



مجموعه شرکت های مهندسی دانش بنیان رها

مانیتورینگ ترافیک شبکه؛ راه حلی قدرتمند برای کنترل ترافیک شبکه

شرکت رهاکو



فهرست

- 3 مانیتورینگ ترافیک شبکه چیست؟
- 3 چرا باید ترافیک شبکه را مانیتور کنید؟
- انواع ترافیک شبکه 4
- 4 ابزارهای موجود برای مانیتورینگ ترافیک شبکه
- 5 نحوه اجرای مانیتورینگ ترافیک شبکه در سازمان ها
- نتیجه گیری 5



هیچ کسب و کاری نمی تواند اهمیت مانیتورینگ شبکه را نادیده بگیرد. تا سال 2021، 4.66 میلیارد کاربر فعال اینترنت در سراسر جهان وجود داشت و انتظار می رود با افزایش دسترسی افراد به اینترنت در سال های آینده ترافیک شبکه نیز بیشتر شود. با مانیتورینگ ترافیک شبکه می توانید مطمئن شوید که سیستم های شما به خوبی کار می کنند و مشکلات را قبل از وقوع فاجعه شناسایی کنید. در این مقاله انواع ترافیک شبکه و ابزارهای موجود برای مانیتورینگ را با هم بررسی می کنیم.

مانیتورینگ ترافیک شبکه چیست؟

به فرآیند جمع آوری، تجزیه و تحلیل و گزارش داده های ترافیک شبکه به منظور عیب یابی، بهینه سازی عملکرد و به طور کلی درک فعالیت شبکه مانیتورینگ گفته می شود. نظارت بر ترافیک شبکه یک بخش جدانشدنی در فرآیند مدیریت شبکه است و به جلوگیری از بروز مشکلات کمک می کند. به عنوان مثال، در فوریه 2020 آمازون با استفاده از سرویس مانیتورینگ AWS Shield از یک حمله شدید DDOS جلوگیری کرد. سازمان ها برای تحلیل ترافیک شبکه باید نیازهای خاص خود را در نظر بگیرند. چرا که برخی از راهکارها ممکن است برای شبکه های بزرگ تر مناسب باشند، در حالی که برخی دیگر برای شبکه های کوچک تر کاربرد دارند.

چرا باید ترافیک شبکه را مانیتور کنید؟

همانطور که می گویند "بهترین حمله دفاع است." همین امر در مورد امنیت شبکه نیز کاربرد دارد. با نظارت بر ترافیک شبکه می توانید تهدیدات بالقوه را شناسایی کرده و اقداماتی را برای از بین بردن آن ها قبل از ایجاد هرگونه آسیب انجام دهید. دلایل زیادی وجود دارد که چرا باید بر شبکه خود نظارت داشته باشید و در اینجا به چند مورد اشاره می کنیم.

عیب یابی مشکلات شبکه: وقتی مشکلی در شبکه پیش می آید، مانیتورینگ ترافیک شبکه به شما کمک می کند منبع مشکل را مشخص نمایید تا هرچه سریع تر آن را برطرف کنید. اخیرا سیکو دو ابزار مانیتورینگ جدید معرفی کرده است تا در مدیریت چالش های روزانه در محیط شبکه به تیم فناوری اطلاعات کمک کند.

انطباق با الزامات نظارتی: راهکارهای مانیتورینگ اقداماتی را برای بهبود مشکلات ناشی از عدم نظارت ارائه می دهند. در همین راستا الگوهای نظارتی IBM چندین سیاست امنیتی ارائه می دهند.

محافظت در برابر بدافزارها و سایر تهدیدات: با نظارت بر ترافیک می توانید فعالیت های غیرعادی را شناسایی کنید. این فعالیت ها ممکن است نشان دهنده نفوذ بدافزار یا سایر تهدیدات امنیتی باشند. FBI اعلام کرد که شکایات باج افزار از سال 2019 تا 2021 حدودا 82 درصد افزایش یافته است.

مدیران فناوری اطلاعات باید به طور فعال سیستم ها را نظارت کنند و از مشکلات احتمالی جلوگیری نمایند. یک ابزار نظارتی مفید ویژگی های زیر را ارائه می دهد:



- نظارت فوری بر شبکه
- توانایی تشخیص قطعی در کمترین زمان ممکن
- استفاده از یک مکانیزم برای ارسال هشدار

انواع ترافیک شبکه

انواع ترافیک شبکه را می توان بر اساس داده های در حال انتقال طبقه بندی کرد: صدا، ویدئو یا داده. ترافیک صوتی از PSTN استفاده کرده و مکالمات صوتی دیجیتالی را منتقل می کند. رایج ترین نوع ترافیک صوتی تماس های تلفنی معمولی است و البته که VoIP و سایر خدمات صوتی دیجیتال نیز در این دسته بندی جای می گیرند.

ترافیک ویدیویی از اینترنت برای حمل سیگنال های دیجیتال استفاده می کند و شامل پخش ویدئو و سایر خدمات ویدیویی است. طبق گفته سیسکو، تا سال 2022 ترافیک ویدیویی 82 درصد از کل ترافیک اینترنت را تشکیل می دهد. ترافیک داده نوعی ترافیک شبکه است که از اینترنت برای انتقال تمام داده های غیر صوتی استفاده می کند. ترافیک داده شامل ایمیل، مرور وب، انتقال فایل و انواع دیگر تبادل داده می باشد.

ابزارهای موجود برای مانیتورینگ ترافیک شبکه

در این بخش لیستی از بهترین ابزارها برای نظارت بر ترافیک شبکه ارائه می دهیم. مزایای این ابزارها چیزی بیش از نظارت بر شبکه است. به عنوان مثال، درجات مختلفی مانیتورینگ عملکرد سیستم، وب و برنامه را نیز انجام می دهند. ابزارها بدون ترتیب خاصی فهرست شده اند.

OpManager

OpManager یک نرم افزار مانیتورینگ با امکانات کامل می باشد. این ابزار دارای پشتیبانی قوی برای نظارت و مجموعه ای از ابزارهای عیب یابی است و هشدارها را از طریق ایمیل یا پیامک ارسال می کند. برخی از ویژگی های کلیدی OpManager به شرح زیر است:

- مدیریت رویدادها در کنسول برای شناسایی الگوها
- رابط مدیریتی قابل تنظیم
- تشکیل نمودار برای ارائه آمارهایی مانند پهنای باند در پورت های شبکه

زبیکس

Zabbix یک پلتفرم مانیتورینگ منبع باز است. این ابزار دارای مجموعه کاملی از قابلیت های مانیتورینگ ترافیک شبکه می باشد. زبیکس به راحتی قابل دانلود و نصب است و مجموعه گسترده ای از قالب های plug-and-play را برای سخت افزار شبکه ارائه می دهد. از ویژگی های اصلی Zabbix می توان به موارد زیر اشاره کرد:



- اسکن فعال و غیرفعال سخت افزار و سرورهای شبکه
- تشخیص دستگاه های جدید و تغییرات پیکربندی
- ابزارهایی برای ساخت نمودار بر اساس داده های در دسترس
- ادغام کامل SNMP با الگوهای تجهیزات شبکه

PRTG

برنامه PRTG روی سرور ویندوز اجرا می شود و روی هر مرورگری قابل مشاهده است. علاوه بر این، می توان آن را در برنامه های اندروید و IOS نیز اجرا کرد. مانیتورینگ شبکه با PRTG ویژگی های زیر را ارائه می دهد:

- نظارت بر ترافیک شبکه
- گزارش دهی
- نقشه شبکه قابل تنظیم
- مدیریت و نظارت SNMP

نحوه اجرای مانیتورینگ ترافیک شبکه در سازمان ها

بیشتر مشاغل کوچک و بزرگ از نوعی نظارت بر ترافیک شبکه استفاده می کنند. این اقدام اغلب برای بهبود خدمات مشتری یا رفع مشکلات احتمالی شبکه قبل از ایجاد هرگونه اختلالات قابل توجه صورت می پذیرد. همچنین نظارت بر ترافیک به شما کمک می کند تا ببینید کارکنان چگونه از اینترنت استفاده می کنند.

چند راه مختلف برای پیاده سازی نظارت بر ترافیک در سازمان ها وجود دارد. رایج ترین روش استفاده از راهکارهای مبتنی بر سخت افزار مانند روتر با قابلیت های نظارت داخلی است. از طرف دیگر، راهکارهای مبتنی بر نرم افزار روی سرور یا رایانه های اختصاصی قابل اجرا هستند. هنگامی که ابزار مناسب را در اختیار داشته باشید، نظارت بر ترافیک شبکه بسیار آسان خواهد شد. در بیشتر موارد برای کنترل بهینه ترافیک شبکه باید روتر یا نرم افزار خود را برای ثبت تمام ترافیک های ورودی و خروجی تنظیم کنید. بسته به نیاز می توان این اطلاعات را به روش های مختلف روی نمودار مشاهده کرد.

نتیجه گیری

مانیتورینگ از خرابی شبکه جلوگیری می کند و مزایای بی شماری را به دنبال دارد. با نظارت بر آنچه در شبکه شما می گذرد، شانس شناسایی و رفع مشکلات را در کمترین زمان ممکن خواهید داشت. مانیتورینگ ترافیک شبکه برای همه سازمان ها و مشاغل امری حیاتی می باشد. با درک روش های مختلف نظارت بر ترافیک و استفاده از بهترین ابزارهای موجود، سازمان ها اطمینان حاصل خواهند کرد که شبکه هایشان به خوبی کار می کند.

انتخاب ابزار مناسب برای مانیتورینگ ترافیک شبکه به بررسی های اساسی نیاز دارد. ابزارهای خوب زیادی در این حوزه وجود دارند که هر کدام از آن ها نقاط قوت و ضعف خود را ارائه می دهند. خبر خوب این است که این نرم افزارها دارای نسخه آزمایشی رایگان هستند. ابزاری را پیدا کنید که به بهترین وجه با نیازهای سازمانی شما مطابقت دارد.



مجموعه شرکت های مهندسی دانش بنیان رها