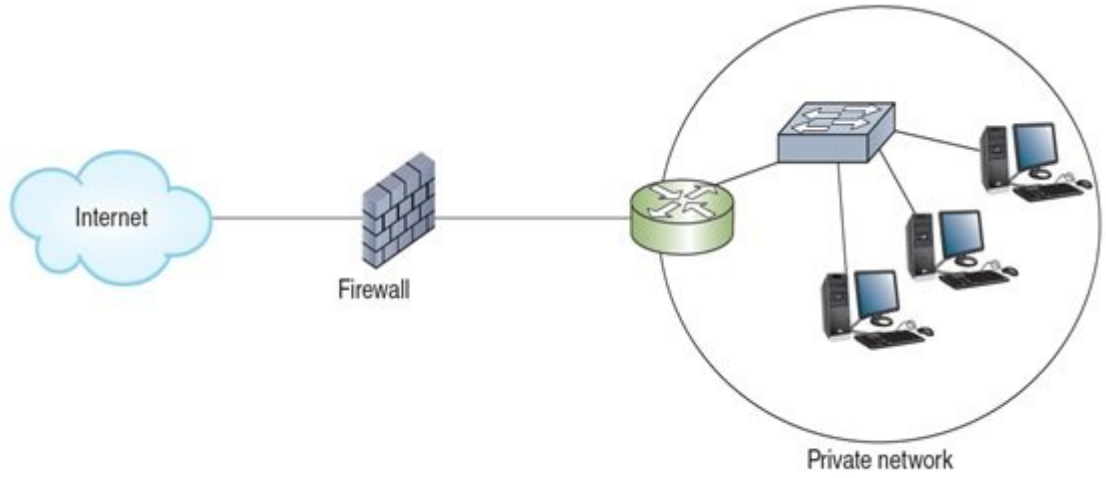
آموزش رایگان دوره نتورک‌پلاس (بخش 55)

در شماره گذشته آموزش نتورک‌پلاس مبحث امنیت در طراحی شبکه‌ها را آغاز کرده، به سراغ پروکسی سرورها و فهرست‌های کنترل دسترسی را بررسی کردیم. در این شماره مبحث فوق را ادامه خواهیم داد.

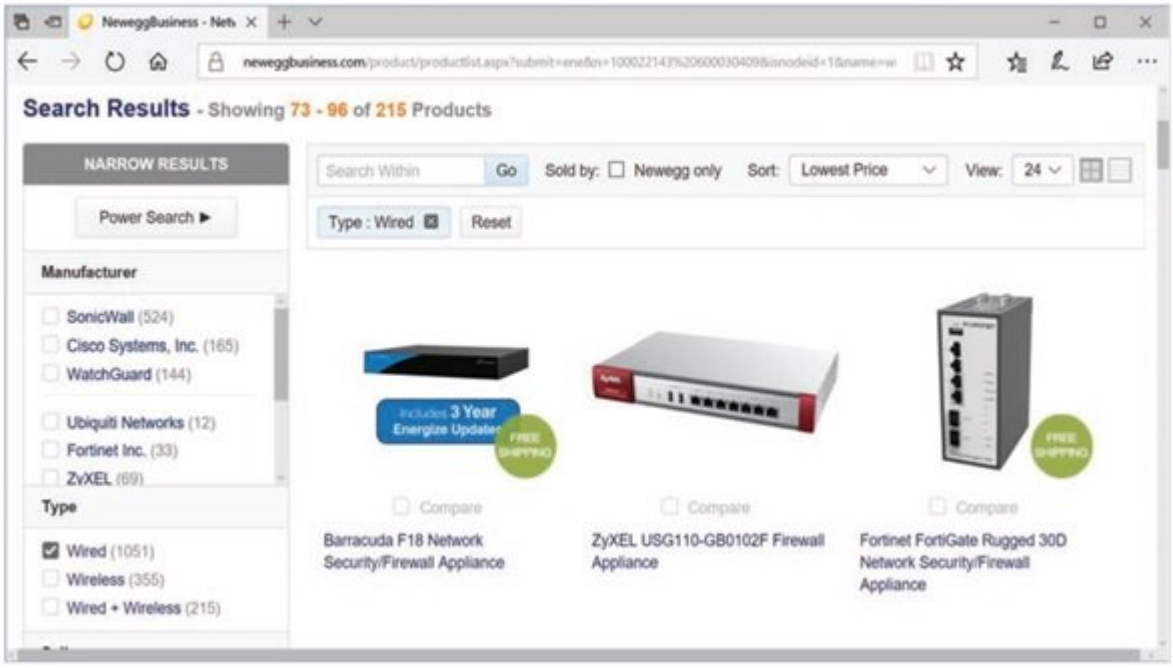
برای مطالعه بخش پنجاه و چهارم آموزش رایگان و جامع نتورک پلاس (Network+) اینجا کلیک کنید

دیوارهای آتش

دیوارآتش یک دستگاه تخصصی یا نرم‌افزار ویژه‌ای است که بر مبنای قواعدی ترافیک بین شبکه‌ها را فیلتر یا مسدود می‌کند. یک دیوارآتش با مسدود کردن ترافیک خاصی که به دیوارآتش وارد شده، شبیه به مکانیزم‌های امنیتی که روی درب‌ها تعبیه شده و مانع از ورود افراد غیرمجاز می‌شود از یک شبکه محافظت می‌کند. در حالی که دیوارهای آتش شامل فیلترهای فهرست کنترل دسترسی هستند، آن‌ها همچنین طیف گسترده‌ای از راهکارهای مختلف را برای ارزیابی، فیلتر کردن و کنترل ترافیک شبکه به کار می‌گیرند. یک دیوارآتش ممکن است به شکل داخلی و میان دو شبکه خصوصی قرار گرفته و شبیه به پلی امنیتی این دو شبکه را به یکدیگر متصل کند. به‌طور معمول، دیوارهای آتش در لبه یک شبکه خصوصی قرار گرفته و ارتباطات میان یک شبکه خصوصی و یک شبکه عمومی (مانند اینترنت) را زیر نظر قرار می‌دهند. شکل زیر این موضوع را نشان می‌دهد.



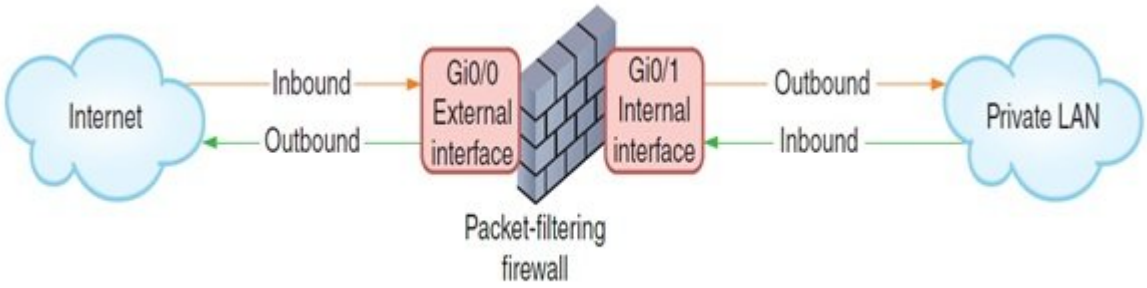
در شکل زیر تجهیزات امنیتی و دیوارهای آتش سخت‌افزاری را مشاهده می‌کنید که برای حفاظت از یک شبکه متوسط یا بزرگ استفاده می‌شوند.



لازم به توضیح است که شما برخی از ویژگی‌های یک دیوارآتش را روی دستگاه‌هایی همچون روترها، سوئیچ‌ها و سایر دستگاه‌های شبکه در اختیار دارید. دقت کنید عملکرد همه دیوارهای آتش یکسان نیست. به‌طور مثال، یک دیوارآتش مبتنی بر میزبان تنها از کامپیوتری که روی آن نصب شده است محافظت می‌کند.

نکته امتحانی: انواع مختلفی از دیوارهای آتش وجود دارند و می‌توان آن‌ها را به روش‌های مختلفی پیاده‌سازی کرد. برای درک نحوه طراحی یک شبکه امن و موفقیت در آزمون **نتورک‌پلاس** باید به خوبی این مسئله را بدانید که دیوارهای آتش می‌توانند چه کارهایی انجام دهند، در چه بخشی از شبکه قرار می‌گیرند و چگونه باید ویژگی‌های مورد نیاز خود در یک دیوارآتش را تشخیص دهید.

ساده‌ترین شکل یک دیوارآتش، یک دیوارآتش فیلترکننده بسته‌ها است که یک دستگاه یا برنامه تحت شبکه است که سرآیند هر بسته داده‌ای دریافتی از رابط‌های مختلف (ترافیک ورودی) را آزمایش می‌کند. شکل زیر این مسئله را نشان می‌دهد.



دیوارآتش برای بررسی این مسئله که آیا نوع بسته دریافتی برای ارسال به مقصد مجاز است یا خیر (صرفنظر از این موضوع که مقصد در یک شبکه داخلی یا یک شبکه خارجی قرار دارد) به فهرست کنترل دسترسی (ACL) خود مراجعه می‌کند. اگر بسته مغایر با معیارهای فیلترینگ باشد، دیوارآتش مانع از ارسال بسته می‌شود. اما اگر بسته مطابق با معیارهای فیلترینگ باشد، دیوارآتش اجازه می‌دهد تا بسته به شبکه‌ای که تحت نظارت دیوارآتش قرار دارد انتقال پیدا کند. تقریبا همه روترها می‌توانند به گونه‌ای پیکربندی شوند تا از طریق فهرست‌های کنترل دسترسی به

صورت یک دیوارآتش فیلترکننده بسته‌ها به کار گرفته شوند.

شکل بالا نشان می‌دهد که دیوارآتش چگونه ترافیک واردشده از سمت اینترنت به سوی شبکه محلی را فیلتر کرده و همچنین چگونه اجازه می‌دهد ترافیک از سمت شبکه محلی به اینترنت انتقال پیدا کند. یکی از دلایلی که دیوارهای آتش ترافیک وارد شونده از اینترنت را مسدود می‌کنند به عدم شیوع کرم‌ها باز می‌گردد. اغلب دیوارهای آتش همراه با پیکربندی از پیش تعیین شده ارائه می‌شوند، اما بیشتر مدیران شبکه‌ها تمایل دارند پیکربندی‌های خاص خود را روی آن‌ها اعمال کنند.

از جمله معیارهای مشترکی که دیوارهای آتش فیلترکننده بسته‌ها بر مبنای آن‌ها ترافیک را مسدود کرده یا اجازه عبور به ترافیک را می‌دهند به شرح زیر هستند:

• آدرس‌های آی‌پی مبدا و مقصد

• پورت‌های مبدا و مقصد (به‌طور مثال، پورت‌هایی که ارتباطات TCP / UDP از آن‌ها استفاده می‌کنند، FTP، Telnet، ARP، ICMP، و....)

• پرچم‌ها در سرآیند TCP (به‌طور مثال، SYN یا ACK)

• انتقال‌هایی که از پروتکل‌های UDP یا ICMP استفاده می‌کنند

• وضعیت بسته‌ای که به شبکه خصوصی شما وارد شده یا از آن خارج می‌شود

بر مبنای این معیارها، یک مدیر شبکه می‌تواند دیوار آتش خود را به‌گونه‌ای پیکربندی کند تا به‌طور مثال، مانع از آن شود تا آدرس‌های آی‌پی که با مقدار 10.121 شروع نمی‌شوند به شبکه دسترسی پیدا کنند. یک مدیر همچنین می‌تواند پورت‌های شناخته شده‌ای همچون پورت‌های غیرایمن NetBIOS به شماره 137، 138 و 139 را مسدود کرده یا باز کند. این تکنیک مانع از آن می‌شود تا فرآیند انتقال از طریق پورت‌های مسدود شده امکان‌پذیر باشد. پورت‌ها نه تنها از طریق دیوارهای آتش، بلکه از سوی روترها، سرورها یا هر دستگاهی که از پورت‌ها استفاده می‌کند قابل مسدود شدن هستند. برای آن‌که امنیت شبکه را بیشتر کنید، بهتر است دیوارآتش را برای انجام کارهای پیچیده‌تری نسبت به مسدود کردن بسته‌ها تنظیم کنید. در زمان به‌کارگیری یا انتخاب یک دیوارآتش بهتر است برای پرسش‌های زیر پاسخ مناسبی داشته باشید:

• آیا دیوارآتش از رمزگذاری پشتیبانی می‌کند؟

• آیا دیوارآتش از تأیید و احراز هویت کاربر پشتیبانی می‌کند؟

• آیا دیوارآتش به شما اجازه می‌دهد تا آن‌را به صورت مرکزی و از طریق یک رابط استاندارد مدیریت کنید؟

• آیا به سادگی می‌توانید به قواعد دیوارآتش دسترسی داشته باشید یا آن‌ها را منتشر کنید

• آیا دیوارآتش از فیلتر کردن لایه‌های بالایی مدل OSI و نه فقط لایه‌های پیوند داده و انتقال پشتیبانی می‌کند؟ به‌طور مثال، دیوارآتش فیلترکننده محتوا می‌تواند گونه‌های مشخص شده ترافیک را براساس داده‌های یک برنامه که درون یک بسته اطلاعاتی قرار دارند مسدود کند؟

• آیا دیوارآتش قابلیت ثبت و ضبط گزارش‌های داخلی ارائه شده از سوی IDS یا IPS را دارد؟

• آیا دیوارآتش از آدرس داخلی شبکه شما در مقابل دنیای بیرون محافظت می‌کند؟

• آیا دیوارآتش می‌تواند بسته‌ها را بر مبنای ترافیک موجود زیر نظر بگیرد؟ یک دیوارآتش فارغ از حالت (stateful firewall) می‌تواند هر بسته ورودی را بررسی کند تا مشخص شود که آیا بسته متعلق به یک اتصال فعال و قانونی است یا خیر.

یک روتر بیسیم SOHO به‌طور معمول به عنوان یک دیوارآتش عمل می‌کند و شامل گزینه‌های فیلترکردن بسته‌ها

است. دستگاه‌های ساخته شده از سوی سیسکو یا Fortinet با درجه امنیت سازمانی نیز جزء تجهیزات امنیتی قدرتمندی برای شبکه‌ها شناخته می‌شوند که قادر هستند علاوه بر فیلتر کردن بسته‌ها، به رمزگذاری، متعادل‌سازی بار و... بپردازند. نمونه‌هایی از نسخه‌های نرم‌افزاری دیوارهای آتش نیز یک کامپیوتر را قادر می‌سازند به عنوان یک دیوارآتش فیلترکننده بسته‌ها عمل کند که از آن جمله می‌توان به iptables (یک ابزار دیوارآتش خط فرمان برای سیستم‌های لینوکس)، ZoneAlarm و Comodo Firewall اشاره کرد. برخی از سیستم‌عامل‌ها، همچون ویندوز 10 نیز شامل دیوارآتش از پیش ساخته شده هستند.

Unified Threat Management

در پاسخ به پیچیدگی‌های روبه‌رشد تهدیدات سایبری و محافظت از منابع پردازشی، فروشندگان دیوارهای آتش و محصولات مرتبط با آن‌ها یکسری راهکارهای نوآورانه ابداع کرده‌اند. یکی از این نوآوری‌ها مدیریت یکپارچه تهدیدات (UTM) سرنام **Unified Threat Management** است که یک استراتژی امنیتی است که ترکیبی از فناوری‌ها و تجهیزات امنیتی است که در قالب یک موجودیت واحد یک مکانیزم امنیتی را ارائه می‌کند. یک راه‌حل مدیریت یکپارچه تهدیدات می‌تواند طیف گسترده‌ای از خدمات امنیتی که از طریق یک مکان مرکزی مدیریت می‌شوند را ارائه کند. اما این مکانیزم معایبی نیز دارد. به‌طور مثال، اگر یک لایه امنیتی کیفیت پایینی داشته باشد، مکانیزم حفاظتی به‌طرز قابل توجهی آسیب‌پذیر می‌شود. این مکانیزم به دلیل این‌که از بخش‌های مختلفی ساخته شده است به توان پردازشی زیادی نیاز دارد. در مجموع UTM به عنوان یک استراتژی امنیتی پیش‌رو، به ویژه برای کسب‌وکارهای کوچک و متوسطی که تمایل دارند یک مکانیزم امنیتی را با حداقل مدیریت و پیکربندی در اختیار داشته باشند مفید است.

Next Generation Firewalls

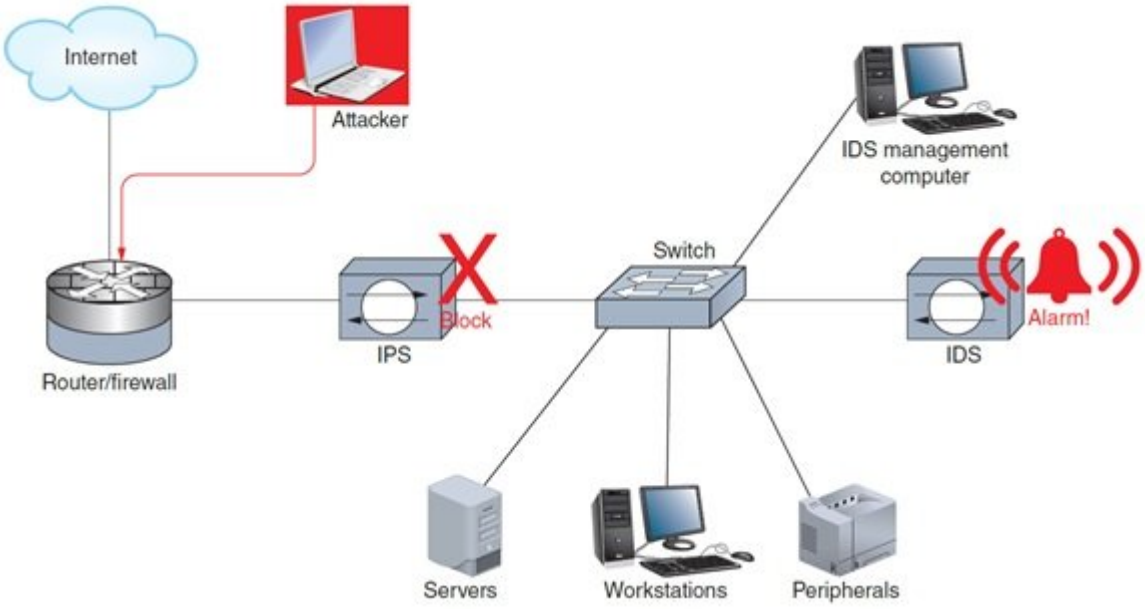
از آن‌جایی که دیوارهای آتش فیلترکننده بسته‌ها در لایه شبکه از مدل OSI کار می‌کنند، تنها آدرس‌های شبکه را بررسی کرده و قادر نیستند میان کاربری که سعی دارد به دیوارآتش آسیب وارد کرده و کاربری که قصد انجام کار مثبتی را دارد تمایز قائل شوند. در چنین شرایطی ما به دیوارآتشی نیاز داریم که بتواند فرآیند تحلیل داده‌ها در لایه‌های بالاتر را انجام دهد. به همین دلیل به سراغ دیوارهای آتش لایه هفت (Layer 7 firewall) می‌رویم که به آن‌ها دیوارهای آتش نسل بعدی (NGFWs) سرنام Next Generation Firewalls نیز گفته می‌شود. دیوارهای آتشی که قابلیت‌هایی همچون application aware (مانیتور و محدود کردن ترافیک برنامه‌های خاص، user aware (هماهنگ با یک یا گروه خاصی از کاربران) و context aware (هماهنگ شدن با برنامه‌ها کاربران و دستگاه‌های خاص) دارند. دیوارهای آتش NGFW گزینه ایده‌آلی برای سازمان‌های بزرگی هستند که مجبور هستند خط‌مشی‌های امنیتی را به شکل سفارشی پیاده‌سازی کنند.

عیب‌یابی دیوارهای آتش

شایع‌ترین عاملی که باعث می‌شود دیوارهای آتش در دفاع از یک شبکه با شکست روبرو شوند به تنظیمات اشتباه دیوارآتش باز می‌گردد. پیکربندی دیوارآتش سطح سازمانی می‌تواند چندین هفته طول بکشد تا بهترین نتایج را ارائه کند. پیکربندی یک دیوارآتش نباید بیش از اندازه سخت‌گیرانه تنظیم شده باشد که کاربران مجاز موفق نشوند به راحتی اطلاعات را ارسال کرده یا دریافت کنند و در عین حال نباید بیش از اندازه ساده باشد که امنیت شبکه را در معرض خطر قرار دهد. همچنین در برخی موارد شما باید استثناءهایی را برای یکسری از قوانین در نظر بگیرید. به‌طور مثال مدیر منابع انسانی یک سازمان ممکن است مجبور شود به سرور سازمان که در شهر دیگری قرار دارد دسترسی پیدا کند. در چنین حالتی مدیر شبکه باید استثنایی را قائل شود تا شما بتوانید به شبکه سازمان که درون شهر دیگری قرار دارد دسترسی پیدا کنید. ایجاد یک استثنا در قوانین فیلترینگ دیوار آتش punching a hole نامیده می‌شود.

Intrusion Detection System

یک سیستم تشخیص نفوذ (IDS) سرنام **Intrusion Detection System** یک دستگاه، نرم‌افزار یا قابلیت از پیش ساخته شده‌ای است که روی یک ایستگاه کاری، سرور، روتر یا دیوارآتش اجرا می‌شود. سیستم تشخیص نفوذ ترافیک شبکه را رصد کرده و در مورد هرگونه فعالیت مشکوکی هشداری را نشان می‌دهد. شکل زیر این مسئله را نشان می‌دهد.



در حالی که یک فهرست کنترل دسترسی روتر یا یک دیوارآتش عملکردی شبیه به نگهبانی دارند که مقابل درب یک ساختمان قرار گرفته و شناسه افراد را بررسی کرده و مطمئن می‌شود که تنها افراد مجاز می‌توانند به سازمان وارد شوند، اما یک سیستم تشخیص نفوذ یک مکانیزم نظارت امنیتی درون شبکه‌ای را ارائه می‌کند که شبیه به فردی است که درون یک اتاق کنترلی نشسته و به دوربین‌های مداربسته نصب شده درون یک سازمان نگاه کرده و هرگونه فعالیت مشکوکی را که مشاهده کند، هشداری را صادر می‌کند. امروزه IDS اغلب به عنوان یک ویژگی جاسازی شده درون راه‌حل‌های UTM یا NGFWها استفاده می‌شود.

IDS از دو روش اصلی برای شناسایی تهدیدهای پیرامون یک شبکه به شرح زیر استفاده می‌کند:

• تشخیص ناهنجاری آماری – یک نمونه‌گیری از ترافیک شبکه انجام داده و آن‌را با مقیاس از پیش تعیین شده مقایسه می‌کند. با این روش مشخص می‌شود که آیا ناهنجاری‌های فعلی فراتر از پارامترهای خاص رفته‌اند یا در وضعیت عادی قرار دارند.

• تشخیص مبتنی بر امضا – این روش بر پایه الگوهای قابل تشخیص یا امضاء که در حقیقت کدی است که نشانه‌های آسیب‌پذیری یا اکسپلویت در آن قرار دارد کار کرده و ترافیک ناخواسته در شبکه سازمان را شناسایی می‌کند. برای حفظ اثربخشی این مکانیزم، امضاها باید به‌طور منظم در فرایندی که مدیریت امضا (signature management) نام دارد به‌روز شوند. بازنویسی امضاهای نامناسب و انتخاب امضاهایی که متناسب با نیازهای خاص شبکه است، باعث می‌شود تا منابع پردازشی همچون حافظه و پردازنده در زمان پویش ترافیک شبکه به بهترین شکل استفاده شوند.

سامانه های تشخیص نفوذ بر مبنای معماری به سه گروه NIDS، HIDS و DIDS تقسیم می‌شوند.

• **HIDS** (سیستم تشخیص نفوذ مبتنی بر میزبان) روی یک کامپیوتر واحد اجرا می‌شود تا حملات به یک میزبان را شناسایی کند. به‌طور مثال، HIDS ممکن است تلاش برای بهره‌برداری از یک برنامه غیرایمن که روی یک سرور در حال اجرا است یا تلاش‌های مکرر برای ورود به سرور را شناسایی کند. راه‌حل HIDS همچنین ممکن است شامل نظارت بر یکپارچگی فایل (FIM) سرنام file integrity monitoring باشد که سیستم را از وجود هرگونه تغییری در فایل‌هایی که نباید تغییر پیدا کنند همچون ویرایش فایل‌های سیستمی آگاه می‌کند.

• **NIDS** (سیستم تشخیص نفوذ مبتنی بر شبکه) برای محافظت از یک شبکه یا بخشی از یک شبکه استفاده شده و معمولا در لبه شبکه یا در یک محیط محافظت شده شبکه که منطقه غیرنظامی (demilitarized zone) نام دارد نصب می‌شود. در اینجا، سامانه فوق می‌تواند انواع مختلفی از الگوهای ترافیکی مشکوک همچون حملات انکار سرویس یا حملات smurf را شناسایی کند.

• **DIDS** (سامانه تشخیص نفوذ توزیع شده) این سامانه‌ها ترکیبی از دو مکانیزم قبلی همراه با یک ایستگاه مدیریت مرکزی هستند. در این مکانیزم هر سیستم تشخیص نفوذ موجود در شبکه گزارش خود را برای یک ایستگاه مدیریت مرکزی ارسال می‌کند. ایستگاه مرکزی نیز گزارش‌های دریافتی را ارزیابی کرده و اگر مورد مشکوکی را پیدا کند، هشداری برای مسئول امنیت سیستم ارسال می‌کند.

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

تاریخ انتشار:

07 خرداد 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/15439/%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%B4-55