**Universitatea Politehnică Bucureşti**

**Facultatea de Electronică, Telecomunicaţii si Tehnologia Informaţiei**

**Port forwarding. Tunelarea SSH.**

**Student: Oprea Cristinel**

**Grupa: 443A**

**Disciplina: Rețele calculatoare**

**Profesor: Ştefan Stăncescu**

**Cuprins:**

1. **Port forwarding**
   1. **Necesitatea expedieri de porturi**
   2. **Context; NAT**
   3. **Port forwarding**
   4. **Aplicatii**
   5. **Securitatea**

**2. SSH in port forwarding  
   2.1. Necesitatea tunelarii SSH  
   2.2. Tunelarea cu port forwarding Local  
   2.3. Tunelarea inversa cu port forwarding la distanta**

**2.4. Dynamic Port Forwording**

**3. Bibliografie**

* 1. **Necesitatea expedieri de porturi**

Providerul de servicii internet aloca o adresa IP pentru conexiunea personala la internet. Toate calculatoarele din internet au nevoie de o adresa IP unica. Apare atunci problema in care dorim sa folosim mai multe calculatoare dar avem la dispozitie o singura adresa.

* 1. **Context; NAT**

Ruterele au o functie integrata numita Network Address Translation, sau NAT. In interiorul retelei, caculatoarele au adrese ca 192.168.1.100. Toate adresele in intervalul 192.168. sunt considerate “private” sau “reservate”.Acestea sunt official asignate de catre JANA pentru a fi utilizate in interiorul retelelor private. Ruterul asigneaza automat astfel de adrese fiecarui calculator conectat, via DHCP. In acest mod calculatoarele comunica cu ruterul si cu alte calculatoare in cadrul unei retele.

Ruterul are o interfata separata de retea care se conecteaza la internet. Acesta interfata foloseste adrese foarte diferite fata de cea furnizata de providerul ISP. Ruterul foloseste adresa de la ISP pentru a comunica cu alte calculatoare din internet. Calculatoarele din retea private au o adresa IP private non-rutabila, insemnand ca daca acestea trimit direct pachete in internet, pachetele vor fi anulate automat(pachetele cu adresa private nu au voie sa traverseze internetul din motive de stabilitate), insa ruterul are o adresa ruterul are o adresa rutabila. Network Address Translation, dupa cum sugereaza numele, translateaza aceste doua adrese, permitand astfel ca mai multe calculatoare din interiorul retelei sa apara ca un computer cu o singura adresa.

De fiecare data cand , un calculator din interiorul retelei doreste sa se conecteze la un alt calculator din retea, trimite cererea de conectare catre ruter (sties a o trimita catre ruter pentru ca parametru Default Gateway este setat pe adresa routerului). Ruterul preia aceasta cerere (cerere SYN in TCP/IP) si schimba adresa sursei dintr-o adresa private IP a calculatorul intr-o adresa publica a ruterului. Aceasta procedura se inregistreaza intr-o baza de date (tabelul NAT) pentru a stii mai tarziu ca aceasta conexiune a fost initializata.

Cand raspunsul vine de la calculatorul la distanta (SYN-ACK), ruterul se uita in tabelul NATsi vede conexiunea pentru host-ul si port-ul ce a fost anterior initializat de catre calculatorul privat din reteaua personala. Apoi, ruterul schimba adresa destinatiei cu adresa private a calculatorului si o expediaza la reteaua personala. In acest fel, pachetele pot sa tranziteze inainte si inapoi intre retele cu ajutorul ruterului care schimba transparent adresele astfel incat sa functioneze. Cand conexiunea se incheie, ruterul o va sterge din tabelul NAT.

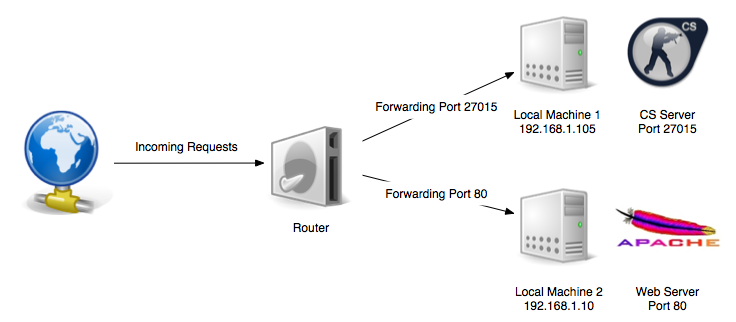
* 1. **Port forwarding**

Port forwarding este raspunsul la problema mai sus enuntata. Este o metoda de a spune ruterului la ce calculator trebuie sa ajunga conexiunile primite din internet. Exista mai multe metode pentru a face acest lucru.

* Faux-DMZ: multe rutere au o proprietate numita DMZ., Demilitarized Zone, care este o configuratie de securitate a retelolor. DMZ pe ruterele personale este numit faux-DMZ, pentru ii lipsesc unele proprietati al DMZ-ului original. Ceea ce face este foarte simplu: toate conexiunile venite din internet vor fi directionate catre un calculator specificat. Astfel se seteaza adrese IP in configuratiile ruterului si toate conexiunile venite vor merge la acea adresa.

Port forwarding. Toate cererile de conexiune la retea include un “port”. Acest port este doar un numar, si este modul prin care un calculator stie despre ce pachet este vorba. JANA spune ca portul 80 este utilizat pentru HTTP. Aceasta inseamna ca un pachet primit ce contine portul 80, trebuie sa apartina unei cereri pentru un web server. Port forwarding specific ruterului permite tastarea unui numar de port (sau un interval de porturi) si a unei adrese IP. Toate conexiunile venite cu un numare de port ce se potrivesc cererii vor fi expediate catre calculatorul cu adresa specificata.

* UPnP port forwards: UPnP functioneaza la fel ca port forwarding, dar in loc de a seta manual ruterul, se utilieaza un software de un computer din interiorul reteleicare seteaza automat ruterul.



* 1. **Aplicatii**

Multe din jocurile video multiplayer permit rularea unui server pe calculatorul personal prin care alti parteneri se pot conecta pentru a juca in modul multiplayer. Calculatorul personal nu stie toti userii care vor sa joace, astfel incat acestia trebuie sa trimita o noua cerere de conexiune la calculatorul personal pe care este serverul. Daca nu este nimic configurat la ruter, cererile primite nu vor stii unde se afla serverul in cadrul retelei, asa ca acestea vor fi ignorate (cu mesaj de informare). Asadar, pe ruter se seteaza un port forward cu numarul portului pe care serverul jocului il asteapta, de exemplu 27015, si adresa IP a calculatorului cu serverul de joc.

Un alt exemplu ar fi unul al unei retele locale cu doua masini, unde a doua cu adresa IP 192.168.1.10 gazduieste un site cu ajutorul serverului apache. Asadar, ruterul ar trebui sa expedieze cererile primite cu numarul portului 80 catre a doua masina catre aplicatia apache. Utilizand port forwarding, ambele masini pot rula pe aceeasi retea in acelasi timp.

* 1. **Securitatea**

Unul din lucrurile interesante in legatura cu NAT este ca furnizeaza o Securitate integrate, fara effort. Multe personae se pot uita in internet in cautarea unor masini vulnerabile prin incercarea de a deschide conexiuni cu diverse porturi. Ruterul va anula aceste cereri venite. Aceasta inseamna ca doar ruterul este vulnerabil la atacurile privind conexiunile venite din internet. De observant ca prin setarea destinatiei DMZ se va pierde acest strat de Securitate.

**2.1. Necesitatea tunelarii SSH**Port forwarding via SSH(tunelare SSH) creeaza o conexiune securizata intre un calculator local si o masina la distanta si prin care servicile pot fi retransmise. Pentru ca acesta conexiune este criptata, tunelarea SSH este utila pentru transmiterea informatiei care utilizeaza protocoale necriptate cum sunt IMAP, VNC, IRC.

Un tunel SSH consta intr-un tunel criptat creat in cadrul unei conexiuni SSH. Un tunel SSH poate fi utilizat pentru a transfera trafic necriptat de-a lungul unei retele printr-un canal criptat. De exemplu, putem utiliza un tunel ssh pentru a transfera in siguranta fisiere intre un server FTP si un client, chiar daca serverul FTP nu este criptat insusi. Tunelele SSH furnizeaza un mijloc pentru a evita firewall-ul care poate interzice sau filtra anumite servicii in internet. De exemplu, o organizatie va bloca anumite site-uri utilizand un filtru proxy. Dar utilizatorii ar dorii sa nu aiba traficul monitorizat sau sa le fie interzis accesul la anumite site-uri. Daca userii se pot conecta la un server extern SSH, ei pot crea un tunel SSH pentru a expedia un port dat de pe masina lor locala la portul 80 al web-serverului la distanta printr-un server SSH extern.

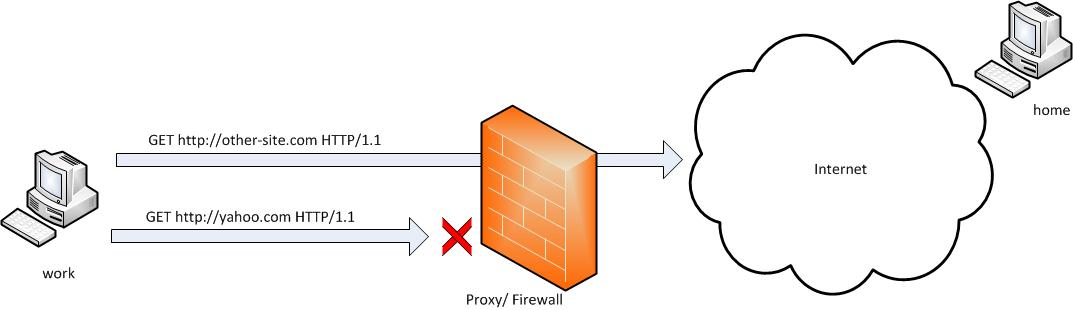
Tunelele SSH pot fi create in multe moduri utilizand diferite metode de port forwarding.

**2.2. Tunelarea cu port forwarding Local**Sa spunem ca site-ul yahoo.com este blocat printr-un filtru proxy la Universitate. Un tunel SSH poate fi creat pentru a evita restrictia. Sa numim masina de la universitate „work” si masina de acasa „home”. „home” trebuie sa aiba o adresa IP publica si sa ruleze un server SSH. Pentru a crea un tunel SSH se executa urmatoarea comanda de la masina „work”

|  |  |
| --- | --- |
|  | ssh -L 9001:yahoo.com:80 home |

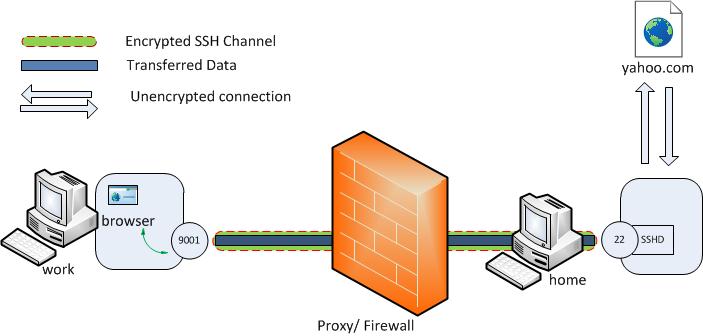
„L” indica faptul ca un port forward local trebuie creat. Sintaxa e urmatoarea:

|  |  |
| --- | --- |
|  | -L <local-port-to-listen>:<remote-host>:<remote-port> |



Astfel clientul SSH de la masina „work” se va conecta la serverul SSH care ruleaza pe masina „home”, legand portul 9001 al „work” sa asculte cererile locale. La capatul celalat, „home” va crea o conexiune la „yahoo.com” la portul 80. Deci „work” nu trebuie sa stie cum sa se conecteze la domeniu. Canalul intre „work” si „home” va fi criptat in timp ce conexiunea intre „home” si „yahoo” va fi necriptata.

In acest mod este posibil sa se navigheze pe yahoo.com visitand <http://localhost:9001> in browserul web al masinii „work”. Calculatorul „home” va juca rolul de gateway si va accepta cereri de la „work” iar apoi va returna informatii.



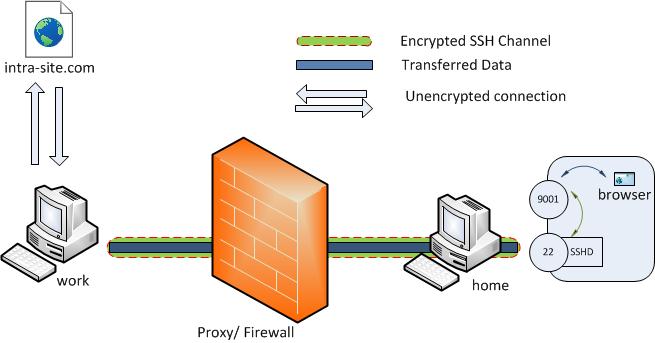
**2.3. Tunelarea inversa cu port forwarding la distanta**

Sa spunem ca este necesar sa ne conectam la un website intern al universitatii de acasa. Firewall-ul universitatii bloacheaza tot traficul care vine. O configurare VPN ar putea fi o solutie, insa una mai costisitoare.

Ca si mai devreme vom initializa tunelul de la masina „work” in spatele firewall-ului. Acest lucru este posibil pentru ca numai receptionare este blocat, cel de expediere permite traficul. In schimb clientul va fi acum definit la masina „home”, iar in loc de optiunea –L vom folosii –R ceea ce specifica initializarea unui tunel invers.

|  |  |
| --- | --- |
| 1 | ssh -R 9001:intra-site.com:80 home (Executed from 'work') |

Odata executata, serverul va lega portul 9001 la masina „home” sa asculte cererile venite care vor fi ulterior rutate intre „home” si „work”, prin canalul SSH creat. Astfel este posibil sa se navigheze intra-site-ul si de a retrimite raspunsul inapoi la „home” prin canalul SSH creat.



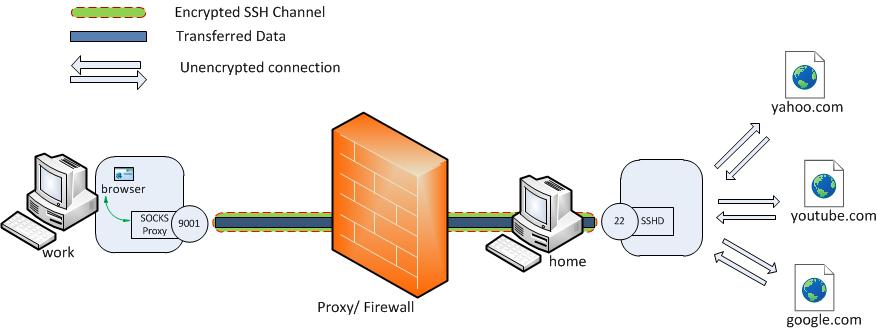
O problema ar mai fi nevoia de a crea un alt tunel daca am avea nevoie sa ne conectam la un alt website in ambele cazuri. Ar fi interesant daca am avea posibilitatea sa evitam traficul proxy la orice website prin tunele SSH create. Aceasta se poate realiza cu ajutorul dynamic port forwardin.

**2.4. Dynamic Port Forwording**

Permite configurarea unui port local pentru tunelarea datelor catre toate destinatiile de la distanta. Totusi, pentru a utiliza aceasta aplicatia client care se conecteaza la portul local ar trebui sa trimita traficul utilizand protocolul SOCKS. In partea de client a tunelului, un proxy SOCKS ar trebui creat, iar aplicatia utilizeaza acest protocol pentru a specifica unde ar trebui trimis traficul ce paraseste celalat capat al tunelului ssh.

|  |  |
| --- | --- |
|  | ssh -D 9001 home (Executed from 'work') |

Aici SSH creeaza un proxy SOCKS ce asculta portullocal 9001 si peste o cerere va ruta trAficul prin tr-un canal SSH intre „work” si „home”. Pentru aceasta este nevoie sa se configureze browserul sa indice catre proxiul SOCKS la portul 9001 al masinii locale.



**3. Bibliografie**

1. help.ubuntu.com
2. http://chamibuddhika.wordpress.com
3. http://superuser.com/