بسم الله الرحمن الرحیم

پیشنهاد

فرایند دورکاری امن

شرکت مهندسی پیام‌پرداز

آذر ماه ۱۳۸۹

این پیشنهاد توسط شرکت پیام‌پرداز تهیه شده است و هرگونه استفاده از تمام یا بخشی از آن منوط به اجازه کتبی از این شرکت می‌باشد.

فهرست

عنوان **صفحه**

۱- مقدمه ۱

۲- نیازمندی‌های امنیتی ۳

۳- راه‌کارهای امن‌سازی ۵

۳-۱- استفاده از سامانه *UTM* طریق برای محافظت از شبکه سازمان ۵

۳-۲- استفاده از سامانه کیهان برای امن‌سازی دورکاری ۵

۴- جمع‌بندی ۹

۱- مقدمه

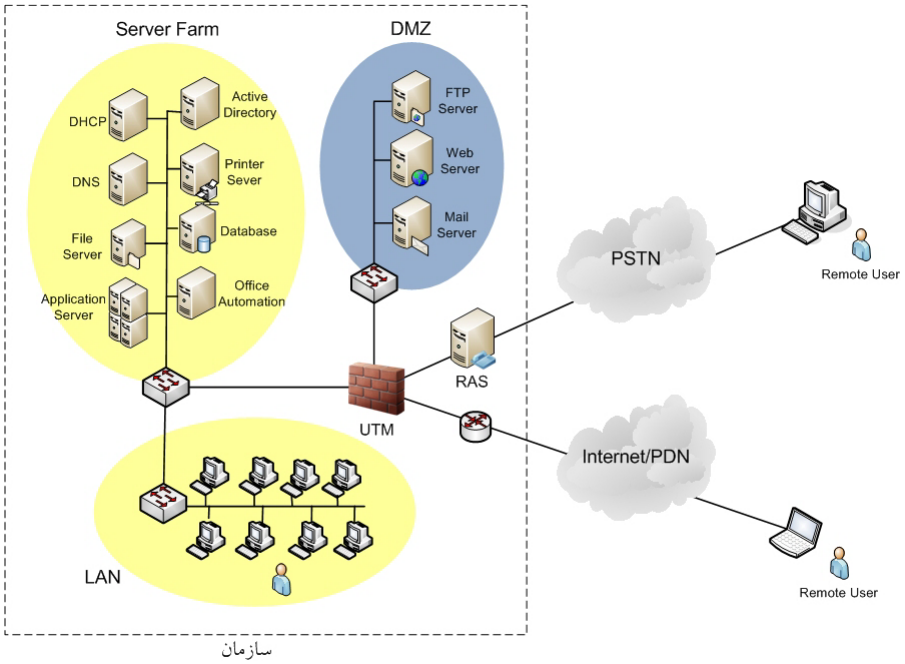
امروزه گسترش شبکه‌های همگانی نظیر اینترنت در بین اقشار مختلف جامعه باعث شده است که ایجاد ارتباط الکترونیکی در هر زمان و هر مکان به سادگی میسر باشد. برقراری آسان ارتباطات راه دور مبتنی بر شبکه، مدیران سازمان‌ها را به این فکر انداخته است که در همه حال با کارکنان سیار و ثابت خود ارتباط داشته و حتی به کارکنان خود امکان انجام دورکاری[1] یا در واقع اجرای کارهای اداری در خارج از وقت اداری و یا خارج از محل کار را بدهند. اما مشکل بزرگی که در این بین پیش روی مدیران سازمان‌ها و شبکه‌ها است و باید چاره‌ای اساسی برای آن اندیشیده شود مشکل تأمین امنیت این فرایند است.

به طور کلی در کاربردهای تحت شبکه، به دلیل این که اطلاعات کاربران بر روی یک فضای عمومی مانند اینترنت مبادله می‌شوند، مخاطرات امنیتی زیادی وجود دارند و همین موضوع باعث می‌شود مسأله‌ی امنیت در این کاربردها از اهمیت فوق العاده‌ای برخوردار باشد. این در حالیست که پروتکل‌های معمول شبکه از قبیل پروتکل *HTTP*، *FTP* و ... که بر اساس پروتکل *TCP/IP* به مبادله اطلاعات در شبکه می‌پردازند بدون ملاحظات امنیتی طراحی شده‌اند و از آن‌جا که در این پروتکل‌ها داده‌ها به صورت فاش منتقل می‌شوند، به راحتی می‌توان اطلاعات را در داخل شبکه شنود نموده و یا آن را دستکاری کرد. علاوه بر این کاربردهای تحت شبکه جهت احراز اصالت از روش نام کاربری و کلمه‌ی عبور استفاده می‌کنند که یک روش احراز اصالت یک عاملی محسوب می‌شود و دارای ضعف‌های زیادی است. این موارد نمونه‌هایی از تهدیدات محیط شبکه هستند که می‌توانند امنیت فرایند دورکاری را نیز تحت تاثیر قرار دهند.

شکل ۱ توپولوژی کلی شبکه یک سازمان نوعی را نشان می‌دهد.

---

[1] *Teleworking*



شکل ۱: توپولوژی شبکه یک سازمان نوعی

همانگونه که این شکل نشان می‌دهد معمولا شبکه سازمان را می‌توان متشکل از بخش‌های زیر دانست:

- بخش ایستگاه‌های کاری کاربران
- بخش سرویس‌دهنده‌ها شامل:
  - سرویس‌دهنده‌های زیرساختی مثل سرورهای *DNS*، *Domain Controller*، *DHCP* و ...
  - سرویس‌دهنده‌های کاربردی مثل سرورهای اتوماسیون اداری، حسابداری و ...
- بخش سرویس‌دهنده‌های عمومی در اینترنت مثل سرورهای وب، ایمیل و ...

به طور معمول یک دیواره آتش و یا به طور جامع‌تر یک سیستم مدیریت یکپارچه تهدیدات[1] (*UTM*) در سر راه ورودی شبکه سازمان قرار گرفته و شبکه سازمان را در برابر تهدیدات بیرونی محافظت می‌کند. کاربران راه دور با اتصال به سیستم *UTM* به شبکه داخلی سازمان مرتبط شده و فعالیت‌های خود را انجام می‌دهند.

ارتباط راه دور کارکنان می‌تواند از راه‌های زیر انجام گیرد:

۱- ارتباط از طریق شبکه اینترنت با استفاده از مودم‌های *ADSL* یا *WiMAX*

۲- ارتباط از طریق شبکه اینترانت ملی (*PDN*) با استفاده از مودم‌های *DSL*

[1] *Unified Threat Management*

۳- ارتباط تلفنی از طریق شبکه اینترنت (*Dialup*)

۴- ارتباط تلفنی مستقیم با سرور دسترسی راه دور[1] (*RAS*) سازمان

هر یک از این روش‌ها مزایا و معایب خاص خود را دارد. در روش‌های ۱ و ۲ پهنای باند بالاتر بوده و ضمنا خط تلفن کاربر نیز اشغال نمی‌شود. روش‌های ۳ و ۴ از لحاظ پهنای باند محدودیت داشته و بنابراین برای کاربردهایی از سازمان که حجم ترافیک زیادی را بین کاربر و سرور مبادله می‌کنند مناسب نیستند. روش ۴ اگرچه این حسن را دارد که به شبکه عمومی اینترنت متصل نیست ولیکن به شبکه عمومی تلفنی (*PSTN*) اتصال داشته و تهدیدات خاص خود را دارد.

۲- نیازمندی‌های امنیتی

جهت پشتیبانی از فرایند دورکاری کاربران، سرویس‌های امنیتی زیر لازم به نظر می‌رسد.

- **احراز اصالت کاربر برای سرویس‌دهنده‌های سازمان**: لازم است هویت کاربر در هنگام درخواست سرویس به صورت کاملا مطمئن برای سرور احراز گردد. روش معمول در این حالت استفاده از نام و کلمه عبور است. این روش در عین حال که بسیار ساده و کم‌هزینه است اما از لحاظ امنیتی ضعیف بوده و در صورت عدم حفاظت درست کاربران از کلمه‌های عبور خود، باعث ایجاد تهدیدات امنیتی جدی برای سازمان خواهد گشت. روش کلمه عبور که یک روش احراز اصالت یک عاملی محسوب می‌شود به وسیله حملات زیادی آسیب‌پذیر است. به عنوان مثال انتخاب کلمات عبور ضعیف توسط کاربران، شنود کلمه عبور از روی شبکه، سرقت کلمه عبور با استفاده از برنامه‌های *Key Logger* از روی کامپیوتر کاربر، حمله دیکشنری و حمله تکرار نمونه‌هایی از تهدیدات این روش هستند. برای رفع ضعف‌های مطرح، روش‌های احراز اصالت دوعاملی پیشنهاد می‌شود که در آن علاوه بر کلمه عبور (یا اصطلاحا *PIN*) از یک توکن امنیتی نیز برای بررسی هویت کاربر استفاده می‌شود.
- **احراز اصالت سرویس‌دهنده برای کاربران:** کاربران در هنگام اتصال به شبکه باید مطمئن باشند که طرف مقابل ایشان سرویس‌دهنده جعلی نیست. در غیر این صورت ممکن است یک سرور جعلی اقدام به سرقت اطلاعات کاربر نماید.
- **کنترل دسترسی:** کارمندان سازمان بسته به شغل و سمت خود، وظایف و مسئولیت‌های

[1] *Remote Access Server*

متفاوتی دارند و بنابراین هر کاربر ممکن است اجازه دسترسی به برخی برنامه‌های کاربردی یا سرورها را داشته باشد. پس از احراز اصالت کاربر لازم است سطح دسترسی وی به منابع بررسی و کنترل گردد.

- **ردگیری فعالیت‌های کاربر:** به منظور پیش‌گیری از وقوع اقدامات خلاف توسط کارمندان و نیز تشخیص و ردگیری این‌گونه فعالیت‌ها در صورت وقوع، سیستم‌های اطلاعاتی کلیه فعالیت‌های انجام گرفته را رویدادنگاری کرده و آنها را در اختیار مدیر سیستم قرار می‌دهند. بسته به سطح رویدادنگاری و جزییات مورد نظر، ممکن است عملیات ردگیری توسط برنامه‌های کاربردی و یا تجهیزات شبکه انجام بگیرد.
- **انکارناپذیری:** کاربران نباید بتوانند عملیاتی که انجام داده‌اند را انکار نمایند.
- **محرمانگی داده‌های مبادله شده:** محرمانگی اطلاعات حساس مبادله شده بین کامپیوتر کارمند و شبکه سازمان باید با روش‌های مدرن رمزنگاری تامین گردد تا هیچ‌کس امکان شنود و دسترسی به اطلاعات سازمان را از روی شبکه نداشته باشد.
- **صحت داده‌ها و پیامهای مبادله شده:** از آنجا که اعتبار داده‌های ارزشمند سازمان‌ها از حساسیت زیادی برخوردار است لذا باید با بکارگیری روش‌های مناسب، صحت اطلاعات مبادله شده بین کامپیوتر کارمند و سازمان را بر روی شبکه تضمین کرد.
- **جلوگیری از نفوذ افراد غیرمجاز به سرورهای سازمان:** از آنجا که ناچاریم شبکه محلی سرویس‌دهنده‌های سازمان را به شبکه‌های عمومی نظیر اینترانت ملی یا اینترنت متصل کنیم امکان نفوذ هکرها به شبکه سازمان و انجام فعالیت‌های خراب‌کارانه مطرح می‌گردد.
- **جلوگیری از نفوذ کدهای مخرب به سرورهای سازمان:** با توجه به اتصال شبکه سرویس‌دهنده‌ها به شبکه‌های عمومی لازم است از ورود کدهای مخرب اعم از ویروس‌ها، کرم‌ها، اسب‌های تروا و ... به شبکه محلی سازمان جلوگیری شود.
- **جلوگیری از دسترسی غیرمجاز به سرورهای سازمان از طریق آلوده نمودن کامپیوتر کاربر:** یک حمله مهم که می‌تواند موجب نشت اطلاعات و یا تهدیدات دیگر برای سازمان شود استفاده غیرمجاز هکرها، ویروس‌ها و به طور کلی بدافزارها از کانالی است که کاربر مجاز در حین انجام عملیات خود با سازمان برقرار کرده است. در این حالت بدون اینکه کاربر مطلع شود نفوذگر از کامپیوتر وی برای نفوذ به شبکه سازمان استفاده می‌کند.

- **جلوگیری از حملات نفوذگران داخلی:** شبکه سازمان‌ها همواره می‌تواند از طرف کاربران مجاز مورد تهدید قرار گیرد. اگرچه مکانیزم رویدادنگاری می‌تواند به عنوان یک عامل پیش‌گیرانه از این نوع حملات جلوگیری نماید ولیکن ابزارهای خودکاری نیز برای کشف و ممانعت از حملات نفوذگران داخلی وجود دارد.

۳- راه‌کارهای امن‌سازی

راه‌حل‌های امن‌سازی متنوعی برای کاربردهای تحت شبکه وجود دارد که هر یک برخی از سرویس‌های امنیتی مورد نیاز را ارائه می‌دهند.

۳-۱- استفاده از سامانه *UTM* طریق برای محافظت از شبکه سازمان

همانگونه که قبلا بیان گردید مستقل از بحث دورکاری، یک روش مهم حفاظت از شبکه سازمان در برابر تهدیدات خارجی استفاده از سیستم *UTM* است. شرکت پیام‌پرداز با ارایه یک سامانه *UTM* با نام طریق پاسخی به این نیاز مهم فراهم کرده است. سرویس‌های مهم امنیتی ارایه شده به وسیله *UTM* طریق عبارتند از:

- دیواره آتش حالت‌مند
- شبکه اختصاصی مجازی[1] (*VPN*) با پروتکل‌های *IPSec* و *PPTP*
- احراز اصالت کاربران در دسترسی به اینترنت (بصورت محلی یا ارتباط با *Active Directory* سازمان)
- امکان گروه‌بندی کاربران و تعریف سیاستهای مختلف امنیتی برای هر گروه
- تعریف سیاستهای مختلف زمانی و حجمی در دسترسی به اینترنت
- ویروس‌یابی و فیلترینگ روی ترافیک وب
- *Caching*
- سیستم تشخیص نفوذ
- مدیریت پهنای باند

۳-۲- استفاده از سامانه کیهان برای امن‌سازی دورکاری

به طور معمول جهت امن‌سازی اتصال راه دور کارکنان از روش‌های ایجاد شبکه اختصاصی مجازی

[1] *Virtual Private Network*

(*VPN*) استفاده می‌شود. از آنجا که این سرویس در سیستم‌های *UTM* ارایه می‌گردد می‌توان ارتباط *VPN* کاربر راه دور را با سیستم *UTM* برقرار کرده و دسترسی کاربر به شبکه سازمان را تامین نمود. در این حالت احراز اصالت کاربر مستقلا در *UTM* و یا با کمک سرور *Active Directory* انجام می‌شود. پس از احراز اصالت کاربر، دسترسی وی بنا بر سیاست‌های تعریف شده در *UTM* کنترل می‌گردد.

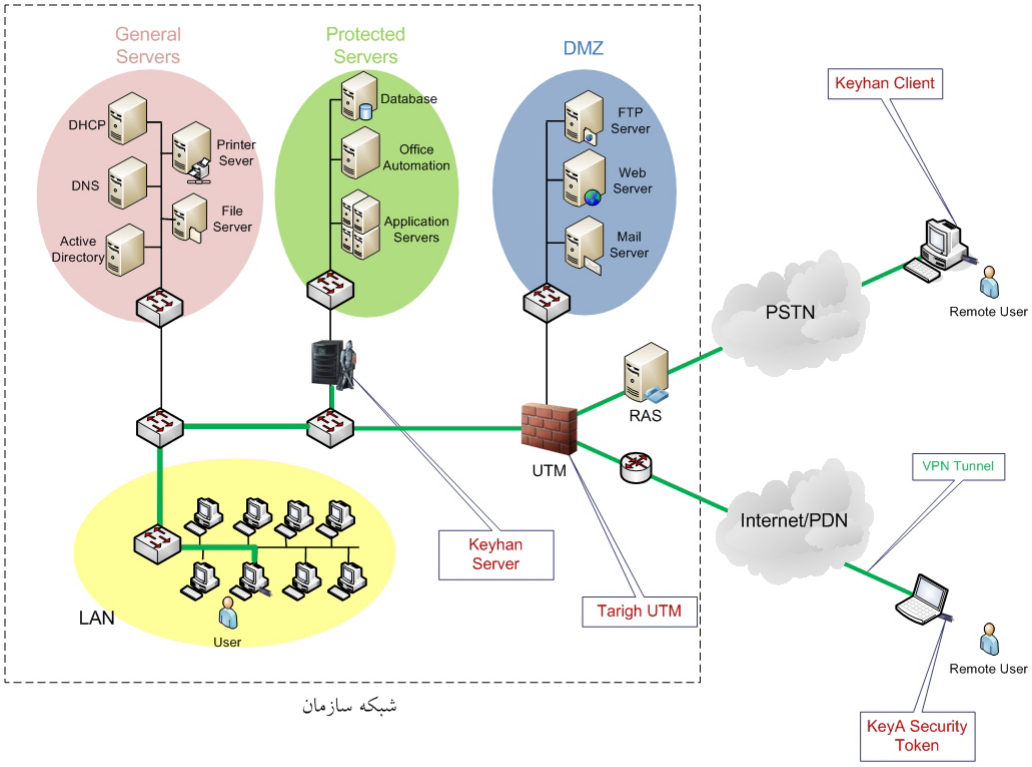
اگرچه معمولا سامانه *UTM* در ورودی شبکه سازمانها وجود دارد و می‌توان از سرویس *VPN* آن برای امن‌سازی فرایند دورکاری نیز استفاده کرد ولیکن به دلایلی (از قبیل روش‌های احراز اصالت یک‌عاملی، استفاده از الگوریتم‌های رمز با طول کلید پایین، عدم امکان تعریف سیاست‌های امنیتی با ریزدانگی در سطح کاربر و ...) این سطح امنیت معمولا کافی نبوده و باید از راه حل‌های دیگری به منظور امن‌سازی دورکاری استفاده نمود.

یک راه حل امن‌سازی که می‌تواند سطح امنیت بالایی را در فرایند دورکاری تامین نماید استفاده از محصول امن‌ساز شبکه کیهان است. این محصول توسط شرکت پیام‌پرداز طراحی و پیاده‌سازی شده است.

شکل ۲ طرح پیشنهادی برای دورکاری امن را نشان می‌دهد. در این طرح سرویس‌دهنده‌های زیرساختی سازمان از سرویس‌دهنده‌های کاربردی جدا شده‌اند. معمولا سرویس‌دهنده‌های زیرساختی باید به طور عمومی به همه کاربران سرویس بدهند و نیازمندی‌های امنیتی از قبیل احراز اصالت قوی، کنترل دسترسی و ارتباط امن با کاربر در مورد آن‌ها مطرح نیست. اما سرویس‌دهنده‌های کاربردی سازمان معمولا حساس بوده و باید از سطح امنیت ویژه‌ای برخوردار باشند. در این طرح یک سرویس‌دهنده کیهان در جلوی سرویس‌دهنده‌های حساس سازمان قرار گرفته و بر روی هر یک از کامپیوترهای کاربران نرم‌افزار *Client* کیهان نصب می‌شود. ابتدا مدیر شبکه کاربران و سیاست‌های امنیتی هر یک را تعریف کرده و برای هر کاربر یک توکن امنیتی سخت‌افزاری برنامه‌ریزی می‌نماید.

هر کاربر (اعم از داخل سازمان یا خارج آن) برای ارتباط با سرویس‌دهنده‌های حساس سازمان ابتدا لازم است از طریق سرور کیهان احراز اصالت شده و اجازه دسترسی وی صادر گردد. فرایند احراز اصالت کاربر با استفاده از یک پروتکل احراز اصالت دوطرفه و به صورت دوعاملی (با بکارگیری ماژول کیای کاربر و *PIN* وی) انجام می‌گیرد. پس از احراز اصالت موفقیت‌آمیز دوسویه کاربر و سرور، یک تونل امن (*VPN*) بین کامپیوتر کاربر و سرور کیهان برقرار می‌شود که کلیه داده‌های مبادله شده درون آن رمز می‌شود و بدین ترتیب سرویس‌های محرمانگی و صحت تامین می‌گردد. همچنین سرور کیهان به

عنوان یک دیواره آتش قوی عمل کرده و از نفوذ افراد غیرمجاز و بدافزارها به شبکه سرویس‌دهنده‌های حساس سازمان جلوگیری می‌کند.



شکل ۲: امن‌سازی فرایند دورکاری با استفاده از سامانه کیهان

سیستم کیهان در لایه شبکه عمل کرده و از دید لایه کاربرد کاملا شفاف است. بنابراین نیازی به تغییر در برنامه‌های کاربردی سازمان وجود نخواهد داشت.

با استفاده از امکانات سامانه کیهان می‌توان سرویس ورود یک‌باره[1] (*SSO*) را به لایه کاربرد ارایه نمود. به کمک این سرویس کاربر با یک بار ورود[2] به سیستم کیهان احراز اصالت می‌شود و برنامه‌های کاربردی سازمان به جای گرفتن نام و کلمه عبور از کاربر، از سرور کیهان برای احراز اصالت کاربر استعلام می‌کنند. البته در این حالت لازم است در برنامه‌های کاربردی سازمان تغییرات جزیی صورت گیرد. از آنجا که سرویس احراز اصالت سامانه کیهان از سطح امنیت بالایی برخوردار است اتکا به این روش احراز اصالت به جای روش یک عاملی بکار رفته در برنامه کاربردی، امنیت بالاتری را فراهم

[1] *Single Sign-On*
[2] *Login*

می‌آورد. به عنوان مثال با استفاده از این روش، امکان استفاده غیر مجاز یک کاربر از کلمه عبور کاربر دیگر نیز از بین خواهد رفت.

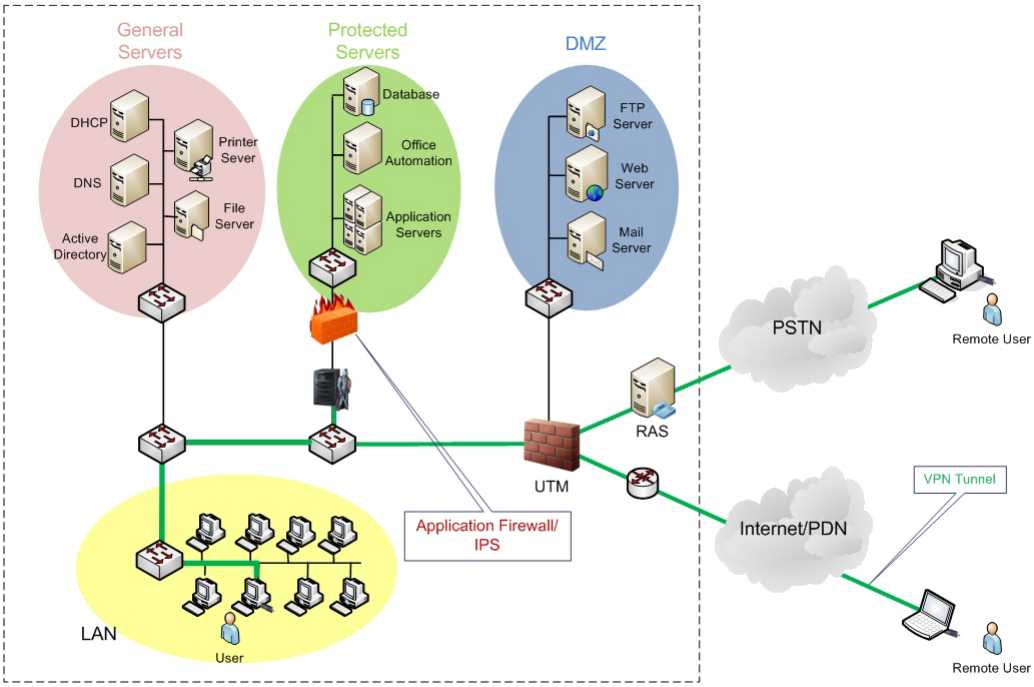
قابلیت خاص دیگری از سیستم کیهان که در اینجا می‌تواند به کار برده شود این است که می‌توان کاربر را محدود به یک کامپیوتر خاص کرد. در این حالت کاربر تنها از روی یک کامپیوتر مشخص که به وسیله مدیر تعیین شده قادر است به شبکه سازمان متصل شود.

با استفاده از سامانه کیهان می‌توان از آسیب‌های احتمالی ناشی از بدافزارها بر روی کامپیوتر کاربر تا حد زیادی در امان ماند. بدین منظور با استفاده از سرویس دیواره آتش موجود در برنامه کلاینت کیهان، در حالتی که کاربر به شبکه سرویس‌دهنده‌های سازمان متصل است تمامی ارتباطات دیگر کاربر با شبکه اینترنت را قطع نموده و بدین ترتیب از فعالیت‌های خرابکارانه این بدافزارها که غالبا بدون اطلاع کاربر انجام می‌شود جلوگیری خواهد گردید.

سامانه کیهان با تهیه رویداد از اتفاقات سیستم می‌تواند کمک شایانی در ردگیری فعالیت‌های کاربر ارائه نماید. در موقع اتصال کاربر به سرور کیهان، نام کاربری، آدرس *IP* کامپیوتر، نام دامنه، نام کاربر وارد شده به سیستم‌عامل و شناسه یکتای ماژول کاربر در سیستم ثبت می‌شوند. بنابراین با توجه به مکانیزم احراز اصالت قوی کیهان و رویدادنگاری انجام شده، معیار انکارناپذیری به خوبی برآورده می‌گردد. در حقیقت در سیستم کیهان امکان سوء استفاده از هویت کاربر توسط سایر اعضا و حتی مدیر وجود نخواهد داشت.

دیواره آتش سرور کیهان در ترکیب با دیواره آتش حالت‌مند *UTM*، شبکه سازمان را در برابر حملات نفوذگران خارجی که از روی شبکه‌های عمومی انجام می‌شوند مصون می‌نمایند. اما در شرایطی که حمله کننده یکی از کاربران مجاز سازمان باشد نیاز است تا با کمک یک دیواره آتش در لایه کاربرد و یا سیستم جلوگیری از نفوذ[1] (*IPS*)، از سرورهای حساس سازمان محافظت نموده و در صورت لزوم از فعالیتهای کاربر در لایه کاربرد رویدادنگاری کرد. بدین ترتیب می‌توان سطح امنیت بالاتری را به شبکه سازمان عرضه نمود. شکل ۳ توپولوژی شبکه را در این حالت نشان می‌دهد.

[1] *Intrusion Prevention System*



شبکه سازمان

شکل ۳: جلوگیری از تهدیدات نفوذگران داخلی با استفاده از دیواره آتش لایه کاربرد

۴- جمع‌بندی

از سامانه *UTM* طریق می‌توان به عنوان دروازه امنیتی برای حفاظت از شبکه سازمان در اتصال به شبکه‌های عمومی نظیر اینترنت استفاده نمود. همچنین به منظور ایجاد سطح بالایی از امنیت در فرایند دورکاری می‌توان از سامانه امن‌ساز شبکه کیهان بهره جست. سرویس‌های امنیتی ارایه شده در این راهکار عبارتند از: احراز اصالت کاربر، احراز اصالت سرور، کنترل دسترسی کاربر، محرمانگی و صحت داده‌های مبادله شده، جلوگیری از نفوذ (افراد غیرمجاز و کدهای مخرب) به سرورها، ردگیری فعالیت‌های کاربر در سطح شبکه، انکارناپذیری، جلوگیری از دسترسی غیر مجاز به شبکه سازمان از طریق آلوده نمودن کامپیوتر کاربر و سرویس *SSO*.

با استفاده از یک دیواره آتش در لایه کاربرد و یا سیستم *IPS* در مقابل سرویس‌دهنده‌های حساس سازمان، می‌توان از حملات نفوذگران داخلی نیز جلوگیری کرد.