**Universitatea Politehnica Bucuresti**

**Facultatea de Electronica, Telecomunicatii si Tehnologia informatiei**

**Firewall**

**Tema de casa Retele de calculatoare**

 **Studenti:**

 **Palaga Cosmin – 442A**

 **Matei Vlad – 442A**

**2015**

**Cuprins**

**Descriere generala 3**

**Filtrarea de pachete 5**

**Serverul Proxy 6**

**Translatarea de adrese (NAT) 9**

**Bibliografie 13**

**FIREWALL**

**(Palaga Cosmin)**

**DESCRIERE GENERALA**

Firewall-ul este un sistem de securitate care controleaza traficul unei retele, bazandu-se pe un set aplicat de reguli, stabilind o bariera intre o conexiune interna, de incredere, si alt tip de conexiune, spre exemplu, Internetul, care se presupune a nu fi sigura din punct de vedere al datelor. Acesta exista ca software sau ca aparat hardware. Foarte multe firewall-uri de tip hardware ofera functionalitati in plus retelei interne pe care o protejeaza, cum ar fi preluarea rolului de server DHCP (Dynamic Host Configuration Protocol) pentru acea retea. Multe sisteme de operare includ firewall-uri de tip software pentru a proteja computerul respectiv de amenintari din partea internetului.



Un firewall, in general, va filtra:

- IP-uri individuale (host-uri) si/sau retele

- Porturi (21, 22, 23, 25, 80, etc)

- Pachete

- Protocoale (ex. TCP, UDP, ICMP etc).

Firewall-ul inspecteaza fiecare pachet primit dinspre/spre reteaua pe care dorim sa o protejam si, pe baza unor reguli de filtrare, va stabili daca un anumit pachet va fi lasat sau nu sa treaca. Este de asemenea posibila notificarea celui care trimite ca pachetele nu au fost lasate sa treaca. Ordinea regulilor in tabela de filtrare este foarte importanta. De obicei aceasta este sursa majoritatii erorilor ce apar la un firewall.

Firewall-urile pot fi clasificate in patru mari clase:

-integrate in routere: sunt folosite pentru a inlatura neajunsul anterior. Ele nu pot sustine acelasi numar de conexiuni dar se descurca mai bine in topologii mai complexe, unde este nevoie de facilitatile unui router. Multe produse oferta facilitati de firewall integrate in routere, de la module de firewall pentru routere high-end, pana la routere extrem de compacte, dedicate utilizarii in retele SOHO.

-integrate in servere: sunt implementate ca un software aditional peste un sistem de operare de retea (Linux, NT, Win2K, Novell, Unix). Exemple de astfel de pachete software sunt: Netfilter, Microsoft ISA Server, etc. Ele sunt comparabile ca facilitati si performante cu firewall-urile integrate in routerele de nivel mediu.

-dedicate: sunt masini ce ruleaza un sistem de operare special conceput pentru filtrarea de pachete si translatarea de adrese. Exemple de astfel de firewall-uri sunt sistemele PIX sau CheckPoint. Aceste sisteme sunt capabile sa sustina un numar mare de conexiuni, dar facilitatile de rutare sunt extrem de limitate. Pentru o retea simpla se poate folosi firewall-ul ca router, insa pentru retelele mai complexe este necesar un router.

-personale: sunt instalate pe calculatoarele personale. Ele sunt concepute pentru a preveni atacuri doar asupra calculatorului care ruleaza. Este important de retinut ca aceste tipuri de firewall nu sunt optimizate pentru retele intregi de calculatoare. Exemple de firme ce produc firewall-uri personale sunt McAfee si Symantec.

**FILTRAREA DE PACHETE**

**(Palaga Cosmin)**

Filtrarea de pachete este procesul prin care firewall-ul lasa sa treaca in reteaua locala doar anumite pachete, pe baza unor reguli. Filtrarea de pachete este folosita pentru a proteja o retea de atacuri din exterior (Internet) si se realizeaza la nivelurile OSI 3 si 4. Regulile de filtrare sunt formate dintr-o parte care identifica pachetul si o parte care specifica cum sa se trateze pachetul. In partea de identificare se poate specifica adresa sursa, adresa destinatie, adresa de retea sursa, adresa de retea destinatie, protocolul (TCP, UDP, ICMP), portul sursa sau destinatie (doar pentru TCP sau UDP), tipul mesajului (pentru ICMP), interfata de intrare sau iesire, adresele de nivel doi, etc. Partea de tratare a pachetului specifica ce anume trebuie facut cu pachetele identificate de regula. Pentru filtrare exista in general 3 posibilitati de tratare: acceptare, ignorare sau respingere. In cazul acceptarii, pachetul este lasat sa treaca. In cazul ignorarii pachetului nu este lasat sa treaca si nu se trimite notificare catre sursa. In cazul respingerii pachetul nu este lasat sa treaca, dar se trimite notificare catre sursa (un mesaj ICMP al carui tip poate fi, in unele implementari, ales de cel care construieste regula; de cele mai multe ori se foloseste un mesaj ICMP de tip port-unreachable).

**Filtrare de pachete si translatare de adrese avansata**

Anumite protocoale, datorita felului in care sunt concepute, pot sa nu functioneze corect atunci cand clientul si serverul sunt separate de un firewall care filtreaza pachete sau implementeaza PAT. In general, pentru astfel de protocoale clientul si serverul negociaza un port pentru client si apoi serverul initiaza o conexiune catre client pe portul negociat. Din aceasta cauza, implementarea unui mecanism de filtrare care sa permita functionarea acestui protocol, dar sa protejeze statia de atacuri din exterior, se complica extrem de mult. La fel stau lucrurile si pentru PAT.

Exemplu de astfel de protocoale : FTP.

Protocolul FTP foloseste doua porturi:

- portul de date (ftp-date)

-portul de comenzi (ftp-comenzi).

La conectarea la server, clientul initiaza o conexiune catre portul ftp-comenzi. In momentul in care clientul doreste transferul unui fisier el va pregati un port pe care va asculta cereri de conexiuni de la server, dupa care va trimite pe canalul de comenzi un mesaj in care i se cere serverului fisierul de transferat si in care ii trimite serverului portul pe care clientul asculta. Serverul va initia apoi o conexiune de pe portul ftp-date catre portul specificat de client. Aceste este modul de functionare normal pentru protocolul FTP. Clientul poate fi insa configurat sa ceara de la server un mod de lucru pasiv, in care doar clientul initiaza conexiuni. Fie o situatie in care dorim sa utilizam filtrarea de pachete pentru a proteja reteua locala de atacuri din exterior. Astfel, pe firewall nu vom permite ca statiile din exterior sa initieze conexiuni catre statiile din interior. Din acest motiv, in momentul in care o statie locala va incerca sa transfere un fisier in mod normal de pe un server de FTP, firewall-ul va bloca incercarea de deschidere a unei conexiuni a serverului catre client. Cum portul este negociat de client, problema aparuta nu se poate rezolva foarte simplu. Singura solutie posibila este ca firewall-ul sa analizeze toate pachetele schimbate de client si server si sa identifice portul negociat. Cu aceasta informatie va putea apoi permite stabilirea conexiunii initiate de server cu clientul. Folosirea unei astfel de abordari este denumita stateful inspection sau connection tracking.

**SERVERUL PROXY**

**(Palaga Cosmin)**

In retelele de calculatoare, proxy-ul reprezinta un server ce joaca rolul unui intermediar pentru cererile clientilor care cauta anumite date in reteaua externa. Un client se conecteaza la proxy cerand anumite informatii sau servicii, precum fisiere, conexiuni, pagini de internet sau alte resurse aflate pe un alt server.

Scopurile unui proxy pot fi:

• Pastrarea anonimatului clientilor din spatele sau ( pentru securitate )

• Cresterea vitezei de acces la resursele cerute de catre client folosind memoria cache

• Prevenirea descarcarii aceluiasi material de mai multe ori ( si salvarea benzii de internet)

• Pentru colectionarea datelor statistice ( supravegherea angajatilor unei companii )

• Scanarea fisierelor transmise si verificarea lor impotriva malware-ului

• Scanarea continului pachetelor de date pentru a prevenit pierderea de pachete7

• Accesul sau restrictia clientilor

**Tipuri de servere proxy:**

-**open proxy**: expediaza date si este accesibil oricarui utilizator al Internetului. Se estimeaza ca ar exista sute de mii de proxy-uri de acest tip pe Internet. Un proxy deschis anonim permite utilizatorului sa isi ascunda adresa IP in timp ce navigheaza pe Web.

Un computer poater juca rolul unui proxy de tip open fara ca posesorul acestuia sa stie. Acest lucru este posibil din cauza unei greseli de configurare a softwareului folosit ca firewall, sau din cauza unei infectii cu malware. Proxy-urile open prezinta un risc pentru operatori deoarece pot incalca diferite legi. Aceste sisteme sunt folosite pentru accesarea frauduloasa a computerelor din retele externe, sau pentru transferul de fisiere cu continut ilegal. Consumul excesiv de banda, ducand la depasirea acesteia atunci cand reteaua este supraincarcata. Configurarea gresita a unui proxy open poate permite accesul catre subretelele private sau DMZ. Din cauza configurarii gresite un proxy open poate functiona foarte greoi, cu viteze sub 14,4 kbit/s.



-**reverse proxy**: apare ca un server obisnuit. Solicitarile sunt transmise unuia sau mai multor servere proxy, acolo unde sunt procesate. Raspunsul de la serverul proxy este inapoiat ca si cum ar fi venit direct de la serverul de origine, clientul neavand cunostinta cu privire la acesta. Acest tip de proxy se instaleaza de obicei in apropierea unui sau mai multor servere web. Tot traficul ce vine din internet ce are ca destinatie unul din serverele web din retea va trece prin proxy.

Criptarea: site-urile web securizate create folosesc proxyurile de tip “reverse” deoarece criptarea SSL ( Secure Sockets Layer ) se face direct pe server. Acest lucru este posibil datorita echipamentelor harware dedicate criptarii SSL aflate in server. Criptarea cu ajutorul proxy-ului “reverse” se poate face simultan pentru mai multe echipamente conectate. Acest lucru atrage dupa sine utilizarea aceluiasi DNS ( Domain Name Server) si aceleiasi adresa IP.

Impartirea traficului in mod egal: proxy-uri ca JSCAPE MFT pot face automat impartirea in mod egal a traficului intre serverele de transfer din retea si asigura o disponibilitate foarte mare a informatiilor. Astfel se elimina timpii pierduti la accesarea datelor, iar in cazul companiilor se pot observa cresteri ale productivitatii. In cazul in care un server se defecteaza sau nu mai poate fi folosit, tehnici precum “round robin” folosite de catre proxy vor trimite tot traficul catre celelalte servere ramase online in retea.

 

**FIREWALL PROXY SERVER**

**(Matei Vlad)**

Opereaza in stratul aplicatiei firewall-ului unde ambele capete ale conexiunii sunt fortate sa conduca sesiunea prin proxy. Acest lucru este posibil prin crearea si rularea unui proces in firewall care dubleaza un serviciu ca si cum acesta ar rula pe gazda finala.

Un firewall proxy server practic transforma o sesiune care are doua capete intr-o sesiune ce implica patru capete, procesul intermediar simuland cele doua gazde reale.

Firewall-ul realizeaza conexiunea catre server folosind propria adresa sursa.

Firewall-ul poate opțional sa analizeze pachetele la nivel superior sau sa logheze anumite informatii.

 

**Translatarea de adrese (NAT)**

**(Matei Vlad)**

Translatarea de adrese sau NAT (Network Address Translation) este procesul prin care un ruter modifica adresele sursa (SNAT) sau destinatie (DNAT) din anumite pachete care trec prin ruter pe baza unor reguli. Putem considera ca translatarea adreselor este o functie definita pe o multime de adrese (A) cu rezultate intr-o alta multime de adrese (B). Astfel, fiecare pachet cu o adresa sursa sau destinatie (dupa cum este specificat in regula) din multimea A va fi inlocuita cu o adresa din multimea B.

 Se spune ca avem o translatare de adresa statica daca multimile A si B sunt fiecare formate dintr-un singur element. In caz contrar avem o translatare de adrese dinamica. Avantajul folosirii translatarii de adrese dinamice consta in faptul ca se poate folosi o partajare a adreselor rutabile disponibile organizatiei. Astfel, calculatoarelor din reteaua locala li se aloca adrese private, iar routerul va face o translatare de adrese dinamice din multimea de adrese private in multimea de adrese publice alocate organizatiei. Se observa insa ca aceasta abordare permite ca doar Card(B) calculatoare din reteaua locala sa aiba conversatii TCP sau UDP cu Internetul.

Alt avantaj al folosirii translatarii de adrese este acela ca se ascunde astfel exteriorului maparea reala de adrese. Translatarea de adrese statica se foloseste atunci cand in reteaua locala avem un server pe care dorim sa il accesam din exterior. In acest caz se face o mapare unu la unu intre adresa din interior si cea din exterior.

O metoda mai avansata de translatare de adrese o reprezinta PAT (Port Address Translation), uneori denumita si NAT overloaded. Aceasta metoda permite un numar de aproximativ 64000 de conversatii simultane de la orice host intern catre exterior cu o singura adresa externa. Implementarea inlocuieste pachetul din reteaua locala cu adresa sursa S, adresa destinatie D, portul sursa P, portul destinatie Q, cu altul nou ce va avea adresa sursa M (adresa ruterului), adresa destinatie D, portul sursa K. Portul destinatie nu se schimba. De asemenea se memoreaza asocierea (S,P) - K. Daca un pachet ajunge pe ruter din exterior, avand adresa destinatie M, adresa sursa Q si portul destinatie K, atunci acest pachet va fi inlocuit cu un altul cu adresa destinatie S, adresa sursa Q, portul destinatie P si va fi trimis in reteaua locala. Portul sursa nu se schimba. Un caz special al PAT il reprezinta redirectarea. In acest caz se va inlocui pachetul primit din reteaua locala avand adresa sursa S, adresa destinatie D, portul P cu un altul avand adresa sursa S, adresa destinatie M (adresa ruterului), portul R (portul in care se face redirectarea, specificat de utilizator). Redirectarea este in general folosita pentru a implementa un proxy transparent, caz in care pe ruterul M portul R asculta un proxy configurat pentru proxy transparent.

**Tipuri de NAT:**

**(Matei Vlad)**

-„full-cone” NAT: odata ce o adresa interna (iAddr:iPort) este mapata unei adrese externe (eAddr:ePort), orice pachete din iAddr:iPort sunt trimise prin eAddr:ePort. Orice gazda externa poate trimite pachete catre iAddr:iPort, trimitand pachete catre eAddr:ePort.



-„port restricted cone” NAT: o gazda externa (hAddr:hPort)  poate trimite pachete catre iAddr:iPort, trimitand pachete catre eAddr:ePort numai daca iAddr:iPort a trimis inainte un pachet catre hAddr:hPort.

-„restricted cone” NAT: o gazda externa (hAddr:any) poate trimite pachete catre iAddr:iPort, trimitand pachete catre eAddr:iPort numai daca iAddr:iPort a trimis inainte un pachet catre hAddr:any. „Any” indica faptul ca numarul portului nu conteaza.



-NAT simetric: fiecare solicitare de la aceeasi adresa IP interna si de la acelasi port catre o adresa IP specifica si catre un port specific, este mapata unei adrese IP si unui port de la o sursa externa; daca aceeasi gazda interna trimite un pachet cu aceeasi adresa si acelasi port dar catre o destinatie diferita, se va folosi o mapare diferita. Doar o gazda externa care primeste un pachet de la o gazda interna poate trimite un pachet inapoi.



**Bibliografie**

### Andrew S. Tanenbaum – Retele de calculatoare, ed a 4-a, Editura Agora

**Răzvan Rughiniș, Răzvan Deaconescu, Andrei Ciorba, and Bogdan Doinea. Rețele locale. Editura Printech, București, 2008**

[**http://en.wikipedia.org/wiki/Firewall\_(computing)**](http://en.wikipedia.org/wiki/Firewall_%28computing%29)

[**www.cs.ubbcluj.ro/~forest/HtmlFolder/firewall.doc**](http://www.cs.ubbcluj.ro/~forest/HtmlFolder/firewall.doc)

[**http://stst.elia.pub.ro/news/RCI\_2009\_10/Teme\_RCI\_2012\_13/TEME\_RCI\_SIVA\_12\_13/AnghelAlexandru/Firewall%20%E2%80%93%20soft%20de%20sistem\_Alexandru%20Anghel.pdf**](http://stst.elia.pub.ro/news/RCI_2009_10/Teme_RCI_2012_13/TEME_RCI_SIVA_12_13/AnghelAlexandru/Firewall%20%E2%80%93%20soft%20de%20sistem_Alexandru%20Anghel.pdf)

[**http://en.wikipedia.org/wiki/Network\_address\_translation**](http://en.wikipedia.org/wiki/Network_address_translation)