Firewall, definitie, caracteristici

Definitie:

- Numim firewall un echipament care examineaza traficul si ia deciziile pentru controlul accesului.
- Uzual spunem ca realizeaza filtrarea datelor

Caracteristici:

- Separa reteaua sigura de rest
- Permite trecerea numai a traficului autorizat
- Actioneaza ca o bariera intre “noi” si rest
- Limiteaza comunicatia din afara retelei, chiar daca lumea exterioara este o alta parte a aceleiasi organizatii
- Prin ascunderea dupa firewall numai cateva masini ale organizatiei sunt expuse atacurilor

Utilizare firewall

Motivatie:

- Exista brese de securitate datorate bugurilor software (prezente si in software de securizare)
- Codul rulat pentru implementarea firewall este restrans -> numarul bugurilor posibile este foarte mic
- Administrarea firewall este supusa unui set de reguli stricte
- Firewall forteaza partitionarea retelei in domenii de securitate diferite
- Firewall executa putine instructiuni, suport pentru loguri si monitorizari
- Fara partitii o retea este vazuta ca o masina virtuala uriasa cu un set necunoscut de utilizatori obisnuiti si privilegiati

Observatii:

- Nu este o solutie la problemele retelei, ci un raspuns la problemele de securitate ale masinilor din retea
- Nu stie cum se produce un software sigur, corect si usor de administrat
- Protocoalele de retea “sigure” nu inlocuiesc firewall.
- Nicio metoda criptografica nu poate proteja impotriva codului cu buguri.

Avantaje firewall

- Ruleaza pe servere sau echipamente de retea
- Software conservativ, nu necesita tehnologie “ultimate”
- Pastreaza orice log dorim in functie de reguli
- Poate opera la diferite niveluri ale stivei de retea (link, network, application)
- Examineaza headerele pachetelor la nivelul corespunzator
- Este transparent (spre deosebire de proxy)

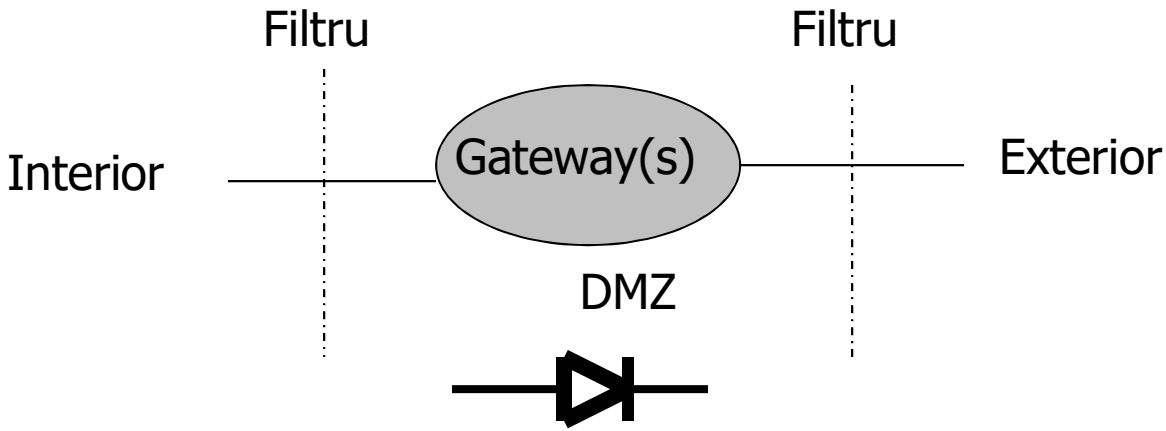
Statefull versus stateless;

- “Statefull”- un produs care se uita in fiecare pachet si aplica regulile, insa regulile sau testele aplicate la fiecare pachet pot fi modificate in functie de pachetele care au fost deja procesate.
- “Stateless” – un produs care se uita la fiecare pachet si aplica regulile independent de pachetele precedente, determinand cand inainteaza sau elimina pachetul independent pe baza unui set de reguli prestabilit

Structura schematica

Componente:

- Interior – oricine din interior este presupus a fi bine intentionat
- Exterior – cei rau intentionari sunt plasati aici
- DMZ – se plaseaza serverele neecesare, dar potential periculoase aici.



Caracteristici

1. Demilitarized Zone – DMZ. Daca discutam din perspectiva serverului de mail sau web rezulta:

- Cei din exterior pot trimite email, accesa pagini web
- Cei din interior pot obtine emailurile, actualizare pagini web
- Masinile trebuie monitorizate cu mare atentie

2. Forteaza politici de limitari administrative, nu fizice

3. Filozofie firewall:

- Blocheaza toate destinatiile periculoase – Utilizata cand exista cunostinte despre existenta unor potentiale pericole in anumite parti ale retelei
- Blocheaza orice cu exceptia pachetelor cunoscute ca fiind sigure si necesare – mult mai sigura.
- Blocarea traficului de iesire. Daca se permite trafic de iesire o serie de elemente trebuie avute in vedere: existenta persoanelor rau intentionate in interior, cerinte de reglementare interna, politici ale corporatiei.

Tipuri de firewall

Tipuri de firewall:

- Filtrarea de pachete
- Filtrarea dinamica a pachetelor
- Gateway pentru aplicatii
- Comutarea circuitelor
- Firewall personale si/sau distribuite

Obs: Majoritatea implementarilor firewall sunt combinatii ale acestor tipuri

Filtrarea pachetelor

- Filtrele sunt realizate cu ajutorul ruterelor, sunt ieftine
- Nu sunt utilizate informatii de context sau conexiune, pachetele individuale sunt acceptate sau rejectate
- Sunt greu de stabilit reguli avansate de filtrare, unele sunt inadecvate si regulile diferite pot interactiona
- Filtrarea pachetelor nu este adecvata pentru unele protocoale
- Gestionarea accesului la servicii dinamice este greoaie

Stateless packet filtering

- Dorim sa permita conexiunile in exterior
- Permit pachetele generate ca raspuns
- Pentru comunicatie TCP aceasta poate fi realizata fara stare;
  - Primele pachete intr-o conexiune TCP are numai bitul SYN setat;

Obs: La cererea unei legaturi clientul transmite un pachet cu bitul SYN setat si numar secventa 0 in headerul TCP. Serverul raspunde cu un pachet SYN_ACK, pachet in care sunt setati bitii SYN si ACK. Apoi clientul transmite o confirmare cu ACK catre server si se considera conexiunea stabilita.

  - Toate celelalte pachete au bitul ACK setat

Solutie: Permite toate pachetele cu ACK setat

Reguli firewall

- Action:
  - Permit (Pass, Allow) – permite inaintarea pachetului;
  - Deny (Block) – elimina pachetul;
- Direction:
  - Source - de unde vine pachetul: <IP address, port>;
  - Destination – unde merge pachetul: <IP address, port>;
- Protocol:
  - TCP;
  - UDP;
- Indicatori (flags) pachete;
  - ACK;
  - SYN;
  - RST, etc.

Exemplu reguli setare firewall

Presupunem ca dorim sa blocam spammer si sa permitem oricui sa trimita mail la propriul server de mail (OUR-MAIL);

- Block: Source IP Address = SPAMMER

- Allow: Source IP Address = any
  and
  Source port = any
  and
  Destination IP Address = OUR-MAIL
  and
  Destination port = 25

Exemplu: Setare incorecta

- Cerinta: Dorim sa permitem toate conexiunile TCP la serverele de mail

Allow: Source IP Address = any
and
Source port = 25
and
Destination IP Address = any
and
Destination port = any

- Problema: Nu putem controla selectia portului la masina remote si orice proces de la portul sursa 25 este permis

Exemplu: Alegere corecta

- Allow: Source IP Address = any
  and
  Source port = any
  and
  Destination IP Address = any
  and
  Destination port = 25

- Rezultat: Permite apelurile care pleaca

Exemplu: Crearea unui filtru propriu

- Cerinta: In politica companiei s-a decis ca nu se permite angajatilor web browsing

- Rezolvare:
  - Se creaza un filtru care elimina navigarea web pentru toate masinile din interiorul companiei.
  - Se presupune ca toate adresele IP in companie sunt cunoscute.
  - Pachetele iesite la portul 80 (web servers)

Obs: Filtrarea pachetelor In-bound. Daca filtram pachetele care pleaca la DMZ trebuie sa spunem de unde vin aceste pachete

Filtrare UDP

Particularitati:

- La UDP nu exista notiunea de conexiune si ca urmare este imposibil a se distinge raspunsul de o cerere, care ar trebui permis, fata de un pachet malitios.
- Address spoofing este fara conexiune

O prima metoda: O metoda care pare buna este blocarea tuturor porturilor cunoscute ca fiind periculoase.

Alta solutie: Permiterea pachetelor UDP numai prin intermediul serverelor sigure cunoscute.

Exemplu UDP: DNS

Pentru filtrarea pachetelor UDP ce permit acces la DNS sunt necesare:

- Acceptarea cererilor la portul 53
- Block daca manipuleaza numai cereri interne
- Allow daca permite cereri externe
- Problema cererilor recursive se poate aplica una dintre strategiile
  - Legarea socketului local de raspuns cu vreun alt port: permite accesul spre interior a pachetelor UDP
  - Accesarea masinii DNS in DMZ

Probleme ICMP si RPC

Pachetele ICMP:

- Pot fi generate ca raspuns la pachete TCP sau UDP: exemplu raspunsul “Path MTU”
- Trebuie sa fie permise cand avem conectivitate cat si la intreruperea sa

Concluzie: Simpla filtrare a pachetelor nu poate realiza aceste lucruri.

La RPC:

- Serviciile RPC se leaga de numere de port aleatoare;
- Nu exista nici un mod de a cunoaste apriori porturile care sa fie blocate si care sa fie permise
- Aceleasi probleme apar si la clientii RPC

Concluzie : Sistemele care utilizeaza RPC nu pot fi protejate prin simpla filtrare a pachetelor.

O abordare incorecta

Blocarea unui set de porturi UDP. Rapunsul la *rpcinfo –p nume_host*

Program	Versiune	Protocol	Port	serviciu
100000	4	tcp	111	rpcbind
100000	2	udp	111	rpcbind
390113	1	tcp	7937	
100005	1	udp	32800	mountd
100005	3	tcp	32776	mountd
100003	3	udp	2049	nfs
100227	2	udp	2049	nfs_acl
100003	2	tcp	2049	nfs
100227	2	tcp	2049	nfs_acl
100011	1	udp	36613	rquotad
100008	1	udp	36614	walld
100001	2	udp	36614	rstatd

FTP si SIP

Proprietati:

- Clientii FTP si alte servicii utilizeaza canale secundare
- Folosesc numere de poart aleatoare
- Filtrarea simpla a pachetelor nu este posibila
- O incercare de creare de reguli simple pe baza pachetelor nu va functiona

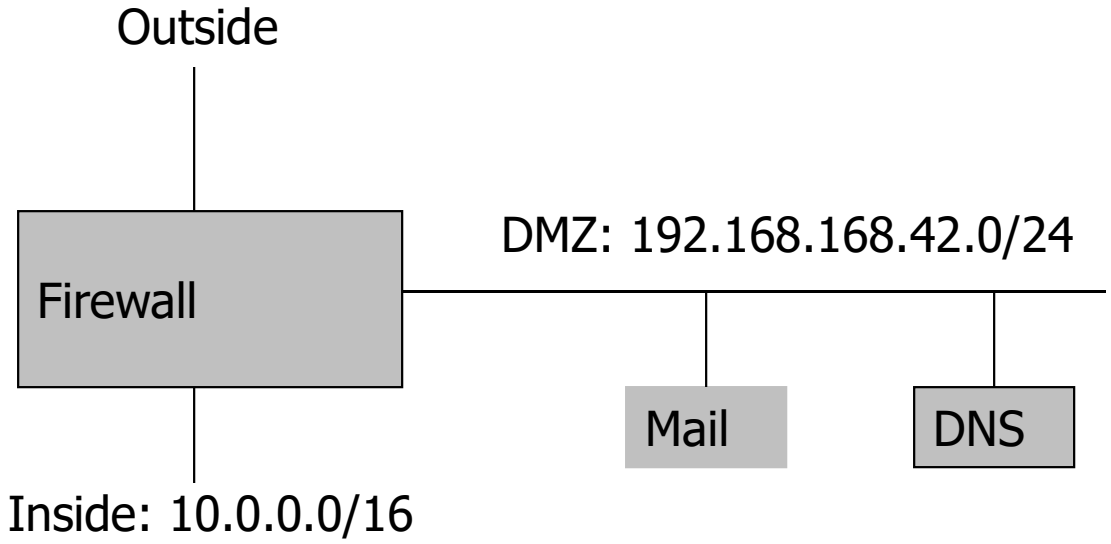
Solutii:

- Clientii FTP trimit comanda PORT pentru a specifica adresa pentru conexiunea catre interior
- Daca se utilizeaza comanda PASV canalul de date foloseste o conexiune separata spre exterior;
- Daca politica locala permite conexiuni arbitrare catre exterior aplicarea metodei da rezultate bune.

Rolul filtrelor de pachete

- Filtrele de pachete nu reprezinta o modalitate completa de implementare firewall
- Cu toate acestea este foarte eficienta si poate fi aplicata chiar pe legaturile de mare capacitate (de ce?)
- Sunt cateva situatii speciale in care este perfecta;
- Poate fi utilizata pentru a taia conexiunile care nu dorim sa ajunga la nivel de firewall aplicatie

Fie structura din figura



Exemplu de reguli

Interfata	*Actiune*	*Adresa*	*Port*	*Flags*
Outside	Block	Src = 10.0.0.0/16		
Outside	Block	src = 192.168.42.0/24		
Outside	Allow	Dst=Mail	25	
Outside	Block	Dst=DNS	53	
Outside	Allow	Dst=DNS	UDP	
Outside	Allow	Any		ACK
Outside	Block	Any		
DMZ	Block	Src#192.168.42.0/24		
DMZ	Allow	Dst=10.0.0.0/16		ACK
DMZ	Block	Dst=10.0.0.0/16		
DMZ	Allow	any		
Inside	Block	Src # 10.0.0.0/16		
Inside	Allow	Dst=Mail	993	
Inside	Allow	Dst=DNS	53	
Inside	Block	dst = 192.168.42.0/24		
Inside	Allow	any		

Statefull Packet Filters

Caracteristici:

- Cel mai obisnuit tip de filtrare pachete
- Rezolva destul de multe (dar nu toate) din problemele filtrelor simple de pachete
- Necesita stare pe conexiune in firewall

Pastrarea starii:

- Cand un pachet este trimis in exterior se inregistreaza acest lucru in memorie;
- Asociaza pachetele spre interior cu starea creata de pachetele catre exterior

Probleme rezolvate, probleme ramase

Probleme rezolvate:

- Poate manipula mesajele UDP de tip cerere/raspuns
- Poate asocia pachetele ICMP cu conexiunea
- Rezolva unele dintre problemele filtrarii in-bound/out-bound, insa tabelele de stare sunt necesar asociate cu pachetele spre interior
- In continuare necesita blocare pentru address-spoofing

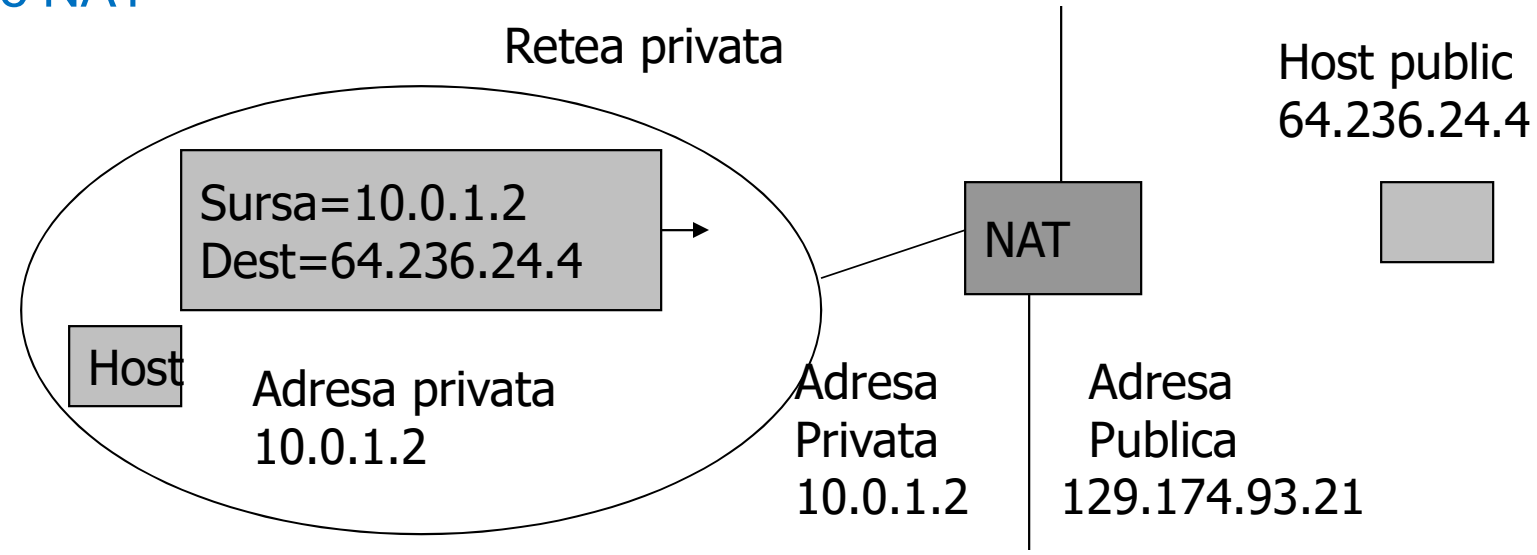
Probleme ramase:

- Inca are probleme cu porturile secundare
- Inca are probleme cu RPC
- Inca are probleme cu semanticile complexe (ca de ex. DNS)
- Multimea starilor ce por fi pastrate este limitata

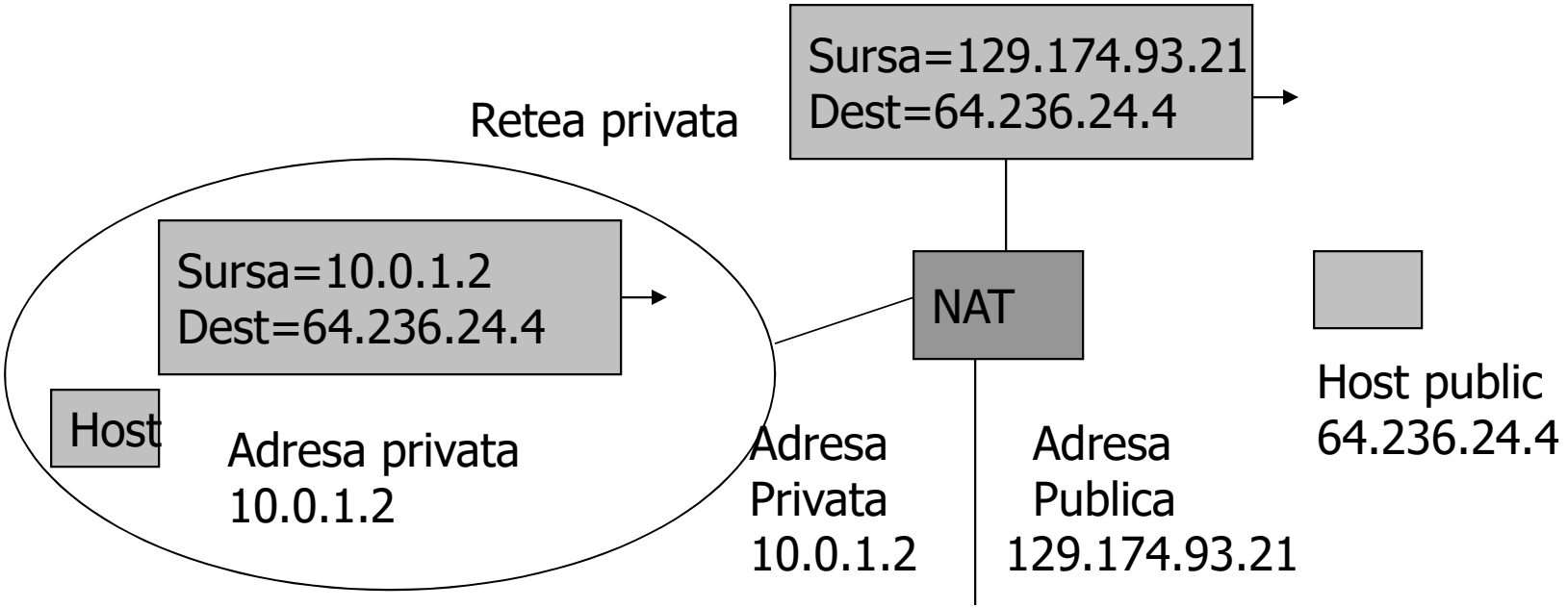
Firewall si Network Address Translators (NAT)

- NAT traslateaza adresa sursa si in anumite cazuri si numerele de port;
- Uneori in piata se recomanda ca firewall foarte puternice
- In realitate nu sunt mai puternice decat statefull packet filter

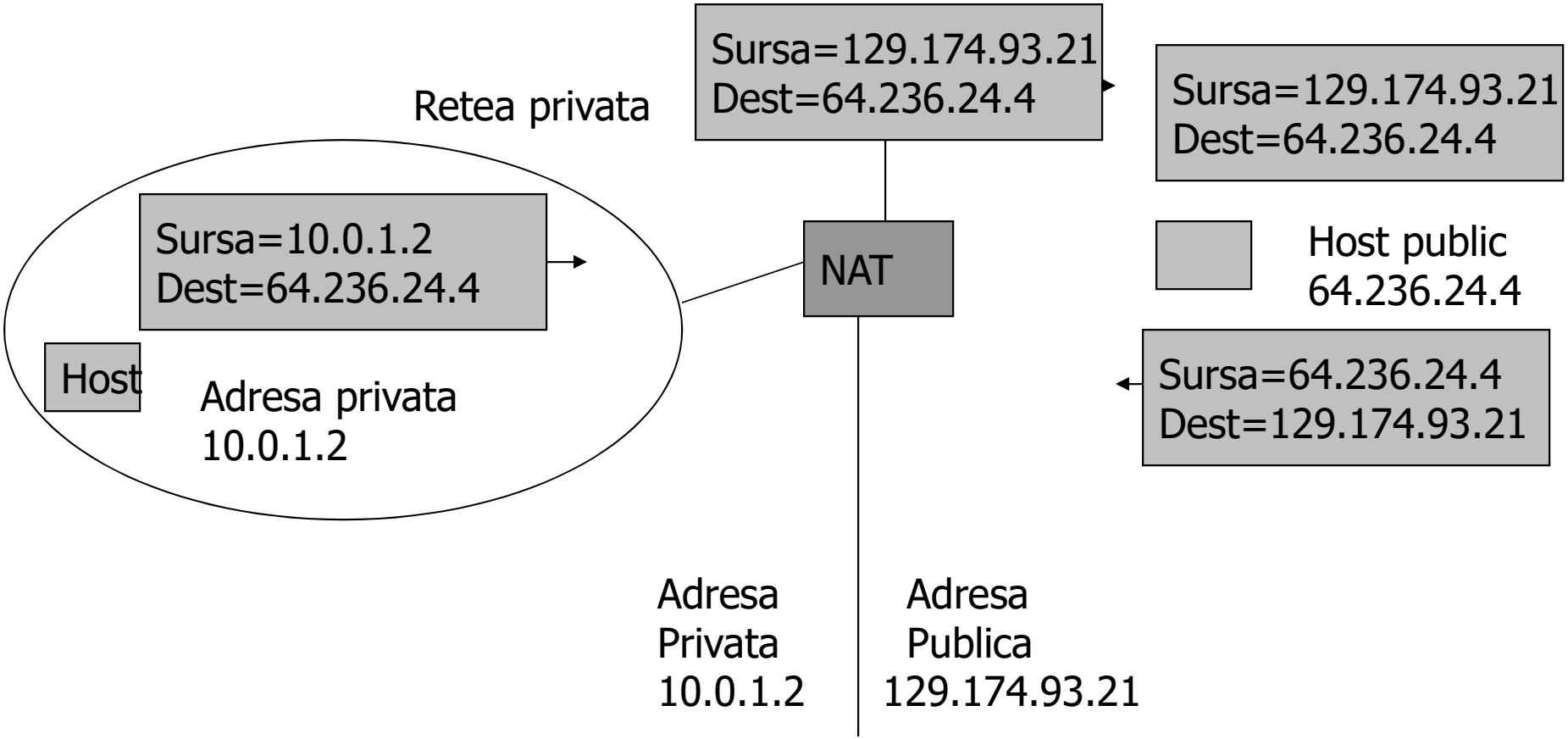
Operare NAT



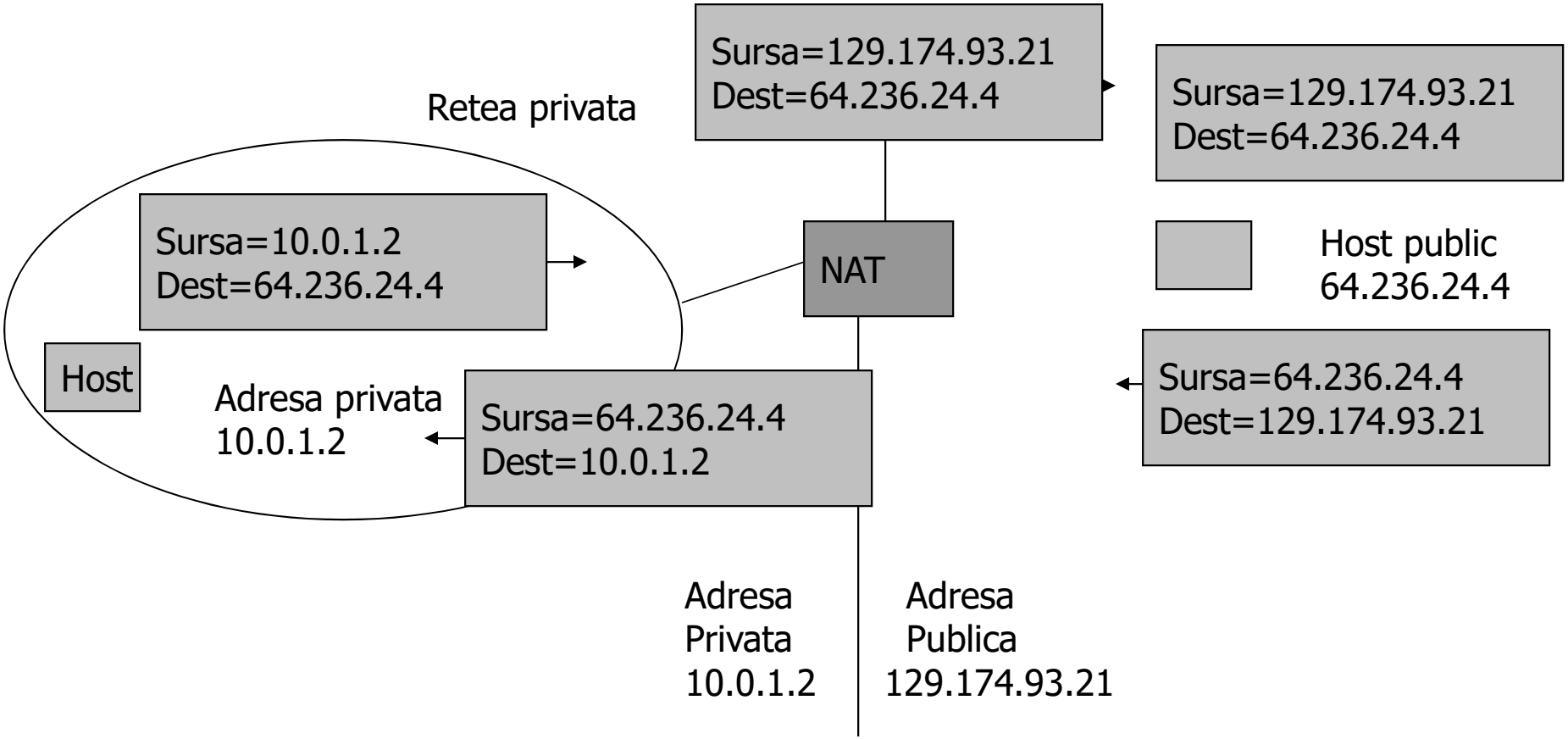
Operare NAT (1)



Operare NAT (2)



Operare NAT (3)



Comparatie stateful packet filter - NAT

Cele doua opereaza la fel in faza de analiza si decizie daca un pachet trece sau este distrus. Toate deosebirile apar daca adresa este translatata sau nu.

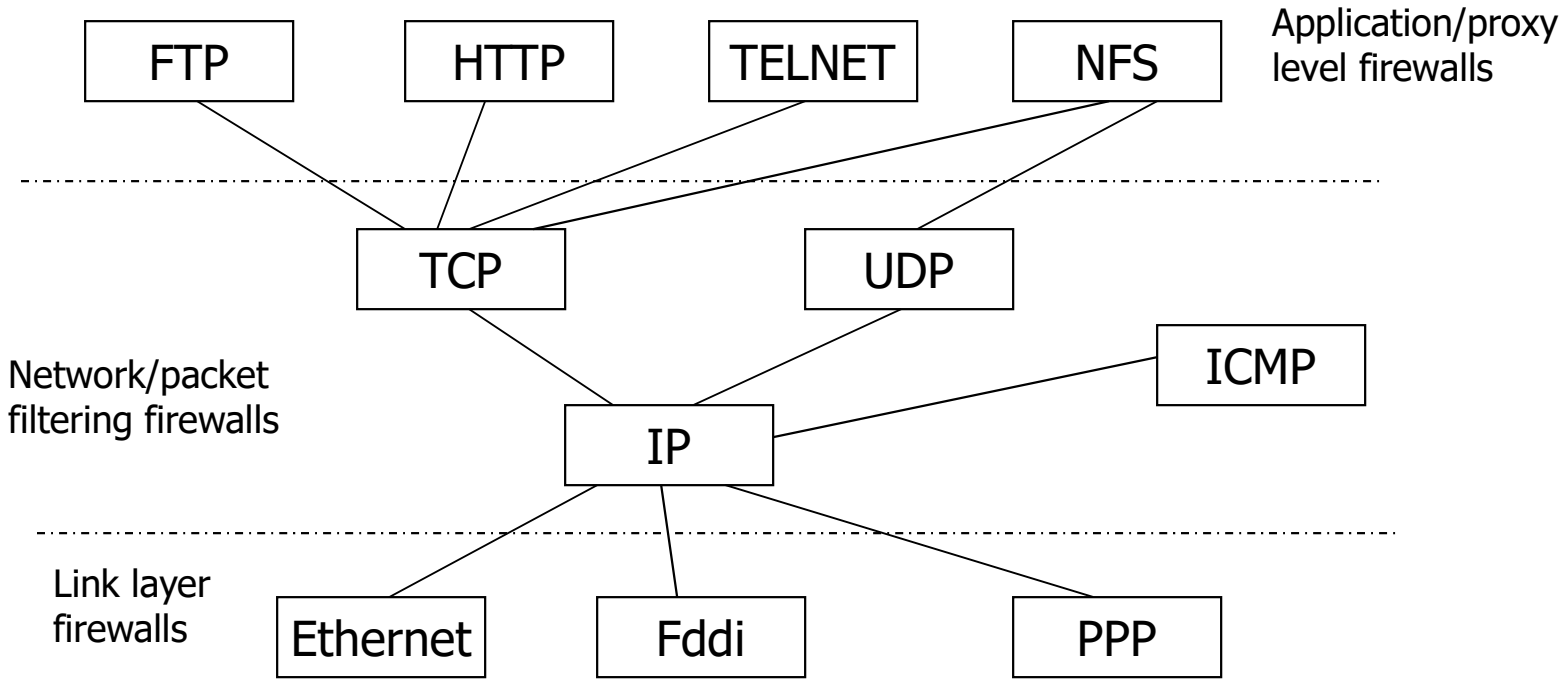
Statefull Packet Filter	NAT
Out-bound: Scrie intrare in tabela de stare	**Out-bound**: Creaza intrare in tabela de stare si translateaza adresa
In-bound: Se uita in tabela de stare si daca nu este intrare prezenta elimina pachetul, daca exista il inainteaza	**In-bound:** Se uita in tabela de stare si daca nu este intrare prezenta elimina pachetul. Daca exista traslateaza adresa si il inainteaza

Relatie firewall – stiva OSI

Efecte pe niveluri:

- Pornind de la limitarile filtrarii pachetelor discutate deja, firewall este incapabil sa protejeze de atacuri pe layere de nivel inalt OSI;
- Filtrarea pachetelor IP, inclusiv numarul de port nu poate proteja impotriva pachetelor TCP malitioase;
- Un firewall la nivel TCP nu poate proteja impotriva bugurilor SMTP;
- Proxy SMTP nu poate proteja impotriva problemelor din aplicatiile de email si alte aplicatii;

Filtre pe niveluri



Avantaje/dezavantaje filtrare pe niveluri

Avantaje:

- Protectia poate fi canalizata pe o aplicatie individuala
- Este disponibila mai multa informatie de context
- Doar aplicatia este afectata, overhead nu este global

Dezavantaje:

- Firewall la nivel aplicatie nu poate proteja impotriva atacurilor la nivelurile inferioare
- Necesita cate un program separat pentru fiecare aplicatie
- Aceste programe pot fi destul de complexe
- Aceste programe pot fi destul de nepotrivite pentru aplicatiile utilizator

Exemplu: email

Probleme protejare email:

- Protejarea email pe fluxul spre interior sau spre exterior? Codul este comun, dar pot fi destule deosebiri.
- Actiunea la nivel SMTP (RFC 2821) sau la nivel de continut email (RFC 2822)?
- Ce se intampla cu MIME care extinde formatul email: alte seturi de caractere decat ASCII, atasamente nontext, continut de mesaj cu parti multiple, informatii de context in header.

Amenintari:

- Uzual: apararea impotriva erorilor de implementare a protocolului
- Scanarea impotriva virusilor
- Anti spam
- Atacuri prin javascript
- Atacuri prin violarea politicii organizatiei referitoare la email
- Atacuri impotriva verificarii semnaturii

Email: mesaje catre interior

- Mesajul email este usor de interceptat prin inregistrarile MX.
- O inregistrare MX (Mail eXchanger record) este un tip de inregistrare resursa in DNS specificand cum un mail trebuie rutat utilizand SMTP. Fiecare inregistrare MX contine preferinta si nume host, asa ca o colectie de inregistrari MX pentru un nume de domeniu dat specifica serverele care trebuie sa receptioneze mail pentru acel domeniu si prioritatea lor relativa
- Posibilitatea de a utiliza "*" pentru manipularea intregului domeniu. Ex: DNS aii.pub si *.aii.pub. toate mesajele sunt trimise la masinile terminale

Niveluri de protectie posibile:

- Masina receptoare poate filtra adresele IP realizand protectie la nivel de retea
- Masina receptoare poate rula un SMTP puternic realizand protectia la nivel de aplicatie
- Un mail receptionat poate fi scanat la nivel de continut pentru orice tip de amenintari;
- Firewall poate combina mai multe functii

Combinare firewall

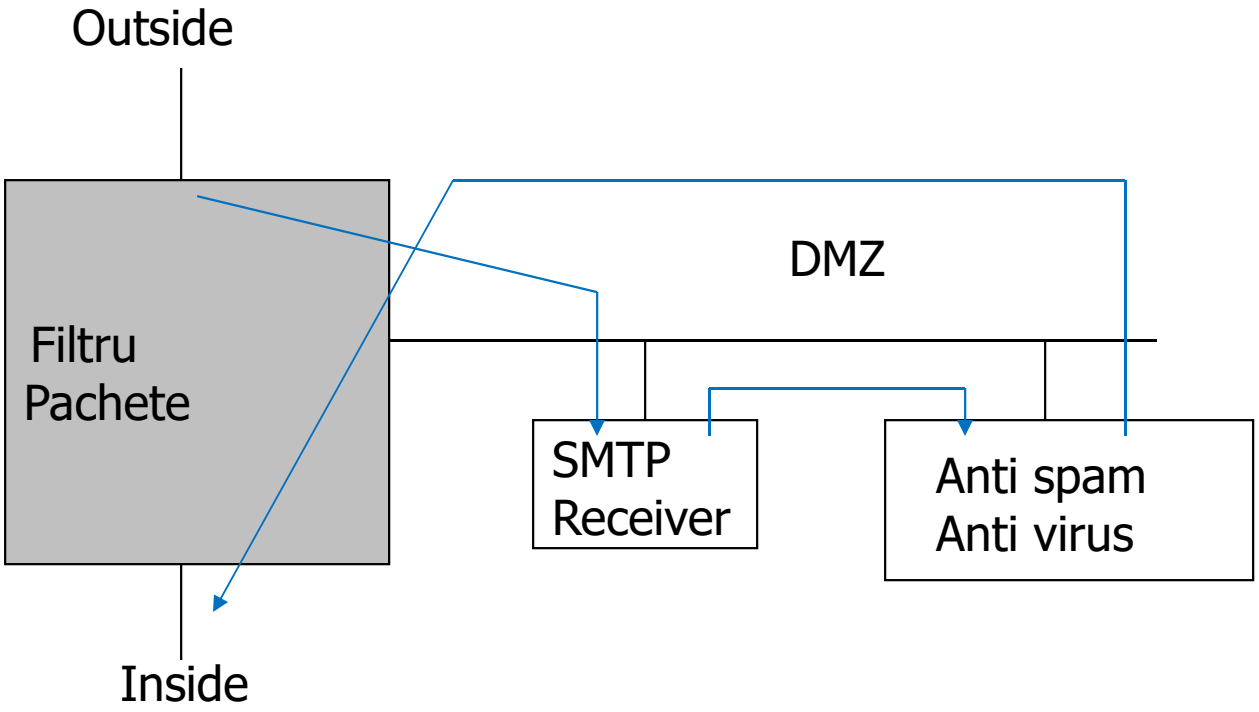
Email spre exterior:

- Multe implementari au posibilitatea de a inainta unele / toate mesajele la o masina specificata
- Se creaza o politica prin care toate mesajele email trec pe la o masina pentru a fi transmise. Se forteaza aici filtrarea pachetelor

Combinarea tipurilor firewall:

- Utilizarea unei aplicatii firewall ce manipuleaza atat email spre interior cat si spre exterior
- Utilizarea filtrelor de pachete pentru implementarea regulilor

Protejare email prin firewall



Politici privind protectia email

Stabilirea unui flux pentru mesajele email

La email catre interior:

- Numai un server SMTP din exterior poate discuta cu SMTP receiver
- SMTP receiver inainteaza email la filtrele anti-spam/anti-virus prin anumite protocoale
- Aceste masini discuta cu SMTP printr-un mail gateway din interiorul zonei protejate
- Efect benefic: Daca SNMP receiver este compromis nu poate discuta direct cu interiorul zonei protejate

La email catre exterior:

- Se utilizeaza filtrarea pachetelor pentru a bloca conexiunile catre exterior cu portul 25
- Singura masina care poate discuta cu un SMTP exterior este un gateway email dedicat mesajelor catre exterior
- Acest gateway poate fi plasat fie in interior, fie in DMZ

Solutii DNS

UDP:

- Localizarea server DNS in DMZ; De fapt utilizarea unui nivel aplicatie care sa lucreze cu restrictiile de fitrarea pachetelor;
- DNS nu necesita schimbari in aplicatie care sa faciliteze acest lucru.

Perspectiva interna fata de cea externa:

- Pot cei din exterior sa vada numele masinilor interne? Solutie: utilizarea a doua servere DNS, unul pentru cereri interne, altul pentru cereri externe
- Dispunerea unui firewall in fiecare parte;
- Trebuie asigurat ca masinile interne nu vad inregistrarile name server ca apoi sa incerce iesirea in exterior direct.

Atacuri prin contaminare cache:

- Serverele DNS pastreaza in cache rezultatele cererilor;
- Raspunsurile pot contine informatii aditionale ce pot fi utile, dar nu sunt parti ale raspunsului la cerere;
- Cale atac: Trimiterea de inregistrari fictive ca informatii aditionale pentru a face urmatoarele cereri confuze.

Filtrare DNS

- Toate cererile interne DNS merg la DNS switch;
- Daca o cerere interna este inaintata la un server intern sau se da inapoi raspunsul cu inregistrarea NS interna;
- Daca este o cerere externa inainteaza cererea catre alta locatie, dar:
  - Curata rezultatul prin inlaturarea oricarei referinte la masinile interne;
  - Curata rezultatul prin inlaturarea oricarei referinte la inregistrari name server.
- Utilizeaza o filtrare de pachete pentru a bloca comunicatia DNS directa.

Aplicatii gateway mici:

- La anumite aplicatii simpla filtrare de pachete nu este adecvata;
- Solutia: examinarea traficului printr-un proxy specific si reactie corespunzatoare

Atacuri prin FTP Proxy

Caracterizari:

- Va reamintiti utilizarea comenzii PORT?
- Daca apare o comanda PORT, se anunta firewall sa deschida acel port temporar pentru primirea unei conexiuni;
- Aceeasi situatie cu RPC – definirea filtrelor bazate pe aplicatii RPC, nu pe numere port.

Atacuri prin proxy:

- Appleturile Java descarcate pot apela masina originala;
- Un applet rau intentionat poate deschide un canal FTP si poate da o comanda PORT provocand deschiderea portului pe o masina care altfel era protejata
- Firewall o va trata ca pe o conexiune valida;
- Solutia: firewall senzitiv la ce host si port poate aparea in comenzile de tip PORT.

Personal firewall

Caracteristici:

- Adaugate la principalele protocoale din stiva;
- Prin termenul ‘inside’ se intelege masina, orice altceva este ‘outside’;
- Cele mai multe actioneraza ca filtre de pachete;
- Setul de reguli poate fi definit individual sau de administrator.

Probleme:

- Este simplu sa rejectam protocoale, nu este asemanator cu personal firewall;
- Partea dificila: raspuns afirmativ in conditii de siguranta;
- Nu putem vorbi de topologie – tot ce avem este adresa IP a transmitatorului;
- Inlocuirea adresei IP nu este foarte dificila, mai ales la pachete UDP.

Application-Linked Firewalls

- Cele mai multe firewall personale actioneaza la numere port;
- Cel putin un astfel de firewall securizeaza aplicatii – programelor individuale le este permis sau nu sa discute local sau global;
- Nu ingrijoreaza numerele de port criptice: sunt manipulate foarte bine porturile auxiliare;
- Numele aplicatiilor pot fi de asemenea criptice; aplicatiile opereaza in folosul unor alte aplicatii.

Distributed Firewalls

- Din unele puncte de vedere sunt similare cu personal firewall aflate direct sub controlul politicii centrale;
- Se utilizeaza IPsec pentru a face distinctia intre “inside” si “outside”;
- Cei din interior detin certificate, cei din exterior nu;
- Numai masinile cu certificat propriu sunt de incredere fata de alte masini;
- Nu se sprijina pe topologie: laptopuri din interior sunt protejate cand calatoresc, cele din exterior nu sunt un pericol atunci cand ne viziteaza.

.

Probleme suplimentare (1)

Intentii rele in interior:

- Un firewall presupune ca toti cei din interior sint OK, ceea ce nu este totdeauna adevarat;
- Cei din interior pot provoca stricaciuni mari intrucat nu sunt controlati (ex: deschidere proxy peste canale criptate);

Echipamente mobile:

- Cand un echipament mobil este in afara zonei de protectie a firewall cum va fi protejat?
- Solutie posibila: Personal firewall si securizarea/inchiderea tuturor serviciilor ne-necesare.

Probleme suplimentare (2)

Conectivitatea dinamica:

- Firewall se sprijina pe topologie si servicii statice;
- Daca sunt prea multe conexiuni, unele vor ocoli firewall;
- La anumite momente nu este posibil sa protejeze efectiv toate legaturile externe;
- Companiile mari pot avea sute sau mii de conexiuni externe multe fiind necunoscute de catre personalul ce administreaza reteaua.

Eschivare (evitare):

- Firewall sau administrator firewall nu sunt suficient de bune;
- Unele dintre aplicatii nu sunt capabile de ruleze;
- Furnizorii initializeaza conexiunea crezand ca ruleaza peste porturi cunoscute apriori;
- Conexiunile HTTP se realizeaza uzual peste firewall si chiar web proxy.