عنوان مقاله:
جلوگیری از حملات منع سرویس توزیعی با استفاده از دیوار آتش میکروتیک

محل انتشار:
اولین کنفرانس ملی پژوهش های کاربردی در علوم مهندسی و فناوری اطلاعات (سال: 1397)

تعداد صفحات اصل مقاله: 21

نویسندگان:
علی شفائی - *دانشجوی کارشناسی ارشد دانشگاه آزاد اسلامی واحد میانه*

محمدرضا ابراهیمی دیشابی - *استادیار و عضو هیئت علمی دانشگاه آزاد اسلامی واحد میانه*

خلاصه مقاله:
باتوجه به گسترش روزافزون حملات منبع سرویس توزیع شده، لزوم ابداع روش های کارآمد به منظور جلوگیری از این حملات، بیش از پیش مشهود است در این راستا قصد داریم شیوه ای نوین و کارآمد را برای جلوگیری از حملات منع سرویس توسط دیوار آتش میکروتیک در این مقاله ارائه دهیم که روشی کاملا پویا و کارآمد بوده و به جای مسدودسازی پورت ها و آدرس های مربوطه به پایش شبکه پرداخته و فقط ترافیک های غیر مجاز را مسدود می کند. از مزیت های این روش نسبت به روش های موجود می توان به این مورد اشاره کرد که در این روش، تجهیزات ما به پایش ترافیک و آنالیز ترافیک ورودی و خروجی واسط کاربر پرداخته و در صورت مشاهده ترافیک غیر مجاز نسبت به مسدودسازی آن، طبق سوابق قبلی اقدام می کند و پس از مسدودسازی ترافیک، یک بار دیگر به کاربر فرصت می دهد تا فعالیت های عادی خود را در پیش بگیرد. در صورتی که باز هم ترافیک کاربر، ترافیک غیر عادی تشخیص داده شد، دسترسی او به شبکه مسدود می شود. در واقع در روش پیشنهادی ما، بسته های شبکه قبل از اینکه به سیستم تشخیص نفوذ اصلی تحویل داده شوند، مورد پالایش قرار می گیرند. سه روش مختلف برای این کار در نظر گرفته شده است، یک روش پالایش مبتنی بر لیست سیاه از آدرس های IP است. روش دوم از یک الگوریتم تطبیق انحصاری بهره می برد که نوع خاصی از عدم تطبیق ها را با هزینه کم شناسایی می کند. در روش سوم نیز، این دو مفهوم برای تولید یک روش فیلتر کارمدتر با هم ترکیب شده و روش EFM را بوجود می اروند. نتایج ارزیابی نشان می دهد که روش پالایش بسته در روش پشنهادی ما با نام TGT در اکثر اوقات منجر به بهبود زمان مصرفی می شود که مزیت عمده ای در شبکه ها محسوب می شود.

کلمات کلیدی:
حملات منع سرویس توزیع شده، دیوار آتش میکروتیک، آنالیز و پایش ترافیک، ترافیک سبز، RouterBoard.