# Sare Segurtasuna

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus

Universidad del País Vasco
Euskal Herriko Unibertsitatea
BILBOKO INGENIARITZA ESKOLA
ESCUELA DE INGENIERÍA DE BILBAO

# Sare Segurtasuna

https://doi.org/10.5281/zenodo.4302267

https://github.com/mikel-egana-aranguren/EHU-issks-31

# Aurkibidea

- Definizioak
- Arriskuak eta babesak
- Adibideak
- Eraso ohikoenak

# Definizioak

Sare telematikoa: datuak transmititzeko bitarteko baten bidez konektatutako ekipoen multzoa (kableak, uhinak)

Helburua informazioa, baliabideak eta zerbitzuak partekatzea da

# Definizioak

Protokolo telematikoa: komunikazioaren sintaxia eta semantika definitzen dituen erregela-multzo zorrotza (HTTP, DNS, TCP/IP,...)

Interkonexio-elementuak (routerra, sare-txartela...)

# HTTP

Hipertestua transferitzeko protokoloa (Hypertext Transfer Protocol edo HTTP) World Wide Webean informazioa transferitzea ahalbidetzen duen komunikazio-protokoloa da

HTTP estaturik gabeko protokoloa da, ez du aurreko konexioei buruzko informaziorik gordetzen

Web aplikazioekin bezero-egoera mantentzea: cookieak

# DNS

Domeinu-izenen sistema (Domain Name System edo DNS). IP sareetara (Internet edo sare pribatu bat) konektatutako gailuetarako banatutako nomenklatura hierarkikoko sistema bat da

Pertsonentzako izen ulergarriak sarera konektatutako ekipoekin lotutako identifikatzaile bitarretan "itzuli"

Ekipo horiek mundu osoan aurkitzea eta konexioa bertara zuzentzea

# TCP/IP

TCP/IP eredua sareetako komunikazioetarako erabiltzen da

Eragiketa-gida orokorren multzo bat deskribatzen du, ekipo bat sare batean komunikatu ahal izateko

TCP/IPk muturretik muturrerako konektagarritasuna ematen du, zehaztuz nola formateatu, bideratu, transmititu, bideratu eta jaso datuak

# Definizioak

Sareko segurtasuna: ahuleziak minimizatzea ahalbidetzen duten tekniken multzoa: babestutako informazioa lortzearen kostua haren balioa baino handiagoa izatea lortu nahi da

Sare seguru bat lortzeko, segurtasun-mekanismoak zehazten dira

# Definizioak

Segurtasun-mekanismo horiekin komunikazio-protokolo seguruak zehazten dira

Komunikazio-protokolo seguruek segurtasun-zerbitzuak ematea errazten dute

# Arriskuak eta sareen babesa

Segurtasun-zerbitzu garrantzitsuenak:

- Erakundeen autentifikazioa
- Datuen konfidentzialtasuna
- Datuen osotasuna
- Sarbide-kontrola
- Zapuztezintasuna
- Prestasuna
- Anonimotasuna

# Arriskuak eta sareen babesa

Entitateen autentifikazioa: erakunde komunikatzaile batek esaten duena dela bermatzen du

Datuen konfidentzialtasuna: datuen babesa ematen du, baimenik gabeko erabiltzaile bati ustekabean edo nahita ezagutaraztea saihesteko

# Arriskuak eta sareen babesa

Datuen osotasuna: jasotako informazioa igorleak bidalitakoa dela egiaztatzeko eta informazio hori aldatu den jakiteko aukera ematen dio informazioaren hartzaileari

Sarbide-kontrola: baimendu gabeko pertsonek zerbitzuak/informazioa erabiltzea saihesten du

# Arriskuak eta sareen babesa

Zapuztesintazuna:

- Jatorri-proba dutenak: informazioa jasotzen duenak igorgailua nor den froga dezake
- Bidalketa-probarekin: hartzaileak/igorleak bidalketaren data eta orduaren proba bat dauka
- Entrega-proba dutenak: igorleak froga dezake hartzaileak jaso duela informazioa

# Zapuztezintasun adibidea

Whatsapp-a zifratzeko sistema

Klik bikoitza jasotzean, urdin irakurriz

Ezin dugu ukatu bidali izana

Ezin dute ukatu jaso dutela

# Arriskuak eta sareen babesa

Prestasuna: Beharrezkoa denean informazioa/baliabideak eskuragarri egongo direla ziurtatzen du (eskuratu, kontsultatu/erabili ahal izango dira)

# Arriskuak eta sareen babesa

Anonimotasuna: Zerbitzu jakin bat erabiltzen duen pertsonaren nortasuna ezkutatzen du

Ezinbestekoa da zenbait zerbitzutan: inkestak, boto elektronikoa, zenbait transakzio ekonomiko

# Eraso ohikoenak

Kautotzeari: intertzeptazioa, ordezkapena

Informazioari: errebelazioa, berrigortzea, manipulazioa, arbuioa (Zapuztea)

Zerbitzuei: ukatzea, jabetzea

# Nola babestu sareak?

Segurtasun perimetrala:

- Sare arkitektura eta elementuak erabili sare baten perimetroari, beste baten aurrean, babesa ematen diona
- Normalean barne-sarea eta Internet

# Segurtasun-mekanismo erabilienak

Segurtasun perimetrala:

- Suebaki (Firewall)
- Atzemateko eta Intrusioak Prebenitzeko Zerbitzuak
- Birusen eta spamen aurkako pasabideak
- Sare birtual pribatuak (VPN)
- Proxy-ak
- UTM-ak
- Honeypot-ak

# Segurtasunik gabeko arkitekturaren adibidea

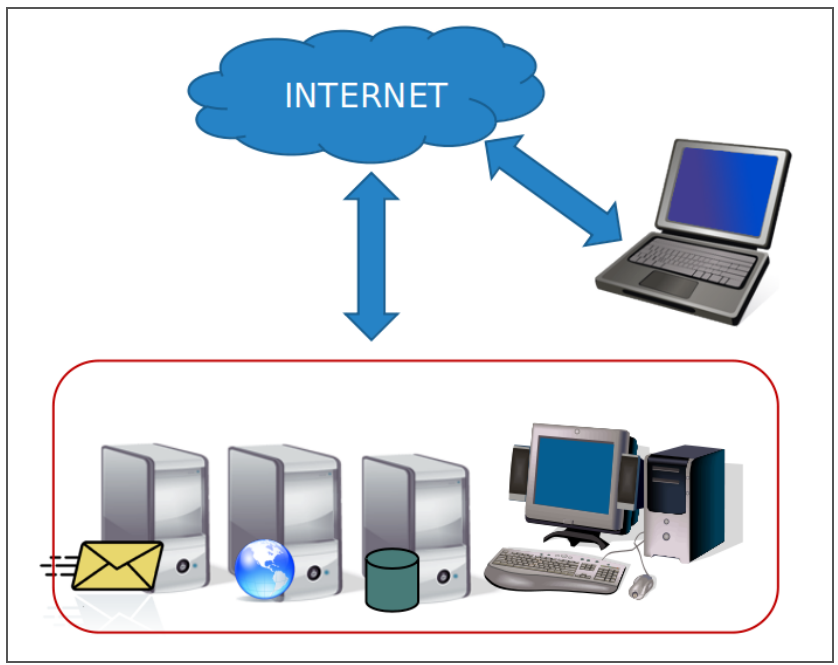
Ez da trafikoa iragazten

Barne-zerbitzuak argitaratzea (BD)

Ez da malware edo SPAM egiaztatzen

Urruneko bezeroa zuzenean sartzen da zerbitzuetara

# Segurtasunik gabeko arkitekturaren adibidea



# Firewall

Sarbide-politika definitzen duen sare-elementua (hardwarea edo softwarea), trafikoa baimenduz edo ukatuz, haren arauak definitu ahala

Erabilera:

- Politika murriztailea (zerrenda zuria): esplizituki onartzen den guztia ez beste guztia ukatzen da
- Politika baimentzailea (zerrenda beltza): dena onartzen da, esplizituki ukatzen dena izan ezik

# Firewall: zeren aurka babesten duzu?

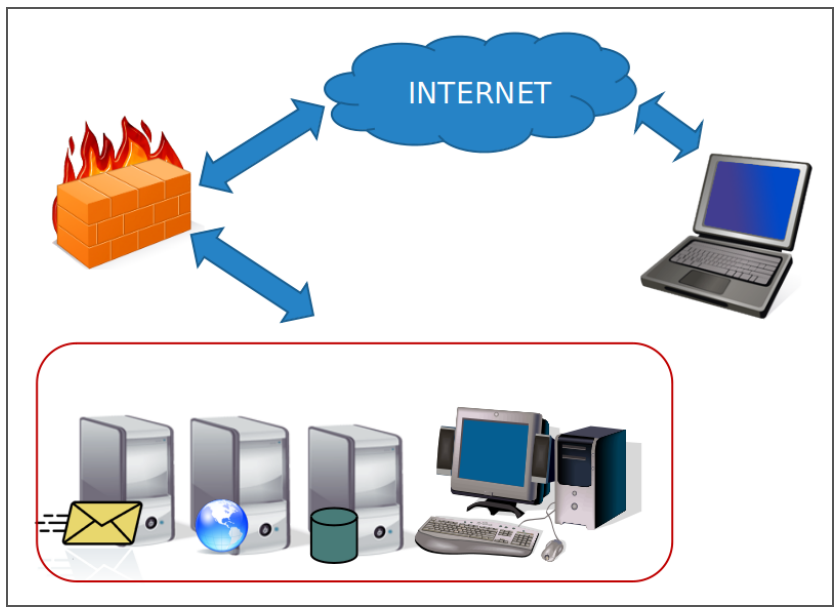
Kanpotik autentifikatu gabeko sarbideen aurka

Kanpotik baimendu gabeko trafikoaren aurka

Barrutik irteera baimendua ahalbidetzen du

Puntu bakarra ematen du segurtasun- eta auditoretza-politika ezartzeko

# Firewall



# Firewall: zeren aurka ez du babesten?

Suebakitik igarotzen ez diren kanpoko sarbideen aurka

Barrutik egindako erasoen aurka

Birusen aurka, troiarrak, SPAM

Informazioa beste bide batetik irtetearen aurka (USBak, posta elektronikoa, etab.)

# Firewall motak

Pasabide-mailakoak: aplikazio zehatzak iragazten ditu, hala nola FTP edo Telnet

Sare-geruzakoa: jatorriko/helmugako IParen eta jatorrizko/helmugako portuaren araberako iragazkia

Aplikazio-geruzakoa: komunikazio-protokoloaren araberako iragazkia

Pertsonalak: makinan bertan instalatuta, makinaren sarrera- eta irteera-konexioak iragazten ditu

# Firewall

| Regla | Acción | IP Origen | IP Destino | Proto-colo | Puerto Origen | Puerto Destino |
|---|---|---|---|---|---|---|
| 1 | Aceptar | 172.16.0.0/16 | 192.168.0.4 | tcp | cualquiera | 25 |
| 2 | Aceptar | cualquiera | 192.168.10.8 | tcp | cualquiera | 80 |
| 3 | Aceptar | 172.16.0.0/16 | 192.168.0.2 | tcp | cualquiera | 80 |
| 4 | Negar | cualquiera | cualquiera | cualquiera | cualquiera | cualquiera |

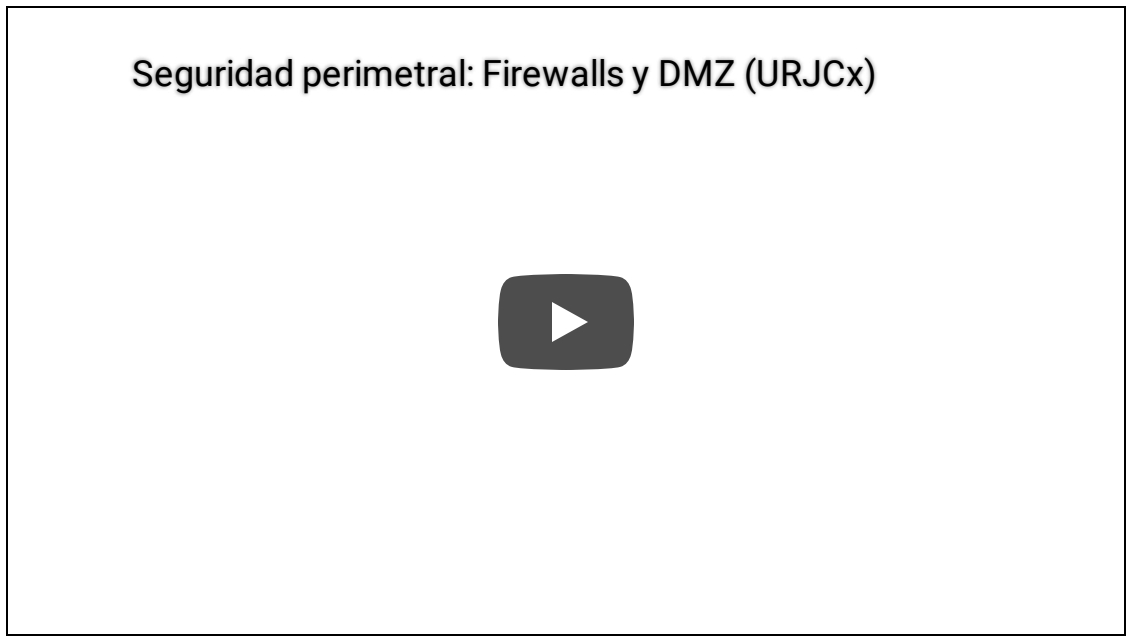
# DMZ, DeMilitarized Zone

Zerbitzu publikoak (posta, ftp, etab.) segurtasun-arazoen arrisku handiagoa dutenez intranet eta Internet artean jartzen dira

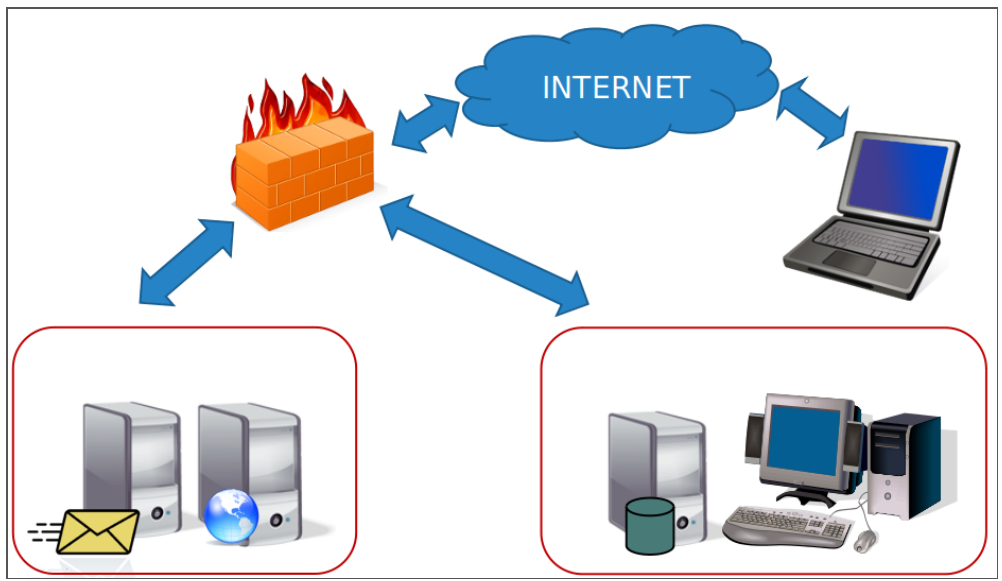
Sareen arteko sarbidea mugatzen duen suebaki bat edo bi erabiliz sortzen da

Eremu desmilitarizatutik ezin da zuzenean intranetera sartu

# DMZ



# DMZ



# Detektatzeko eta Intrusioak Prebenitzeko Sistemak (IDS/IPS) (IDS/IPS)

Baimendu gabeko sarbideak detektatzen ditu/sarean edo makina batean

behar ez bezala erabiltzea

IDSek administratzaileari abisatzen diote (erreaktiboak)

IPSak blokeatu egiten dituzte eraginik izan ez dezaten (proaktiboak)

# IDS/IPS motak

HIDPS (Host IDPS): makinan instalatzen da eta aldaketak detektatzen ditu sistema eragilean eta aplikazioetan

NIDPS (Network IDPS): sare lokaleko trafikoa monitorizatzen du

WIDPS (Wi-Fi IDPS): hari gabeko trafikoa monitorizatzen du

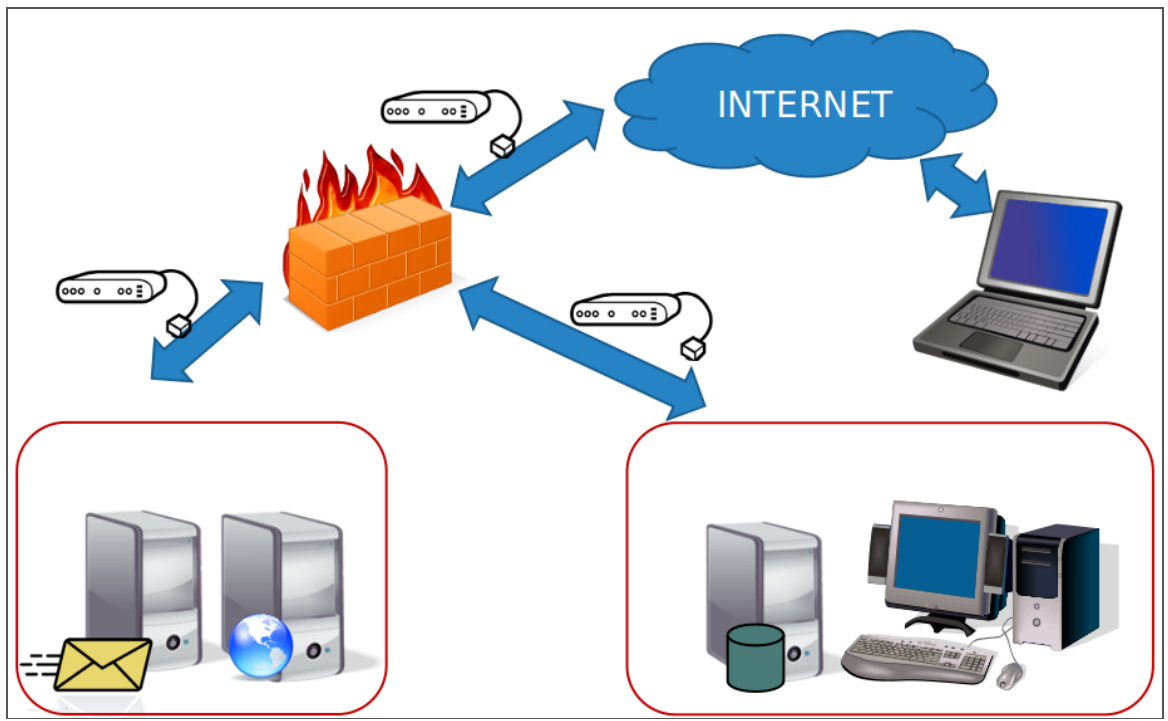
NBA (Network Behaviour Analysis): sareko trafikoaren portaera aztertzen du

# IDS/IPS baten funtzionamendua

Heuristika: portaera "arraroak" aztertzen ditu, eta detektatzen dituenean, alarma pizten du

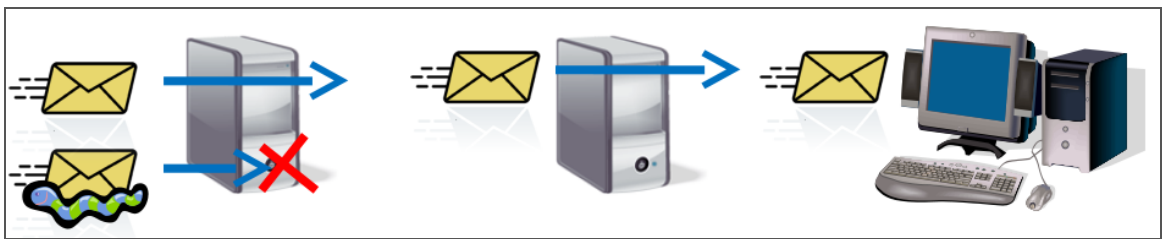
Sinadurak: eraso eredu ezagunak detektatzen ditu (Arazo eraso berrien aurrean)

# IDS/IPS



# Birusen eta spamen aurkako pasabideak

Trafikoa aztertzen dute eta eduki maltzurrak barne-sarera iragazten dituzte



# Sare Birtual Pribatuak (VPN)

Segurua ez den azpiegitura erabiltzen duen sarea (Internet), barne-sare batera modu seguruan sartzeko

Barne-sarera urrutitik konektatzeko erabiltzen direnak

VPN EHU

# Sare Birtual Pribatuak (VPN)

Baimentzen du:

- Erabiltzaileak, rolak eta baimenak kudeatuz autentifikatzea eta baimentzea
- Osotasuna hash funtzioekin
- Konfidentzialtasuna, informazioa enkriptazio-algoritmo baten bidez zifratuta doalako
- Zapuztezintasuna, datuak sinatuta transmititzen direlako

# Proxy

Bitartekari-lanak egiten dituen programa edo gailua

Bezeroak proxyari egiten dizkio eskaerak, eta proxy horrek kudeatzen ditu

Proxy bat erabiltzeak segurtasun handiagoa ematen du nabigazioan,

zerbitzariak ez baitaki benetan nor konektatu den

Bezeroak kanpoko mundutik isolatu

# Mehatxuen kudeaketa bateratua (UTM) (UTM)

Komunikazioen segurtasunarekin lotutako hainbat alderdi biltzen dituen gailua:

- Firewall
- IDS / IPS
- Birusen eta spamen aurkako pasabideak
- VPN

# Honeypots

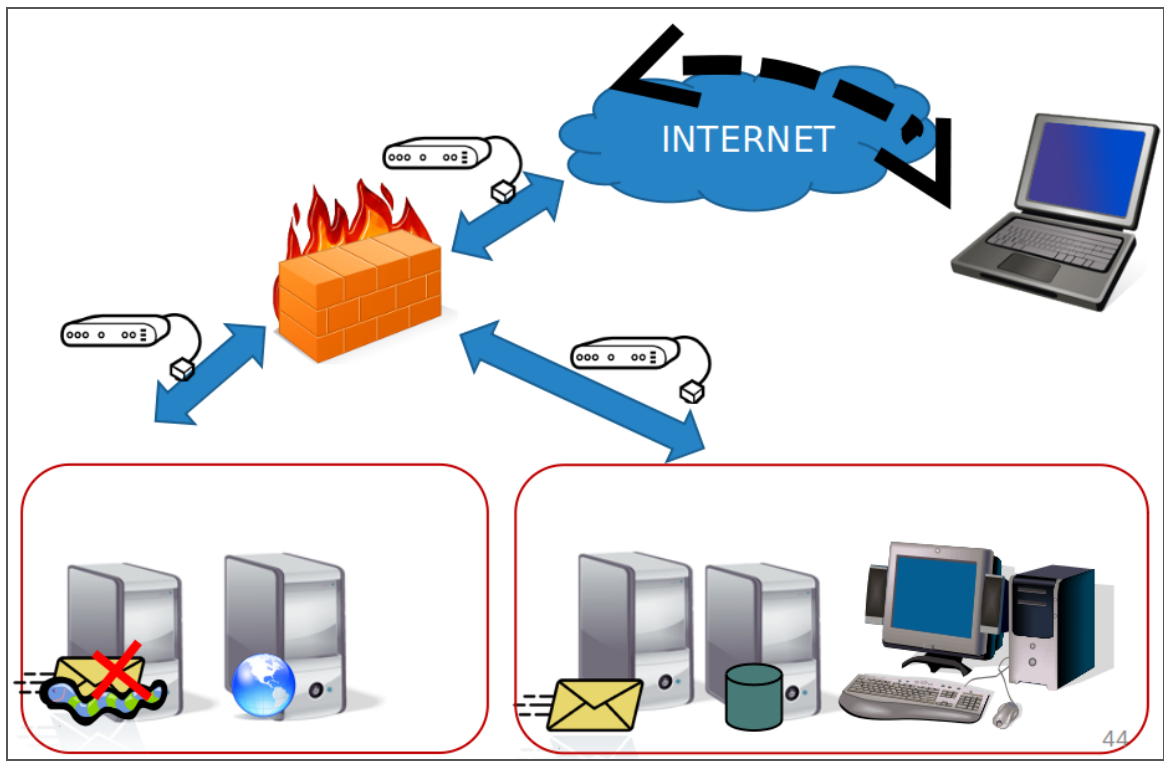
Erasoak jasotzeko eta teknika berriak aztertzeko konfiguratutako sistema

Birusen eta spamen laginak jasotzeko ere erabiltzen dira

Bereziki kontrolatuta egon behar dute eta edozein barne-saretatik kanpo

# Honeypots

# Arkitektura seguruaren adibidea



# Arkitektura seguruaren adibidea

Suebakia instalatzea:

- DMZ eta barneko sarea
- Politika murriztailea

Antispam eta antibirusak instalatzea

NIDS-ak instalatzea hiru interfazetan

# Arkitektura seguruaren adibidea

Segmentazioa:

- Publikoa: Web, antispam/antibirus pasabideak
- Pribatua: DB, posta zerbitzaria

Urruneko bezeroek VPN erabiltzen dute

# Eraso ohikoenak

Sniffing: Sarean zehar doan informazioa intertzeptatzea

Man in the middle: Informazioa intertzeptatzeaz gain, nahierara txertatu eta alda daiteke

# Eraso ohikoenak

Hijacking: Sisteman baimendutako erabiltzaile bati konexioak lapurtzea

- IP Hijacking
- Session hijacking
- DNS Hijacking
- ...

# Eraso ohikoenak

Spoofing (Ordezpen)

- IP Spoofing
- MAC Spoofing
- DNS Spoofing
- ...

# Eraso ohikoenak

"Denegación de Servicio (DoS)": Hardwarea edo softwarea "saturatzen" da erantzuteari utzi arte

"Ataque Distribuido de Denegación de Servicio (DDoS)":

- Hainbat makinatatik egiten da.
- Batek master lanak egiten ditu eta besteak koordinatzen ditu

GitLab servers are being exploited in DDoS attacks in excess of 1 Tbps