشینگ در همه دستگاه ها بدون نیاز به نصب نرم افزار از سوی مشتری
- حفاظت در مقابل وب سایت های مخرب و exploit ها

URL Protection



رایان نیک تجهیز

www.rayan-net.com

سرویس ایمیل همواره مورد حملات هدفمند قرار می گیرد و امنیت سازمان ها را تهدید می کند. سیسکو یکی از بروزترین راهکارهای امنیت ایمیل خود را تحت عنوان ESA ارائه کرده تا سازمان ها از Inbox کاربر در برابر تهدیداتی همچون اسپم، بدافزارهای پیشرفته، باج افزارها، BEC و از بین رفتن داده ها محافظت کنند.

ESA (Email Security Appliance)



رایان نیک تجهیز



www.rayan-net.com

Reputation Filtering

با بررسی تعداد دفعات ارسال اسپم از دریافت اسپم جلوگیری می‌نماید.

Anti-Virus

جلوگیری از دریافت ویروس از طریق ایمیل با استفاده از دو موتور آنتی‌ویروس McAfee و So-phos.

Connection Filtering

جلوگیری از Domain Spoofing با استفاده از عناصر موجود در اینترنت مانند رکورد، SPF و DKIM DMARC

موتورهای File Analysis و File Reputation

به کمک این دو موتور اگر اطلاعاتی از سالم بودن فایل موجود در ایمیل ارسالی در دیتابیس‌های آنتی‌ویروس‌ها وجود نداشته باشد آن را به صورت جداگانه در Sandbox مورد بررسی قرار داده و در صورت سالم بودن، اجازه‌ی عبور می‌دهد.

مهم‌ترین امکانات
سرویس ESA سیسکو:



رایان نیک تجهیز



WWW.RAYAN-NET.COM

CONTENT FILTERING و GRAYMAIL DETECTION

این دو ابزار به بررسی دقیق ایمیل های ارسالی از سوی شبکه های اجتماعی می پردازند تا حاوی محتوای نامناسب و لینک های خطرناک برای سازمان ها نباشند.

DATA LOSS PREVENTION

این ابزار امکان تعریف قوانین و اعمال این قوانین بر ایمیل های ارسالی را به صورت خودکار ایجاد می کند تا از خروج داده های حساس جلوگیری کند.

امکان دریافت گزارش از سرویس ایمیل

دریافت گزارش از ایمیل های ارسالی و دریافتی در یک محیط کاملاً امن.

مهمترین امکانات سرویس ESA سیسکو:



رایان نیک تجهیز

www.rayan-net.com

OTP Server Authentication به کمک احراز هویت چندعاملی بر روی سیستم‌عامل‌هایی همچون لینوکس، مک و ویندوز امنیت دسترسی به ایمیل‌های سازمانی را افزایش می‌دهد. همچنین می‌توانید از طریق همکاری Exchange و OTP server فرآیندهای ورود به outlook خود را با احراز هویتی قوی و مطابق با سطح ریسک سازمانتان پیاده سازی کنید.

OTP-Exchange



رایان نیک تجهیز

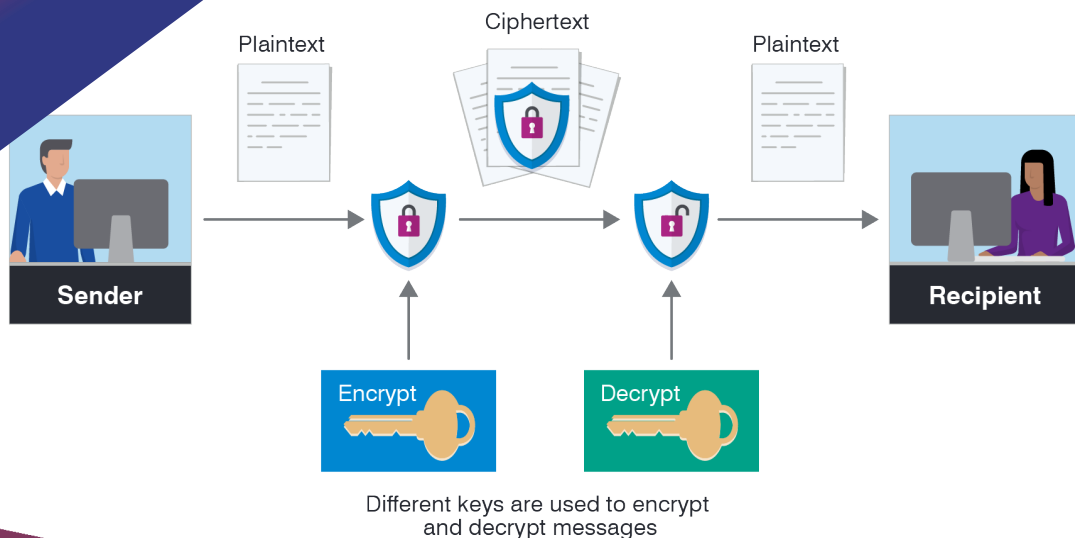
www.rayan-net.com

به کمک ساختار OTP server می توان OTP های ارسالی و همگام شده با Exchange server را در قالب پیامک، Mobile Authenticator، Push Token و ایمیل در اختیار سازمان ها قرار داد تا کاربران با استفاده از آن ها بتوانند به Outlook Web Access (OWA) و یا نرم افزار Outlook بر روی سیستم خودشان وارد شوند. با کمک این روش کاربران دیگر نگران دزدیده شدن رمزهای عبورشان نخواهند بود.

نحوه تامین امنیت Exchange server توسط OTP Server:



رایان نیک تجهیز



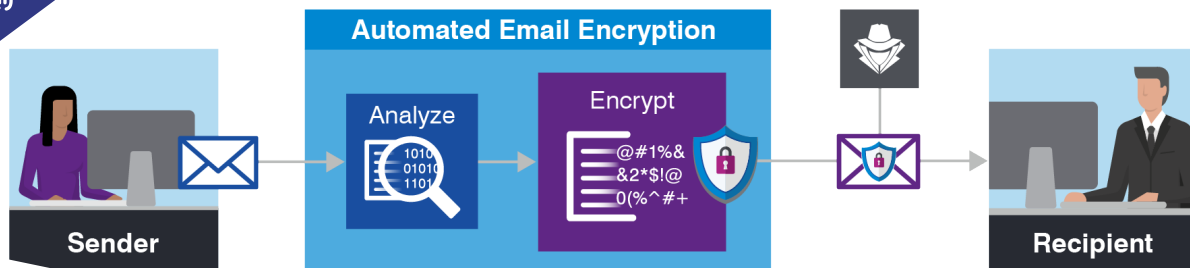
www.rayan-net.com

سرویس رمزنگاری ZIX جهت رمزنگاری ایمیل های مهم سازمانی طراحی شده است. از قابلیت های این سرویس امکان احراز هویت کاربران برای تضمین دریافت ایمیل به صورت محرمانه و رمزنگاری شده توسط فرد گیرنده می باشد. همچنین این سرویس با قابلیت شناسایی کلمات کلیدی در محتویات موضوع یا متن ایمیل طراحی شده و در صورتی که ایمیل حاوی کلمات کلیدی باشد، به صورت اتوماتیک رمز نگاری خواهد شد. قابلیت دیگر این سرویس امکان رمزنگاری دستی یک ایمیل خاص برای کاربران می باشد. همچنین این امکان وجود دارد که رمزنگاری به صورت درون سازمانی و بدون هیچ گونه وابستگی به سرویس خارج از سازمان انجام شود و کلیه فرایندهای امنیتی رمزنگاری در داخل سازمان انجام پذیرد. با توجه به اینکه اکثر سرویس های رمزنگاری در دنیا به صورت کلاسیک می باشند و کشور در وضعیت تحریم قرار گرفته است این ویژگی بسیار کاربردی خواهد بود. کاربران این اطمینان را خواهند داشت که ایمیل های ارسالی به دامین های خارجی نیز رمز نگاری شده اند. به طور مثال در صورت ارسال پیام بر روی سرور های Gmail، با استفاده از سرویس رمزنگاری ZIX، امکان مشاهده محتویات ایمیل برای کمپانی Gmail وجود ندارد.

سرویس رمزنگاری
ایمیل ZIX



رایان نیک تجهیز



www.rayan-net.com

پروتکل Secure PDF

در این راهکار همه پیغام های ارسال شده توسط فرستنده، به همراه ضمیمه های آن به یک فایل PDF رمز شده تبدیل می شود و پسورد آن نیز بصورت Hash شده می باشد که قابل شکستن و رمزگشایی نمی باشد. سپس کاربران با اعتبار سنجی و احراز هویت در سامانه زیکس برای خود یک رمز تعریف می کنند و پس از آن تمامی فایل های PDF دریافت شده فقط با این رمز قابل رمزگشایی و خواندن می باشند.

انواع پروتکل های سرویس زیکس:



رایان نیک تجهیز



www.rayan-net.com

در این راهکار پیغام های ارسالی توسط دستگاه رمزنگار ZIX رمزنگاری می شوند و برای گیرنده یک اعلان با مضمون ایمیل رمزنگاری شده ارسال می شود. گیرنده پس از دریافت این پیغام به سامانه زیکس وارد می شود و پس از اعتبار سنجی، پیغام رمز شده آن توسط سیستم از حالت رمز خارج می شود و به آن نمایش داده می شود.

پروتکل
Webmail



رایان نیک تجهیز



www.rayan-net.com

رمزنگاری براساس کلمات کلیدی:

رمزنگاری ایمیل ها به طرق مختلفی امکان پذیراست. به عنوان مثال، کاربر می تواند کلمه یا کلماتی را بر روی سرویس تعریف نماید و در صورتی که عنوان و یا محتوای ایمیل شامل یکی از این کلمات بود، ایمیل به صورت خودکار رمزنگاری شود.

همچنین این امکان وجود دارد که گیرندگان و فرستندگان خاصی بر روی سرویس تعریف شوند و بدین شکل در صورت ارسال و یا دریافت ایمیل از این اشخاص، عملیات رمزنگاری خود به خود انجام شود. در صورتی که کلمه و یا شخصی (به عنوان فرستنده و گیرنده) تعریف نشده باشد، کاربر می تواند به صورت دستی رمزنگاری را انجام دهد.



رایان نیک تجهیز



www.rayan-net.com

در سرویس زیکس، کاربران علاوه بر امکان رمزنگاری ایمیل ها، از این قابلیت نیز برخوردارند که به عنوان فرستنده ایمیل، نام کاربری خود را مخفی نمایند. همچنین سازمان می تواند تمامی ایمیل های ارسالی از بخش های مختلف سازمان را تحت عنوان یک نام واحد ارسال کند.

پنهان کردن آدرس فرستنده ایمیل

Enter OTP

Check your email for the OTP

One Time Password

Submit

www.rayan-net.com

Pretty Good Privacy به معنای حریم خصوصی کامل، یک پروتکل رمزنگاری دو مرحله ای برای ایمیل می باشد. در مرحله اول محتوای ایمیل رمزنگاری می شود و در مرحله دوم کلید رمزگشایی اطلاعات به صورت کد گذاری شده، با رمزنگاری جدید به فرد گیرنده ارسال می شود.

Secure/Multipurpose Internet Mail (Extensions) S/MIME

در این راهکار، رمزنگاری بصورت End-to-End انجام می شود. فرستنده و گیرنده هر کدام کلیدهای عمومی یکدیگر را دارند و کلید های خصوصی را نزد خود نگه می دارند. فرستنده، پیام را با کلید عمومی گیرنده رمز می کند و این پیام رمز شده فقط با کلید خصوصی مربوط به گیرنده امکان بازگشایی دارد. در واقع این راهکار مشابه PGP بوده با این تفاوت که نیاز به ساخت کلید تصادفی ندارد.

پروتکل PGP



رایان نیک تجهیز

www.rayan-net.com

همانطور که بارها دیده شده هکرها با نام دامنه سازمان های بزرگ ایمیل هایی با مضمون پرداخت وجه ارسال می کنند. با استفاده از پروتکل ارتباط امن DKIM سرویس زیکس، سازمان ها می توانند این اطمینان را داشته باشند که کلاهبرداران و هکرها حرفه ای نیز نمی توانند با استفاده از نام دامین آن سازمان ایمیلی ارسال کنند.

پروتکل DKIM (Domain Keys Identified Mail)

مشتریان شرکت رایان نیک تجهیز



● رایان نیک تجهیز

● شماره تماس: ۸۸۲۰۹۲۶۷ - ۸۸۲۰۹۲۱۹

● فکس: ۸۸۲۰۸۲۱۳

● آدرس: تهران - میدان ونک - خیابان خدامی

بن بست لیلا- ساختمان لیلا- پلاک ۹ طبقه ۶ واحد ۱۲

● www.rayan-net.com



رایان نیک تجهیز