چهارمین
همایش ملی تجارت الکترونیکی
The 4th e-Commerce
CONFERENCE
تهران- ۳ و ۴ آذرماه ۱۳۸۶

مدیریت یکپارچه تهدیدات الکترونیکی توسط محصول UTM

محسن رضوانی

عضور هیئت علمی دانشکده مهندسی کامپیوتر، دانشگاه صنعتی شاهرود

چکیده

از آنجا که اداره جوامع کنونی بدون استفاده از راه‌حل‌های مبتنی‌بر فنآوری اطلاعات تقریباً غیرممکن بنظر می‌رسد و مفاهیمی چون دولت الکترونیکی، تجارت الکترونیکی، بهداشت، آموزش و بانکداری الکترونیکی جزء راهبردهای اصلی حکومت‌هاست، اهمیت پرداختن به موضوع امنیت اطلاعات بیش از پیش نمایان می‌گردد.

به‌طور کلی فایروال یکی از محصولات امنیتی پرکاربرد در برقراری امنیت شبکه‌های کامپیوتری است. به همین دلیل تکنولوژی فایروال‌های در طول عمر این محصول تغییرات زیادی داشته است. این تغییرات بیشتر به دلیل تولد ایده‌های جدید در تهدیدات شبکه‌ای بوده است. در این مقاله تلاش خواهد شد که اخیرترین تکنولوژی در تولید فایروال معرفی شود. این تکنولوژی که منجر به تولید محصول UTM می‌شود، سطوح مختلفی از تهدیدات شبکه‌ای را کنترل می‌کند و پیش‌بینی می‌شود تا چند سال آینده جایگزین فایروال‌های امروزی شود.

کلمات کلیدی: امنیت شبکه، فایروال، امنیت محتوای ترافیک، UTM

گسترش استفاده از فضای تبادل اطلاعات در کشور طی سال‌های گذشته و برقراری ارتباط از طریق وب، موجب افزایش بکارگیری فنآوری اطلاعات و وابستگی نهادهای مختلف اجتماعی به این پدیده گردیده است.
از زمانیکه برخی از نگرانی‌ها در خصوص تعرض به حریم خصوصی افراد و سازمان‌ها ظاهر گردید، متخصصان فنآوری اطلاعات جهت جلوگیری از این تهدیدات و حمایت از اطلاعات خصوصی بنگاه‌ها، افراد و دستگاه‌های مختلف تلاش‌های ارزشمندی را ساماندهی نمودند تا فضای اعتماد به تبادلات الکترونیکی دچار آسیب کمتری شود.
تولید محصولات مختلف امنیتی اعم از تجهیزات سخت‌افزاری و نرم‌افزارها در حوزه‌های گوناگون ICT، ارائه راهکارها و تدوین سیاست‌های خرد و کلان جهت صیانت از فضای تبادل اطلاعات، تربیت نیروهای مختصص به منظور حفاظت از شبکه‌های تبادل اطلاعات همچنین ایجاد آمادگی در برابر حوادث ناشی از تهدیدات الکترونیکی، همگام با پیشرفت دانش IT در صحنه دنیای دیجیتال نمود بیشتری پیدا کردند. در این میان همزمان با رشد و توسعه انواع آسیب‌پذیری‌ها در سیستم‌های رایانه‌ای، تکنولوژی در راستای محافظت از این سیستم‌های نیز ارتقاء یافته‌اند.
رویکرد جدید تهدیدات الکترونیکی عموماً براساس تهدید بر محتوا تلقی می‌شود. این رویکرد بیشتر به دلیل حضور تجهیزات امنیتی پایین‌تر از لایه محتوا صورت گرفته است. بدیهی است که امنیت در لایه‌های بالا، مخصوصاً در محتوا بسیار پیچیده است و البته بالاترین سطح امنیت سازمان نیر امنیت در سطح محتوا می‌باشد. بر این اساس تکنولوژی تجهیزات امنیتی نیز باید به سمت محافظت از تهدیدات محتوایی حرکت کنند. تکنولوژی UTM اخیرترین ایده در تجهیزات امنیتی است که تلاش می‌کند امنیت سازمان را تا سطح محتوا حفظ نماید. این تکنولوژی به عنوان نسل جدید از محصولات فایروال منظور می‌شود و پیش‌بینی می‌شود که در آینده نزدیک، محصول UTM به‌عنوان محصول امنیتی ضروری در سازمان‌ها جایگزین فایروال شود [1 و 2].
در این مقاله تلاش خواهد شد که محصول UTM معرفی شده و مزایا و معایب آن برشمرده شود. براین اساس در ادامه این مستند، و در بخش دوم ضمن بیان نیازمندی‌های امنیتی محصول فایروال و UTM، ضرورت وجود این تکنولوژی بررسی می‌شود. در بخش 3 معماری و مکانیسم‌های امنیتی محصولات UTM شرح داده می‌شود. در پایان نتیجه‌گیری و جمع‌بندی ارائه می‌شود.

2 تکنولوژی فایروال و نیازمندی‌های جدید

2-1 تهدیدات محتمل سیستم‌های رایانه‌ای

به منظور مقابله با تهدیداتی که حوزه‌های مختلف فنآوری اطلاعات ممکن است با آن‌ها مواجه باشد، شناخت نوع تهدید ضروری به نظر می‌رسد. بدیهی است سیستم یکپارچه مقابله با تهدیدات باید بصورت مشخص انواع مورد نظر را پوشش داده و راه‌کارهای پیشنهادی را ارائه نماید.
انواع حملات و تهدیدات را می‌توان به صورت زیر دسته‌بندی نمود:

- حملات تخریب سرویس
- حمله از طریق برنامه مخرب
- حمله انسانی و فیزیکی

در هر یک از دسته حملات فوق، فعالیت‌های متفاوتی از سوی مخربین قابل انجام است. در این بخش فهرستی از این فعالیت‌ها بیان می‌شوند.

2-1-2 حملات تخریب سرویس

در این نوع حمله، مهاجم تلاش می‌نماید تا دسترسی منابع رایانه توسط سایر کاربران را ناممکن سازد. برای دستیابی به این هدف، چنانچه منابع مشترک سیستم به گونه‌ای توسط مهاجم اشغال گردیده و حجم استفاده از آن‌ها افزایش یابد که دیگران قادر به استفاده از آن‌ها نباشند، عملاً حمله به منابع سیستم صورت گرفته است. این نوع حمله می‌تواند به تخریب منابع منجر گردد و یا استفاده از آن‌ها را غیرممکن سازد. برخی از فعالیت‌های این نوع تهدید بصورت زیر قابل بیان است.

- تخریب، پر کردن و خذف فایل‌های اساسی دیسک
- تولید پردازش و اشغال پهنای باند پردازنده
- تخریب و کنترال سرویس‌های شبکه توسط مهاجم
- ذخیره پیام‌های پخش شده، ارسال پیام و درخواست پاسخ از رایانه‌های شبکه
- استفاده از اتصال‌های غیر باز

2-1-2 حمله از طریق برنامه مخرب

در این نوع حملات، برنامه‌ها به‌گونه‌ای نوشته می‌شوند که رفتاری مخرب و غیر عادی داشته باشند. معمولاً این برنامه‌ها از طرق مختلف برای کاربران رایانه ارسال شده و کاربر بدون توجه به وجود دستورالعمل مخرب نسبت به اجرای آن اقدام می‌نماید. شیوه‌های مختلف تخریب این برنامه‌ها بصورت زیر می‌باشد.

- حمله به برنامه‌های سرویس‌دهنده شبکه
- تخریب نرم‌افزارها از طریق ارسال پست الکترونیکی
- ارسال هرزنامه‌ها
- استفاده از درب‌های مخفی جهت دسترسی غیرمجاز
- اسب‌های تراوا و کرم‌ها

2-1-3 حمله انسانی و فیزیکی

چنانچه بر اساس ضعف‌های موجود در برخی از سیستم‌ها، نفوذگر بتواند به عنوان راهبر سیستم شناخته شود، با در دست گرفتن کنترل سیستم می‌تواند صدماتی را وارد نماید.

بعلاوه هر مخربی می‌تواند بصورت فیزیکی منابع سیستم را مورد حمله قرار داده و کارکرد آن را دچار مشکل سازد. فعالیت‌های زیر توسط مخاجم قابل انجام می‌باشد:

- سرقت رمز عبور
- نفوذ از طریق برقراری روابط اجتماعی
- تخریب فیزیکی منابع رایانه‌ای و شبکه‌ای

2-2 نقش ابزارهای کنترل ترافیک

امروزه فایروال‌های حالت‌مند[1]، IDSها، و آنتی ویروس‌های مبتنی بر میزبان[2] محبوب‌ترین محصولات امنیتی را تشکیل می‌دهند. اما این راه‌حل‌ها به سرعت در حال از دست دادن تاثیر خود در برابر نسل جدید تهدیدات می‌باشند و متخصصان فن-آوری اطلاعات حملات و سرایت‌های موفق متعددی را بر ضد امنیت و زیرساخت شبکه مشاهده می‌کنند.

---

۱ Stateful

۲ Host Based Antivirus

2-2-1 نقش سیستم‌های فایروال سنتی و کمبودهای آن‌ها

فایروال‌های حالت‌مند در ابتدا برای امن‌سازی ارتباط با اینترنت بوسیله یک واسط امن بین شبکه‌های قابل اعتماد و غیر قابل اعتماد طراحی شدند. این فایروال‌ها با دقت در سرآیند لایه شبکه (L3)، و لایه پروتکل (L4) بسته را نظارت کرده و بر اساس آن به ترافیک اجازه ورود داده، درخواست ورود آن را رد کرده، و یا ترافیک را دوباره بر اساس مجموعه‌ای از خط‌مشی‌های فایروال مسیریابی می‌کنند. مشکل اصلی فایروال‌ها در این است که هکرها روش‌های متعددی را برای گذشتن از خط‌مشی‌های فایروال توسعه داده‌اند. بعضی از این روش‌ها شامل موارد زیر می‌باشند:

- پویش پورت‌های باز روی فایروال و یا سیستم‌های موجود در ناحیه قابل اعتماد
- نرم‌افزارهای مخرب نظیر تروژان‌هایی که روی سیستم‌های موجود در ناحیه قابل اعتماد نصب شده‌اند و می‌توانند به عنوان شروع کننده حملات نقش داشته باشند.
- عدم توانایی فایروال‌های نسل قدیمی در بازرسی بخش داده‌ای بسته جهت شناسایی انواع کدهای مخرب نظیر ویروس، کرم و یا تروژان، می‌تواند به‌عنوان یک مسیر قابل نفوذ برای حمله مورد استفاده قرار گیرد.
- بسیاری از فایروال‌های جدید که قابلیت بازرسی عمیق[3] را پشتیبانی می‌کنند، در مقابل بسته‌های تکه‌تکه شده آسیب‌پذیر هستند.
- کاربران با استفاده از سیستم‌های قابل حمل نظیر Laptop و یا PDA، می‌توانند حامل انواع کدهای مخرب و آلوده از بیرون به داخل سازمان شوند.

در نتیجه باید اذعان داشت که فایروال‌هایی که ما را احاطه کرده‌اند کمکی در جهت ممانعت از حملات و سرایت‌هایی که از داخل شبکه قابل اعتماد آغاز شده باشند نمی‌کنند.

2-2-2 نقش سیستم‌های IDS سنتی و کمبودهای آن‌ها

همانند فایروال‌های سنتی، IDSهای سنتی با آمدن تهدیدات مدرن و پیچیده جای خود را به فن‌آوری‌های جدیدتر می‌دهند. حمله کنندگان ضعف‌های سیستم‌های IDS را شناخته و متدهای جدیدی برای گذشتن از این سیستم‌های نظارتی پیاده‌سازی کرده‌اند. مثال‌هایی از ضعف سیستم‌های IDS عبارتند از:

- محصولات IDS معمولاً در نقاط لبه‌ای شبکه مستقر می‌شوند و نظارتی بر کل شبکه ندارند.
- سیستم‌های IDS معمولاً به عنوان ابزارهای نظارتی کاربری دارند و قابلیت ممانعت از ترافیک مشکوک در این سیستم‌های وجود ندارد.
- به‌دلیل نحوه بازرسی در سیستم‌های IDS، این سیستم‌ها معمولاً در مقابل حجم بالای ترافیک آسیب‌پذیر می‌شوند.
- اغلب سیستم‌های IDS حجم زیادی false positive تولید می‌کنند که برای جلوگیری از این امر نیاز به نظارت مداوم بر کار IDS می‌باشد.

برای حل مشکلات فوق، بسیاری از تولید کنندگان محصولات IDS، به سمت تولید نسل جدیدی از این محصولات به نام IPS روی آورده‌اند. سیستم‌های IPS می‌توانند به صورت Inline در توپولوژی شبکه قرار گیرند و کنش‌های مورد نیاز مدیر نظیر Drop و یا Reset را اِعمال نمایند. این محصولات همچنین می‌توانند از مکانیسم‌های تشخیص Anomaly بهره‌مند شوند.

---

[3] Deep Inspection

2-2-3 آنتی ویروس‌های مبتنی بر میزبان و کمبودهای آن‌ها

یکی از پر کاربردترین نرم‌افزارهای امنیتی، سیستم‌های آنتی ویروس مبتنی بر میزبان است. این نرم‌افزارهای آنتی ویروس به‌عنوان یکی از معمول‌ترین راه‌حل‌های امنیتی در سازمان‌ها استفاده می‌شوند. قدمت استفاده از این نرم‌افزارهای از سال 1980 میلادی و به‌دلیل حضور فایل‌های ویروسی می‌باشد. گرچه حضور نرم‌افزارهای آنتی ویروس مبتنی بر میزبان یک ضرورت در سازمان‌های تلقی می‌شود ولی این راه‌حل‌ها شامل نقاط ضعف نیز می‌باشند که در ادامه برخی از آن‌ها بررسی می‌شوند.

- فرآیند نصب، نگهداری و ارتقای الگوهای ویروسی برای این نرم‌افزارهای پیچیده است. باید توجه داشت که این نرم‌افزارها باید در تمامی میزبان‌های موجود در سازمان نصب شوند.
- کاربران به‌صورت عمدی و یا غیرعمدی می‌توانند آنتی ویروس خود را غیرفعال نمایند.
- اغلب کاربران یک فرایند منظم جهت به‌روز رسانی الگوهای ویروس برای نرم‌افزار آنتی ویروس خود اتخاذ نمی‌کنند و معمولاً در مقابل اخیرترین نسخه ویروس‌ها آسیب‌پذیر هستند.
- برخی از تروژان‌های پیشرفته قادرند قبل از فعال شدن آنتی ویروس روی میزبان فعال شوند و همچنین از فعال شدن آنتی ویروس نیز جلوگیری می‌کنند.

بدیهی است سازمان‌هایی که از نرم‌افزارهای آنتی ویروس مبتنی بر میزبان استفاده می‌کنند، در زمینه امنیت سیستم عامل میزبان و برنامه کاربردی از سطح امنیتی خوبی برخوردارند. ولی باید توجه داشت که این سطح امنیتی برای سازمان کافی نیست. به‌طور خاص باید توجه داشت که بسیاری از کدهای مخرب از ناحیه غیرقابل اعتماد وارد نواحی قابل اعتماد شبکه می‌شوند. بنابراین سازمان باید بتواند این کدهای مخرب را قبل از رسیدن به میزبان‌های تشخیص داده و بلاک نماید.

2-3 تعریف UTM

نام UTM[4] یا مدیریت یکپارچه تهدیدات الکترونیکی عبارتی است که برای اولین بار توسط شرکت IDC در سال 2004 ابداع شد. محصول UTM یک راه‌حل جامع امنیتی است که مسئول محافظت سیستم در برابر چندین نوع تهدید می‌باشد. یک محصول UTM معمولا شامل فایروال، VPN، نرم افزار آنتی ویروس، فیلترینگ محتوا، فیلتر اسپم، سیستم‌های جلوگیری و تشخیص حمله (IPS)، حفاظت از Spywareها، و نظارت، گزارش‌گیری، و مدیریت یکپارچه می‌باشد.

از UTM می‌توان به عنوان نسل تحول یافته محصولات Firewall/VPN و حتی دروازه‌های امنیتی نام برد که سعی در ارائه سرویس‌های امنیتی به کاربران یک سازمان به ساده‌ترین شکل دارد. در واقع بدون وجود UTM و در راه‌حل‌های قدیمی برای بدست آوردن تک تک این سرویس‌های امنیتی ابزارهای مجزا به همراه پیچیدگی‌های نصب، به‌روز سازی، و مدیریت آن‌ها نیاز بود، اما UTM با یکپارچه سازی و مدیریت متمرکز، تمامی نیازمندی‌های امنیتی در یک سازمان در برابر تهدیدات الکترونیکی را برآورده می‌سازد.

2-4 نیاز به محصول UTM

2-4-1 روش‌های سنتی (امنیت لایه‌ای به‌صورت چند نقطه‌ای)

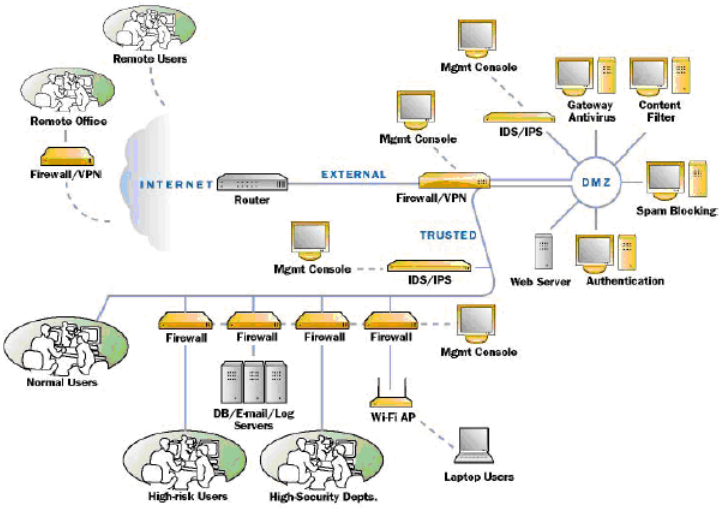
امروزه بسیاری از سازمان‌ها سعی در پیاده‌سازی سیستم‌های امنیتی با ترکیب راه‌حل‌های مختلف از فروشندگان متفاوت دارند. همگی این محصولات می‌بایست به صورت مجزا خریداری، نصب، مدیریت، و بروزرسانی شوند. این رویکرد مشکلاتی شامل تعامل و همکاری نامناسب بین سیستم‌های امنیتی مجزا، حفاظت ناکامل، و آزمون و درستی‌یابی زمانبر دارد، که همگی باعث

---

[4] Unified Threat Management

کاهش پاسخ شبکه به حملات می‌شوند. محصولاتی که برای کار با هم طراحی نشده باشند، می‌توانند در نرخ کارایی شبکه تاثیر بگذارند. همچنین هزینه لازم برای تهیه انواع محصولات مختلف امنیتی برای رسیدن به امنیت جامع در یک سازمان کوچک یا متوسط بسیار سنگین می‌باشد. پیچیدگی طراحی چنین راه‌حلی نیز در شکل 1 مشاهده می‌شود.

سازمان‌ها به ندرت دارای زیرساخت IT لازم برای نگهداری و مدیریت یک چنین مخلوطی از محصولات متفاوت هستند، که هر کدام دارای سیستم مدیریت خاص خود می‌باشند. و در نهایت هزینه نگهداری و پشتیبانی از رویکردهای چند نقطه‌ای برای یک سازمان کوچک یا متوسط بسیار زیاد می‌باشد. به دلیل این مشکلات، پیچیدگی‌ها، و ضعف‌ها، رویکرد یکپارچه سازی محصولات UTM در سطح سازمان‌ها مطرح می‌شود.



شکل 1 پیچیدگی امنیت لایه‌ای به‌صورت چند نقطه‌ای و با استفاده از محصولات متفاوت

2-4-2 راه‌حل مدرن (ابزارهای امنیتی مجتمع)

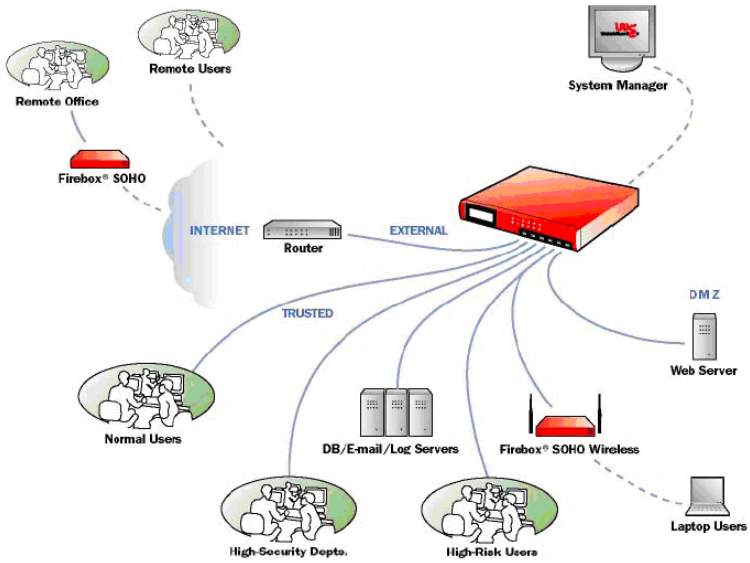
مفهوم اولیه ابزارهای امنیتی مجتمع، مفهوم جدیدی نیست و به زبان ساده به معنای ترکیب چندین کارکرد امنیتی در یک راه‌حل یا ابزار واحد می‌باشد. برخی از فروشندگان راه‌حل‌های امنیتی، ابزارهای امنیتی مجتمعی در گذشته ارائه کرده‌اند. با این وجود، این راه‌حل‌های جوان دارای کمبودهای زیادی بوده‌اند. به خصوص اگر یکپارچه سازی کارکردها نامناسب بوده و به صورت ضعیفی پیاده‌سازی شده باشد. این کمبودها می‌تواند شامل موارد زیر باشد:

- کارایی نامناسب
- کاهش قابلیت اعتماد[5]
- مقیاس‌پذیری محدود
- افزایش پیچیدگی مدیریت
- امنیت نامناسب

به‌طور کلی رویه یکپارچه سازی کارکردهای امنیتی باید به‌نحوی انجام شود که تکنولوژی‌های مختلف استفاده شده بتوانند در کنار یکدیگر فعالیت نمایند. نتیجه این یکپارچه سازی محصول Appliance خواهد شد که قابلیت توسعه سرویس‌های امنیتی

° Reliability

جدید را خواهد داشت و از یک مکانیسم دفاع امنیتی لایه‌ای جهت مقابله با تهدیدات امروز و آینده بهره‌مند می‌باشد. همچنین محصول نهایی در کنار توان دفاع امنیتی بالا، باید بتواند لحاظ هزینه مقرون به‌صرفه باشد. در شکل 2 استفاده از راه‌حل یکپارچه سازی مکانیسم‌های امنیتی در قالب یک محصول UTM در شبکه مورد نظر آورده شده است.



شکل 2 استفاده از راه‌حل یکپارچه سازی مکانیسم‌های امنیتی در قالب یک محصول UTM

3 محصول UTM

3-1 پیش‌بینی توسعه در دنیا

بازار چشمگیر محصولات امنیتی UTM روند تولید محصولات تک کاربرد را به سمت ارائه چندین ویژگی امنیتی در یک سکو، در محیط‌هایی منعطف‌تر می‌برد. به گفته چالرز کولوجی مدیر بخش تحقیقات محصولات امنیتی در IDC، UTM با ارائه برنامه‌های کاربردی امنیتی با کارایی بالا، و صرفه‌جویی در هزینه‌های عملیاتی و سرمایه، به سرعت در حال محبوب‌تر شدن است [1].

بر طبق آمار IDC، بخش فروش UTM در گروه ابزارهای امنیت شبکه سریعترین رشد را در بازار داشته است. (بیش از 100 میلیون دلار سود در سال 2003 که با افزایش 160 درصدی نسبت به سال 2002 همراه بود.) طبق همین گزارش در سال 2008 از کل سود فروش 3,45 میلیارد دلاری دسته محصولات مدیریت امنیت شامل UTM، فایروال‌های سنتی، و ابزارهای VPN، UTM به تنهایی 58 درصد سود فروش را خواهد داشت. همین پیش‌بینی نشان می‌دهد که سود فروش فایروال‌های سنتی رو به کاهش خواهد بود و این نشان از جایگزینی نیاز مشتریان در زمینه فایروال با محصولات UTM خواهد بود. بخشی از این پیش‌بینی در شکل 3 آورده شده است [1].

Worldwide Unified Threat Management Security Appliance and Firewall/VPN Security Appliance Revenue, 2003-2008 ($M)

	2003	2004	2005	2006	2007	2008	2003-2008 CAGR (%)
UTM Security Appliance	105	225	518	828	1,325	1,987	80.1
Firewall/VPN Security Appliance	1,479	1,668	1,792	1,804	1,623	1,462	-0.2

Source: IDC, 2004

شکل 3 پیش‌بینی IDC در مورد رشد سود فروش UTM]1[

با توجه به رشد نیاز به محصولات UTM در بازار، فرآیند تولید این محصول در بسیاری از شرکت‌های تولید کننده محصولات امنیتی شکل گرفته است. این فرآیند در شرکت‌های تولید کننده محصولات Firewall/VPN با نگرش ارتقاء محصول به UTM با سرعت بیشتری به نتیجه رسیده است، به‌طوری که بیشتر شرکت‌های معتبر در زمینه تولید محصولات Firewall/VPN، امروزه محصول خود را برای تبدیل به UTM ارتقاء داده و با این نام در بازار تجارت می‌کنند.

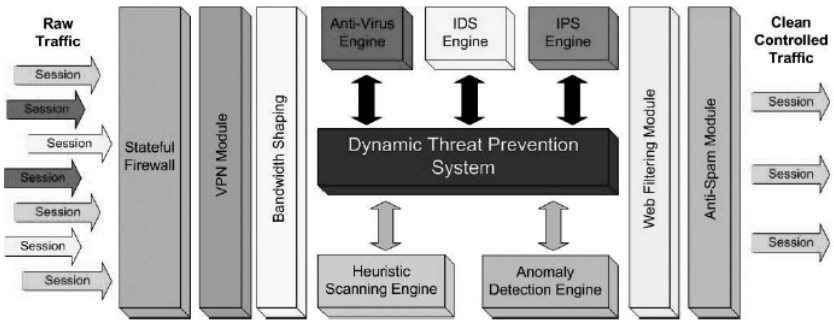
2-3 معماری محصول

همان‌طور که در بخش قبلی شرح داده شد، محصول UTM امنیت را در کل لایه‌های شبکه و به‌طور خاص در لایه محتوا ارائه می‌کند. برای این منظور باید چندین مکانیسم امنیتی را به‌صورت یکپارچه ارائه نماید. این مکانیسم‌های امنیتی شامل موارد زیر می‌باشد.

- فایروال با قابلیت بازرسی حالت‌مند ترافیک
- ارائه سرویس VPN با قراردادهای متنوع
- امکان تشخیص و جلوگیری از حمله (IPS)
- آنتی ویروس مبتنی بر دروازه
- فیلترینگ محتوای ترافیک (به‌طور معمول برای محتوای Web و Mail ارائه می‌شود.)
- فیلترینگ اسپم روی ترافیک Mail
- مدیریت پهنای باند

نکته کلیدی در تولید محصولات UTM ارائه یک معماری مناسب برای چیدمان مکانیسم‌های فوق می‌باشد که بتواند بهترین کارایی را روی محصول ارائه نماید. بدیهی است با افزایش میزان بازرسی ترافیک در مکانیسم‌های امنیتی مختلف، امکان تاخیر و کاهش کارایی شبکه نمایان می‌شود. در این راستا استفاده از ایده‌هایی نظیر استفاده از شتاب‌دهنده‌های سخت‌افزاری می‌تواند برخی از مشکلات را مرتفع سازد. این ایده در بسیاری از شرکت‌های بزرگ تولیدکننده محصولات امنیتی استفاده می‌شود.

شکل 4 یک معماری نمونه از محصول UTM را نشان می‌دهد. چیدمان مکانیسم‌های امنیتی و ترتیب بازرسی ترافیک در این محصول یکی از پارامترهای اصلی این معماری می‌باشد. در این معماری اولین بازرسی امنیتی توسط ماژول حالت‌مند انجام می‌شود که منجر به حذف بسیاری از تهدیدات می‌شود. همچنین این ایده می‌تواند منجر به تولید مفهوم نشست برای بازرسی در ماژول‌های امنیتی دیگر شود. از نکات دیگر این معماری قرار دادن بازرسی‌های محتوا در انتهای حرکت بسته می‌باشد. این ایده به‌دلیل عدم نیاز به بازرسی محتوای ترافیک‌های مشکوک می‌باشد. بدیهی است ترافیکی که توسط ماژول حالت‌مند متوقف شود، نیاز به بازرسی محتوایی توسط ماژول AntiSpam نمی‌باشد.



شکل 4 جریان بازرسی ترافیک در یک محصول UTM

معماری ارائه شده در شکل 4 می‌تواند در یک محصول UTM مورد استفاده قرار گیرد ولی نکته کلیدی در پیاده‌سازی این معماری ملاحظات پیاده‌سازی ارتباطات بین ماژول‌ها می‌باشد. برای نمونه معماری ارائه شده در [] با هدف کاهش تعداد IPCها بین مولفه‌های محصول می‌باشد. همچنین نکته دیگری که در پیاده‌سازی این معماری باید در نظر گرفت، نوع مدل مدیریتی است که محصول برای مدیر ارائه می‌کند.

3-3 مزایای UTM

- مدیریت یکپارچه
  - ♣ مدیریت چندین کاربرد از یک محل و توسط یک ابزار
  - ♣ ایجاد و پیاده‌سازی آسان و سریع خط‌مشی‌های سراسری سازگار
  - ♣ تکیه بر گزارشات و نظارت‌های برخط و تعاملی
  - ♣ استفاده از تنها یک واسط مستقیم برای نصب و مدیریت تمامی ویژگی‌های امنیتی
- UTM به عنوان یک محصول یکپارچه فرآیند انتخاب محصولات امنیتی مورد نیاز، یکپارچه سازی آن‌ها، و پشتیبانی‌های آتی را ساده کرده است.
- محصولات UTM دارای مراحل نصب کم، ساده و عمدتاً به‌صورت plug and play هستند.
- از آنجائیکه کاربران عمدتاً تمایل به دستکاری تنظیمات دارند، در بسته‌هایی مانند ابزار UTM با کاهش تعامل اپراتور، خرابی‌های ایجاد شده توسط آن‌ها کاهش می‌یابد و در نتیجه امنیت افزایش می‌یابد.
- به دلیل اینکه تنها یک ابزار واسط امنیتی وجود دارد، در مواقع بروز مشکل برای عیب‌یابی، این وسیله حتی توسط یک فرد غیر متخصص قابل خارج شدن از مدار می‌باشد.
- هزینه لازم برای فراهم آوردن سطح امنیت مورد نیاز در یک سازمان توسط ابزارهای مجزای امنیتی بسیار بیشتر از هزینه راه‌حل UTM می‌باشد.

4-3 چالش‌های تولید محصول

با توجه به توصیف ارائه شده از محصول UTM، می‌توان این محصول را در رده محصولات پیچیده برای تولید قرار داد. بنابراین چالش‌های یک محصول پیچیده و بزرگ را برای تیم تولید خواهد داشت. علاوه‌بر این طبق نظر تولیدکنندگان این محصول، چالش اصلی برای تولید مساله کارایی محصول و میزان تاخیر شبکه برای بازرسی تمامی مکانیسم‌های امنیتی است 3[و]4. این چالش به‌عنوان مساله اصلی برای انتخاب بین مشتریان نیز مورد نظر می‌باشد. در این راستا تولیدکنندگان به دنبال ایده‌های جدید در تولید این محصول با معماری کاراتر می‌باشند و در این حین تحقیقاتی نیز نظیر 3[، 5 و]6 انجام شده است.

4 جمع‌بندی و نتیجه‌گیری

در این مقاله تکنولوژی جدید محصولات امنیت شبکه با نام UTM ارائه شد. همچنین مزایا، معماری و چالش‌های اصلی در تولید این محصول مورد بررسی قرار گرفت. طبق پیش‌بینی‌های انجام گرفته، آینده محصولات امنیت شبکه نظیر فایروال‌ها به سمت محصول UTM خواهد بود[1 و]2. این محصول چندین مکانیسم امنیتی را در کنار هم و به‌صورت یکپارچه ارائه می‌کند. همچنین ایده اصلی محصول UTM مدیریت تهدیدات شبکه در تمامی لایه‌ها، خصوصاً در محتوا می‌باشد. با توجه به رشد سریع در تولید محصول UTM و نیاز اساسی شبکه‌های کامپیوتری به این محصول، به‌نظر می‌رسد که دولت و شرکت‌های خصوصی باید برنامه ویژه‌ای را برای تولید این محصول در داخل کشور تدوین نمایند.

5 مراجع

1. Charles J. Kolodgy , Worldwide Threat Management Security Appliances 2005-2009 Forecast and 2004 Vendor Shares: Security Appliances Remain a Well Oiled Machine, IDC #33997, Volume 1, September 2005.
2. Greg Young, John Pescatore, Magic Quadrant for Enterprise Network Firewalls, Gartner RAS Core G00141050, June 2006.
3. Ying-Dar Lin, Chih-Wei Jan, Po-Ching Lin, and Yuan-Cheng Lai, Designing an Integrated Designing an Integrated Content Security Gateways, IEEE Computer 39(11): 66-72 (2006).
4. Ellen Messmer, All-in-one Security Devices Face Challenges, Network World, 2006.
5. Ying-Dar Lin, Po-Ching Lin, Meng-Fu Tsai, Tsao-Jiang Chang, Yuan-Cheng Lai: kP2PADM: An In-kernel Gateway Architecture for Managing P2P Traffic. IPDPS 2007: 1-9
6. Ying-Dar Lin, Kuo-Kun Tseng, Chen-Chou Hung, Yuan-Cheng Lai: Scalable Automaton Matching for High-Speed Deep Content Inspection. AINA Workshops (1) 2007: 858-863