Solutii pentru protectia si securizarea unui INTRANET

Prof.dr. Ion Gh. ROSCA, Ing. Octavian PAIU, Asist.drd. Carmen STANCIU,
Catedra de Informatica Economica, A.S.E., Bucuresti

Conectarea la Internet a sistemului informatic al unei companii o face vulnerabila daca nu este acompaniata de masuri de protectie si securitate a datelor. Aspectele de securitate sunt importante atât pentru companiile care au resurse si informatii confidentiale, cât si pentru cele în care informatiile nu sunt "sensibile". Cele din urma trebuie sa se protejeze pentru a nu deveni baza de atac contra unor retele de interes. Penetrarea unui Intranet nu este o simpla problema de tehnica, pentru ca poate atrage consecinte neasteptate (costuri de refacere a retelei, pierderi de credibilitate si prestigiu, trecerea pe "liste negre"). Articolul de fata ofera câteva solutii pentru protectia si securizarea unui Intranet.
Cuvinte cheie: *proxy, firewall, Kerberos, SOCKS, NIS, NDS, domenii NT.*

Solutii de protectie împotriva accesului neautorizat la Intranet

Ziduri de protectie

Un zid de protectie (*firewall*) este un sistem plasat între reteaua interna (Intranet) si reteaua externa (Internet). Principalul sau rol este de a proteja Intranet-ul în conformitate cu anumite reguli si criterii ce pot fi stabilite prin configurare.

Zidurile de protectie creeaza înregistrari ce includ informatii precum: adresele sursei si destinatiei, numarul de port, tipul aplicatiei, unele informatii de audit dau date suplimentare precum durata sesiunii, numarul de pachete transmise/ receptionate etc. Toate acestea ajuta la identificarea încercarilor neautorizate de acces la Intranet si, totodata, masoara calitatea politicii de securitate.

Principalele cerinte impuse unui firewall sunt urmatoarele:

- Trebuie sa fie capabil sa analizeze întregul trafic, în ambele sensuri, între un Intranet si Internet; în acest mod doar traficul autorizat (conform politicii de securitate adoptate) este permis, eliminând pachetele (mesajele) care ar putea afecta functionalitatea retelei interne.
- Trebuie sa fie capabil sa ascunda adresele din reteaua interna fata de exterior, facând mai dificile potentialele atacuri din afara.
- Trebuie sa suporte traficul din ce în ce mai mare din Internet, ca si vitezele crescânde ale conexiunilor, astfel încât sa nu devina o gâtuire în retea.

În figura 1 este ilustrata configuratia generala a unui firewall.

Tehnici de acces din exterior

♦ **Autentificare si autorizare**

Un aspect important de securitate îl constituie accesul utilizatorilor externi la resursele Intranet-ului. Accesul presupune *autentificarea* (identificarea utilizatorilor care doresc accesul la serverele sau aplicatiile din Intranet) si *autorizarea* (stabilirea drepturilor asupra resurselor sau aplicatiilor). Pentru un acces sigur, este necesara, în primul rând, identificarea si autentificarea utilizatorului care cere accesul si apoi autorizarea pentru folosirea resurselor. Exista mai multe tehnologii care furnizeaza diferite niveluri de autentificare: mecanismele de baza nume/parola functioneaza bine pentru accesul prin modem al utilizatorilor mobili. Solutii mai avansate sunt bazate pe parole "one-time" generate de sisteme de card-uri speciale. Exista si tehnologii intermediare. Se pot instala mai multe niveluri de autorizare si mai multe politici de securitate.

Accesul multiplu al utilizatorilor este asigurat de un server specializat.

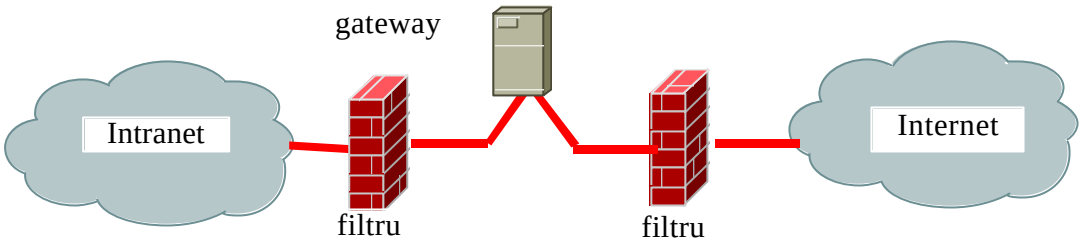

Fig.1. Configuratia generala a unui zid de protectie

♦ **Kerberos**

Kerberos este protocolul de autentificare elaborat în proiectul Athena la MIT, fiind folosit azi în multe sisteme, printre care Windows 2000. Protocolul a trecut prin mai multe versiuni, cele mai cunoscute si utilizate fiind patru si cinci. Kerberos permite utilizatorilor de la statiile de lucru sa acceseze serviciile unui Intranet. Se presupune ca statiile de lucru sunt nesigure si se cere clientului sa se identifice ori de câte ori cere un serviciu. Pentru a simplifica procedeul folosit la autentificare, Kerberos foloseste urmatoarele idei:

- utilizatorul trebuie sa se prezinte sistemului o singura data, la începutul unei sesiuni (prin nume si parola);
- parolele nu sunt niciodata transmise prin retea în clar, ci doar criptate; mai mult, ele nu sunt pastrate în clar în statiile de lucru;
- fiecare utilizator are o parola si fiecare serviciu are o parola;
- singura entitate care cunoaste toate parolele este serverul de autentificare.

♦ **Accesul pe linii comutate**

Accesul prin modem si linii telefonice comutate poate reprezenta una din importantele surse de nesiguranta. Solutiile oferite de Cisco sunt Password Authentication Protocol (PAP) si Challenge Handshake Authentication Protocol (CHAP). Protocolul PAP foloseste o parola partajata, transmisa în clar. Spre deosebire de PAP, CHAP este mai robust, parola nefiind niciodata transmisa în clar. O secventa de acces se deruleaza dupa urmatoarele etape:

- când un utilizator cere o conexiune la retea, ruter-ul sau (din oficiul de comutare) transmite o cerere de acces;
- serverul de acces trimite catre ruter un pachet continând o valoare aleatoare;
- ruter-ul cripteaza parola, ataseaza numarul aleator si transmite un unic raspuns criptat catre serverul de acces;
- serverul verifica identificatorul si parola utilizatorului, folosind informatia din propria baza de date; în cazul reusitei (corectitudinea verificarii), serverul ofera utilizatorului accesul la acele resurse care îi sunt permise prin politica implementata în listele de acces.

În cazul unui numar mare de utilizatori, sau a mai multor puncte de acces, este preferabila gestiunea centralizata a politicilor de autentificare si autorizare, asa cum se regaseste de exemplu în sistemul CiscoSecure.

Servicii si servere de tip proxy

Un server proxy permite evitarea accesarii directe a unor servicii din Intranet, sau identificarea locului exact în care aceste resurse sunt localizate. Un proxy intercepteaza o cerere externa pentru un anumit serviciu, determina daca cererea poate fi satisfacuta si trece cererea server-ului intern corespunzator, fara ca adresa acestuia sa fie dezvaluita clientului extern. Prin ascunderea adreselor resurselor interne, proxy-urile maresc securitatea Intranet-urilor, facând dificila sarcina unor atacatori de a identifica si compromite serviciile Intranet. Figura 2 ilustreaza modul de lucru al unui proxy, pentru protejarea informatiei

confidentiale si a serviciilor dintr-un Intranet.

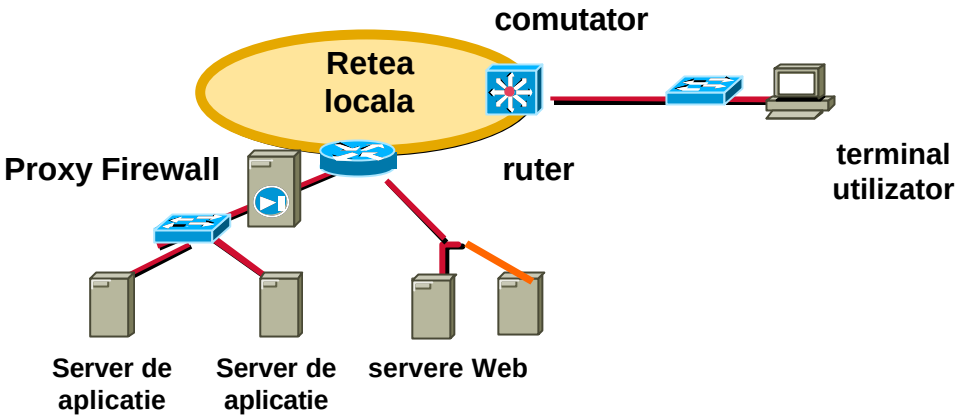

Fig.2. Utilizarea Proxy firewall

Un exemplu este Centri Firewall, de la Cisco. Centri foloseste o arhitectura proprie de kernel, pentru a furniza o solutie foarte performanta. Un alt exemplu de server proxy pentru cache si securitate este Microsoft Proxy Server.

SOCKS

SOCKS este un protocol proxy generic pentru aplicatii de retea bazate pe TCP/IP. El include doua componente, una pentru client si una pentru server. Server-ul este implementat la nivelul aplicatiei, in timp ce clientul este plasat între nivelurile transport si aplicatie. Rolul server-ului proxy este de intermediar între client si server. Când un client trebuie sa se conecteze la un server, el se conecteaza la un proxy SOCKS. Acesta, la rândul sau, se conecteaza la server, pe seama clientului, facând transferul de date si comenzi între client si server. Pentru server-ul de aplicatie, serverul proxy este un client.

SOCKS a fost gândit initial ca un firewall. Datorita simplitatii sale, SOCKS a fost folosit ca proxy generic de aplicatii, în retele virtuale private si pentru aplicatii de tip Extranet. SOCKS V5 are urmatoarele avantaje:

- acces transparent la retea prin multiple servere proxy;
- incorporarea simpla a metodelor de criptare si autentificare;
- gestiunea simpla a politicilor de securitate.

Solutii de protectie si autentificare în Intranet

Cele mai populare sisteme de autentificare existente în sistemele de operare actuale, sunt: NIS - pentru sistemele Unix, NDS - pentru sistemele NetWare si domeniile - pentru Windows NT.

Serviciul NIS- la sistemele Unix

Sistemele Unix, desi construite de la început cu facilitati de conectare în retea, au fost lipsite de un mecanism de autentificare unica. Serviciul aditional care rezolva problema, oferind un mod elegant de lucru si pentru alte servicii din retea, se numeste NIS (Network Information Service). NIS este o baza de date distribuita care permite calculatoarelor dintr-o retea sa partajeze fisiere de parole (*/etc/passwd*), de grup (*/etc/group*), fisiere de informatii despre calculatoare si alte fisiere. Ea faciliteaza o administrare unitara a masinilor din întreaga retea.

NIS a fost lansat de firma Sun în anii ’80 si a reprezentat prima baza de date larg folosita pentru administrarea unei retele. Initial, NIS s-a numit “Yellow Pages”.

Majoritatea comenzilor NIS încep cu prefixul *"yp"*, iar unele referinte catre NIS folosesc înca numele initial, "Yellow Pages".
Fisierele bazei de date NIS sunt denumite *harti* NIS. În functie de sistemul de operare utilizat, ele se gasesc în directoarele */etc/yp*, */usr/etc/yp* sau */var/yp*. Desi aceste fisiere par sa existe pe fiecare calculator, în realitate sunt stocate pe un singur calculator, numit *server master*. Hartile NIS pot fi replicate pe unul sau mai multe calculatoare, numite *server-e slave*. Datorita în special securitatii precare a NIS, dar si a altor cauze, cum ar fi viteza redusa, Sun a elaborat la începutul anilor '90 un nou standard, NIS+.
Serviciul NIS+ nu a preluat nici o portiune de cod de la NIS. Majoritatea comenzilor NIS+ încep cu prefixul *"nis"*. NIS+ este, la rândul sau, o baza de date distribuita. El poate administra retele mari de calculatoare, are incluse facilitati de securitate, permite ca mai multe domenii sa poata fi administrate de oriunde din retea si transfera datele eficient. Însa este foarte complex.

NDS - la Novell Netware
O retea consta din mai multe retele locale conectate între ele. De cele mai multe ori, pentru ca un utilizator sa foloseasca imprimante sau volume de stocare din retea trebuie sa cunoasca localizarea resurselor. Pentru a accesa resursele unui server, utilizatorul trebuie sa se autentifice (login) pe server-ul respectiv. Acest lucru, pe lânga faptul ca este deranjant pentru utilizator, implica si existenta unui cont pe fiecare server. Pe masura ce dimensiunea retelei creste este din ce în ce mai greu de controlat si retinut locul în care se afla o anumita resursa.
Mecanismele de securitate sunt globale si se aplica la întregul acces asupra resurselor din retea. În Netware 3.x, accesul la resurse este controlat prin mecanisme de securitate care sunt locale fiecarui server (baza de date numita *bindery*). Aceasta baza de date nu are o semnificatie globala la nivelul retelei, motiv pentru care toate serviciile sunt centrate pe server-e (server-centric). Pentru a permite un singur acces în retea, proiectantii Netware 4.x si 5.x au creat o baza de date globala numita *Netware Directory Service (NDS).* Acesta este mecanismul prin care versiunile noi de Netware ofera utilizatorilor o vedere logica a retelei.
NDS ofera o baza de date distribuita care functioneaza ca un repertoar (repository) de informatii al tuturor resurselor partajate din retea. Baza de date este distribuita si ierarhica. Cele mai importante avantaje ale NDS sunt:

- o organizare logica a resurselor din retea;
- o singura autentificare în retea;
- vedere globala asupra gestiunii retelei, gestiune care poate fi centralizata sau distribuita;
- independenta fata de localizarea fizica a resurselor;
- partajarea resurselor, cum ar fi partajarea de fisiere si imprimante;
- niveluri multiple de securitate

NDS este bazat pe standardul X.500 al ITU (sau CCITT), permitându-se integrarea cu alte produse de tip repertoar. În cadrul standardului X.500 baza de date echivalenta cu NDS este numita *Directory Information Base* (DIB). În plus, tipurile obiectelor din baza de date pot fi descrise prin ASN.1, fapt care face ca extinderea NDS sa fie usoara. Baza de date NDS nu este legata de o resursa fizica cum ar fi un server, dar trebuie stocata pe un volum fizic. Deoarece dimensiunea bazei de date NDS poate creste mult, nu este stocata pe un server central. Partitii din baza de date sunt distribuite pe volume diferite în puncte strategice din retea. Resursele logice NDS sunt reprezentate de *obiecte.* Deoarece resursele logice sunt asociate cu NDS, ele sunt de multe ori numite obiecte NDS.

Obiectele NDS pot fi vazute, conceptual, ca înregistrari dintr-o baza de date.

Domenii Windows NT si relatii de încredere

Desi sistemul de operare Windows NT este folosit pe scara larga, de multe ori conceptele implicate în spatele acestui sistem nu sunt bine întelese de administratori.

Un domeniu este un set de calculatoare cu o autoritate centrala de securitate, numit controlorul primar de domeniu (PDC, Primary Domain Controller), care acorda accesul la acel domeniu. În mod curent domeniul contine, unul sau mai multe controloare secundare de domeniu (BDC, Backup Domain Controller) care ofera servicii de autentificare distribuita în cazul unor defecte aparute la PDC, precum si echilibrarea încarcarii pentru serviciile de autentificare. În general, functiile de PDC si BDC sunt îndeplinite de server-e Windows NT, dar exista solutii de implementare a lor si pe alte sisteme de operare (Solaris, Digital Unix).

Încrederea este o relatie într-un singur sens, care se poate stabili între domenii, pentru a partaja resursele si a usura administrarea. Aceste relatii permit unui utilizator sau unui grup sa fie creat doar o data într-un set de domenii si sa acceseze resurse din mai multe domenii. Exista mai multe modele de configurarea a încrederii între domenii.

Tehnici de integrare în medii eterogene a solutiilor prezentate

Eterogenitatea este o caracteristica fundamentala a retelelor de calculatoare. Deseori vom întâlni mai multe sisteme de operare coexistând în aceeasi retea. Chiar se recomanda folosirea mai multor sisteme de operare, pentru a rezolva fiecare problema cu cel mai adecvat sistem. Din pacate, cele trei solutii prezentate în acest capitol (domeniile NIS, NDS si NT) sunt proprietare si nu sunt sprijinite direct de ceilalti competitori. Cu toate acestea, prin intermediul unor programe utilitare de la terti sau chiar de la firmele producatoare de sisteme de operare de retea este posibila integrarea a doua sau mai multe astfel de sisteme de autentificare si protectie.

Una din solutiile recomandate de specialisti este convertirea tuturor sistemelor de autentificare pentru a folosi **NDS**. NDS este bazat pe standarde internationale (X.500), este un produs matur si testat îndelung. Aceasta convergenta spre NDS este posibila deoarece exista produsul *NDS for NT* care schimba modul în care se face autentificarea unei statii de lucru NT: nu mai este necesar un domeniu NT, ci este suficienta existenta unui server NDS în retea. Exista solutii NDS si pentru medii Unix (pentru Linux si Solaris). În plus, NetWare poate fi folosit si ca server de conectare sigura din Internet si server de Web, deci aceeasi baza de date NDS poate servi utilizatorii interni, vizitatorii externi si utilizatorii înregistrati ai site-ului Web.

Pentru integrarea NT cu Unix exista doua solutii: ca NT-ul sa foloseasca NIS (exista astfel de clienti, unii chiar în domeniul public) sau ca Unix-ul sa se transforme în controlor de domeniu. Pentru cea de-a doua varianta exista atât produse de firma (Sun ofera controlor primar de domeniu pe Solaris), cât si produse în domeniul public. Samba este unul din produsele din domeniul public de mare succes, care a primit sprijinul marilor producatori Unix - HP, SGI, Compaq. Samba a fost creat cu ideea de a transforma un server Unix în server de fisiere pentru un domeniu NT, dar produsul a evoluat si, la ora actuala, poate prelua functii specifice server-elor NT (browsing sau participare în controlul domeniului).

Concluzii

Pe masura ce tot mai multi utilizatori au acces la Internet si Intraneturi este de asteptat ca "razboiul" Internet sa se intensifice la toate nivelurile: guvernamental, societati si organizatii, cetatean. În

acest context, fiecare utilizator trebuie sa posede un minim de cunostinte privind modalitatile de aparare folosind cel putin "armamentul" standard.

Bibliografie

- Evi Nemeth, s.a. : *"UNIX System Administration Handbook"*,1996.
- Ion Gh. Rosca, Nicolae Tapus, Valentin Cristea, Irina Atanasiu, Bogdan Costinescu, Gavril Gozdea, Floarea Nastase, Stanciu Carmen, Octavian Paiu –*INTRANET* - (133 pagini), Editura ASE, Bucuresti, 1999.
- Ion Gh. Rosca, Nicolae Tapus, Valentin Cristea, Irina Atanasiu, Bogdan Costinescu, Gavril Gozdea, Floarea Nastase, Stanciu Carmen, Octavian Paiu **–** *INTRANET – partea a II-a-*, Editura ASE, Bucuresti, 2000.
- Ion Gh. Rosca, Stanciu Carmen, Octavian Paiu, s.a. - *Noi paradigme ale managementului modern al întreprinderii – Intranet*, Contract nr. 18, cod CNCSIS 55/1999, beneficiar Ministerul Educatiei Nationale, 1999.
- Ion Gh. Rosca, Nicolae Tapus, Valentin Cristea, Irina Atanasiu, Bogdan Costinescu, Gavril Gozdea, Floarea Nastase, Stanciu Carmen, Octavian Paiu - *Solutii arhitecturale pentru subretele de comunicatii utilizate în INTRANET si solutii software suport pentru activitati cooperative în INTRANET*, faza 2.1. - *Solutii pentru protectia si securizarea unui INTRANET*, Contract nr. 131/1999, Act aditional nr. 46/I/18.01.2000, Beneficiar - Agentia Nationala pentru Stiinta, Tehnologie si Inovare, 2000**.**
- Garfinkel s.a.: *"Practical Internet & Unix Security*", O'Reilly & Associates.
- Thorsten Kukuk: *"The LINUX NIS (YP)/NYS/NIS+ HOWTO*", /doc/howto/ NIS-HOWTO (CD-ROM-ul Linux Red Hat), ian. 1998
- Victor Patriciu si colectivul: Securitatea în Unix si Internet, Editura Tehnica, 1998.
- Andrew Tanenbaum, Retele de Calculatoare, Computer Agora Press, 1998.
- SunOS : Paginile de manual NIS+
- ***: Maximum Internet Security: A Hacker's Guide, Editura SAMS, 1999.
- NIS-HOWTO page: http://sunsite.unc.edu/mdw/HOWTO/NIS-HOWTO.html

Documentatii tehnice de referinta:

- CERT (www.cert.org)
- ISS (www.iss.com)
- Verisign (www.verisign.com)
- CISCO (www.cisco.com)
- Netscape (www.netscape.com)
- Novell (www.novell.com)
- Microsoft (www.microsoft.com)