Firewall: wat?

- letterlijk: brandvrije of vuurbestendige muur
- tussen intern en extern netwerk (waar het steeds *brandt*)
- controleert aard en hoeveelheid trafiek
- beleid bepaalt de manier van doorvoerbeperking van data
- twee benaderingen bepalen welke gegevens bij verstek (default) worden doorgelaten of tegengehouden:
  - permit
    - alleen vermelden wat wordt tegengehouden
    - niet vermelde protocols en adressen (hosts) passeren
    - eenvoudige configuratie
  - deny
    - alleen vermelden wat mag worden doorgelaten
    - je bepaalt zelf de *veilige* protocols en hosts
- geen van beide is zaligmakend

1

Firewall: gebruik

- maakt deel uit van strategie
- kan bovendien
  - bepaalde gebruikers verhinderen bepaalde sites of services te gebruiken
  - trafiek monitoren (bv. loggen van eindpunten van TCP-connecties)
  - luistervinken en alle trafiek tijdelijk opslaan
  - opzetten van VPN tussen verschillende bedrijfslocaties
- kan niet
  - beschermen tegen aanval die FW niet passeert (dial-out naar ISP voor systeembeheer, dial-in)
  - beschermen tegen interne bedreigingen
  - beschermen tegen transport van virussen (hoewel, …)

Firewalls 2

Definities (1)

- host
  computersysteem verbonden aan een netwerk
- bastion host
  extra beveiligde host
  – door de systeemadministrator als kritisch punt aangewezen in netwerkbeveiliging
  – invalsbasis vanaf het internet
- dual-homed / dual-ported host
  host aangesloten op twee netwerken

Firewalls 3

Definities (2)

- choke / screening router / packet filter
  choke = smoorklep
  computer of communicatie-device
  – beperkt de vrije doorgang van (IP)-pakketten tussen netwerken
  – vaak geïmplementeerd als router
- gate / gateway
  device, computer, programma (bastion host+programma)
  – ontvangt connecties van buiten
  – extra beveiligd (geen accounts, auditing+extra software)
  – gateway-functies vaak als bastion host bestempeld

Firewalls 4

Software op gateways (1)

- network client software
  - gebruikerstoegang tot gateway = eenvoudige manier om ze restrictief toegang tot internet te verschaffen
  - ftp, telnet, mail, …
  - vereist accounts op gate
  - dus: **niet doen !!**
- network servers
  - SMTP, HTTP, NNTP, DNS,…
  - al dan niet als proxy
  - meestal **slecht idee !!**
- bastion host
  - steeds mikpunt van aanvallen
  - keep it simple !

Firewalls 5

Software op gateways (2)

- network server = vaak proxy server
  - proxy = gevolmachtigde
  - geeft aanvragen van interne clients door naar externe servers
  - antwoorden van externe servers worden doorgegeven naar interne clients
  - kan op verschillende niveaus (applicatie, transport)

Firewalls 6

Proxy servers

- Application Level Gateway (later meer)
  - verstaat en interpreteert commando's in applicatieprotocol
  - zeer extreem voorbeeld is sendmail
- Circuit Level Gateway (later meer)
  - creëert een verbinding (circuit) tussen client en server
  - trekt zich niets aan van applicatieprotocol
  - SOCKS

Firewall Ontwerp: doelstellingen

- alle verkeer van binnen naar buiten en omgekeerd moet door de firewall passeren
  - dmv fysische configuratie
  - verschillende mogelijkheden
- alleen verkeer doorlaten conform de veiligheidspolitiek
  - controle van service (ip-addr, tcp-poort), van richting
  - controle van gebruikers (welke interne gebruikers mogen welke diensten gebruiken? eventueel externe authenticatie via vpn/ipsec)
  - controle van gedrag (eliminatie van e-mail spam)
- de firewall is samengesteld uit één of meerdere bouwstenen (choke, gate)
- de firewall is immuun tegen aanvallen (trusted system)

Firewall Ontwerp: bastion host

- draait “secure” versie van OS ➔ trusted system
- draait alleen de nodige applicaties waaronder de proxy services (dus geen algemene software)
- vereist bijkomende authenticering vooraleer proxy toepassing mag gebruikt worden
- ondersteunt alleen subset van normale commando’s
- …

Firewall Ontwerp: bastion host (2)

- alleen toegang vanuit welbepaalde hosts van beveiligde netwerk
- proxy-modules
  - voorzien in uitgebreide logging
  - zijn klein in omvang (grote programma’s zijn gevaarlijk)
  - zijn onafhankelijk van mekaar
  - lezen niet van disk behalve configuratie-file
  - draait als user zonder rechten in beveiligde omgeving

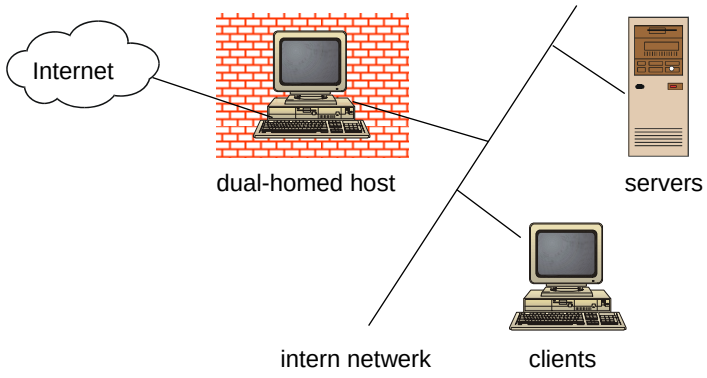
Firewall architecturen

- Single Box architecturen
  - dual-homed gateway / dual-ported host
  - choke (screening router / packet filtering)
- Screened Host architecturen

  choke +
  - **single-homed bastion host**
  - **dual-homed bastion host**
- Screened Subnet architecturen
  - enkelvoudig
  - meervoudig

Single Box architecturen

1. **dual-homed gateway / dual-ported host**



Dual-Homed Gateway (1)

- host fungeert zowel als choke en als gate
- eenvoudig te implementeren
- diensten op 2 manieren aanbieden
  - gebruikers kunnen inloggen op host (gevaarlijk)
  - proxy server
- gevaren:
  - mag geen pakketten forwarden, anders bypass van functies op transort- of applicatielaag
    - **ip-forwarding (zorgt voor routing) off**
    - **ip-source-routing off (optie in IP-header; negeert routing tables)**
  - inbraak via directe login

Firewalls 13

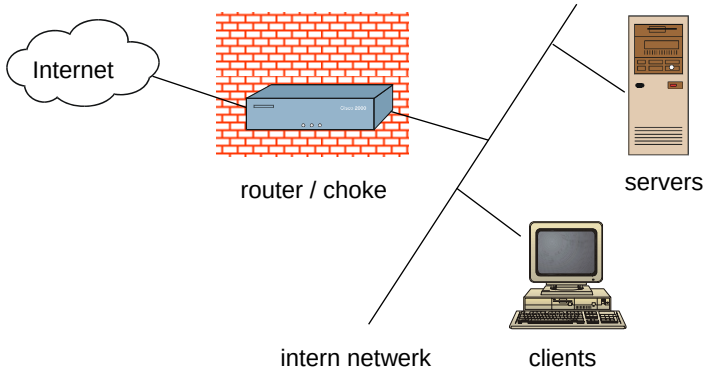
Dual-Homed Gateway (2)

- niet performant
- voordeel: slechts 1 gevaarlijk punt
- best gebruikt in volgende situaties:
  - weinig trafiek naar het Internet
  - internettrafiek is niet echt kritisch
  - het intern netwerk bevat niet echt extreem waardevolle gegevens

Firewalls 14

Single Box architecturen (2)

2. **Screening router / packet filter**



Firewalls 15

Screening router / packet filter (1)

- blokkeert pakketten
  - voor niet gebruikte services
  - die expliciet IP-source-routing opties zetten
- laat pakketten door
  - van inkomende TCP-connecties naar welbepaalde servers
  - van uitgaande TCP-connecties vanaf welbepaalde clients

Firewalls 16

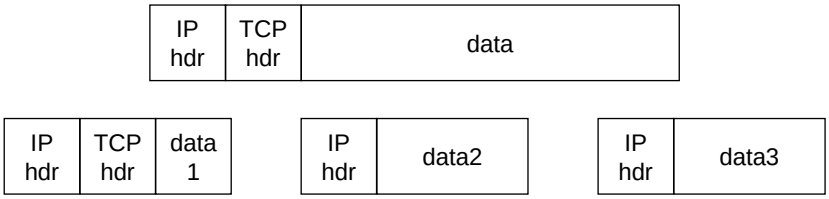
Screening router / packet filter (2)

Aanvallen:

- ip-source-routing:
  - filter aanvaardt geen pakketten met deze optie
- kleine fragmenten (tiny fragment attack)
  - IP-pakketten fragmenteren om TCP-header en data te verdelen over meerdere pakketten
  - filter aanvaardt niet:
    protocol==TCP && IP-fragment-offset !=0
- IP-spoofing:
  filter aanvaardt geen pakketten op externe interface met een intern bronadres

Zijsprong 1: IP–fragmentatie

- groot IP-pakket verdelen in meerdere kleine pakketten (=fragmenten)



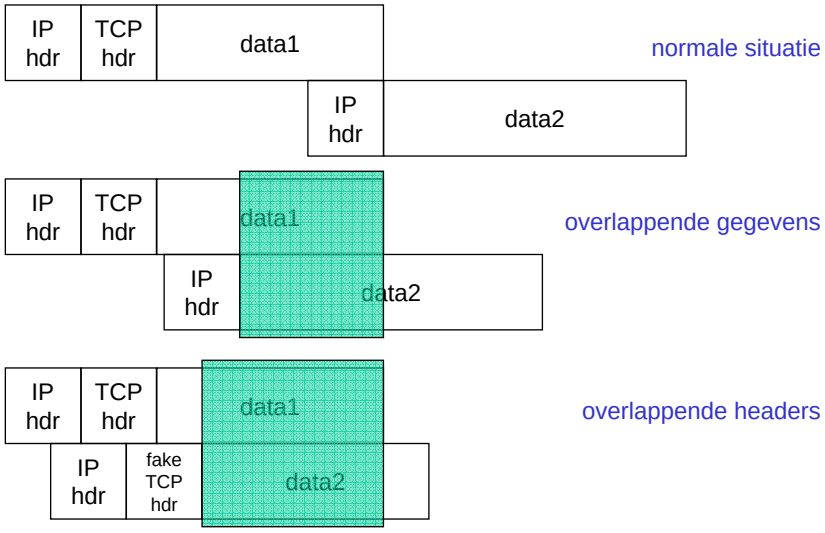
IP–fragmentatie (2)

- reden: router kan het oorspronkelijk pakket niet versturen wegens overschrijding maximale pakketgrootte
- elke router kan beslissen te fragmenteren
- flag in IP-hoofding van pakket kan dit verbieden
- moet router pakket dan verwerpen?
- MTU (maximum transmission unit) is oplossing
  - wat is de maximale grootte van een pakket zo dat het nergens moet worden opgesplitst tijdens het afgelegde pad?
  - is bekend bij versturen van pakket
  - zorgt voor efficiëntere doorvoer van pakketten

IP–fragmentatie (3)

- verband met packet filter?
- alleen eerste fragment bevat hoofding van protocols op hogere lagen
  - filteren gebeurt op het eerste pakket
  - indien 1ste tegengehouden, andere pakketten worden doorgelaten
- veilig?
  - op eerste gezicht: ja
  - doelbestemming kan pakket niet meer samenstellen
- maar …
  - doorgelaten fragmenten worden in geheugen gehouden
    - **mogelijkheid tot DOS-attack**
  - ontvanger geeft het op → ICMP-pakket naar afzender
    - **aanvaller weet: host bestaat en connectie is niet geslaagd + reden**

IP–fragmentatie: overlapping (1)



IP–fragmentatie: overlapping (2)

- aanvaller
  - hoopt op doorlaten van IP-pakketten met TCP-data
  - maakt fragmenten met zelfde data-adressen (gegevens over waar gegevens beginnen en eindigen)
- komt niet voor in normale situatie
- hoe reageert het besturingssysteem?
  - beschouwt het als abnormaal
  - moet het de eerste of laatste gegevens behouden?
  - assembleert foutieve pakketten
- mogelijke aanvallen
  - DOS
  - verbergen van info: vb. introductie van virussen
  - verzamelen van info over geblokkeerde poorten
    - **2de fragmenten worden niet tegen gehouden door filter**

IP–fragmentatie (slot)

- wat doet packet filter?
- laat hem opnieuw assembleren
- als dit niet mogelijk is:
  - laat hem alle niet eerste fragmenten verwerpen
    - ip-fragment-offset niet gelijk aan nul

- ip-fragement offset:
  Used with fragmented datagrams, to aid in reassembly of the full datagram. The value is the number of 64-bit pieces (header bytes are not counted) that are contained in earlier fragments. In the first (or only) fragment, this value is always zero.

Screening router / packet filter (2)

Aanvallen:

- ip-source-routing:
  - filter aanvaardt geen pakketten met deze optie
- kleine fragmenten (tiny fragment attack)
  - IP-pakketten fragmenteren om TCP-header en data te verdelen over meerdere pakketten
  - filter aanvaardt niet:
    protocol==TCP && IP-fragment-offset !=0
- IP-spoofing:
  filter aanvaardt geen pakketten op externe interface met een intern bronadres

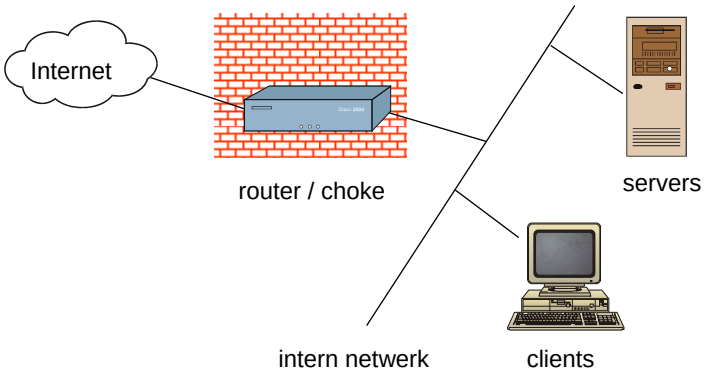
Zijsprong 2: IP-spoofing

- aanvaller zendt pakketten met incorrect bronadres
- antwoorden worden naar verkeerd adres gestuurd, niet noodzakelijk naar de aanvaller
- drie mogelijkheden:
  - de aanvaller kan de antwoorden onderscheppen en zo een onbeperkte *gekaapte* verbinding in stand houden
  - de aanvaller hoeft de antwoorden niet te zien, bijvoorbeeld bij een *denial of service* aanval
  - de aanvaller wil de antwoorden niet zien
    - er worden antwoorden gestuurd naar een ander slachtoffer door een nietsvermoedende afzender
    - adres van afzender en bron is zelfde, computer hangt

Firewalls 25

Single Box architecturen (2)

2. **Screening router / packet filter**



Firewalls 26

Packet filtering

pakketten worden selectief doorgegeven tussen interne en externe hosts op basis van

- pakketinformatie
  - IP bron- en bestemmingadres
  - protocol (TCP, UDP, ICMP)
  - TCP/UDP bron- en bestemmingspoort
  - ICMP boodschaptype (Internet Control Message Protocol)
  - pakketgrootte
- interface (in/out)
- historiek
  - is pakket een antwoord op ander pakket (bron == bestemming)
  - hoeveel pakketten van zelfde host?
  - zelfde pakket reeds gekregen?
  - gefragmenteerd pakket?

Firewalls 27

Packet filtering (2)

- **Filtering gebeurt op basis van**
  - service (TCP/UDP poortnummers)
  - IP-adres van bron en bestemming
  - geavanceerde opties (IP options, fragmentgrootte, …)

Voorbeeld van Rule-set (verzameling regels):

- blokkeer alle binnenkomende connecties behalve die op poort 25 (SMTP)
- aanvaard pakketten met TCP-poortnrs 20 en 21 (FTP)
- laat TFTP, Xwindows, RPC en r-services (rlogin, rsh, …) niet door
- blokkeer alle connecties met systemen die je niet vertrouwt

Firewalls 28

Packet filtering (3)

- **Packet filters kunnen**
  - pakket naar vermelde bestemming sturen
  - pakket *vergeten*, afzender niet verwittigen
  - pakket weigeren, afzender wel verwittigen
  - informatie loggen
  - alarmeren en iemand verwittigen
  - optioneel
    - pakket wijzigen (bv. adresvertaling, masquerading)
    - pakket versturen naar ander adres (proxy)
    - filterregels zelf aanpassen (bv indien vijandig pakket werd onderschept)

Packet filtering (4)

Voordelen:

- eenvoudig en goedkoop
- kan volledig netwerk beschermen
- eenvoudige filtering (weinig regels) is zeer efficiënt
- veelvuldig gebruikt (hardware en software)

Nadelen:

- niet steeds perfect
  - moeilijk configureerbaar
  - eens opgezet, moeilijk te testen (trial and error)
  - bugs in filtersoftware kan nare gevolgen hebben
- reduceert de performantie van de router
- geen controle op gebruikers of toepassingen (is poort 25 alleen gebruikt door SMTP ?)
- wat indien filter gecompromitteerd en hoe achterhalen ?

Single Box architecturen (slot)

Packet filters

best gebruikt in volgende situaties:

- te beschermen netwerk heeft al een hoge graad van hostbeveiliging
- aantal gebruikte protocols is klein
- zeer goed voor interne firewalls

Multi-Purpose boxes

- combinatie van proxy en filter
- combineert zowel voor- als nadelen van beide
- er is ook hier slechts één entiteit
- best gebruikt als
  - netwerk klein is
  - geen diensten aan het Internet moeten geleverd worden

Firewalls 31

Firewall architecturen

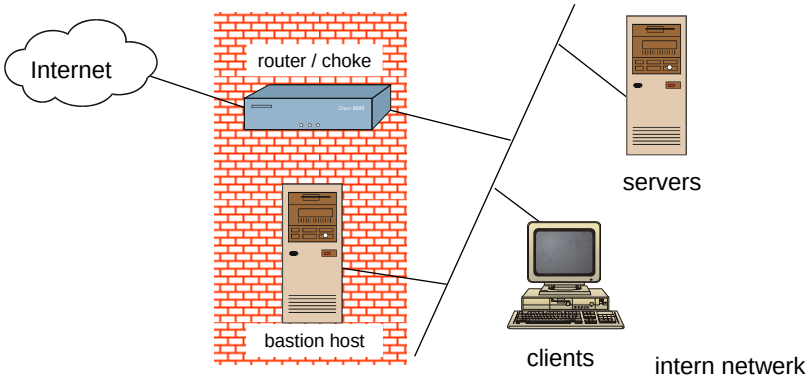
- Single Box architecturen
  - dual-homed gateway / dual-ported host
  - choke (screening router / packet filtering)
- Screened Host architecturen

  choke +
  - single-homed bastion host
  - dual-homed bastion host
- Screened Subnet architecturen
  - enkelvoudig
  - meervoudig

Firewalls 32

Screened Host architecturen

1. choke en single homed gateway



Firewalls 33

Screened Host architecturen (2)

Twee delen:

- router blokkeert alle
  - pakketten van buiten tenzij bestemd voor bastion host
  - pakketten van binnen tenzij afkomstig van bastion host
  - ongewenste pakketten en pakketten met IP source routing
- bastion host
  - voorziet in proxy services (circuit / application)
  - mail server of mail forwarder
  - externe DNS

Firewalls 34

Screened Host architecturen (3)

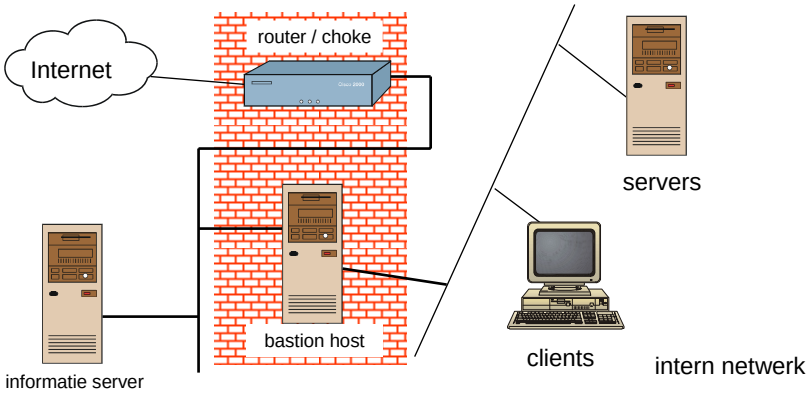
Evaluatie choke en single homed gateway

- duurdere implementatie
- twee systemen te beheren
- flexibele configuratie
- zwakke punten:
  - niet alle verkeer moet langs bastion host
  - slechts 1 in te nemen entiteit (router) = open netwerk
  - bastion host voorziet best niet in vitale diensten met risico (vb. www)

Screened Host architecturen (4)

2. choke en dual homed gateway

beter dan choke + single homed gateway

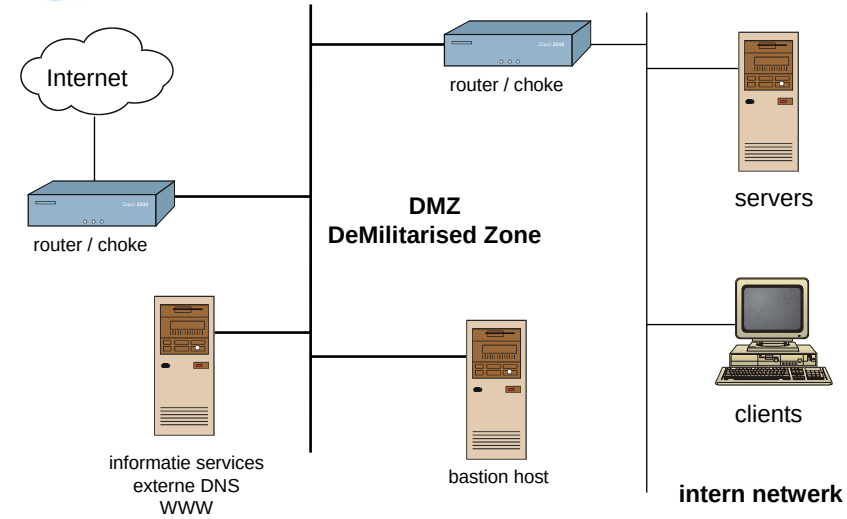


Firewall architecturen

- Single Box architecturen
  - dual-homed gateway / dual-ported host
  - choke (screening router / packet filtering)
- Screened Host architecturen

  choke +
  - single-homed bastion host
  - dual-homed bastion host
- Screened Subnet architecturen
  - enkelvoudig
  - meervoudig

Screened Subnet architectuur



Screened Subnet architectuur (2)

- twee chokes en 1 bastion host
- beste (enig goede) oplossing
- dual-homed gateway toegepast op gans netwerk
- creatie van *gedemilitariseerde zone* tussen intern en extern netwerk
- buiten-router toont alleen DMZ aan buitenwereld
- binnen-router toont alleen DMZ aan binnenwereld
- 3 niveaus van beveiliging
- bastion host mag single homed zijn
- routers van verschillende fabrikanten
- inbelmodems aansluiten op DMZ
- dure oplossing

Screened Subnet architectuur (3)

- Taken routers (cfr 1 choke)
  - blokkeren alle pakketten voor ongewenste diensten
  - blokkeren pakketten met eigenaardige opties
  - externe router:
    - **blokkeert pakketten naar intern netwerk of interne router**
    - **laat alleen pakketten door met IP-(bron/bestemmings)adres van gateway**
  - interne router:
    - **blokkeert pakketten naar extern netwerk of externe router**
    - **laat alleen pakketten door met IP-(bron/bestemmings)adres van gateway voor gedefinieerde proxy-poorten**
  - kan ook minder strict: laat bv HTTP rechtstreeks door

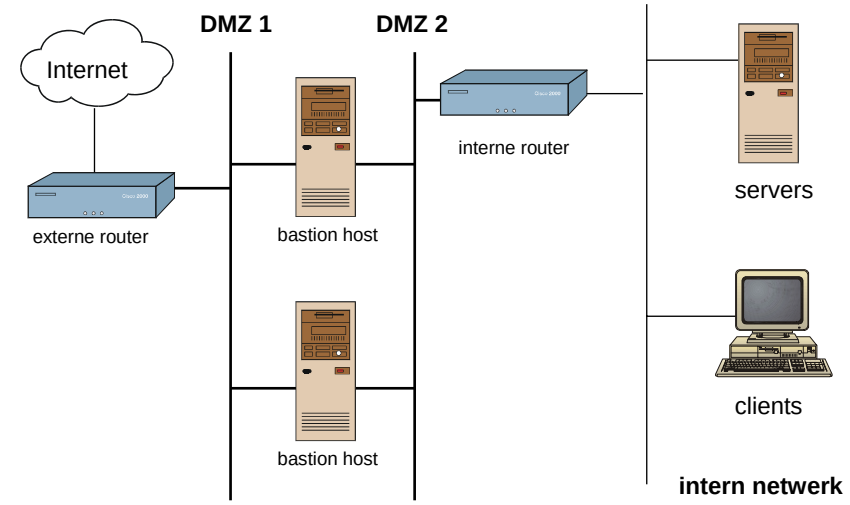
Screened Subnet architectuur (4)

- Taken bastion host (gateway)
  - proxy service voor interne gebruikers van diensten op extern netwerk
  - mail server of mail forwarder
  - externe DNS en WWW (beter op aparte server)

Meerdere Screened Subnets

- interne netwerkdelen verschillende veiligheidseisen
- varianten:
  - split-screened subnet
    - opsplitsing DMZ dmv 1 of meer dual-homed gateways
    - voorziet vb. in bescherming van administratieve protocols op machines in DMZ
    - routing en proxyservices beter af te regelen
  - onafhankelijke screened-subnetten
    - twee toegangen tot Internet via aparte DMZ's
    - voorziet in redundantie
    - no single point of failure
    - ook: inkomend en uitgaand verkeer scheiden
  - interne firewalls

Split Screened Subnets



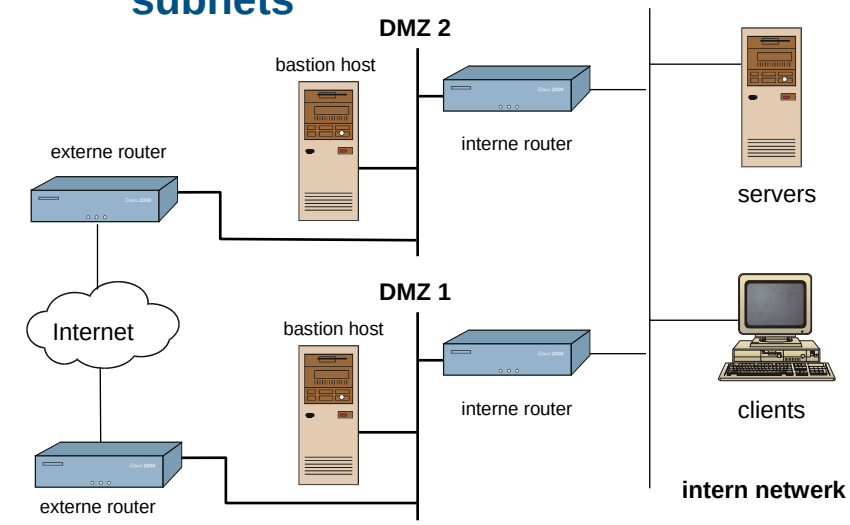
Firewalls 43

Meerdere Screened Subnets

- interne netwerkdelen verschillende veiligheidseisen
- varianten:
  - split-screened subnet
    - opsplitsing DMZ dmv 1 of meer dual-homed gateways
    - voorziet bv in bescherming van administratieve protocols op machines in DMZ
    - routing en proxyservices beter af te regelen
  - onafhankelijke screened-subnetten
    - twee toegangen tot Internet via aparte DMZ's
    - voorziet in redundantie
    - no single point of failure
    - ook: inkomend en uitgaand verkeer scheiden
  - interne firewalls

Firewalls 44

Independent split screened subnets



Firewalls 45

Firewalls: do en don’ts

- vermijd twee interne routers op zelfde intern netwerk
  - mogelijk vertrouwelijk verkeer in DMZ
  - moeilijker onderhoudbaar
- beter verschillende interne netwerken
  - naar 1 router met verschillende interfaces
  - met elk 1 router naar een backbone, vandaar via router naar DMZ
- meerdere externe routers naar zelfde DMZ is O.K.

Firewalls 46

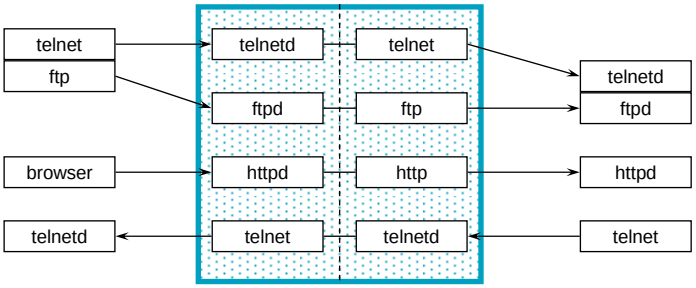
Proxy servers

- Application Level Gateway (later meer)
  - verstaat en interpreteert commando's in applicatieprotocol
  - zeer extreem voorbeeld is sendmail
- Circuit Level Gateway (later meer)
  - creëert een verbinding (circuit) tussen client en server
  - trekt zich niets aan van applicatieprotocol
  - SOCKS

Application Level Gateway

- wordt dikwijls aangeduid als *proxy*
- fungeert als relais voor toepassingsverkeer
- trekt zich niets aan van IP-data
- proxy heeft twee gezichten
  - is server voor client (source)
  - is client voor server (destination)
  - maakt virtuele verbinding tussen client en server
- schijnbaar transparant voor client en server
- proxy kan voorzien in
  - data-monitoring
  - data-filtering

Application Level Gateway (2)



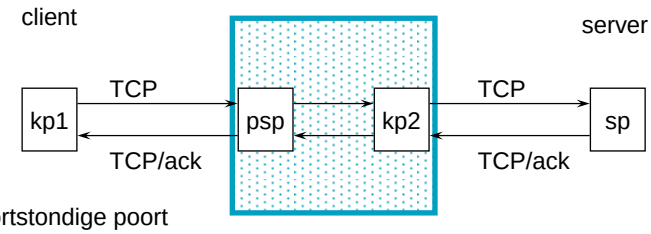
Beveiligd netwerk

Onbeveiligd netwerk

Firewalls 49

Application Level Gateway (3)

- clientsoftware moet proxy-aware zijn
- elke gewenste applicatie vereist corresponderende proxysoftware op gateway
- voorbeeld



kp kortstondige poort
psp proxy server poort
sp server poort

Firewalls 50

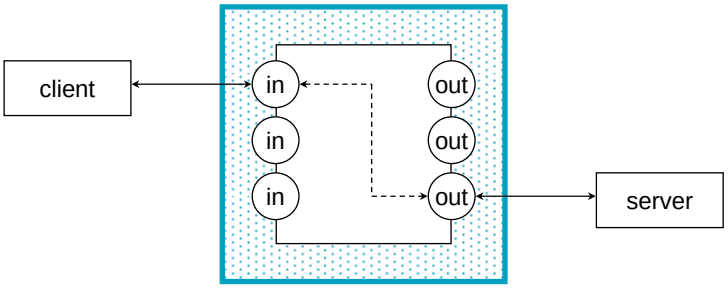
Application Level Gateway (4)

- voor en tegen
  - veiliger dan packet filters
  - eenvoudig op te zetten
  - eenvoudig te loggen (vb url's)
  - gebruikers moeten zich soms extra authenticeren op proxy (vb telnet, ftp)
  - bijkomende processing overhead
    - twee gesplitste verbindingen tussen end-users
    - gateway moet alle verkeer onderzoeken en doorgeven

Web Application Firewall

- speciaal geval van Application Level Gateway
- reverse proxy
- webserver is beschermd door application firewall
- meest nuttig bij dynamische websites
- inkomende aanvragen (url's) worden geanalyseerd
- laat detectie toe van vb. SQL-injectie-aanvragen
- moeilijk te configureren en te testen
- vereist een goede kennis van zwakke punten in de website

Circuit Level Gateway



- relais van TCP (en UDP) connecties
- geen extra verwerking of filtering van pakketten
- laat geen rechtstreekse verbinding toe tussen server en client
- bepaalt welke verbindingen zijn toegelaten

Circuit Level Gateway (2)

- functioneel gelijkaardig aan packet filters
- beveiliging tegen misbruik van pakkethoofdingen
- standaard beveiliging tegen pakketfragmentatie (niet bij packet filters)
- vaak alleen gebruikt voor connecties van verkeer dat naar buiten gaat (interne gebruikers ‘te vertrouwen’)
- vaak gecombineerd met applicatieniveau gateway
  - proxy voor connecties van buiten naar binnen
  - circuit level voor connecties van binnen naar buiten
  - vermindert processing overhead
- Voorbeeld van implementatie: SOCKS

Circuit Level Gateway: SOCKS

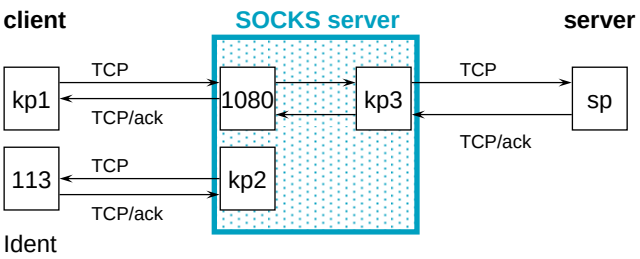
- versie 5 = RFC 1928 (standaard)

  The protocol is designed to provide a framework for client-server applications in both the TCP and UDP domains to conveniently and securely use the services of a network firewall. The protocol is conceptually a "shim-layer" between the application layer and the transport layer, and as such does not provide network-layer gateway services, such as forwarding of ICMP messages.

- componenten:
  - SOCKS server
  - SOCKS client bibliotheek, gebruikt op beschermde hosts
  - aangepaste (*SOCKSified*) versies van de client-software

SOCKS werking (2)

- client wenst TCP-verbinding met host via firewall
- client opent TCP-connectie op poort 1080 met SOCKS-server
- client onderhandelt over authenticatiemethode
- client authentiseert zich met gekozen methode
- client doet een relais-aanvraag
- server zorgt voor de uitgaande verbinding indien alles O.K.
- UDP afgehandeld na TCP-connectie voor authentisering



SOCKS ondersteunt (3)

- Authenticatie
  - username/password en one-time password
  - Kerberos
  - RADIUS (remote authentication dial-in services)
  - PAP (password authentication protocol)
  - IPSEC
- Encryptie
  - DES / 3DES en IPSEC
- Tunneling protocols
  - PPTP (point-to-point tunneling protocol), L2F (layer2 forwarding), L2TP
- Sleutelbeheer
  - ISAKMP/Oakley

Network Addres Translation (NAT)

- RFC 1631
- interne netwerkadressen verschillend van externe
- vertaling door choke (cfr packet filtering)
- korte termijn oplossing voor gebrek aan officiële IP-adressen
- alleen een klein aantal hosts in privaat netwerk is direct verbonden met Internet en moet van buiten af bereikbaar zijn
- voegt op zich geen extra veiligheid toe
- verbergt wel interne netwerkopbouw
- NAT verandert van uitgaand pakket het bronadres (en poortnr)

NAT: werking (2)

- NAT bevat pool met officiële adressen
- uitgaand pakket
  - toegelaten?
  - zo ja, bronadres wordt veranderd in volgend niet gebruikt officieel adres
- inkomend pakket
  - bestemmingsadres gebruikt door NAT?
  - zo ja, bestemmingsadres veranderd in privaat adres
- associaties in de map met overeenkomsten worden wegnenomen na een idle-status van 15 min (default)
- alleen TCP en UDP pakketten worden omgezet

NAT (3)

Nadelen:

- hoe lang adresovereenkomsten bewaren?
- problemen met bv FTP (verborgen adressen)
- niet compatibel met IPSEC
- loggen van vertaalde adressen heeft geen zin
- dynamische toekenning van poorten kan interfereren met packet filtering

Linux: packet filtering en NAT

Packet Filtering: iptables

- ketting van regels
- 3 standaard kettingen:
  - input ketting: verwerkt elk inkomend pakket
  - output: verwerkt elk uitgaand pakket
  - forwarding: verwerkt elk pakket dat naar andere netwerkinterface moet gestuurd worden

NAT: masquerading

- werkt slecht met 1 officieel adres
- gebruikt nieuw poortnr: 1 uit 4096 vanaf 61.000
- max 4096 TCP en 4096 UDP simultane connecties

Linux masquerading