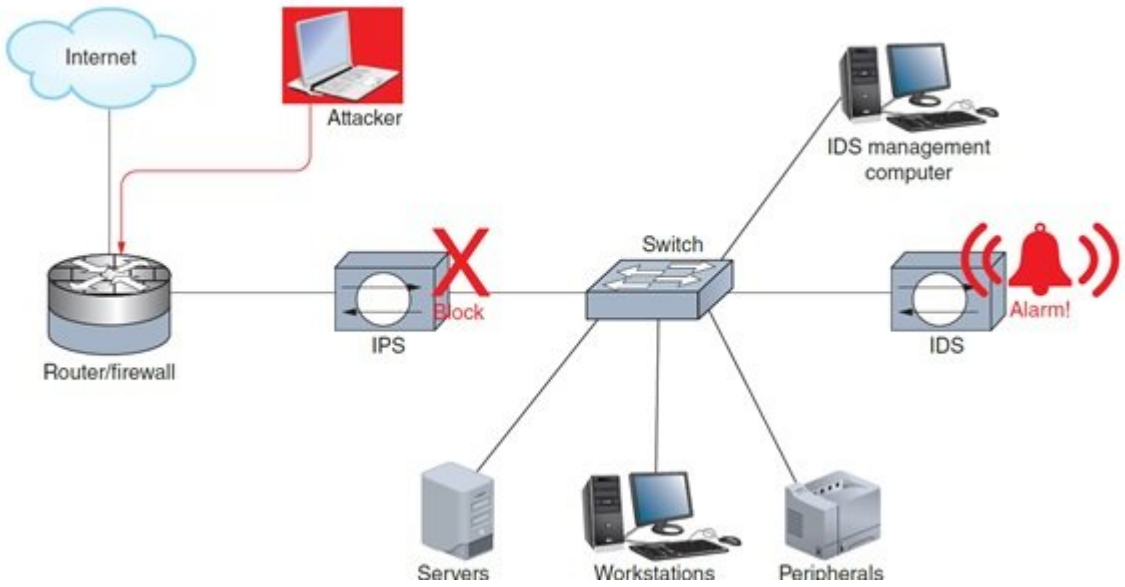
آموزش رایگان دوره نتورک‌پلاس (بخش 56)

در شماره گذشته آموزش نتورک‌پلاس با دیوارهای آتش، سامانه‌های تشخیص نفوذ، مدیریت یکپارچه تهدیدات، دیوارهای آتش نسل بعد و سامانه‌های تشخیص نفوذ آشنا شدیم. در این شماره مبحث فوق را ادامه خواهیم داد.

برای مطالعه بخش پنجاه و پنجم آموزش رایگان و جامع نتورک پلاس (Network+) اینجا کلیک کنید

Intrusion Prevention System

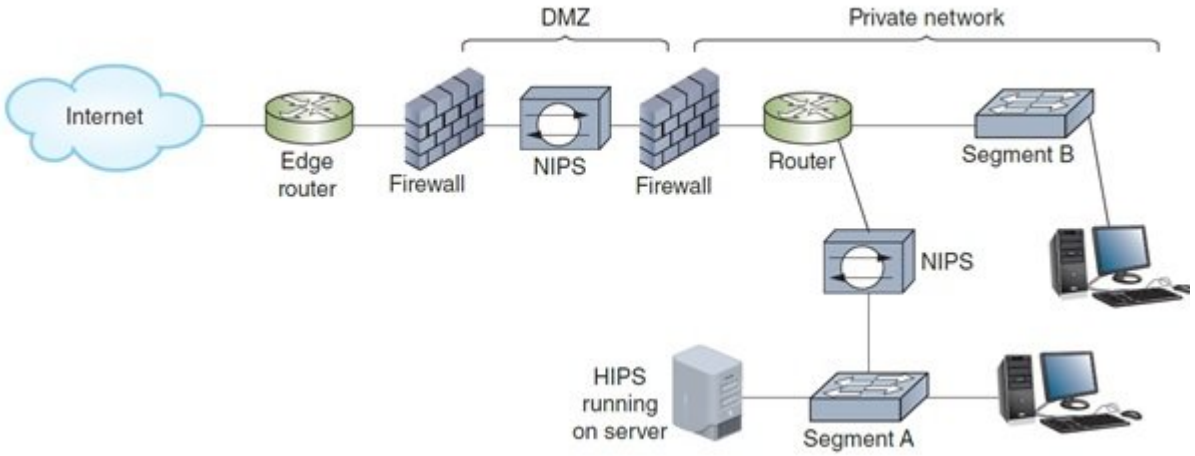
یک سامانه تشخیص نفوذ تنها می‌تواند فعالیت‌های مشکوک را شناسایی کرده و گزارشی در ارتباط با آن‌ها صادر کند، اما یک سامانه پیشگیری از نفوذ (IPS) سرنام Intrusion Prevention System در خطی میان یک مهاجم و شبکه یا میزبان هدف قرار می‌گیرد و این پتانسیل را دارد تا مانع عبور ترافیک از شبکه یا میزبان شود. سمت چپ شکل زیر این مکان قرارگیری یک IPS را نشان می‌دهد.



در حالی یک سامانه تشخیص نفوذ عملکردی شبیه به یک نیروی امنیتی دارد که با استفاده از دوربین‌های مدار بسته

نظارت تصویری یک ساختمان را زیر نظر می‌گیرد، در مقابل یک سامانه پیشگیری از نفوذ شبیه به نیروی امنیتی است که پیرامون یک ساختمان حرکت می‌کند و مانع از آن می‌شود تا افراد خرابکار از طریق درب‌های خروجی به ساختمان وارد شوند. در حالت کلی سامانه‌های پیشگیری از نفوذ عملکردی به مراتب فراتر از آن چیزی دارند که به آن اشاره شد و قادر هستند به عنوان ابزاری برای تجزیه و تحلیل ترافیک‌ها و محافظت از شبکه‌ها (در برخی موارد بهتر از دیوارهای آتش) استفاده شوند. با این حال، دیوارهای آتش به مرور زمان تکامل پیدا کردند و در نتیجه، تفاوت‌های میان یک دیوارآتش و یک سامانه پیشگیری از نفوذ به میزان قابل توجهی کاهش پیدا کرد. از آنجایی که یک IPS در خط حائل ترافیک شبکه قرار می‌گیرد، قادر است یک ترافیک مخرب را متوقف کند. به‌طور مثال، اگر IPS یک تلاش هکری با هدف ایجاد اختلال در ترافیک شبکه شناسایی کند اجازه نخواهد داد ترافیک کاذب، شبکه را تحت‌الشعاع خود قرار دهد. در ادامه IPS ممکن است کاربر متجاوز را بر اساس آدرس آی‌پی او در وضعیت قرنطینه قرار داده و در عین حالت اجازه دهد ترافیک مجاز روی شبکه مبادله شود.

شبیه به یک IDS، یک سیستم پیشگیری از نفوذ مبتنی بر شبکه (NIPS) می‌تواند از کل شبکه محافظت کند، در حالی که یک سیستم پیشگیری از نفوذ مبتنی بر میزبان (HIPS) می‌تواند از یک میزبان خاص محافظت کند. درون یک شبکه یا محیط شبکه می‌توان هر دو مکانیزم IDS و IPS را با یکدیگر استفاده کرد. در شکل زیر یک NIPS برای نظارت و محافظت از ترافیک در DMZ مورد استفاده قرار گرفته و NIPS دوم در داخل شبکه خصوصی در محدوده بلوک A قرار گرفته است تا نظارت و محافظت از ترافیک در این بخش از شبکه به دقت اعمال شود. همان‌گونه که در شکل مشاهده می‌کنید، نرم‌افزار HIPS نیز روی سرور اجرا شده است.



Security Information and Event Management

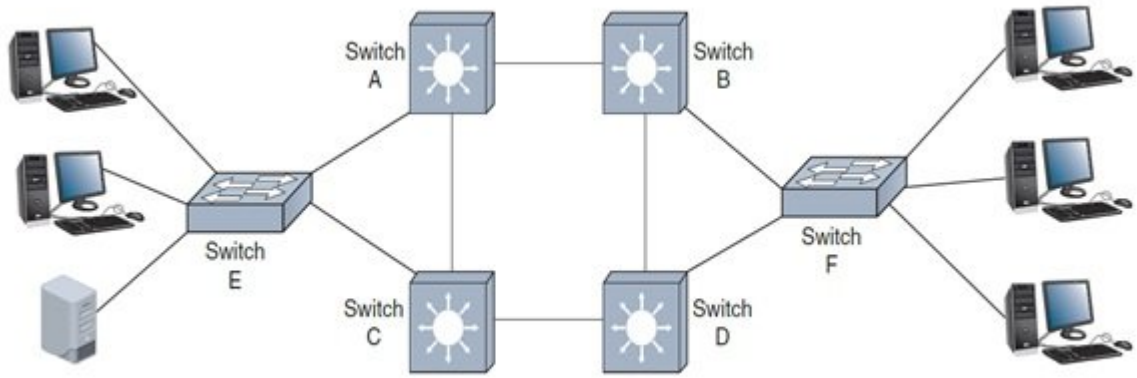
IDS، IPS، دیوارهای آتش و پروکسی سرورها، حجم قابل توجهی از اطلاعات را تولید و در قالب گزارش‌هایی ذخیره‌سازی می‌کنند که این گزارش‌ها باید به صورت بلادرنگ بررسی و تحلیل شوند. سیستم‌های امنیت اطلاعات و مدیریت رویداد (SIEM) سرنام Security Information and Event Management را می‌توان برای ارزیابی تمامی این داده‌ها و جست‌وجو به منظور پیدا کردن رویدادهای قابل توجهی که باید همسو با قوانین از پیش تعریف شده باشند و نیازمند توجه دقیق کارمندان بخش فناوری اطلاعات هستند پیکربندی کرد. در این حالت زمانی که مغایرتی با قوانین از پیش تعریف شده شناسایی شود، سیستم هشداری را تولید خواهد کرد. این هشدار می‌تواند از طریق ایمیل، پیام کوتاه برای گوشی هوشمند یا سایر روش‌ها برای پرسنل بخش فناوری اطلاعات ارسال شود. چالش اصلی این سامانه‌ها در متعادل‌سازی میزان حساسیت و هشداری است که تولید می‌کنند. به‌طور مثال، یک SIEM که به اندازه کافی حساس نباشد، رویدادهای بحرانی را که نیازمند پاسخ و رسیدگی هستند از دست خواهد داد. در نقطه مقابل اگر حساسیت بیش از اندازه بالا باشد، در طول روز صدها اعلان مختلف را برای کارمندان ارسال می‌کند که رسیدگی به آن‌ها کار بسیار مشکلی است که همین مسئله باعث نادیده گرفتن برخی از هشدارها می‌شود. اثربخشی SIEM تا حدی بر مبنای میزان فضای ذخیره‌سازی که برای داده‌های تولیدی در اختیار دارد و همچنین تعداد رویدادهایی که در هر ثانیه قادر به پردازش آن‌ها است ارزیابی می‌شود. زمانی که درباره حجم فضای ذخیره‌سازی داده‌ها صحبت می‌کنیم، باید به داده‌هایی که از سوی دستگاه‌هایی همچون سوئیچ‌ها، روترها، سرورها و سیستم‌های امنیتی برای SIEM ارسال می‌شوند و همچنین ترافیک روبه‌رشد شبکه دقت نظر ویژه‌ای داشته باشیم.

مدیریت سوییچ

یاد گرفتید که چگونه سوئیچ‌ها کار می‌کنند یا عملکرد آن‌ها در یک شبکه محلی مجازی چگونه است. با این حال، مسئولیت مدیریت سوئیچ فراتر از وظایف ساده‌ای همچون اتصال به دستگاه‌ها و پیکربندی VLANها است. همان‌گونه که شبکه‌ها به‌طور فزاینده‌ای در حال حرکت به سمت VLANها و سایر فناوری‌های مبتنی بر سوئیچ‌ها هستند، سوئیچ‌های مدیریت شده و سوئیچ‌های لایه 3 نقش بسیار مهمی در محیط سازمانی ایفا می‌کنند. در عین حال امنیت سوئیچ در حفاظت از منابع شبکه مهم‌تر و پیچیده‌تر می‌شود.

Switch Path Management

فرض کنید قرار است یک شبکه سازمانی با چند سوئیچ متصل را طراحی کنید. برای آن‌که آستانه تحمل شبکه در برابر خطاها زیاد باشد، چندین سوئیچ یا مسیر عبور داده جایگزین (redundant) برای ترافیک شبکه به منظور بالا بردن سطح امنیتی شبکه زمانی که ارتباط کامل قطع می‌شود را نصب می‌کنید. (redundant اجازه می‌دهد تا داده‌ها از طریق بیش از یک سوئیچ به سمت مقصد انتقال پیدا کرده و باعث می‌شود شبکه شما به دلیل خرابی‌های سخت‌افزاری کمترین قطعی را داشته باشد.) به‌طور مثال، اگر یک سوئیچ دچار مشکل خرابی منبع تغذیه شده است، ترافیک می‌تواند از طریق سوئیچ دوم انتقال پیدا کند. شبکه شما ممکن است چیزی شبیه شکل زیر باشد که در آن چند سوئیچ سریع و قدرتمند با یکدیگر و در قلب شبکه کار می‌کنند. در این شبکه سوئیچ‌های ایستگاه کاری به‌طور مستقیم به نقطه‌های انتهایی متصل می‌شوند. (در واقع، گره‌های بیشتری ممکن است به هر دو نوع سوئیچ متصل شوند.)



اما شبکه بالا با مشکل بزرگی به نام حلقه‌های ترافیک روبرو است. اگر یک سرور متصل به سوئیچ E یک فریم پخشی را منتشر کند که سوییچ E دومرتبه برای همه پورت‌ها به جزء پورتی که سرور به آن متصل شده این فریم پخشی را ارسال کند چه اتفاقی رخ می‌دهد؟ در این حالت، سوئیچ E فریم پخشی را برای سوئیچ‌های A و C ارسال می‌کند و سپس فریم پخشی را برای سوئیچ‌های B و D و این چرخه تکرار می‌شود. اگر محدودیتی برای این مسئله در نظر گرفته نشود، این انتقال‌های مستمر باعث از کار افتادگی شبکه شده و به واسطه حجم بالای ترافیکی که تولید می‌کند عملکرد شبکه را مختل می‌کند. برای از بین بردن این مشکل و پیشگیری از به وجود آمدن انواع دیگری از حلقه‌های تکرار، پروتکل درخت پوشا (STP) سرنام Spanning Tree Protocol توسط Radia Perlman از شرکت Digital Equipment Corporation در سال 1985 طراحی شد که بعدها در سال 1990 توسط IEEE اولین نسخه از این پروتکل به نام استاندارد 802.1D برای استفاده در لایه پیوند داده تصویب شد. (پروتکلی که در لایه 2 کار می‌کرد.)

این پروتکل با محاسبه مسیرهایی که باعث بروز حلقه‌ها می‌شوند مانع از بروز مشکل حلقه‌های ترافیکی و حلقه‌های سوییچی می‌شود. رویکرد فوق با مسدود کردن مصنوعی لینک‌هایی که باعث کامل شدن حلقه می‌شوند از بروز این مشکل ممانعت به عمل می‌آورد. پروتکل STP با تغییرات در شبکه نیز سازگار است. به‌طور مثال، اگر سوئیچی حذف شود، STP بهترین مسیرهای اطلاعاتی که باعث ایجاد حلقه نمی‌شوند را میان سوئیچ‌های باقیمانده محاسبه خواهد کرد.

فرآیند مسیریابی با پروتکل STP

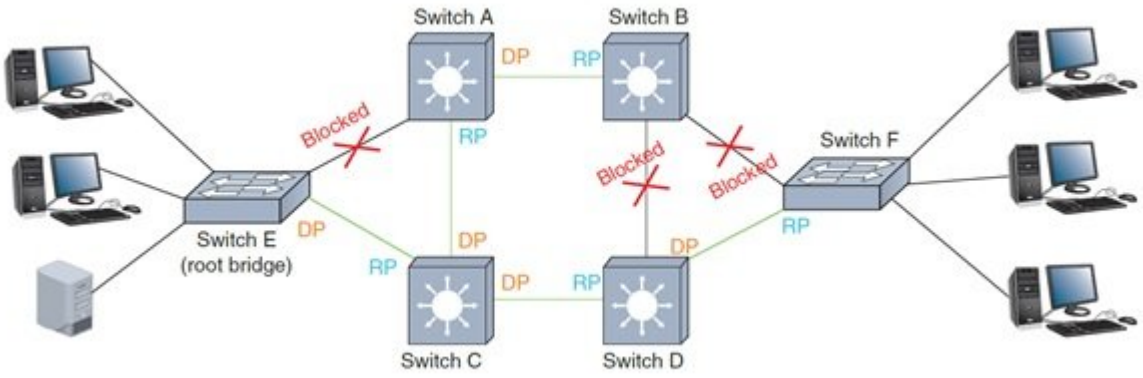
این فرآیند در سه مرحله به شرح زیر انجام می‌شود.

مرحله 1: STP یک پل اصلی یا ریشه را انتخاب می‌کند که زیربنایی برای همه محاسباتی است که برای مسیریابی در آینده از آن استفاده خواهد کرد. دقت کنید در یک شبکه فقط یک پل اصلی (ریشه) وجود دارد. از این پل اصلی، مجموعه‌ای از شاخه‌های منطقی یا مسیرهای داده‌ای شبیه به شاخه‌های یک درخت تولید می‌شود. STP پل اصلی را بر مبنای شناسه پل (BID) سرنام Bridge ID انتخاب می‌کند. BID ترکیبی از یک فیلد اولویت 2 بایتی است که می‌تواند توسط مدیر شبکه تنظیم شده و آدرس مک پل ساخته شده باشد. برای شروع، تمام پل‌ها در شبکه یک شماره اولویت یکسان را به‌اشتراک قرار می‌دهند و در نتیجه پلی با پایین‌ترین آدرس مک به پل اصلی پیش‌فرض تبدیل می‌شود.

مرحله 2: STP مسیرهای احتمالی بین تمام پل‌ها و پل اصلی را بررسی کرده و مسیری که بهترین کارایی را نسبت به سایر مسیرها دارد انتخاب می‌کند. مسیری که برای سایر پل‌ها کمترین هزینه را دارد.

مرحله 3: STP لینک‌هایی که جزء کوتاه‌ترین مسیر نیستند را غیر فعال می‌کند. برای انجام این کار پورتی که کمترین هزینه را روی هر لینک میان دو پل دارد را برای انتقال ترافیک شبکه انتخاب می‌کند. این پورت به نام پورت کاندید شناخته می‌شود. اما تمام پورت‌ها می‌توانند اطلاعات STP را دریافت کنند.

شکل زیر یک شبکه مبتنی بر سوئیچ را همراه با مسیرهای انتخابی و مسیرهایی که توسط STP مسدود شده است را نشان می‌دهد.



در شکل بالا، پورت‌های ریشه که به پل اصلی اشاره دارند با RP نام‌گذاری شده‌اند. در این شکل Designated Ports (پورت‌هایی هستند که می‌توانند یک سوئیچ دیگر را با کمترین هزینه به Root Bridge برساند.) به جریان‌های پایین‌دستی از پل اصلی اشاره دارند که با برچسب DP مشخص شده‌اند. به‌طور مثال فرض کنید، ترافیک از پل ریشه (سوییچ E) قرار است به سمت سوئیچ B برود، برای این منظور ترافیک از سوئیچ‌های C و A عبور می‌کند. حتا زمانی که سوئیچ B به سوئیچ‌ها D و F متصل است، STP عبور ترافیک از طریق سوئیچ‌ها C و A را مسیر منطقی در نظر می‌گیرید. حال فرض کنید سوئیچ A در این زمینه با مشکل روبرو می‌شود. STP به‌طور خودکار با انتخاب یک مسیر منطقی متفاوت برای فریم‌ها فرآیند انتقال را مدیریت می‌کند. اطلاعات STP بین سوئیچ‌ها از طریق پروتکل واحد داده پل (BPDUها) سرنام Units Protocol Data Protocol انتقال پیدا می‌کند. برای محافظت از یکپارچگی مسیرهای STP و اطلاعاتی که توسط BPDUها منتقل می‌شوند، برخی اقدامات امنیتی باید روی رابط‌های مبتنی بر STP اعمال شوند که از آن جمله می‌توان **BPDU guard**(زمانی که مکانیزم فوق فعال می‌شود، اگر روی پورت سوییچ BPDU دریافت شود، فرآیند ارسال روی این پورت متوقف شده و در حقیقت پورت به وضعیت غیر فعال در می‌آید. این مکانیزم مانع از آن می‌شود که یک سوییچ سرکش یا کامپیوتر متصل به یکی از این پورت‌ها بتواند مسیرهای STP شبکه را به سرقت ببرد.)،**BPDU filter** (این مکانیزم STP را روی پورت‌های خاص غیر فعال می‌کند.)، **root guard** (مکانیزم فوق مانع از تغییر مسیر سوییچ شده و اجازه نمی‌دهد سوییچ و پورت‌هایی که قبلا پیکربندی شده‌اند تبدیل به ریشه شوند.) لازم به توضیح است که نسخه‌های جدیدتری از پروتکل STP به نام‌های

پروتکل درخت پوشای سریع (**RSTP**) سرنام **Rapid Spanning Tree Protocol** که در قالب استاندارد IEEE 802.1w تعریف شده و پروتکل درخت پوشای چندگانه **MSTP** سرنام **Multiple Spanning Tree Protocol** که اساسا توسط استاندارد 802.1s تعریف شده و قادر است خطاهای پیوندی را در کسری از ثانیه حل کند، پروتکل **TRILL** سرنام **Transparent Interconnection of Lots of Links** که یک پروتکل مسیریابی چندگانه توسعه یافته از سوی سازمان IETF است و پروتکل کوتاه‌ترین مسیر پل‌زدن (**SPB**) سرنام **Shortest Path Bridging** که در حقیقت فرزند پروتکل STP است (جایگزین این پروتکل بوده و در لایه 3 کار می‌کند) و در قالب استاندارد **IEEE 802.1aq** تعریف شده، هم اکنون در دنیای شبکه استفاده می‌شوند.

• بعضی از تولیدکنندگان سوئیچ، مانند سیسکو و Extreme Networks نسخه‌های اختصاصی STP که بیشتر برای محصولات خود این شرکت‌ها بهینه‌سازی شده است را طراحی کرده‌اند.

(Authentication, Authorization, and Accounting)

کنترل دسترسی کاربران به شبکه و منابع شبکه بر پایه سه رکن اصلی تایید هویت (**authentication**)، مجوز (**authorization**) و حساب‌کاربری (**accounting**) است. ترکیب سه این عنصر با یکدیگر به نام چارچوب **AAA** سرنام (**authentication**, **authorization**, and **accounting**) شناخته شده که تعریف هر یک به شرح زیر است.

Authentication

یک کاربر می‌تواند پس از تایید هویا به یک دستگاه محلی یا شبکه متصل شود. به‌طور مثال، کاربر می‌تواند با احراز هویت محلی و از طریق یک حساب کاربری محلی به ویندوز وارد شود. با احراز هویت شبکه، کاربر می‌تواند از طریق حساب کاربری شبکه خود که در Active Directory و در دامنه ویندوز ذخیره شده است به سیستم وارد شود.

در شماره آینده آموزش **نتورک‌پلاس** مبحث فوق را ادامه خواهیم داد.

تاریخ انتشار:

08 خرداد 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/15453/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-%D8%B1%D8%A7%DB%8C%DA%AF%D8%A7%D9%86-%D8%AF%D9%88%D8%B1%D9%87-%D9%86%D8%AA%D9%88%D8%B1%DA%A9%E2%80%8C%D9%BE%D9%84%D8%A7%D8%B3-%D8%A8%D8%AE%D8%B4-56