Namatek
True Education

www.namatek.com

Mikrotik Firewall

فایروال میکروتیک

www.namatek.com

فهرست مطالب

اگر شما هم جزئی از مجموعه‌های استفاده‌کننده از شبکه‌هایی با روترهای میکروتیک هستید باید با فایروال میکروتیک آشنا باشید.

فایروال میکروتیک بین شبکه شرکت و یک شبکه عمومی قرار دارد و به طور مؤثر رایانه‌های شما را از فعالیت‌های هکرهای مخرب محافظت می‌کند.

برای این مهم در ادامه این مقاله با ما همراه باشید.

#۱ معرفی میکروتیک

پیش از آنکه به پاسخ پرسش فایروال میکروتیک چیست بپردازیم معرفی خلاصه‌ای از میکروتیک خواهیم داشت.

در سال ۱۹۹۶ میلادی در کشور لیتوانی، دو دانشجو از دانشگاه MIT موفق به تأسیس شرکت میکروتیک (MIKROTIK) شدند.

این شرکت در ابتدا کار خود را با روترهای وایرلس شروع کرد.

سپس با توسعه فعالیت‌ها، سیستم‌عامل میکروتیک Router OS را ارائه داد. این سیستم‌عامل مبتنی بر کرنل لینوکس (Linux kernel) که نوعی هسته سامانه عامل نرم‌افزار است طراحی شد.

Router OS از قابلیت‌های بسیاری پشتیبانی می‌کند که برخی از آن‌ها عبارت‌اند از:

- فایروال (firewall)
- روتینگ (routing)
- تکنیک MPLS (Multiprotocol Label Switching)
- وی‌پی‌ان (VPN)
- پراکسی (proxy)
- هات اسپات (hotspot)
- وایرلس (Wireless)

نرم‌افزار Winbox امکان بهره‌برداری از سیستم‌عامل میکروتیک را فراهم می‌کند.

همچنین به‌عنوان یک رابط گرافیکی در تنظیمات مربوط به روتینگ مؤثر خواهد بود.

#۲ محصولات شرکت میکروتیک

در سال ۲۰۰۲ میلادی کمپانی میکروتیک تصمیم گرفت برای سیستم‌عامل خود، بردهای سخت‌افزاری جدیدی طراحی کند؛ بنابراین از محصولی به نام Routerboard رونمایی کرد. این محصول در واقع یک کامپیوتر کوچک (mini PC) است و از قطعات مختلفی تشکیل شده که بعضی از این قطعه‌ها عبارت‌اند از:

- پردازنده (Processor)
- رم (RAM)
- رام (ROM)
- فلش موری (Flash memory)

تفاوت این PC با دیگر سخت‌افزارهای مشابه، در موارد زیر خلاصه می‌شود:

- CPU
- رم
- لایسنس‌ها

علاوه بر این Routerboard، شرکت میکروتیک محصولات دیگری را نیز روانه بازار کرده است.

برخی از آن‌ها عبارت‌اند از:

- **روتر (Router) میکروتیک**: این محصولات در واقع واسطه‌ای برای برقراری ارتباط سخت‌افزار با شبکه (اینترنت) محسوب می‌شوند که با دادن یک IP مخصوص مبدأ و مقصد داده‌ها را مشخص خواهند کرد.
- **سوئیچ (Switch) شبکه میکروتیک**: میکروتیک انواعی از سوئیچ‌های شبکه را به بازار عرضه کرده که یکی از آن‌ها CRS112-8P-4S-IN نام دارد.
- **سیستم وایرلس (Wireless) میکروتیک**: از دیگر محصولات MIKROTIK می‌توان به تجهیزات بی‌سیم این شرکت اشاره کرد. در این مقاله قصد داریم به‌صورت تخصصی به معرفی فایروال این شرکت بپردازیم.

#۳ فایروال میکروتیک چیست؟

فایروال میکروتیک (Mikrotik Firewall) مبتنی بر فناوری فیلترینگ حالت دار (Stateful Filtering) است که می‌تواند برای تشخیص و مسدودکردن بسیاری از اسکن‌های مخفی، حملات DoS و سیل همگام‌سازی (SYN) استفاده شود. ارتباطات شبکه‌ای از تکه‌های کوچکی از داده‌ها به نام بسته تشکیل شده‌اند و چندین مورد از این بسته‌ها صرفاً برای ایجاد، نگهداری و پایان ارتباط استفاده می‌شوند. فایروال حالت دار میکروتیک اطلاعات

مربوط به هر اتصال را که از آن عبور می‌کند در حافظه نگه می‌دارد. هنگامی که یک بسته خارجی سعی می‌کند وارد شبکه شود و ادعا می‌کند که بخشی از اتصال موجود است، فایروال لیست اتصالات خود را بررسی می‌کند.

زمانی که متوجه می‌شود بسته با هیچ یک از موارد موجود در لیست خود مطابقت ندارد، می‌تواند آن بسته را رها کرده و اسکن را شکست دهد!

#۴ مدیریت سیستم در فایروال روتر میکروتیک

مدیریت فایروال میکروتیک بسیار آسان است! معماری سیستم امکان پیکربندی آسان ترجمه آدرس شبکه (NAT)، پروکسی‌های شفاف و تغییر مسیر را فراهم می‌کند. قوانین فیلترینگ فایروال در زنجیره‌ای گروه‌بندی شده‌اند.

اگر بتوان بسته‌ها را با یک معیار مشترک در یک زنجیره مطابقت داد و سپس برای پردازش بر اساس معیارهای رایج دیگر به زنجیره‌ای دیگر منتقل کرد، بسیار مفید است. این امر با استفاده از تعداد کمتری از قوانین برای ایجاد فایروال بسیار دقیق‌تر، مدیریت سیستم را بسیار ساده‌تر می‌کند.

#۵ زنجیره فایروال در روتر میکروتیک

فایروال میکروتیک با قوانین فایروال کار می‌کند.

هر قانون شامل دو بخش است:

۱. منطبق‌کننده که با جریان ترافیک مطابق شرایط معین مطابقت دارد.
۲. اقدامی که مشخص می‌کند با بسته همسان چه باید کرد.

قوانین فیلترینگ فایروال در زنجیره‌ای گروه‌بندی شده‌اند. این گروه‌بندی اجازه می‌دهد تا بسته‌ای که با یک معیار مشترک در یک زنجیره مطابقت داشته باشد، برای پردازش بر اساس برخی معیارهای رایج دیگر به زنجیره‌ای دیگر منتقل شود.

سه زنجیره از پیش تعریف شده وجود دارند که نمی‌توان آن‌ها را حذف کرد:

۱. ورودی: برای پردازش بسته‌های وارد شده به روتر از طریق یکی از رابط‌ها با آدرس IP مقصد که یکی از آدرس‌های روتر است، استفاده می‌شود. بسته‌هایی که از روتر عبور می‌کنند برخلاف قوانین زنجیره ورودی پردازش نمی‌شوند.
۲. هدایت: برای پردازش بسته‌هایی که از روتر عبور می‌کنند استفاده می‌شود.
۳. خروجی: برای پردازش بسته‌هایی که از روتر نشئت‌گرفته و از طریق یکی از رابط‌ها خارج می‌شوند، استفاده می‌شود. بسته‌هایی که از روتر عبور می‌کنند برخلاف قوانین زنجیره خروجی پردازش نمی‌شوند.

نمودارهای جریان بسته نحوه پردازش بسته‌ها در سیستم‌عامل روتر را نشان می‌دهد. هنگام پردازش یک زنجیره، قوانین آن زنجیره به ترتیب ذکر شده از بالابه‌پایین اعمال می‌شوند.

اگر بسته‌ای با معیارهای قاعده مطابقت داشته باشد، آن‌گاه عمل مشخص شده بر روی آن انجام می‌شود و دیگر هیچ قانونی در آن زنجیره پردازش نمی‌شود. اگر بسته‌ای با هیچ قاعده‌ای در زنجیره داخلی مطابقت نداشته باشد، پذیرفته نمی‌شود.

#٦ پایه و اساس Mikrotik Firewall

- فیلترکردن آدرس IP
- فیلتر پروتکل پورت
- فیلترکردن رابط شبکه
- فیلتر آدرس MAC منبع
- گزینه‌های پروتکل TCP

#۷ کاربردهای فایروال در روتر میکروتیک

۱. محافظت از روتر در برابر دسترسی‌های غیرمجاز

شما می‌توانید اتصالات آدرس‌های اختصاص‌داده‌شده به روتر را زیر نظر داشته باشید و اجازه دسترسی فقط از میزبان‌های خاص به پورت‌هایTCP روتر را بدهید.

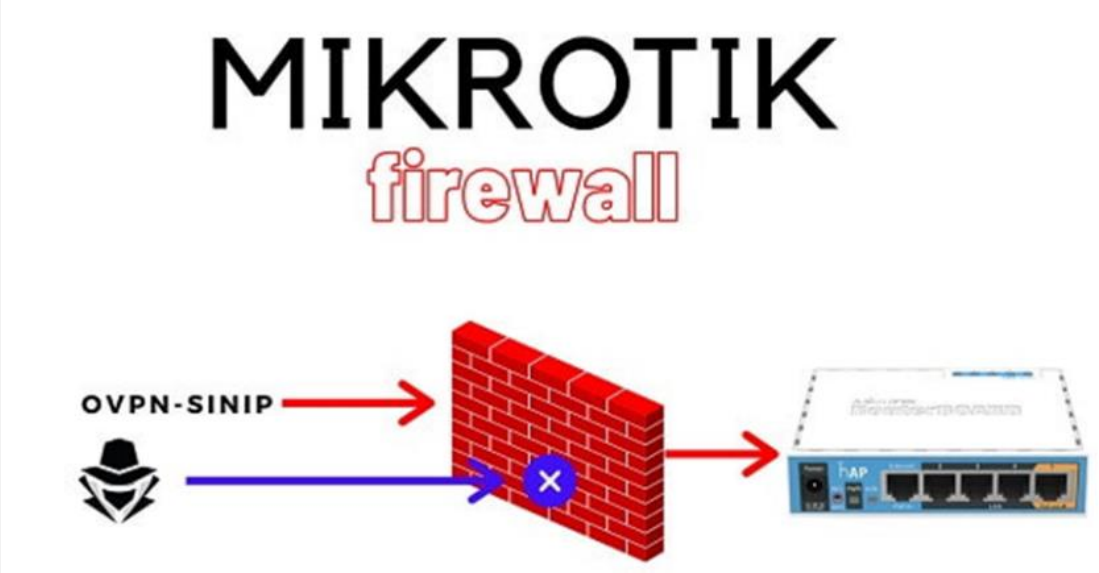
فایروال تمام اطلاعات اینترنت را کنترل می‌کند و بر اساس قوانین سفارشی شده توسط کاربر هشدار می‌دهد و مانع از نفوذ می‌شود.

۲. حفاظت از میزبان مشتری

می‌توانید اتصالات آدرس‌های اختصاص‌داده‌شده به شبکه مشتری را ازطریق فایروال میکروتیک زیر نظر داشته باشید و اجازه دسترسی فقط به میزبان‌ها و سرویس‌های خاص را بدهید.

۳. استفاده از روش ماسکینگ (Masquerading) برای مخفی کردن شبکه خصوصی در پشت یک آدرس خارجی

همه اتصالات از آدرس‌های خصوصی را می‌توان مخفی کرد تا اینکه طوری به نظر برسد که از یک آدرس خارج از آدرس روتر آمده است. فایروال به‌عنوان دروازه‌ای برای کل شبکه شما عمل می‌کند تا شبکه شما بتواند یک اتصال امن به اینترنت را به اشتراک بگذارد.



٤. اعمال سیاست استفاده از اینترنت از طریق شبکه مشتری

فایروال به شما امکان می‌دهد اتصالات شبکه مشتری را کنترل کنید و آمار ترافیک دقیق همه پیوندها را ارائه می‌دهد.

۵. اولویت‌بندی ترافیک

برای اطمینان از سریع‌ترین اتصال به بسته‌های مهم‌تر، می‌توانید بسته‌ها را با اولویت علامت‌گذاری کنید. این موضوع تضمین می‌کند که همه گروه‌ها همیشه پهنای باند مناسب را دریافت کنند و جریان قابل‌کنترل ترافیک شبکه را فراهم و از قحطی ارائه پهنای باند جلوگیری می‌کند.

٦. اعمال صف برای بسته‌های خروجی

این ویژگی اجازه می‌دهد تا سرعت اتصال را به گروه خاصی از بسته‌ها محدود کنید. سلسله‌مراتب کلاس شما را قادر می‌سازد تا یک نمایش انعطاف‌پذیر و بسیار منطقی از ترافیک خود بسازید.

#۸ امنیت Mikrotik Firewall

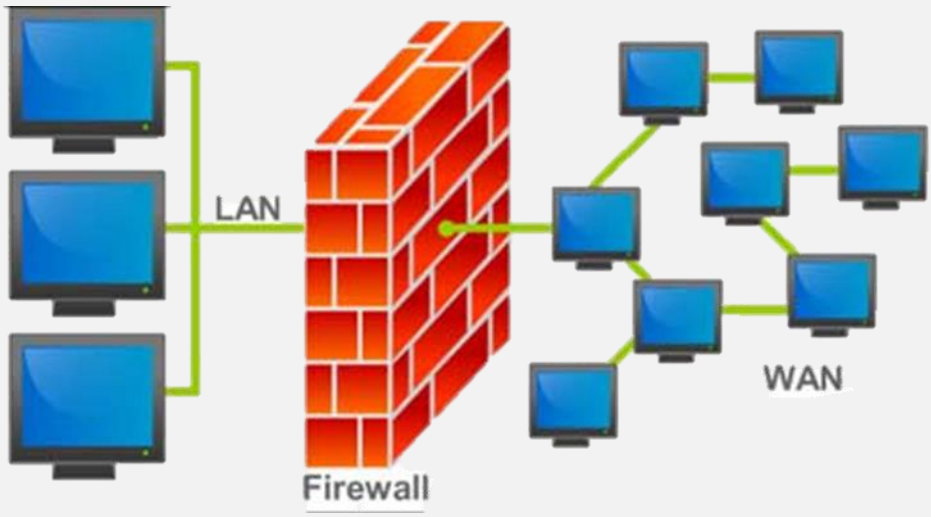
فایروال میکروتیک فیلترینگ بسته را اجرا می‌کند و در نتیجه عملکردهای امنیتی را ارائه می‌دهد که برای مدیریت جریان داده‌ها به داخل و روتر استفاده می‌شود. همراه با ترجمه آدرس شبکه، به‌عنوان ابزاری برای

جلوگیری از دسترسی غیرمجاز به شبکه‌های متصل مستقیم و خود روتر و همچنین فیلتری برای ترافیک خروجی عمل می‌کند. فایروال‌های شبکه تهدیدهای خارجی را از داده‌های حساس موجود در داخل شبکه دور نگه می‌دارند.

هرگاه شبکه‌های مختلف به هم متصل شوند، همیشه این تهدید وجود دارد که فردی از خارج از شبکه شما به شبکه LAN شما نفوذ کند. چنین نفوذی ممکن است منجر به سرقت و توزیع داده‌های خصوصی، تغییر یا نابودی داده‌های ارزشمند یا پاک شدن کل هارددیسک‌ها شود.

فایروال‌ها به‌عنوان ابزاری برای جلوگیری یا به‌حداقل‌رساندن خطرات امنیتی ذاتی اتصال به شبکه‌های دیگر استفاده می‌شوند. فایروال مناسب پیکربندی شده نقش کلیدی در استقرار زیرساخت‌های کارآمد و ایمن شبکه ایفا می‌کند.

#۹ خصوصیات فایروال میکروتیک



- بازرسی بسته‌ها
- تشخیص پروتکل لایه ۷
- فیلترکردن پروتکل‌های نظیر به نظیر
- طبقه‌بندی ترافیک بر اساس:
  - آدرس MAC منبع
  - آدرس‌های IP (شبکه یا لیست) و انواع آدرس (پخش، محلی، چندرسانه‌ای، یکپارچه)
  - پورت یا محدوده پورت
  - پروتکل‌های IP
  - گزینه‌های پروتکل (نوع ICMP و فیلدهای کد، پرچم‌های TCP، گزینه‌های IP و MSS)
  - رابط بسته که ازراه‌رسیده یا از طریق آن خارج شده است
  - جریان داخلی و علائم اتصال
  - بایت DSCP
  - محتوای بسته
  - نرخ رسیدن بسته‌ها و شماره دنباله‌ها
  - اندازه بسته
  - زمان رسیدن بسته
- و موارد بیشتر دیگر