Firewall-ul Mikrotik este un instrument puternic pentru protejarea retelei de atacuri malitioase si filtrarea traficului de retea. In acest document, vom discuta in detaliu despre modul in care functioneaza firewall-ul Mikrotik.

Ce este un firewall?

Un firewall este o solutie software sau hardware care se utilizeaza pentru a controla accesul la o retea privata sau la internet. Firewall-ul poate fi configurat pentru a permite sau a bloca traficul in functie de reguli predefinite.

Cum functioneaza firewall-ul Mikrotik?

Firewall-ul Mikrotik functioneaza pe baza de reguli. Regulile de firewall sunt configurate pentru a permite sau a bloca traficul de retea in functie de criterii precum adresa IP, porturile utilizate sau protocolul de retea. Firewall-ul Mikrotik ofera de asemenea si posibilitatea de a proteja reteaua impotriva atacurilor cibernetice precum SYN Flood sau DoS.

Configurarea Firewall-ului Mikrotik

A. Accesarea interfetei grafice a routerului

Pentru a configura firewall-ul Mikrotik, trebuie sa accesati interfata grafica a routerului prin intermediul unui browser web. Inserati adresa IP a routerului in bara de adrese a browserului si autentificati-va utilizand numele de utilizator si parola setate anterior.

B. Crearea regulilor de firewall

Pentru a crea reguli de firewall, trebuie sa accesati meniul Firewall si sa selectati tab-ul "Filter Rules". Aici veti putea vedea o lista cu regulile de firewall existente. Pentru a adauga o noua regula, selectati butonul "Add New" si completati detaliile necesare precum adresa IP sursa, adresa IP destinatie, porturile utilizate sau protocolul de retea.

Regulile de Firewall Mikrotik

A. Regula de intrare si iesire

Regula de intrare si iesire permite controlul traficului care intra sau iese din reteaua dvs. Regula de intrare permite controlul traficului care intra in retea, in timp ce regula de iesire permite controlul traficului care iese din retea.

B. Regula de forward

Regula de forward permite controlul traficului care trece prin router-ul Mikrotik si este destinata pentru retelele de tip LAN (Local Area Network). Aceasta poate fi utilizata pentru a permite sau a bloca traficul intre retele diferite, sau pentru a redirectiona traficul catre alte destinatii.

C. Regula de masquerade

Regula de masquerade este utilizata pentru a schimba adresa IP a pachetelor care parasesc reteaua dvs. Acest lucru este necesar atunci cand doriti sa va conectati la internet utilizand o singura adresa IP publica.

Verificarea si testarea Firewall-ului Mikrotik

A. Verificarea regulilor de firewall

Pentru a verifica daca regulile de firewall functioneaza corespunzator, puteti utiliza comanda "ping" pentru a testa conectivitatea catre un anumit dispozitiv sau adresa IP. De asemenea, puteti utiliza si un utilitar precum "traceroute" pentru a urmari traseul unui pachet de date prin retea si pentru a identifica eventuale probleme.

B. Testarea Firewall-ului Mikrotik

Pentru a testa daca firewall-ul Mikrotik protejeaza impotriva atacurilor cibernetice, puteti utiliza instrumente de testare a vulnerabilitatilor precum "Nmap" sau "Metasploit". Aceste instrumente pot fi utilizate pentru a identifica eventuale probleme de securitate si pentru a verifica daca firewall-ul Mikrotik poate proteja impotriva acestora.

V. Protectia Impotriva Atacurilor

A. Protejarea impotriva atacurilor de tip SYN Flood

Atacurile de tip SYN Flood sunt utilizate pentru a suprasolicita un server sau o retea prin trimiterea unui numar mare de cereri de conectare SYN. Pentru a proteja impotriva acestor atacuri, puteti utiliza firewall-ul Mikrotik pentru a limita numarul de cereri de conectare SYN pe secunda.

B. Protejarea impotriva atacurilor de tip Smurf Attack

Atacurile de tip Smurf Attack sunt utilizate pentru a suprasolicita un server sau o retea prin trimiterea unui numar mare de cereri de ping catre adrese IP broadcast. Pentru a proteja impotriva acestor atacuri, puteti utiliza firewall-ul Mikrotik pentru a limita numarul de cereri de ping pe secunda.

C. Protejarea impotriva atacurilor de tip DoS si DDoS

Atacurile de tip DoS (Denial of Service) si DDoS (Distributed Denial of Service) sunt utilizate pentru a suprasolicita un server sau o retea prin trimiterea unui numar mare de pachete de date. Pentru a proteja impotriva acestor atacuri, puteti utiliza firewall-ul Mikrotik pentru a limita numarul de pachete de date care pot fi procesate de catre router.

Regulile NAT (Network Address Translation)

sunt utilizate pentru a transforma adresele IP si porturile de comunicare ale unui pachet de date in alte adrese si porturi, astfel incat sa poata fi transmise prin intermediul unei retele si sa ajunga la destinatia dorita. NAT este utilizat in mod obisnuit pentru a permite mai multor dispozitive sa se conecteze la internet utilizand o singura adresa IP publica sau pentru a permite conexiunea catre o retea privata din exterior.

In general, exista doua tipuri principale de reguli NAT: reguli de masquerade si reguli de destinatie.

Regulile de masquerade sunt utilizate pentru a schimba adresa IP a pachetelor care parasesc reteaua dvs. Acest lucru este necesar atunci cand doriti sa va conectati la internet utilizand o singura adresa IP publica. In acest caz, adresa IP a pachetelor este schimbata cu adresa IP publica a router-ului, astfel incat traficul sa poata fi transmis prin intermediul retelei publice catre destinatia dorita.

Regulile de destinatie sunt utilizate pentru a redirectiona traficul catre dispozitivele din reteaua privata. Aceste reguli sunt configurate pentru a permite traficul catre adresele IP si porturile de comunicare ale dispozitivelor din reteaua privata. Acest lucru permite dispozitivelor din reteaua privata sa fie accesate din exterior si sa comunice cu alte dispozitive sau servicii din reteaua publica sau din alte retele.

Pentru a configura reguli NAT in Mikrotik, trebuie sa utilizati interfata de administrare a router-ului si sa creati o regula noua pentru fiecare tip de trafic pe care doriti sa il redirecionati sau sa il masquerade-uiti. Regulile NAT sunt configurate utilizand adrese IP si porturi de comunicare, precum si adrese de retea si protocoale de comunicare.

Este important sa acordati o atentie deosebita securitatii atunci cand configurati regulile NAT, deoarece acestea pot permite traficul de retea sa treaca prin reteaua dvs. si pot face reteaua vulnerabila la atacuri cibernetice. Asigurati-va ca utilizati parole puternice si autentificare multi-factoriala pentru a proteja impotriva accesului neautorizat la router si ca configurati regulile NAT in concordanta cu cele mai bune practici de securitate cibernetica.

QoS (Quality of Service)

Se refera la un set de tehnici si politici de retea utilizate pentru a gestiona si controla fluxul de trafic prin retea, astfel incat sa se asigure o calitate a serviciilor (QoS) adecvata pentru diferite tipuri de aplicatii si servicii de retea. Conceptele QoS includ prioritizarea traficului, limitarea sau modelarea traficului si controlul congestiei.

Pentru a intelege cum functioneaza QoS, trebuie sa se inteleaga cum functioneaza retelele de comunicatii. In general, traficul de retea este format din pachete de date care circula prin intermediul retelei catre destinatia lor. Traficul de retea poate fi de diferite tipuri, cum ar fi trafic de voce, trafic de date sau trafic de streaming video.

In cazul in care reteaua este supra-aglomerata sau traficul nu este gestionat in mod adecvat, aceasta poate duce la intarzieri, pierderi de pachete si, in cele din urma, la o experienta de utilizare proasta. Pentru a evita aceste probleme, QoS utilizeaza o serie de tehnici si politici de retea pentru a gestiona traficul si a asigura ca aplicatiile critice beneficiaza de banda suficienta si de latenta redusa.

Una dintre cele mai importante tehnici QoS este prioritizarea traficului. Aceasta tehnica implica alocarea prioritatii diferite pentru diferite tipuri de trafic, astfel incat traficul de voce sau de video sa primeasca o prioritate mai mare decat traficul de date sau de actualizare software. Prioritizarea traficului se bazeaza pe definirea unor reguli si politici de retea care determina care tipuri de trafic trebuie sa aiba prioritate mai mare si care tipuri trebuie sa aiba prioritate mai mica.

O alta tehnica importanta QoS este limitarea sau modelarea traficului. Aceasta tehnica implica limitarea sau restrangerea traficului, astfel incat traficul de aplicatii mai putin critice sa nu consume intreaga banda a retelei, in detrimentul aplicatiilor critice. Limitarea sau modelarea traficului se bazeaza pe definirea unor limite maxime pentru viteza sau volumul de date pentru anumite tipuri de trafic, astfel incat sa se asigure ca aplicatiile critice beneficiaza de o banda suficienta si ca traficul de aplicatii mai putin critice nu poate depasi o anumita limita.

Controlul congestiei este o alta tehnica importanta QoS. Aceasta tehnica se refera la gestionarea traficului de retea in timp real, astfel incat sa se evite supra-aglomerarea si congestionarea retelei. Controlul congestiei se bazeaza pe utilizarea algoritmului de control al congestiei, care poate detecta supra-aglomerarea retelei si poate reduce automat viteza de transmisie pentru a preveni pierderile de pachete si intarzierile.

In general, QoS este utilizat pentru a asigura o experienta de utilizare buna pentru aplicatiile critice si pentru a optimiza utilizarea retelei. Pentru a implementa QoS, este necesar sa se defineasca politici de retea si reguli care sa determine prioritatile si limitele de banda pentru diferite tipuri de trafic.

Pentru a implementa QoS pe un router Mikrotik, se pot utiliza diferite tehnici si instrumente, cum ar fi:

1. Clasificarea traficului: Aceasta tehnica implica identificarea si clasificarea traficului in functie de tipul si sursa acestuia. Aceasta poate fi realizata prin utilizarea diferitelor criterii, cum ar fi adresa IP sursa, adresa IP destinatie, portul sursa, portul destinatie, protocolul de transport, tipul de aplicatie etc.

2. Marcarea traficului: Aceasta tehnica implica marcarea traficului clasificat cu etichete sau marcaje specifice. Aceste marcaje pot fi utilizate pentru a aplica reguli de QoS pentru traficul respectiv.

3. Prioritizarea traficului: Aceasta tehnica implica alocarea de prioritati diferite pentru traficul marcata. Aceste prioritati pot fi utilizate pentru a asigura ca traficul de voce sau de video beneficiaza de o banda suficienta si de o latenta redusa, in timp ce traficul de date sau de actualizare software poate fi limitat sau modelat.

4. Limitarea sau modelarea traficului: Aceasta tehnica implica limitarea sau modelarea traficului, astfel incat traficul de aplicatii mai putin critice sa nu consume intreaga banda a retelei. Aceasta poate fi realizata prin utilizarea diferitelor tehnici, cum ar fi limitarea vitezei de transmisie, modelarea traficului, limitarea volumului de date, limitarea numarului de conexiuni etc.

5. Controlul congestiei: Aceasta tehnica implica gestionarea traficului in timp real, astfel incat sa se evite supra-aglomerarea si congestionarea retelei. Aceasta poate fi realizata prin utilizarea algoritmului de control al congestiei, care poate detecta supra-aglomerarea retelei si poate reduce automat viteza de transmisie pentru a preveni pierderile de pachete si intarzierile.

Pentru a implementa QoS pe un router Mikrotik, este necesar sa se defineasca politici si reguli de retea care sa determine prioritatile si limitele de banda pentru diferite tipuri de trafic. Aceste politici si reguli

pot fi definite prin intermediul unor instrumente si aplicatii specifice, cum ar fi Simple Queue, Queue Tree, Fast Track, Firewall, RouterOS Scripts etc.

In general, implementarea QoS pe un router Mikrotik poate imbunatati semnificativ performanta si experienta de utilizare a retelei, asigurand o banda suficienta si o latenta redusa pentru aplicatiile critice, in timp ce traficul de aplicatii mai putin critice este limitat sau modelat pentru a evita supra-aglomerarea si congestionarea retelei.

Concluzie

Firewall-ul Mikrotik este un instrument puternic pentru protejarea retelei de atacuri malitioase si filtrarea traficului de retea. Regulile de firewall permit controlul traficului in functie de criterii precum adresa IP, portul de comunicare sau protocolul utilizat. Acesta poate fi configurat si personalizat pentru a se potrivi nevoilor specifice ale retelei dvs. si poate fi utilizat pentru a proteja impotriva unui numar mare de atacuri cibernetice, precum atacurile de tip SYN Flood, Smurf Attack, DoS si DDoS.

Pentru a configura si utiliza firewall-ul Mikrotik, trebuie sa aveti cunostinte solide despre retele si protocoale de comunicare, precum si despre tehnologii de securitate cibernetica. In plus, trebuie sa urmati cele mai bune practici de securitate cibernetica, precum actualizarea regulata a software-ului si a echipamentelor de retea, utilizarea de parole puternice si autentificare multi-factoriala si mentinerea regulata a backup-urilor de date.

In concluzie, firewall-ul Mikrotik este un instrument puternic si esential pentru orice retea care doreste sa protejeze impotriva atacurilor cibernetice si sa filtreze traficul de retea. Configurarea si utilizarea sa trebuie sa fie efectuate cu mare atentie si cunostinte solide despre tehnologii de securitate cibernetica, dar cu efortul potrivit, aceasta poate fi realizata cu succes si poate oferi o protectie excelenta impotriva atacurilor cibernetice.