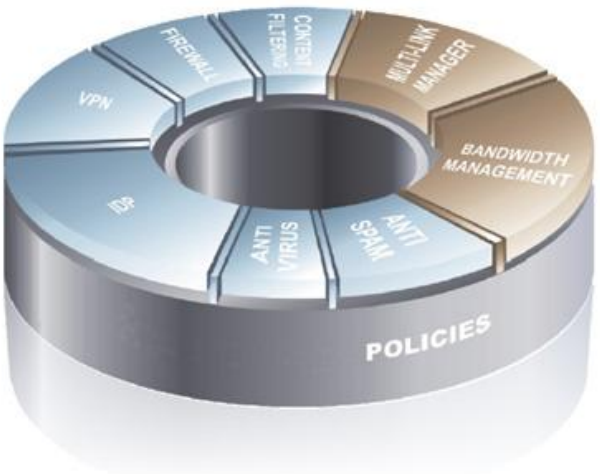
مقدمه ای بر پدافند غیر عامل در حوزه سامانه مدیریت تهدید یکپارچه



فهرست

مقدمه

همزمان با ظهور و گسترش استفاده از فناوری اطلاعات و ارتباطات، برقراری امنیت در فضای سایبر بعنوان یکی از مسائل اصلی در این حوزه مطرح شده است. افزایش وابستگی فعالیت دولت‌ها و زیرساخت‌های اساسی کشورها به فناوری اطلاعات و سامانه‌های اطلاعاتی و ارتباطی، آسیب پذیری‌های جدیدی را پدید آورده است که ممکن است موجب نفوذ و ایراد ضربه و یا از کار انداختن کامل آنها شود.

با توجه به سرعت گسترش حملات در فضای سایبر و تنوع آنها، تأمین امنیت این حوزه تنها با استفاده از آخرین فناوری‌ها و بروز نمودن روش‌ها میسر است. در این میان، بخش قابل توجهی از بار فنی و مسئولیتی برقراری امنیت برعهده کارشناسان امنیت شبکه سازمان‌ها و شرکت‌ها است. این کارشناسان باید با پیاده‌سازی مکانیزم‌ها و استفاده از تجهیزات امنیتی مختلف موجبات برقراری امنیت، ایمنی و پایداری داده‌ها و زیرساخت سازمان متبوع خود را فراهم آورند.

در گذشته، اغلب کارشناسان امنیت با مشکلات زیادی در استفاده از تجهیزات امنیتی مواجه بوده‌اند، از جمله این مشکلات می‌توان به عدم سازگاری دستگاه‌ها با یکدیگر و عدم وجود دستگاهی برای تحلیل گزارشات تولیدشده توسط تجهیزات مختلف اشاره نمود. از این‌رو متخصصین امنیت شبکه مجتمع کردن دستگاه‌های متفاوت و حذف وظایف موازی آن‌ها را به عنوان یک راه‌حل مناسب جهت حذف مشکلات موجود و ایجاد یک نگاه جامع امنیتی مطرح نمودند. نتیجه این تفکر به ساخت و عرضه محصول «سامانه مدیریت تهدید یکپارچه[1]» و توسعه آن بوسیله شرکت‌های مطرح فعال در این حوزه منتهی گردیده است.

---

[1] Unified Threat Management

فصل ۱

سامانه مدیریت تهدید یکپارچه و علل استفاده از آن

برای امن‌سازی ارتباطات درون‌سازمانی، میان‌سازمانی و اینترنتی، استفاده از سرویس‌های متعدد امنیتی در شبکه و مخصوصاً در دروازه[۱] آن ضروری است. استفاده از دستگاه‌های منفرد امن‌سازی به دلایل فراوانی همچون مواردی که در ادامه بیان می‌شود، توصیه نمی‌گردد.

۱- با توجه به چینش دستگاه‌ها و کارگزارها که معمولاً به طور سری پشت سرهم است، هر یک از دستگاه‌ها به عنوان یک گلوگاه[۲] محسوب شده و کندی یا قطعی در هر دستگاه، کار دستگاه‌های دیگر را مختل می‌کند.

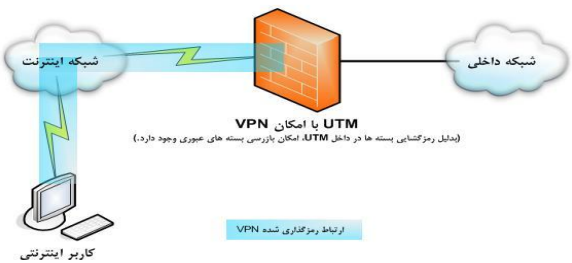
۲- تأخیر زیادی از زمان ارسال بسته تا دریافت بسته در مقصد نهایی بوجود می‌آید؛ چراکه در هر یک از دستگاه‌ها، بسته‌های اطلاعاتی یک بار گشوده شده، بررسی می‌شوند و دیگر بار بسته می‌شوند.

---

[۱] Gateway

[۲] Bottleneck

۳- در برخی موارد به دلیل عدم سازگاری امکانات امنیتی دستگاه‌های مجزا، نمی‌توان از این امکانات در کنار یکدیگر برای امن‌سازی شبکه بهره جست. به عنوان مثال در صورتی که برای امن‌سازی برخی از سرویس‌ها در محیط اینترنت از سرویس IPSec VPN استفاده شود، دیواره آتش[۱] و سایر دستگاه‌ها امکان بررسی بسته‌های عبوری را نخواهند داشت. در صورتیکه اگر بتوان از دیواره آتش موجود در Gateway بعنوان کارگزار VPN نیز استفاده کرد، با رمزگشایی بسته‌های اطلاعاتی در دیواره‌آتش امکان بررسی این بسته‌ها نیز وجود خواهد داشت.



[۱] Firewall

۴- هزینه خرید سخت افزار و یا نرم‌افزار مجزا بازای هر سرویس مقرون به صرفه نیست.

۵- آشنایی مدیر شبکه با نحوه کارکرد تجهیزات متفاوت و بعضاً ناهماهنگ لازم است.

با توجه به موارد فوق، سامانه مدیریت تهدید یکپارچه یک انتخاب مناسب در راستای تأمین امنیت شبکه است. از جمله محاسن استفاده از این سامانه می‌توان به موارد ذیل اشاره کرد:

۱- مدیریت چندین کاربرد از یک محل و توسط یک ابزار

۲- ایجاد و پیاده‌سازی آسان و سریع خط‌مشی‌های سراسری سازگار

۳- ارائه گزارشات جامع و نظارت‌های برخط[۱] و تعاملی

۴- استفاده از تنها یک واسط مستقیم برای نصب و مدیریت تمامی ویژگی‌های امنیتی مشتمل بر سرویس‌های امنیتی پیچیده

۵- کاهش پیچیدگی و سادگی نصب

۶- عیب‌یابی آسان به دلیل وجود تنها یک ابزار واسط امنیتی

[۱] On line

برنامه مدیریت تهدید یکپارچه و عوامل استفاده از آن

فصل ۲

حالتهای کاری سامانه‌های مدیریت تهدید یکپارچه

UTM ها معمولاً در یکی از ۳ حالت زیر فعالیت می‌کنند:

حالت مسیریاب [۱]

در این حالت که Gateway یا Layer۳ نیز نامیده می شود، UTM علاوه بر اعمال سیاست‌های امنیتی بر روی بسته‌ها، برای عبور بسته‌ها و ارسال آنها به مقصد به صورت یک مسیریاب عمل نموده و با توجه به آدرس IP بسته‌ها، آنها را به مقصد ارسال می‌کند. UTM ها به‌صورت پیش‌فرض در این حالت کار می‌کنند.

حالت شفاف [۲]

در این حالت که Bridge یا Layer۲ نیز نامیده می‌شود، UTM در خصوص عبور بسته‌ها به صورت سوئیچ عمل می‌کند. بدین معنا که بسته‌های داده را با توجه به MAC Address آنها به مقصد هدایت می‌کند. در این حالت UTM از بیشتر

---

[۱] Route

[۲] Transparent

قابلیت‌های خود بهره می‌برد، با این تفاوت که سیاست‌های امنیتی، دیگر بر اساس آدرس‌های IP نوشته نمی‌شوند، بلکه بر اساس پورت‌های فیزیکی UTM نوشته می‌شوند. این حالت معمولاً زمانی به کار می‌رود که بخواهیم بدون تغییر در ساختار یک شبکه برای قسمتی از آن امنیت ایجاد کنیم.

حالت پراکسی[1]

این حالت بر روی همه پروتکل‌های شبکه قابل استفاده نیست و معمولاً در مورد پروتکل‌های مورد استفاده در بستر اینترنت مانند HTTP و FTP کاربرد دارد بنابراین از حالت پراکسی معمولاً برای تعریف دسترسی کاربران به اینترنت می‌توان استفاده کرد وقتی از UTM در این حالت استفاده می‌شود در واقع UTM به‌عنوان کارگزار پراکسی تعریف می‌گردد. در این حالت باید بر روی مرورگر وب کاربران آدرس و پورت مورد استفاده UTM برای سرویس پراکسی تنظیم گردد. در این حالت تمام ترافیک وب کاربران به UTM ارسال می‌شود، سپس UTM بسته‌های ارسالی کاربران را بررسی کرده و در صورت عدم وجود اشکال و یا خطر امنیتی در یک بسته، با اعمال تغییرات مورد نظر، بسته‌ای مشابه بسته موجود تولید کرده و در نهایت بسته تولید شده را با جایگزینی آدرس خود به جای آدرس کاربر به سوی مقصد ارسال می‌کند. پاسخ بسته‌ها نیز ابتدا به کارگزار پراکسی می‌رسد. کارگزار، بسته‌ها را بررسی و سپس بسته جدیدی مشابه بسته دریافت شده تولید کرده و به کاربر می‌فرستد. در این حالت می‌توان تغییرات زیادی بر روی بسته ارسالی توسط کاربر اعمال کرد.

[1] Proxy

فصل ۳

قابلیت‌های امنیتی سامانه‌های مدیریت تهدید یکپارچه

سامانه مدیریت تهدید یکپارچه یک دروازه امنیتی برای ارائه مکانیزم‌های مختلف امنیتی در شبکه‌های رایانه‌ای از مقیاس‌های کوچک تا خیلی بزرگ است. UTM بصورت یکپارچه سرویس‌های امنیتی بازرسی ترافیک، شبکه اختصاصی مجازی[۱]، تشخیص و جلوگیری از نفوذ[۲]، پالایش محتوای وب[۳] و مدیریت پهنای باند[۴] را به‌همراه واسط‌های مدیریتی ارائه می‌نماید. این سامانه همچنین با استفاده از مکانیزم‌های Failover قابلیت اطمینان بسیار بالا را در صورت قطع برق و خرابی سخت‌افزار تأمین می‌نماید. از جمله ویژگی‌های دیگر یک سامانه مدیریت تهدید

---

[۱] Virtual Private Network

[۲] Intrusion Detection/Prevention

[۳] Web Content Filtering

[۴] Bandwidth Management

یکپارچه کامل، پشتیبانی از ایجاد پروفایل‌های امنیتی است؛ این ویژگی انعطاف‌پذیری ویژه‌ای به مدیران شبکه در تعریف و پیاده‌سازی سیاست‌های امنیتی می‌دهد.

اجزای اصلی یک UTM شامل موارد ذیل می‌گردد:

دیواره آتش

دیواره‌آتش امکان برقراری امنیت در لایه‌های لینک داده[۱]، اینترنت[۲] و انتقال[۳] را فراهم می‌کند. دیواره آتش با بررسی آدرس های MAC و IP و شماره پورت‌های مبدأ و مقصد بسته عبوری و انطباق این موارد با قوانینی که مدیر شبکه مشخص کرده است، اجازه عبور یا عدم عبور بسته را صادر می‌کند. در واقع دیواره‌آتش وسیله‌ای است که کنترل دسترسی به یک شبکه را بنابر سیاست امنیتی شبکه تعریف و اعمال می‌کند. از جمله ویژگی‌های یک دیواره آتش نسل امروز می توان به موارد ذیل اشاره کرد:

۱. بازرسی حالت‌مند ترافیک
۲. پشتیبانی از NAT/PAT/MAT
۳. تعریف سیاست‌ها، مبتنی بر نواحی امنیتی و زمان
۴. پنهان‌سازی توپولوژی شبکه داخلی
۵. پیاده‌سازی کامل و امن DMZ
۶. تعریف نواحی امنیتی و لایه‌بندی شبکه

---

[۱] Data Link

[۲] Internet

[۳] Transport

ضد بدافزار[1]

سرویس ضد بدافزار موجود در UTM با بررسی محتوای بسته‌های عبوری از UTM، در صورت وجود ویروس در بسته مورد نظر، اجازه عبور بسته را نمی‌دهد. ضد بدافزار با جلوگیری از ورود ویروس‌ها از اینترنت و شبکه‌های دیگر به شبکه داخلی، به میزان زیادی از آلودگی شبکه داخلی در برابر ویروس‌ها محافظت می‌کند. وجود ضدبدافزار به برقراری امنیت در لایه کاربرد کمک می‌کند. ضدبدافزارهای مسیر دروازه به جای جستجوی فایل‌ها، بسته عبوری را جستجو می‌کنند.

در برخی از UTMها با تشخیص ویروس علاوه بر جلوگیری از عبور بسته، ممکن است اقدامات دیگری از قبیل مسدود کردن ارتباط فرستنده ویروس با شبکه داخلی و ... نیز انجام گیرد.

یکی از معیارهای تشخیص قدرت ضدبدافزار مورد استفاده در دروازه، تعداد پروتکل‌های تحت پوشش ضدبدافزار است. بهتر است ضدبدافزار ویروس‌یابی پروتکل‌های HTTP, FTP, SMTP, POP۳ IMAP, IM VPN را پشتیبانی کند. وجود امکان مستثنی‌سازی آدرس IP یا ویروس یکی دیگر از معیارهای قدرت ویروس‌یاب UTM می‌باشد. معیار دیگر، وجود امکانات جانبی ضدبدافزار در تشخیص ویروس‌ها است. به عنوان مثال سرویس ضدبدافزار برخی UTMها امکان جلوگیری از عبور بسته‌هایی با سایز و یا حجم غیراستاندارد، یا جلوگیری از عبور فایل‌هایی با پسوند خاص و ... را نیز دارد. از معیارهای مهم دیگر امکان فعال یا

[1] Anti Virus

غیرفعال کردن ضدبدافزار بر اساس هر سیاست امنیتی[1] است. در برخی از UTMها این امکان فراهم نمی‌باشد و تنها می‌توان به طور کلی ضدبدافزار را برای بررسی ترافیک عبوری از یک یا چندواسط شبکه یا یک ناحیه[2] خاص UTM فعال یا غیرفعال نمود. همچنین برخی از UTMها از دو موتور جستجوی ویروس در ساختار خود بهره می‌برند که می‌توان همزمان هردو و یا یکی از آن‌ها را فعال نمود. استفاده از دو موتور جستجو به طور حتم موجب کاهش احتمال عدم تشخیص ویروس خواهد شد.

شبکه اختصاصی مجازی

VPN شبکه‌ای از مدارهای مجازی برای پیاده‌سازی شبکه خصوصی یک شرکت یا سازمان روی یک شبکه عمومی مانند اینترنت است. شبکه اختصاصی مجازی دو رایانه یا دو شبکه را به کمک یک شبکه دیگر -که به عنوان مسیر انتقال به کار می‌رود- به هم متصل می‌کند. VPN از نگاه کاربر همانند یک شبکه محلی به نظر می‌رسد. برای پیاده‌سازی چنین ارتباطی، VPN با استفاده از رمزگذاری روی داده‌ها برای هر کاربر یک ارتباط مجازی ایجاد می‌کند. تنها کسی که آدرس‌های لازم و رمز عبور را در اختیار داشته باشد می‌تواند به این شبکه وارد شود .

معمولاً ارتباطات VPN براساس یکی از انواع PPTP، L۲TP و IPSec برقرار می‌گردد. IPSec VPN امن‌ترین نوع VPN است و در عین حال بیشترین بار رمزگذاری و رمزگشایی و برپایی ارتباط VPN را بر پردازنده تحمیل می‌کند. معمولاً UTM ها از هر سه نوع VPN پشتیبانی می‌کنند. پشتیبانی از الگوریتم‌های رمز بومی در برقراری ارتباطات VPN از جمله ویژگی هایی است که باید در تولید محصول بومی مد نظر قرار گیرد.

[1] Policy

[2] Zone

تشخیص و جلوگیری از نفوذ

تشخیص و جلو گیری از نفوذ برای محافظت شبکه در برابر بهره‌برداری نفوذگران از ضعف‌های امنیتی سیستم‌ها و نفوذ به شبکه، مورد استفاده قرار می‌گیرد. این امکان، امنیت را در لایه‌های ۵ و ۶ و ۷ شبکه فراهم می‌سازد. بعنوان مثال اگر در شبکه، یک کارگزار وب با آدرس ۱۹۲.۱۶۸.۱۱.۲ وجود داشته باشد، دیواره‌آتش اجازه دسترسی به پورت ۸۰ برای آدرس مذکور را به کاربران می‌دهد. اگر تنظیمات امنیتی کارگزار وب ضعیف باشد، نفوذگران از طریق سرویس HTTP (پورت ۸۰)، کارگزار را مورد حمله قرار می‌دهند، در صورت وجود IDP[۱] امکان جلوگیری از این حملات از طریق UTM وجود خواهد داشت. UTMهای مختلف تعداد نفوذ[۲]های متفاوتی را شناسایی می‌کنند و برای تشخیص موارد نفوذ جدید، باید الگوهای IDP[۳] بروزرسانی شوند.

وجود امکانات زیر برای سرویس IDP در UTM ضروری به نظر می‌رسد:

۱. امکان بروزرسانی

۲. قابلیت تنظیم آستانه‌های تشخیص

[۱] معمولاً از سیستمی که تنها امکان تشخیص و گزارش نفوذ را داشته باشد به عنوان IDS یاد می شود و به سیستمی که علاوه بر تشخیص و گزارش، امکان پیشگیری از نفوذ را دارد IPS یا IDP گفته می شود.

[۲] Intrusion

[۳] IDP Signature

۳. تعریف سیاست‌های مختلف حفاظت از حملات نظیر مستثنی کردن برخی الگوها و عدم اعمال آن‌ها بر روی ترافیک عبوری، انتخاب الگوهایی خاص از بین الگوها بر اساس مواردی چون نوع سیستم‌عامل مقصد، نوع سرویس مقصد، کلاینت یا سرور بودن مقصد و یا اعمال الگوهای انتخابی بر روی هریک از سیاست‌های دلخواه

۴. پشتیبانی از الگوهای بومی و جدید کاربر

۵. کمینه کردن میزان خطاهای مثبت‌غلط[۱]

۶. جلوگیری از حملات به‌صورت بلادرنگ

۷. اعمال سیاست‌های امنیتی سازمان برای تشخیص نفوذ

۸. هشداردهی به روش‌های مختلف در صورت کشف نفوذ

مدیریت و پالایش محتوای وب

این ابزار به منظور تصفیه اتصالات وب استفاده می‌شود. در کشورهای مختلف، فیلترینگ براساس دسته بندی‌های از پیش تعریف شده و یا براساس تعاریف شخصی، به دو روش ذیل انجام می‌شود:

۱. فیلتر کردن نشانی‌های اینترنتی براساس:

- آدرس URL
- آدرس دامنه
- عبارت موجود در URL

[۱] False Positive

۲. فیلتر کردن براساس محتوای هر صفحه اینترنتی که این روش در دنیا به فیلتر محتوا[۱] معروف است.

کنترل برنامه های کاربردی

یکی از راه‌های ورود ویروس و نفوذ هکرها به شبکه، اجرای برنامه‌های کاربردی تحت وب نظیر نرم افزارهای Instant Messaging و برنامه های P۲P در محیط شبکه است.

برنامه‌های P۲P نظیر emule، Kaza و Bittorent برنامه‌هایی هستند که کاربران از طریق آن‌ها داده‌ها و برنامه‌های خود را با افراد دیگر در محیط اینترنت به اشتراک می گذارند. این برنامه‌ها علاوه بر این‌که ممکن است باعث به خطر افتادن امنیت داده‌های یک سازمان گردند، میزان زیادی از پهنای باند اینترنت سازمان را اشغال می کنند.

معمولاً نمی‌توان از طریق مسدودسازی پورت‌ها در دیواره‌آتش، جلوی ارتباط برنامه‌های IM و P۲P با کارگزارهایشان در اینترنت را گرفت. بلکه باید با استفاده از شناسه هر برنامه، از ارتباط آن کارگزار اینترنتی جلوگیری کرد.

ضد هرزنامه[۲]

هرزنامه اصطلاحاً به ایمیل‌هایی گفته می‌شود که به طور ناخواسته به صندوق پستی کاربران فرستاده می شوند و معمولاً جنبه تبلیغاتی دارند.

ضدهرزنامه امکانی است که از طریق آن بسته‌های حاوی پست‌های الکترونیکی عبوری از دروازه – که بطور معمول با یکی از پروتکلهای SMTP،

---

[۱] Content Filter

[۲] Anti Spam

POP۳ یا IMAP منتقل می شود- برای جلوگیری از ورود هرزنامه به شبکه داخلی جستجو می شوند.

UTMها با استفاده از روش‌های ذیل هرزنامه‌ها را شناسایی می‌کنند:

۱. استفاده از لیست سیاه[۱]: لیست سیاه شامل اطلاعاتی از هرزنامه است. این اطلاعات شامل آدرس پست الکترونیک فرستنده‌های هرزنامه، دامنه‌هایی[۲] که معمولاً از آنها هرزنامه ارسال می‌شود و عباراتی که بطور منحصر به فرد در محتوا[۳] و عنوان[۴] هرزنامه وجود دارند، می شود. لیست سیاه معمولاً بر دو نوع از پیش تعریف شده[۵] و شخصی وجود دارد. لیست سیاه از پیش تعریف شده معمولاً از طریق شرکت سازنده UTM بصورت دوره ای بروزرسانی می‌گردد. لیست سیاه شخصی توسط مدیر امنیت شبکه ایجاد می‌گردد.

۲. استفاده از لیست سفید[۶]: شامل اطلاعاتی از دامنه‌ها یا آدرس‌های پست الکترونیکی است که ما به آنها اطمینان داریم و بسته‌های عبوری از آنها نباید جستجو گردند. معمولاً دامنه‌های مورد استفاده در داخل سازمان از این نوع هستند.

---

[۱] Black List

[۲] Domain

[۳] Content

[۴] Subject

[۵] Predefiened

[۶] White List

۳. استفاده از روش RDNS[۱]: در بیشتر هرزنامه‌ها آدرس پست‌الکترونیکی فرستنده هرزنامه یک آدرس جعلی[۲] است. UTM با استفاده از اطلاعات موجود در سایت مرجع RIPE می‌تواند این عدم همخوانی را تشخیص دهد.

۴. استفاده از روش علامتگذاری بر روی نامه‌های الکترونیکی ارسالی: برخی از هرزنامه‌ها خود را بعنوان پیغام‌های خطا[۳] - که در حالت عادی توسط کارگزارهای پست الکترونیکی در صورت وجود خطا در ارسال و دریافت نامه های الکترونیک تولید می‌گردد- نشان می‌دهند. UTM برای تشخیص این هرزنامه‌ها و همچنین هرزنامه‌های الکترونیکی که از نوع پاسخ[۴] باشد، بر روی نامه‌های ارسالی خود علامتگذاری می‌کند و در صورتیکه در پاسخ دریافتی، آن علامت موجود نباشد بسته به عنوان هرزنامه تشخیص داده می‌شود.

رفتار UTM در قبال هرزنامه ها با توجه به تنظیمات انجام شده توسط مدیر شبکه به دو صورت است:

۱. جلوی دریافت هرزنامه را می گیرد.

۲. به هرزنامه برچسب می زند تا کاربر نهایی خود در مورد آن تصمیم‌گیری نماید.

---

[۱] Reverse DNS

[۲] Spoof

[۳] Failure

[۴] Reply

AAA

این سرویس امکان احراز هویت کاربران[۱]، کنترل میزان دسترسی کاربران به منابع شبکه[۲] و کنترل زمان دسترسی کاربر[۳] را فراهم می‌کند. یک UTM با توجه به تنظیماتی که مدیر شبکه بر روی آن انجام می‌دهد، می‌تواند خود به عنوان کارگزار AAA تنظیم گردد و یا از یک کارگزار AAA بیرونی استفاده کند.

در حالتیکه UTM از یک کارگزار AAA بیرونی استفاده می‌کند ارتباط با کارگزار خارجی از طریق یکی از پروتکل‌های LDAP، Tacacs+، RADIUS، Kerberous و ... برقرار می‌گردد. در این حالت امکانات AAA محدود به امکاناتی است که کارگزار AAA بیرونی در اختیار UTM قرار می‌دهد.

گزارش دهی[۴]، رویدادنگاری[۵] و نظارت[۶]

[۱] Authentication

[۲] Authorization

[۳] Accounting

[۴] Repoerting

[۵] Loging

[۶] Monitoring

نظارت یکی از مهمترین بخش‌های هر سامانه است، چرا که اتفاقات زیادی در یک سیستم فعال ممکن است رخ دهد، که می‌تواند، برای عملکرد آن خطرآفرین باشد. یکی از مزایای برجستهٔ یک سامانه این است که امکان نظارت و بازرسی داشته باشد. نظارت می‌تواند، بر روی اجزا و مؤلفه‌های بحرانی و مهم اجرا شود و به روش‌های متفاوتی انجام گیرد. در یک فایروال نظارت، تقریبا بر روی تمام بخش‌های مهم و اساسی از جمله منابع سیستمی که شامل CPU، Memory و Disk می‌باشد، یا برروی واسط‌های شبکه و یا ... می بایست وجود داشته باشد.

برای نظارت بر نحوه استفاده کاربران داخلی و خارجی از سرویس‌های شبکه نظیر اینترنت، برنامه‌های کاربردی و ... وجود امکانات گزارش‌دهی در این دستگاه‌ها ضروری می‌باشد. همچنین این دستگاه‌ها باید امکان ارائه Log از وضعیت کاری قسمت‌های مختلف خود را داشته باشند. بهتر است دستگاه قابلیت تهیه گزارش هم به صورت نمودار و هم به صورت متنی را داشته باشد. ارائه گزارش ترافیک جاری[1] در بسیاری از موارد سودمند خواهد بود.

[1] Live Report

فصل ۴

سایر امکانات سامانه‌های مدیریت تهدید یکپارچه

از آنجا که محل قرارگیری سامانه‌های مدیریت تهدید یکپارچه معمولاً در دروازه شبکه می‌باشد لازم است این سامانه‌ها علاوه بر فراهم کردن امکانات امنیتی، امکانات دیگری را که یک دستگاه موجود در دروازه شبکه با آن‌ها نیاز دارد فراهم کنند. در ذیل به بررسی این امکانات می‌پردازیم.

مدیریت پهنای باند

به منظور تقسیم بهینه پهنای باند اینترنتی بین گروه‌های مختلف کاربران براساس نیاز کاری آنها، می‌توان از این امکان سود برد. همچنین از این امکان می‌توان برای تقسیم پهنای باند خطوط ارتباطی شبکه گسترده[۱] بین نقاط مختلف استفاده کرد.

[۱] Wide Area Network

مسیریابی و پشتیبانی از NAT[1]

از آن‌جا که دستگاه‌های تأمین‌کننده امنیت در Gateway وظیفه برقراری ارتباط شبکه داخلی با اینترنت، شبکه‌های دیگر درون سازمان و شبکه سازمان‌ها و شرکت‌های همکار را نیز بر عهده دارند، بنابراین باید امکان مسیریابی ایستا[2] و پویا[3] و همچنین انواع NAT در UTM وجود داشته باشد.

Multi Link Management

هنگامیکه در یک سازمان دو یا چند لینک ارتباطی با اینترنت موجود باشد وجود امکان توازن بار[4] بین این خطوط، تشخیص قطع بودن خط، تغییر بار خط برمبنای میزان پایداری آن و همچنین تقسیم ترافیک کاربران بر روی خطوط بسیار اهمیت می یابد.

وجود امکان HA[5]

High Availability به امکانی اطلاق می شود که طی آن در صورت بروز اشکال در سرویس دهی دستگاه اصلی در شبکه، یک سامانه کاملاً مشابه دستگاه اصلی و با تنظیمات یکسان، به صورت خودکار وظایف را بعهده می گیرد. High Availability بر دونوع فعال-فعال[6] و فعال-غیرفعال[1] می‌باشد. در نوع فعال-فعال

[1] Network Address Translation

[2] Static

[3] Dynamic

[4] Load Balancing

[5] High Availability

[6] Active-Active

در شرایط عادی هر دو دستگاه اصلی و فرعی به صورت فعال در شبکه کار می‌کنند و ترافیک شبکه بین آنها تقسیم می‌گردد. در نوع فعال-غیرفعال، ترافیک شبکه تنها از دستگاه اصلی عبور می‌کند و در صورت بروز اشکال تمامی ترافیک از دستگاه فرعی عبور داده می‌شود. این امکان به برقراری پایداری در شبکه کمک می‌کند.

وجود امکان توازن یا اشتراک بار[۲]

این امکان، مکمل امکان HA می‌باشد. در صورتی که دستگاه در حالت فعال-فعال تنظیم گردد، با استفاده از توازن بار این امکان فراهم می‌گردد که دستگاه فرعی نیز در پردازش و عبور ترافیک نقش ایفا کند. همچنین می توان نسبت باری را که می بایست توسط هر دستگاه پردازش گردد مشخص کرد.

وجود امکان سیستم مجازی[۳] یا دامنه مجازی[۴]

با استفاده از این امکان، می توان UTM را به صورت مجازی به چند UTM مجزا از هم تبدیل کرد. این امکان مشابه امکان شبکه محلی مجازی[۵] در سوئیچ ها است. امکان VDOM یا VSYS تنها بر روی UTMهای مبتنی بر معماری ASIC[۶] موجود است و کاربردهای فراوانی دارد. بعنوان مثال می‌توان از این مشخصه برای

---

۱ Active-Passive

۲ Load Sharing

۳ Virtual System(VSYS)

۴ Virtual Domain(VDOM)

۵ Virtual LAN(VLAN)

۶ Application Specific Integrated Circuit

جداسازی ترافیک منتهی به کارگزارهای سازمان‌های مختلف در مراکز داده[1] استفاده کرد.

Web Caching

به منظور افزایش سرعت دسترسی کاربران به اطلاعات شبکه اینترنت، می‌توان داده‌هایی را که کاربران به آنها مراجعه بیشتری دارند، در دستگاه UTM ذخیره‌سازی کرد. با این کار، کاربران در زمان‌های بعدی در صورت نیاز به این اطلاعات، به جای اینترنت آن‌ها را از دستگاه UTM دریافت می‌کنند. ممکن است اطلاعات بر روی دیسک سخت[2] یا فلش ذخیره و بازیابی گردد. سرعت ذخیره و بازیابی در فلش بیش از دیسک سخت است. بیشتر UTMها از امکان Caching برخوردار نیستند.

سرویس‌های عمومی

از UTMها می‌توان بعنوان کارگزار DHCP، DNS و WINS استفاده کرد.

[1] Data Centers

[2] Hard disk

فصل ۵

مشخصه‌های متمایز کننده سامانه های مدیریت تهدید یکپارچه

یکی از دغدغه‌های مدیران امنیت شبکه انتخاب یک سامانه مدیریت تهدید یکپارچه مناسب برای شبکه تحت مدیریت خود است. در زیر به بررسی برخی از ویژگی‌هایی که باعث ایجاد تمایز بین سامانه‌های مدیریت تهدید یکپارچه هنگام استفاده در شرایط متفاوت می شوند، می‌پردازیم.

نحوه ارائه امکانات

از آنجا که نحوه و کیفیت ارائه امکانات در UTMهای مختلف متفاوت است، بهتر است قبل از خرید سامانه مدیریت تهدید یکپارچه نسبت به نصب آزمایشی و بررسی امکانات آن اقدام گردد. بعنوان مثال ممکن است تعداد شناسه‌های ضدبدافزار یک UTM بسیار کمتر از UTM دیگر باشد، همچنین ممکن است فعال کردن یکی از سرویس‌های امنیتی UTM، تاخیر زیادی در پردازش بسته‌ها توسط UTM ایجاد کند و یا سرویس کنترل برنامه‌های کاربردی در یک UTM امکان انتخاب و جلوگیری از اجرای برنامه‌های بیشتری را نسبت به UTM دیگر

داشته باشد. تنها راه پی بردن به این تفاوت‌ها، آزمایش و بررسی عملی UTM است.

میزان گذردهی[1] و کارایی[2]

تولیدکنندگان UTM، معمولاً دستگاه‌های خود را در مدل‌های مختلف برای شبکه با ترافیک متفاوت عرضه می‌کنند. برای هر یک از مدل‌ها میزان کارایی سرویس‌های مختلف (بعنوان مثال دیواره آتش، ضدبدافزار، IPS و...) براساس مقادیر Mbps یا Gbps عنوان می‌گردد. ضروری است در هنگام انتخاب مدل UTM، ترافیک شبکه براساس این مقادیر ارزیابی گردد و با در نظر گرفتن گسترش‌های آینده اقدام به خرید UTM کرد. همچنین در برخی موارد ممکن است مقادیر اعلام شده توسط شرکت سازنده با واقعیت تطابق نداشته باشد بنابراین ضروری است قبل از خرید دستگاه، اقدام به تست عملی آن دستگاه در شبکه مقصد گردد.

نوع پردازش بسته‌ها

برخی از UTMها به‌صورت نرم‌افزاری و برخی دیگر به‌صورت سخت‌افزاری بسته‌ها را پردازش می‌کنند. UTMهایی که بسته‌ها را به‌صورت سخت‌افزاری پردازش می‌کنند میزان گذردهی و کارایی بهتری دارند و در ضمن قیمت آن‌ها بالاتر از نمونه‌هایی با پردازشگر نرم‌افزاری است. استفاده از این نوع UTMها نسبت به مدل‌هایی با پردازش نرم‌افزاری ارجحیت دارد.

---

[1] Throughput

[2] Performance

نوع سیستم عامل مورد استفاده در UTM

توصیه می‌گردد UTMای برای استفاده انتخاب گردد که سیستم‌عامل مخصوص به خود را داشته باشد. زیرا در این حالت، امکان حدس زدن نقاط ضعف امنیتی سیستم‌عامل آن توسط نفوذگران وجود نخواهد داشت.

وجود مستندات کامل، پشتیبانی مناسب و امکان بروزرسانی

لازم است تا سازنده برای کار با دستگاه، مستندات کاملی فراهم کرده باشد. در این صورت استفاده از امکانات دستگاه راحت‌تر خواهد شد.

از آنجا که دستگاه UTM معمولاً در گلوگاه شبکه قرار می گیرد، اگر شرکت سازنده از تیم پشتیبانی قوی و سریعی برخوردار نباشد، ممکن است در صورت بروز اشکال برای دستگاه باعث از کار افتادن و قطع سرویس‌های موجود در شبکه گردد. بنابراین می‌بایست دستگاه UTM از پشتیبانی مناسبی برخوردار باشد.

همچنین بهتر است دستگاهی جهت نصب در شبکه انتخاب گردد که احتمال بسیار ضعیفی در اختلال بروزرسانی پایگاه داده ضد بدافزار، IPS ، سامانه پالایش وب و ... آن وجود داشته باشد.

بومی بودن محصول

از زمانیکه برخی از نگرانی‌ها در خصوص تعرض به حریم خصوصی افراد و سازمان‌ها و قطع سرویس‌های ضروری ظاهر گردید، متخصصان فناوری اطلاعات جهت مقابله با این تهدیدات و تأمین پایداری خدمات تحت شبکه بنگاه‌ها، افراد و دستگاه‌های مختلف تلاش‌های ارزشمندی را ساماندهی نمودند تا فضای اعتماد به تبادلات الکترونیکی دچار آسیب کمتری شود. در همین راستا تولید محصولات

مختلف امنیتی اعم از تجهیزات سخت‌افزاری و نرم‌افزاری در حوزه‌های گوناگون، ارائه راهکارها و تدوین سیاست‌های خرد و کلان جهت صیانت از امنیت و پایداری فضای تبادل اطلاعات، تربیت نیروهای متخصص 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 کرده است.

نخستین قدم در مسیر تحقق امنیت و پایداری در فضای تبادل اطلاعات کشور، تأمین و تولید خدمات و محصولات امنیتی مورد نیاز بصورت بومی و با استفاده از دانش پایه این فناوری بمنظور کاهش و قطع وابستگی به محصولات امنیتی دیگر کشورها است. در این راستا لازم است به طور جد نسبت به بومی سازی، افزایش توان داخلی و استفاده از این محصولات در محیط شبکه ملی اقدام شود. از اینرو با توجه به شرایط بین المللی از یک سو و همچنین تحریم‌های مطرح، بومی بودن سامانه‌ها و اتکا به توان داخلی از مهمترین شاخصه‌های انتخاب در این حوزه است. از طریق استفاده از سامانه‌های بومی از طرفی از انتقال اطلاعات داخل سازمانی و بعضاً دارای طبقه‌بندی به خارج از کشور توسط دستگاه‌های تولید بیگانگان تا حد زیادی جلوگیری بعمل می‌آید و از سمت دیگر محدودیت‌های پشتیبانی و ارائه خدمات با جایگزینی توان داخلی مرتفع می‌گردد.