Facultatea de Electronica Telecomunicatii si Tehnologia Informatiei
Universitatea Politehnica Bucuresti

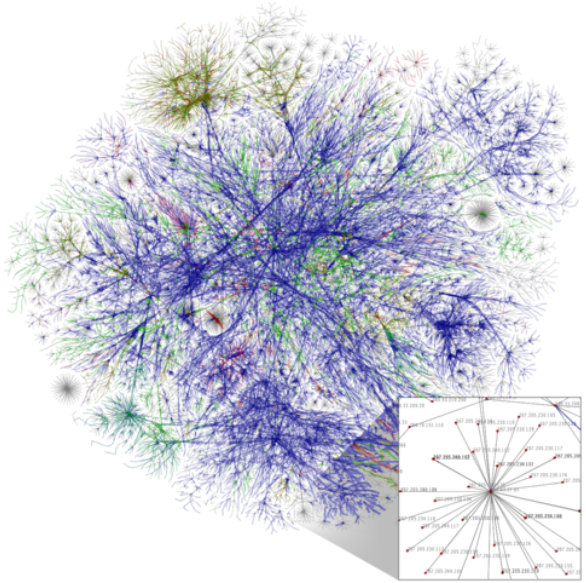
Securitate pe Internet

Coordonator - **Prof. Dr. Ing. Stancescu Stefan**

Masterand SIVA - **Ing. Badea Mihai Bogdan**

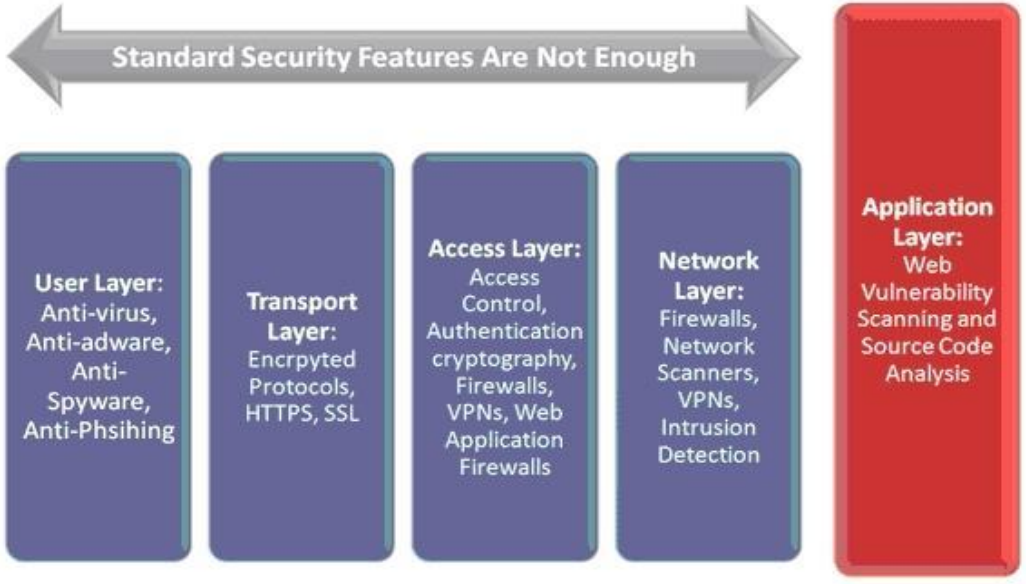
Introducere

Securitatea in Internet este necesara in diverse domenii pentru a proteja, restrictiona accesul la informatii sensibile



Nivele de securitate

Securitatea in Internet poate fi descompusa pe mai multe nivele, acestea fiind prezentate in figura de mai jos



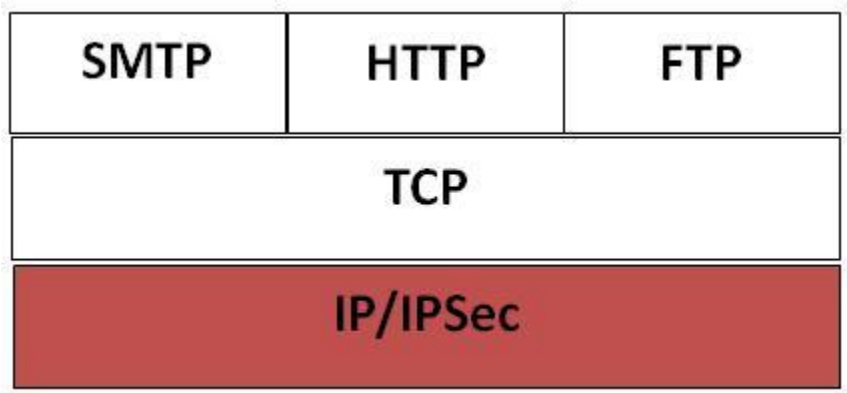
Securitatea la nivel de retea

Securitatea la nivelul retelei - nivelul 3 este asigurata de IPSec, care este un protocol de comunicatii utilizat la securizarea pachetelor Internet Protocol (IP) prin autentificarea si criptarea fiecarui pachet IP al unei sesiuni de comunicatii.

Acest protocol poate fi utilizat pentru protejarea informatiilor intre o pereche de gazde (host-to-host), intre o pereche de porti (retea-retea), sau intre o poarta si o gazda (network-to -host). IPSec reprezintă singura solutie open-source pentru securizarea conexiunilor pe Internet. IPSec poate fi configurat pentru două moduri distincte: modul tunel şi modul transport.

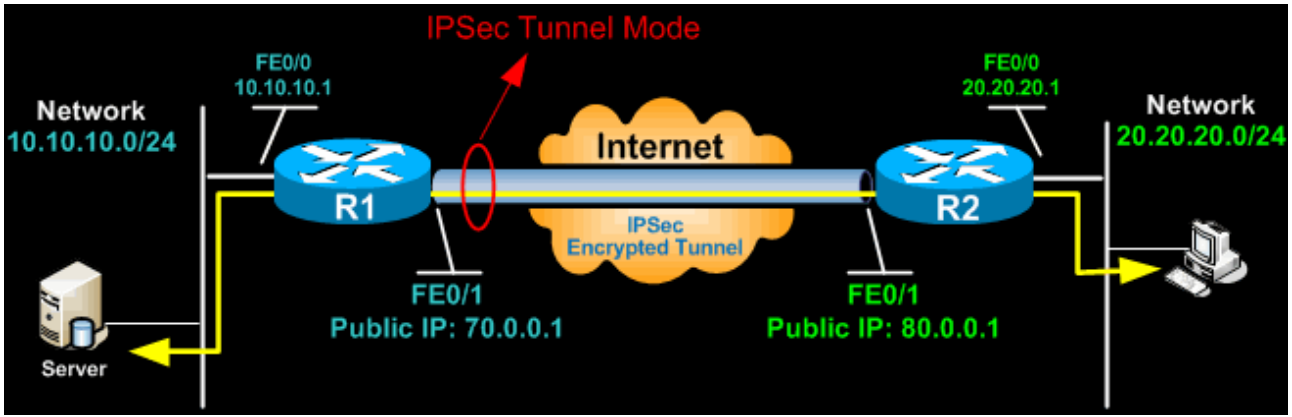
IPSec

Asigurarea securitatii retelei (denumita criptare la nivel de retea) este un procedeu de securitate pe retea care include servicii criptografice la nivelul de transport al retelei – peste nivelul de legatura, dar sub nivelul de aplicatie. Nivelele de transfer in retea sunt layerele 3 si 4 ale modelului de referinta OSI (Open Systems Interconnection), nivelele fiind responsabile pentru conexiune si rutare intre 2 puncte.



IPSec

Utilizand serviciile existente de retea si aplicatie software, criptarea la nivel de retea este transparenta utilizatorului final si functioneaza independent de orice alt proces de criptare utilizat. Datele sunt criptate doar in tranzit, ele fiind in plain-text la cele 2 capete.



Tunelul securizat IPSec.

IPSec

IPSec reprezinta criptarea la nivel de retea care este implementata printr-un ansamblu de standarde IETF (Internet Engineering Task Force) care creaza o platforma pentru comunicatia securizata intre retele IP.

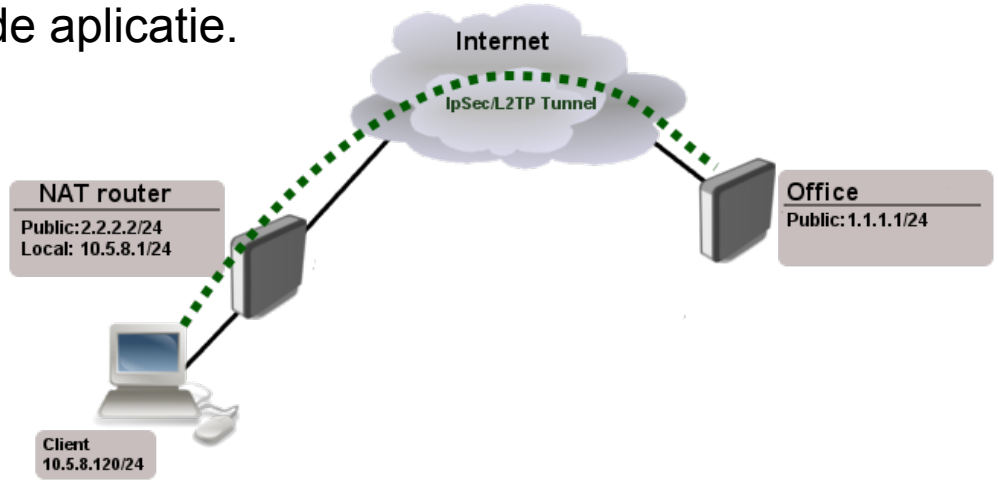
Pachetele criptate apar identice celor necriptate si sunt rutate usor prin orice retea IP. IPSec functioneaza cu ajutorul arhitecturi retelei, ceea ce inseamna ca utilizatorul final si aplicatiile nu trebuiesc modificate in niciun fel.

Protocolul IPSec

Protocolul Ipsec este un ansamblu de securitate end-to-end la nivelul Internet al stivei de protocoale Internet, in timp ce alte sisteme de securitate Internet utilizate majoritar, ca Secure Sockets Layer (SSL), Transport Layer Security (TLS) si Secure Shell (SSH), functioneaza in nivelele superioare ale stivei TCP/IP. In consecinta, IPSec protejeaza orice trafic de aplicatie pe o retea IP.

Protocolul IPSec

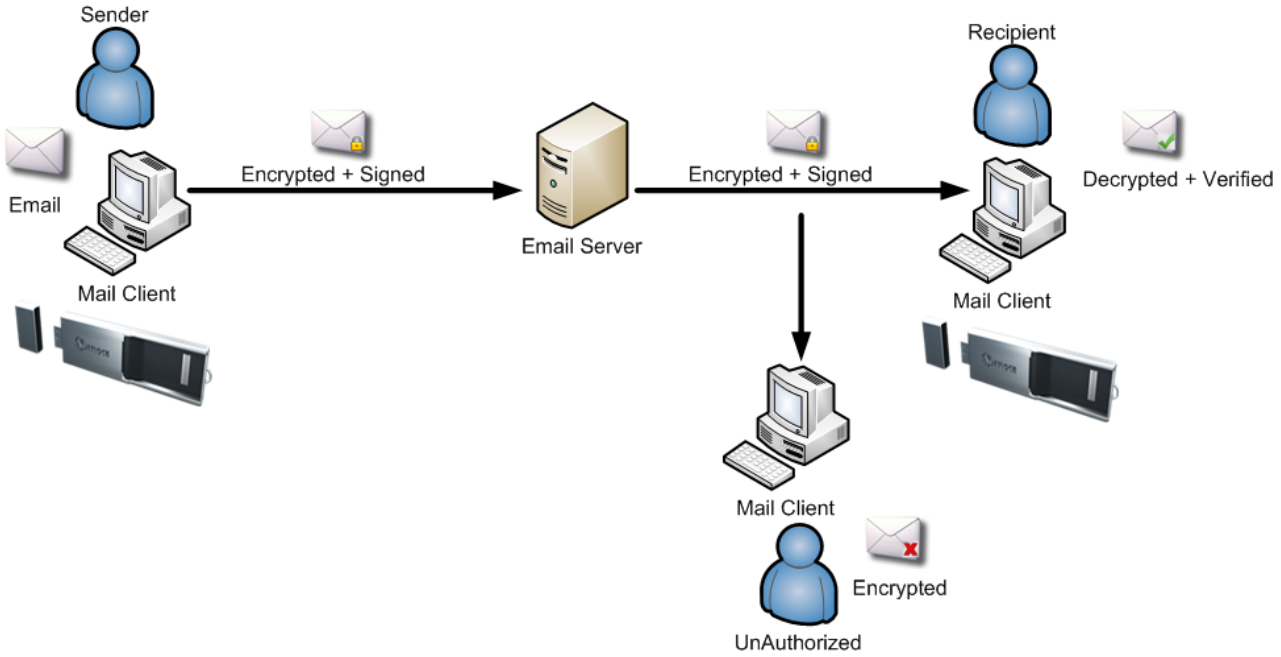
Aplicatiile nu trebuiesc implementate special pentru a utiliza IPSec. Fara IPSec, utilizarea TLS/SSL trebuie implementata in aplicatie pentru a proteja protocoalele de aplicatie.



Securitatea postei electronice

Protejarea emailului de catre un acces neautorizat si analizarea lui este cunoscuta ca securitate electronica.

Securitatea postei electronice

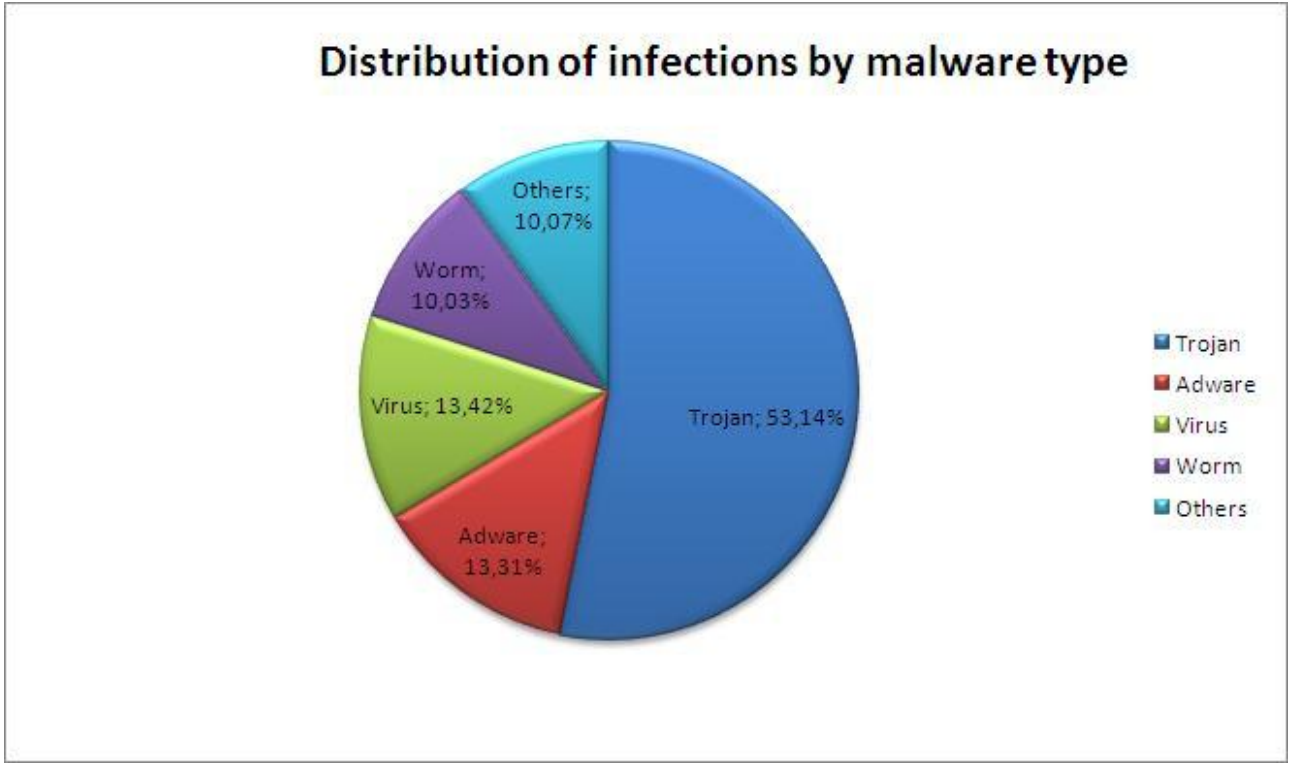


Software malitios

Malware-ul sau software-ul malitios, este un soft utilizat la intreruperea operatiilor unui computer care colecteaza informatii sau capata acces la sisteme private de calculatoare. El poate aparea sub forma de cod, script, continut activ sau alte tipuri de software.

'Malware' este un termen general utilizat la o varietate de forme ostile sau software ostil.

Software malitios



Antivirus

Antivirusul este un program de computer utilizat la blocarea, detectia si eliminarea programelor malitioase. Majoritatea soft-urilor impotriva altor tipuri de malware, cum ar fi Browser Helper Objects, browser hijackers, keyloggers, backdoors, rootkits, trojan horses, worms, malicious LSPs, dialers, adware and spyware.

Securitatea computerelor, incluzand tehnicilor protectiei ingineriei sociale este furnizata in mod comun in serviciile companiilor de antivirusi.

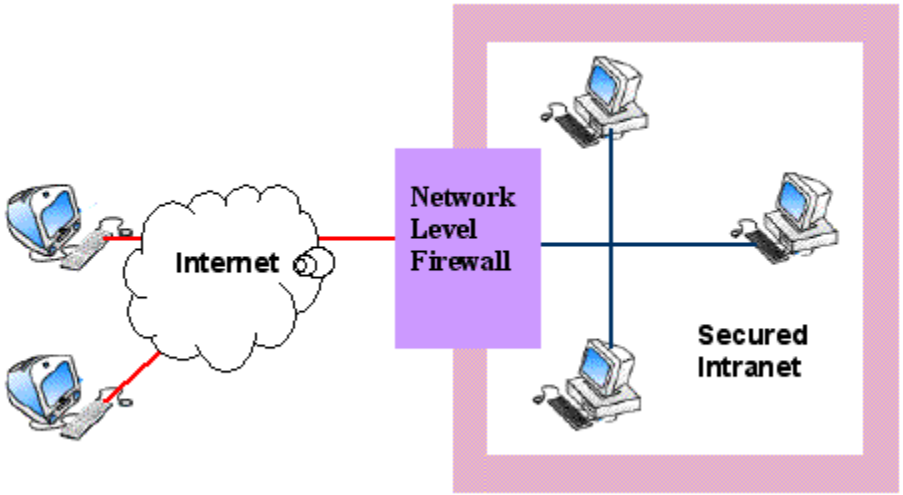
Antivirus


AVG
KASPERSKY lab
NOD32
antivirus system
AVIRA AntiVir®
McAfee
SECURITY
ZONE
LABS
avast! antivirus
bitdefender
secure your every bit
symantec.

Firewall

Un firewall este un program de computer sau un dispozitiv hardware care filtreaza informatia care vine din Internet intr-o retea privata sau sistem de computere. Daca un pachet corespunde filtrelor, acesta este respins.

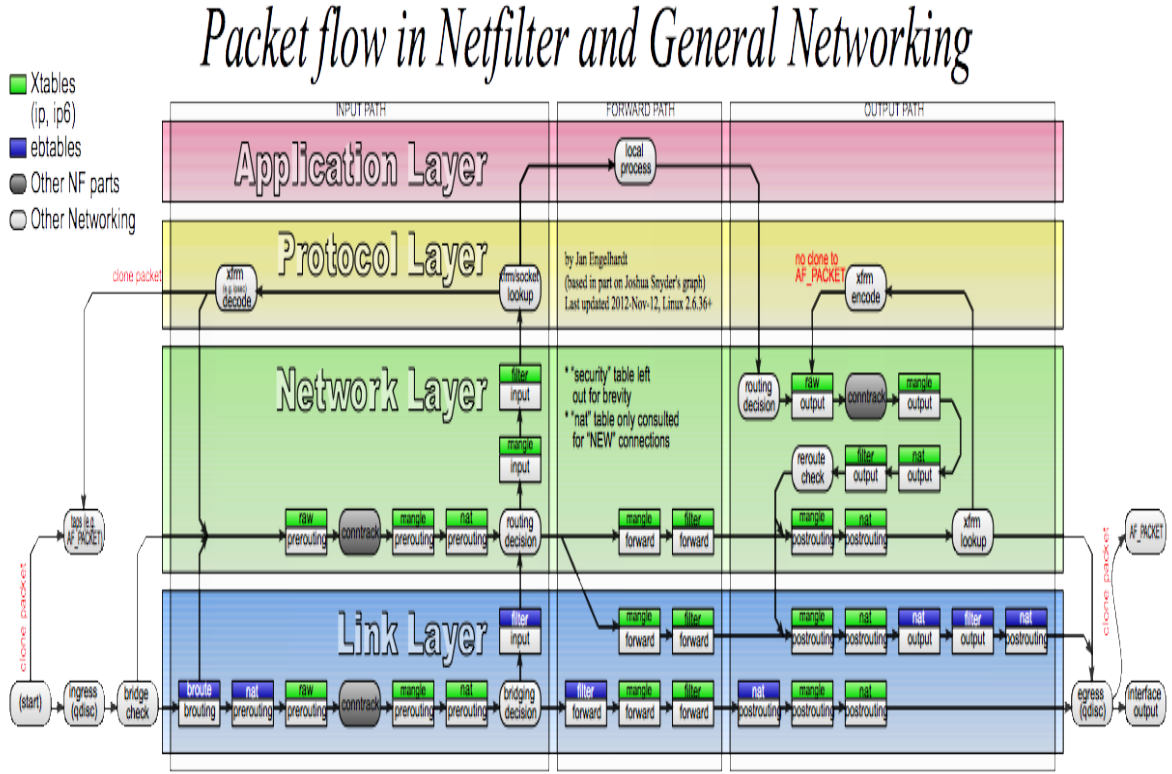
Firewall



Firewall

Cel mai simplu firewall permite celor din reteaua locala sa acceseze pe cea externa (Internetul), dar opreste traficul astfel incat niciun ultilizator din reteaua externa sa nu poata accesa reteaua locala.

Firewall


Packet flow in Netfilter and General Networking
Xtables (ip, ip6)
ebtables
Other NF parts
Other Networking
INPUT PATH
FORWARD PATH
OUTPUT PATH
Application Layer
Protocol Layer
Network Layer
Link Layer
local process
xfrm decode
xfrm/socket lookup
by Jan Engelhardt
(based in part on Joshua Snyder's graph)
Last updated 2012-Nov-12, Linux 2.6.36+
no clone to AF_PACKET
xfrm encode
clone packet
"security" table left out for brevity
"nat" table only consulted for "NEW" connections
routing decision
reroute check
xfrm lookup
AF_PACKET
(start)
ingress (qdisc)
bridge check
broute brouting
bridging decision
egress (qdisc)
interface output
raw
conntrack
mangle
nat
filter
input
output
prerouting
postrouting
forward

DDos

Un atac distribuit prin respingerea serviciului (DDoS) sau Distributed Denial of Service reprezinta particularitatea in care o grupare de sisteme compromise ataca o singura tinta, astfel cauzand blocarea serviciului pentru utilizatorii sistemului atacat.

Multimea mesajelor catre sistemul tinta forteaza oprirea acestuia, astfel respingand serviciul pentru utilizatorii legitimi.

Buffer overflow

In domeniul securitatii computerelor si a programarii software, un buffer overflow este o anomalie in care un program, in timpul scrierii datelor catre un buffer, depaseste limita acestuia si suprascrie memoria adiacenta.

Buffer overflows pot fi incepute de intrari care sunt desemnate de a executa cod, sau modifica modul in care acel program executa. Acesta poate rezulta intr-un comportament haotic al programului.

Concluzii

Protectia sau securitatea informatiilor in Internet este foarte importanta datorita sistemele care sunt interdependente si partii financiare implicate.

In aceasta lucrare am prezentat principalele amenintari, precum si metode de protejare a informatiei in Internet.

Va multumesc!