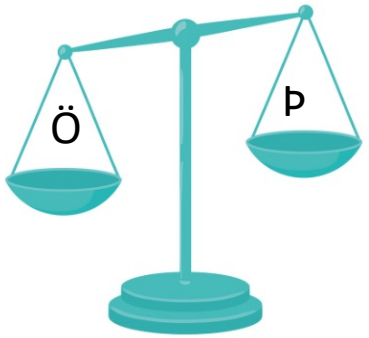
Netöryggi

Cyber Security

Jafnvægið: öryggi - þægindi



Mikilvægt að finna rétt jafnvægi milli öryggis og þæginda

- Starfsmaður getur ekki unnið vinnuna sína vegna öryggis ráðstafanna
- Rekstur fyrirtækis er í hættu vegna öryggsleysis

Við hugsum stundum of mikið um þægindin og bölvum öryggginu

Hvað er verið að verja

- Mikilvæg gögn, t.d.
  - Upplýsingar um fólk
  - Uppýsingar um rekstur

- Starfshæfni, t.d.
  - Getur starfmaður unnið
  - Getur fyrirtækið/sofnun starfað

Einföld og góð ráð

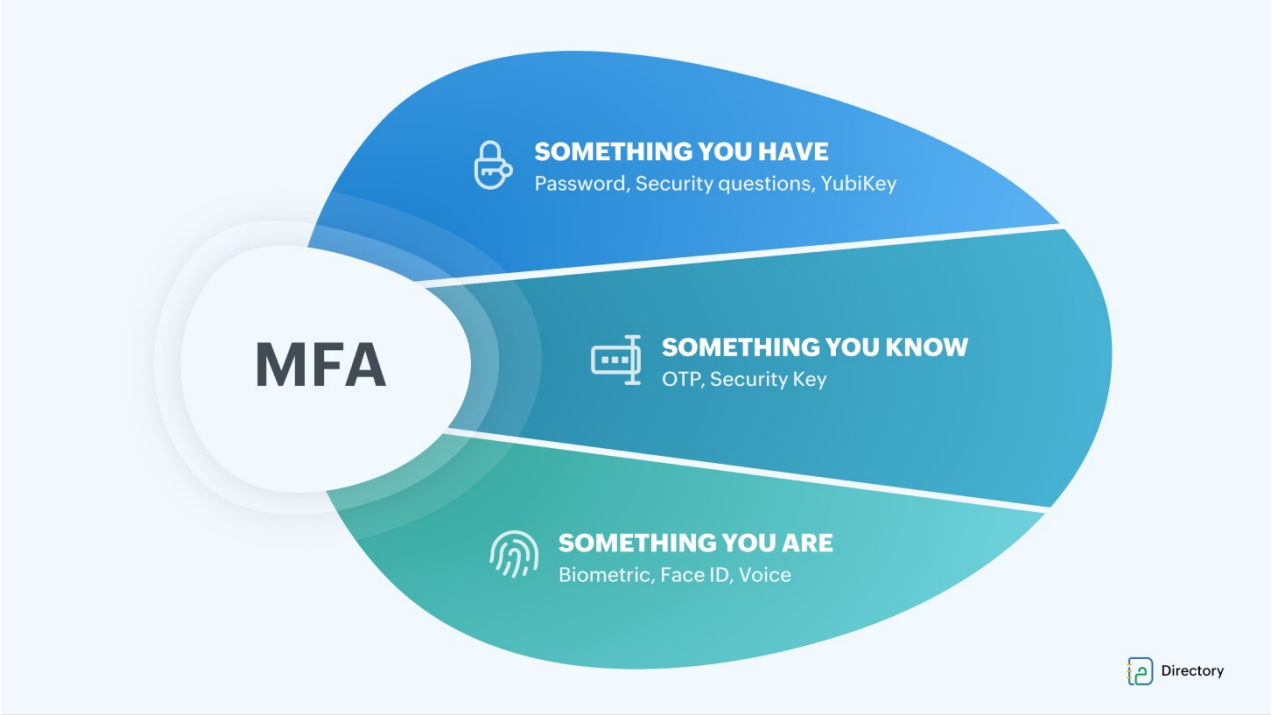
- Setja og fylgja reglum
- Kerfisstjórnun=> kerfisstjóri mikilvægur

- Eyða gömlum aðgöngum
- Ekki leyfa notendum að setja upp forrit
- Ekki nota admin aðgang í hefðbundinni tölvuvinnslu
- MFA: Multi-Factor Authentication: Fjölþátta auðkenning
- Uppfæra stýrikerfi og hugbúnað
- Lágmarka réttindi

https://learn.microsoft.com/en-us/services-hub/health/remediation-steps-ad/regularly-check-for-and-remove-inactive-user-accounts-in-active-directory

MFA: Multi-Factor Authentication: Fjölþátta auðkenning

- Fjölþátta auðkenning:
  - Rafræn skilríki: island.is
  - Google Authenticator
  - Microsoft Authenticator
  - SMS: textaskilaboð
  - RSA Secure ID: (var mikið notað)



Með því að notfæra sér fjölþátta auðkenningu þarf alltaf að sannreyna á annan máta að maður sjálfur sé að fara inn á aðganginn.

Uppfærslur

- Gamall hugbúnaður skapar oft mikla hættu
  - Það er ekki að ástæðu lausu að við erum með sjálfvirka uppfærslu á stýrikerfum og snjalltækjum.

- Það eru til lausnir sem hjálpa
  - Microsoft System Center
  - Atera
  - Freshservice

https://comparisons.financesonline.com/microsoft-system-center-vs-atera

Tvö mikilvæg hugtök

Attack surface : *árasarflötur*

- Árásarflötur er fjöldi staða eða leiða, þar sem óviðkomandi notandi getur komist inn í kerfi, nálgast í gögn eða skaðað kerfið. Því minni sem árásarflöturinn er, því auðveldara er að vernda það.

Social Engineering : *samskiptablekking*

- Samskiptablekking vísar til allra aðferða sem miða að því að finna leið til að afhjúpa tilteknar upplýsingar eða framkvæma ákveðna aðgerð af ólögmætum ástæðum

Social Engineering : *samskiptablekking*

Dæmi um hættur

- Við treystum fólki, stundum þeim sem við eigum ekki að treysta
- Fólk vill hjálpa, jafnvel fólk sem á ekki að hjálpa
- Fólk er upptekið og að flýta sér
- Fólk er forvitið

Social Engineering : *samskiptablekking*

Könnum varnir gegn samskiptablekkingum (social engineering penetration test)

- ATH hvort óviðkomandi komist inn á lokuð svæði
  - Fylgir starfsmanni eftir við lokaða hurð og kemst inn
  - Klæddur í þjónustuföt, öryggisfyrirtæki, tölvufyrirtæki o.frv.
    - Hvað kemst viðkomandi langt – komst eitthvað í samband?
- USB lykkill skilin eftir við inngang
  - Er hann settur í samband?

- Gott að ráða fyrirtæki til að gera svona prófanir

Social Engineering : *samskiptablekking*

Könnum varnir gegn samskiptablekkingum (social engineering penetration test)

- Hvað með rafræn svik. Phishing - fake Surveys
  - Kunna starfsmenn að staðfest uppruna póst?
  - Taka þeir þátt í könnunum á netinu?
  - Þjálfa upp vitund með æfingum, hermun
  - Það er ekki findið að hafa lykilorð undir lyklaborði, það er alvarlegt
- Gott að ráða mismunandi fyrirtæki til að gera svona prófanir

Netöryggisstefna

Employees cyber security policy.

- https://resources.workable.com/cyber-security-policy

- Slóð á síðu sem hefur gott sniðmát til að búa til netöryggistefnu

Fjarvinna og netöryggi

Þegar starfsmaður kemur til vinnu

- Leggur bíl í stæði
- Kemst inn í byggingu
- Hittir samstarfsmenn
- Skráir sig inn á tölvuna sína

Þegar starfsmaður vinnu að heiman

- Skráir sig inn á tölvuna sína
  - Jafnvel einkatölvu

Fjarvinna og netöryggi

Þegar starfsmaður vinnu að heiman

- Layer 2 VPN - Fyrirtækja VPN
  - Sambandið er dulkóða og það er eins og tölvan sé staðset inn í fyrirtækinu
  - Mikilvægt að nota MFA í tengslum við VPN
  - Hvaða tölvur er verið að nota, heimilstölvu sem við höfum ekki stjórna á?
  - Betra að útvega starfsmönnum tölvu sem eru hugsuð til vinnu

Eða

- Nota sýndavélar (virtual desktop) => við getum stýrt betur
  - PCoIP (PC over IP) remote display protocol, VMware notar (*thin client vs thick client*)
  - Blast VMware Blast Extreme nýrra notar onsite grafík kort betur

https://www.techtarget.com/searchvirtualdesktop/definition/PCoIP-PC-over-IP

Best Virtual Desktop Infrastructure (VDI) Software
https://www.g2.com/categories/virtual-desktop-infrastructure-vdi

DDoS Attack – stöðvar þjónustu

Distributed **D**enial-**o**f-**D**ervice (DDoS)

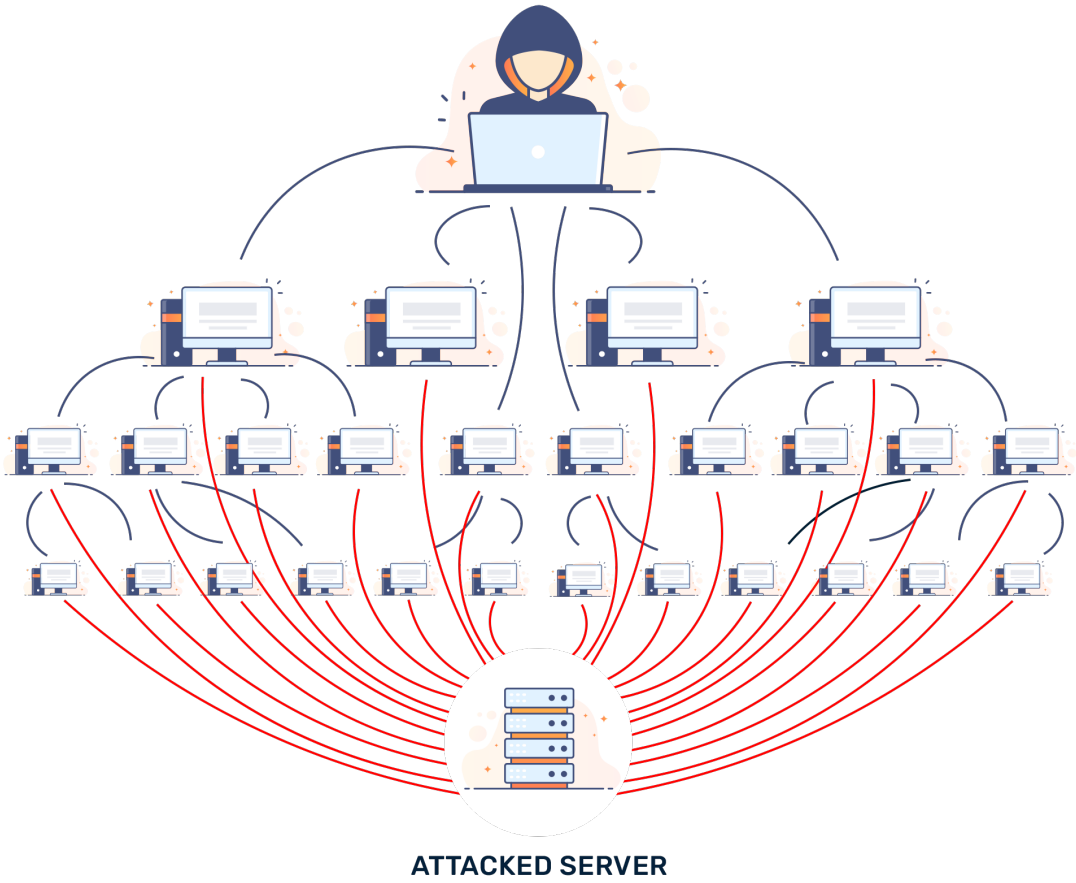
Það er búin til yfirflæði á umferð

t.d. með fyrirspurnum og við það:

Verður yfirálag á NET

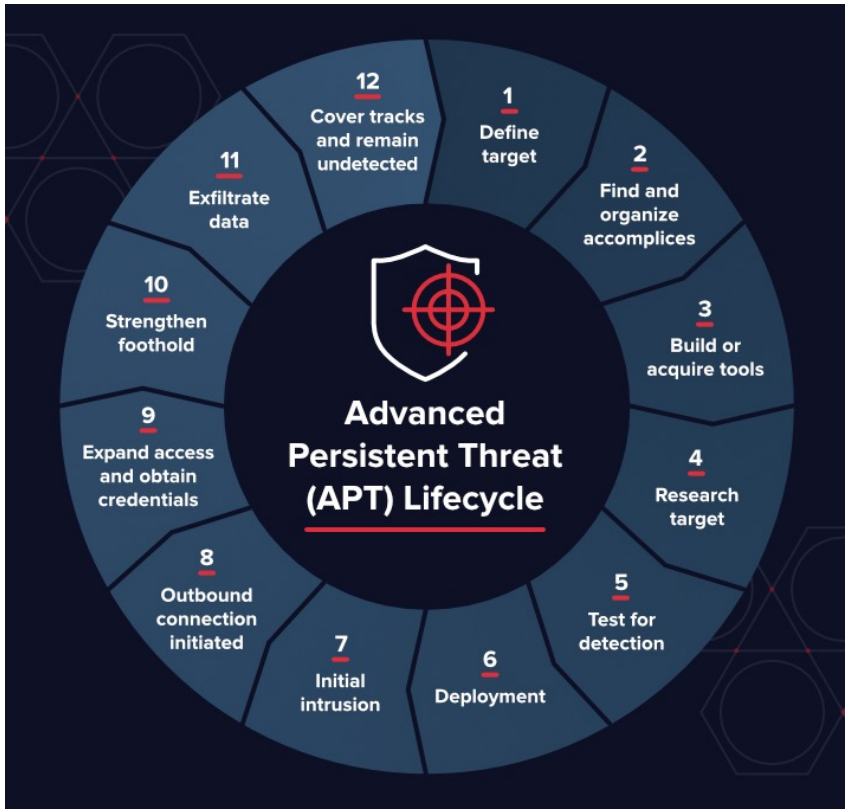
Verður yfirálag á CPU

Hugsað til að skaða þjónustu og skemma!



APT advanced persistent threat

- Háþróuð viðvarandi ógn (APT)
- Langvarandi og markviss netárás þar sem boðflenna fær aðgang að neti og er ógreind í langan tíma.
- APT árásir eru gerðar til að stela gögnum frekar en að valda skemmdum á netkerfi eða þjónustu.



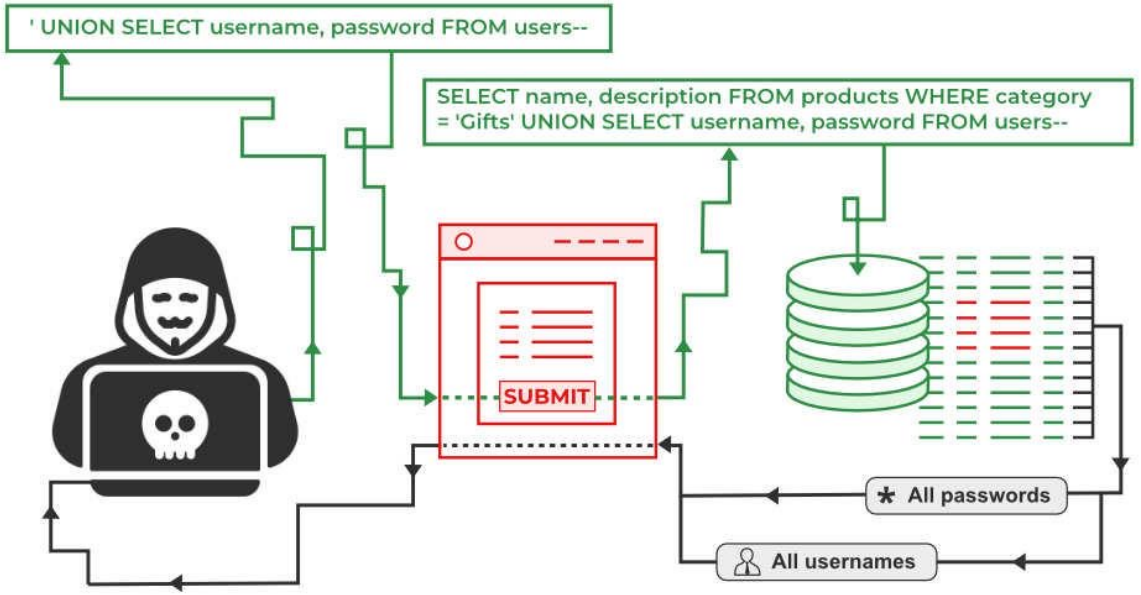
Tailgate *=> kemst inn og stingur í samband við LAN*

Ransomware*: spilliforrit sem meinat notanda aðgang að skrám á tölvunni sinni*

SQL injection

- SQL injection er algeng vef hökkun (web hacking techniques)
- SQL injection
- *usually occurs when you ask a user for input, like their username/userid, and instead of a name/id, the user gives you an SQL statement that you will **unknowingly** run on your database.*

- Markmiðið hér er að fá aðgang til að lesa og breyta og eyða töflum úr gagnagrunni



Ráð

- Takmarka aðgang, læsa tölvuskápum
- Aðgangsstýring að húsnæði og eftirlit, t.d. myndavélar
- Skipta netum rétt upp (VLAN) properly segment network
- Uppfæra netbúnað og vélbúnað
- Uppfæra stýrikerfi og forðast óþarfa hugbúnað

- Hugleiða hýsingu af ýmsum toga

Dæmi um póstþjón og blacklist

Shared responsibility model – Cloud hugtök

Þegar lausnir og/eða búnaður er í hýsingu:

Security OF the cloud

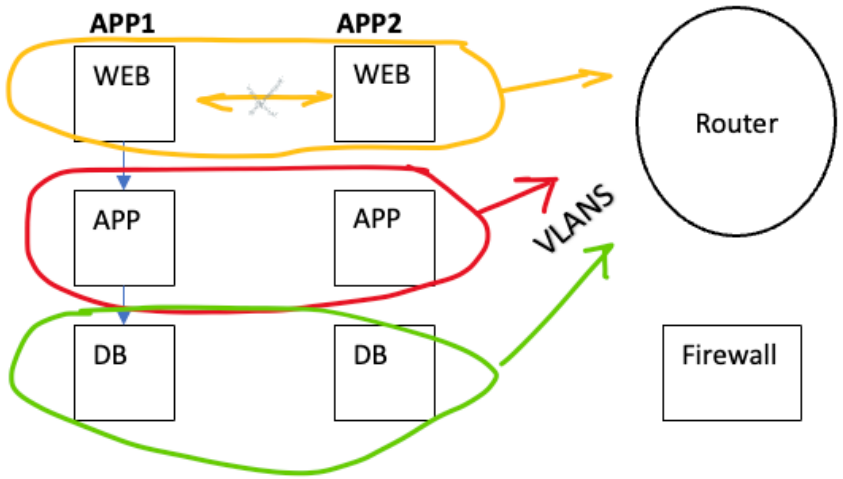
- Aðgengi
- Uppfærslum vélbúnaði á netbúnaði
- Útskiptingu á eldri búnaði
- DDoS varnir

Security IN the cloud

- Takmarka árasarflöt (Attack surface)
- MFA auðkenni notenda
- Admin auðkenni og stýring
- Netöryggisstefna, áhættugreining og varnir

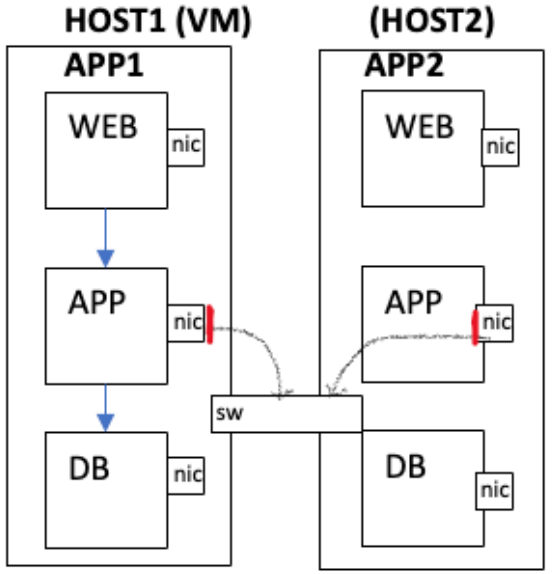
Net-skipting (segmentation)

Segmentations



Hefðbundin netskipting gert með vlans
Notar router og Firewall til að stjóra samskiptum milli web og app og db
Vandamálið er að WEB getur talað við WEB

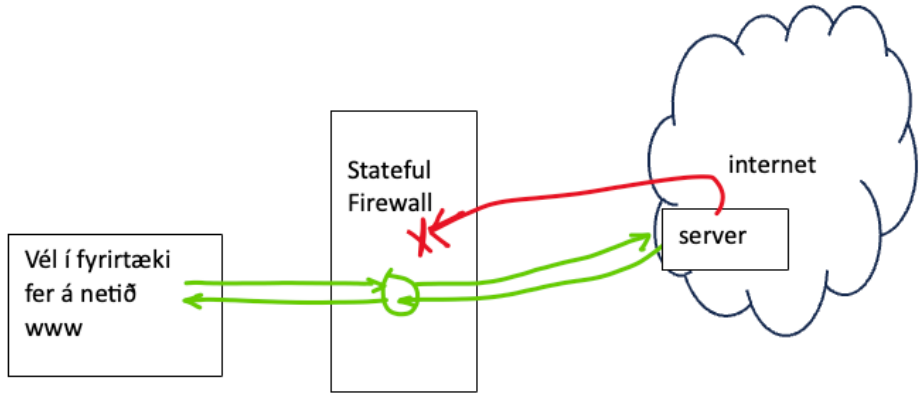
Micro segmentations



Settar reglur um hverja virtual machine beint á netkortið, trafík ekki leyfð á milli véla. Nákvæmar reglur milli véla, leyfir bara tengingu frá þessari vél á **skilgreindu porti.**
Vmware NSX og AWG (Security Group rules) er notað í þetta

Stateful Firewall vs stateless FireWall.

Í eldveggjum er venjan sú að það er búin til listi yfir það sem má og það sem er bannað



- Opið port út skigreint í Firewall og svar til bara leyft
- Opnar tilfallandi göt í eldveginn til baka, því traffíkin passar við þekkta tengingu
- Þess vegna kallað statefull, þekkir stöðu viðkomandi tengingar sem er í gangi

- Seinna reynir sami server sjálfur að fara inn í gegnum FW en þá er lokað því að það er enging tenging sem hefur átt upphafið fyrir innan FW í gangi

PARAMETER	STATELESS FIREWALL	STATEFUL FIREWALL
Philosophy	Treats each packet in isolation and does not relates to connection state	Stateful firewalls maintain context about active sessions and use “state information” to speed packet processing
Filtering decision	Based on information in packet headers	Based on flows
Memory and CPU intensive	Low	High
Security	Low	High
Connection Status	Unknown	Known
Performance	Fast	Slower
Related terms	Header info, IP address, port no etc.	State information, pattern matching etc.

ZERO – TRUST – MODEL

Eldveggyr hefur margar reglur um hvað er leyft og bannað, þetta er listi sem Eldveggurinn fer yfir og **fyrsta reglan sem passar er notuð!**

1. Leyfum traffik frá A to B
2. Bönnum traffík frá A to C
3. Allow all traffic. (Default regla).
   oft í routerum en helst ekki í FW

(Default á við um allt sem passar ekki í aðrar reglur)

ZERO – TRUST – MODEL

1. Leyfum traffik frá A to B
2. Bönnum traffík frá A to C
3. Deny all traffic. (Default regla).
   Á betur við í FW

ROUTER

Í routerum fyrir **heimili** þá leyfum almennt alla netumferð út
Í routerum **fyrirtækja** þá þurfum við að tilgreina hvað umferð er leyfð út
Oft endar það svo með default rútu sem leyfir allt.

Í báum tilfellum skilgreinum við hvaða umferð er leyfð inn!

FIREWALL

Í eldveggjum er skrifaður listi, langur listi yfir hvaða umferð er leyfð
Inn og út.

Eldveggur

L2/3 Firewall (skoðar bara addressur og port en ekki innihald => hraðvirkt)

- Allow traffic from 10.0.0.0/8 80 to 192.168.1.0/24 80. (port 80, leyf)
- Deny traffic from 172.16.0.0/16 80 to 10.0.0.0/8 80
- Deny all traffic

Layer 7 Firewall (AntiVirus Firewall) (application layer Firewall)

- Deep packet inspection
- Dæmi er PaloAlto, Fortinet, Check Point o.fl.
- *Þarft samt alltaf vírusvörn á vélar*

Firewall reglur
Bara leyfa það sem á að fara í gegn og banna annað
Viðhalda reglunum
Nota breytingastjórnun, ekki leyfa hverjum sem er að gera hvað sem er.

Varnir

Intrusion detection systems (IDS)
Intrusion prevention systems (IPS)

IDS
Skoðar hvort eitthvað sé gruggugt
(stoppar ekki, en lætur vita)

IPS
Umferð er skoðuð áður en henni er hleypt í gegn.

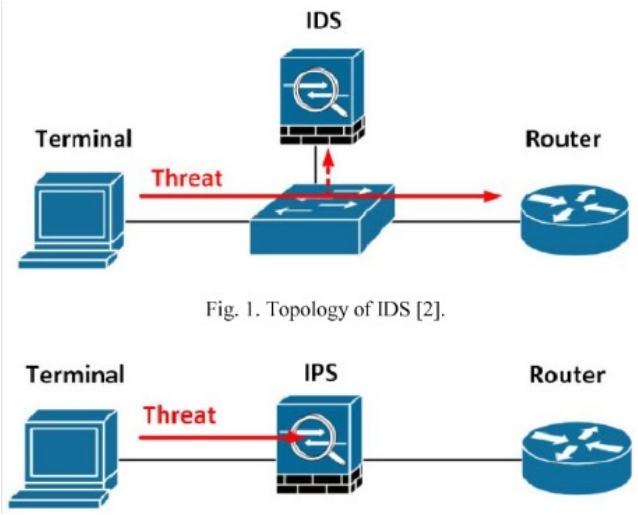
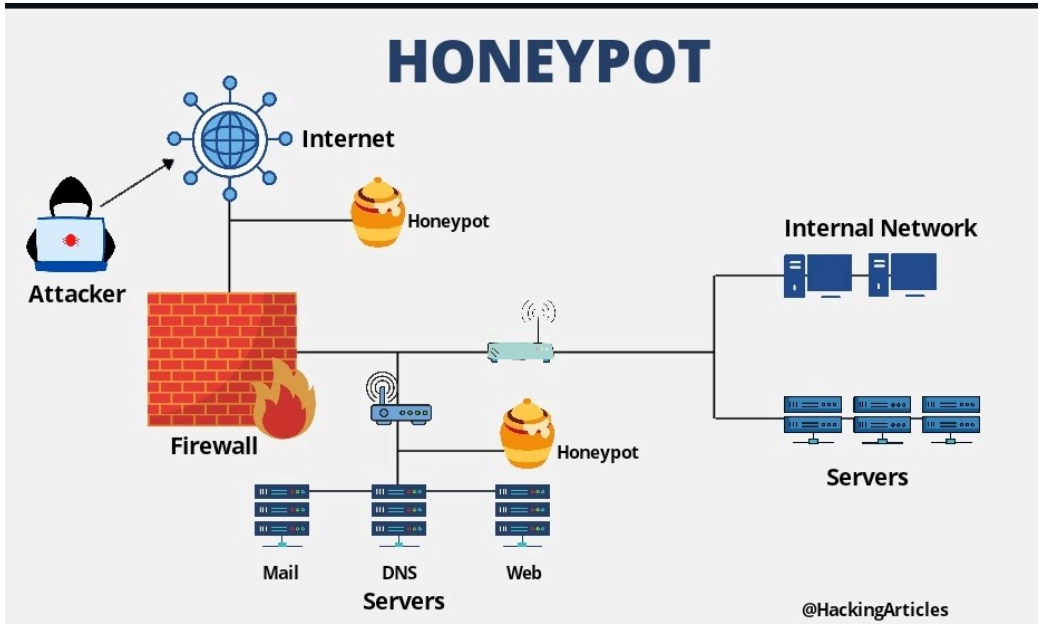


Fig. 1. Topology of IDS [2].

HoneyPots (Misdirection > villum um fyrir þrjótunum)
Skiljum ólæsta druslu eftir á augljósum stað.
En geymum flotta bílinn okkar inn í bílskúr.



Honeypots eru nettengd kerfi sem ætlað er að líkja eftir líklegum skotmörkum netárása, t.d. Illa varin netkerfi. Honeypots eru notaðri til að laða að, greina og þar með afvegaleiða netglæpamenn frá því að brjótast inn í mikilvæg kerfi.

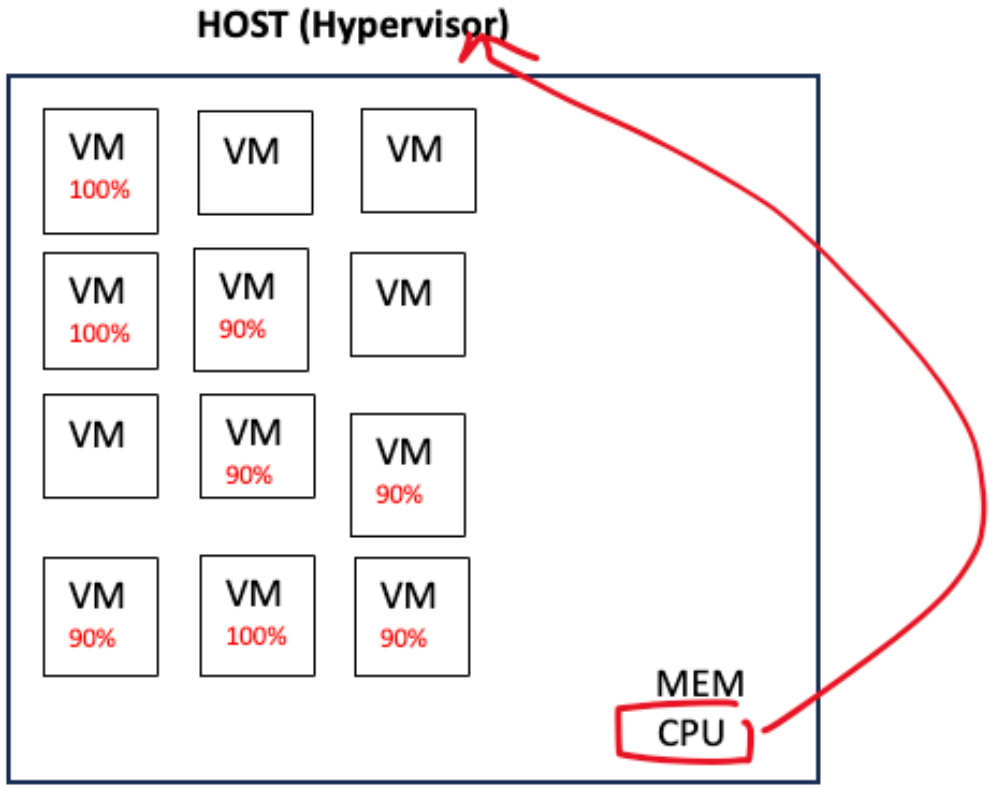
https://threatmap.checkpoint.com/

AntiVirus / **AntiMalware options**

- Sumt er „frítt“ yfirleitt fyrir personal notkun, hentar ekki í fyrirtækjum
- Þar þarf umsýslu tól (management tools)
- https://www.businesstechweekly.com/cybersecurity/application-security/business-antivirus/
  - Síða sem gefur upplýsingar á aðgengilegu formi og góður samanburður

- **Layer 7 firewall** getur verið góður til að stoppa að vírusar berist inn í fyrirtækið en kemur ekki í staðinn fyrir vírusvörn.

AntiVirus í virtual umhverfi



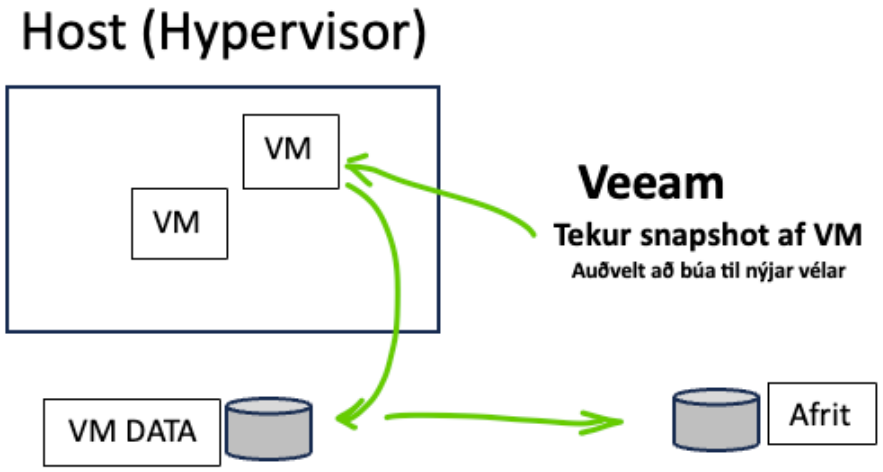
Hugmyndafræðin varðandi sýndarvélar VM og hýsing er að það þurfa ekki allir að nota fullt afl samtímis álagið dreifist yfir tíma

Það koma margir á kaffihús yfir daginn, það þarf ekki að vera borð og stólar fyrir heildar fjöldann.

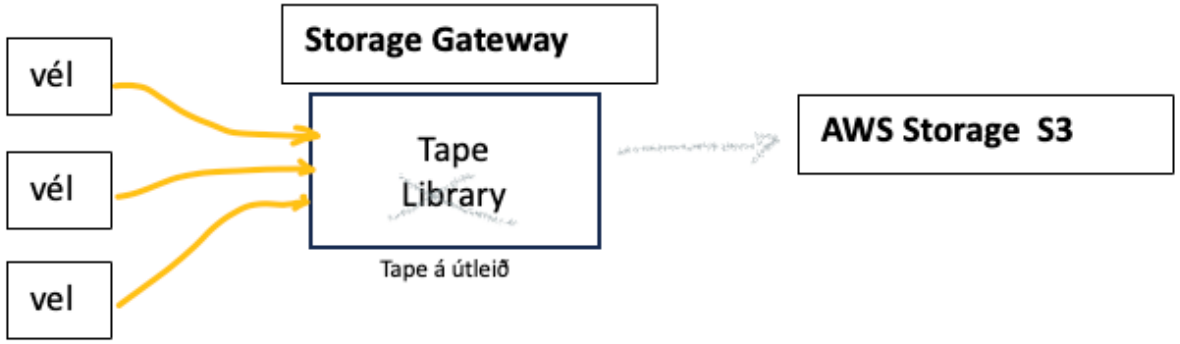
Vírus vörn setur oft mikið álag á vélar!

ATH hefðbundin vírusvörn, mun kaffæra CPU í VM umhverfi
Þarf að velja rétta lausn í VM
https://www.businesstechweekly.com/cybersecurity/application-security/business-antivirus/

Afritun - backup



Þetta umhverfi er að breytast hratt, mikið að fara í hýsingu



RANSOMWARE ➡ Multipoint restore points mikilvægir

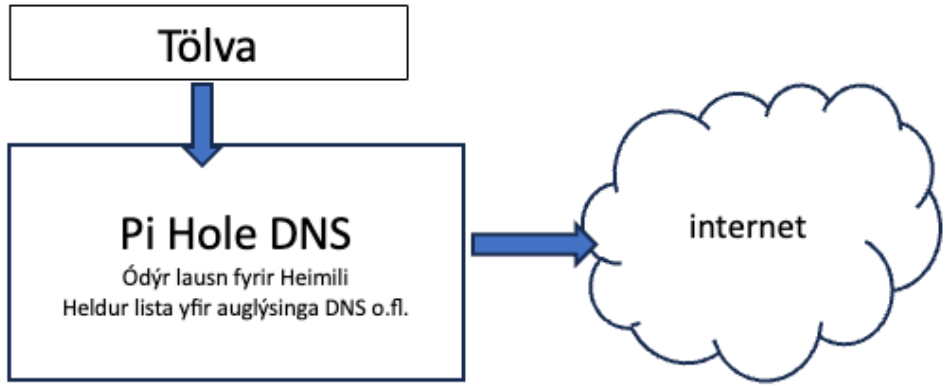
URL filter

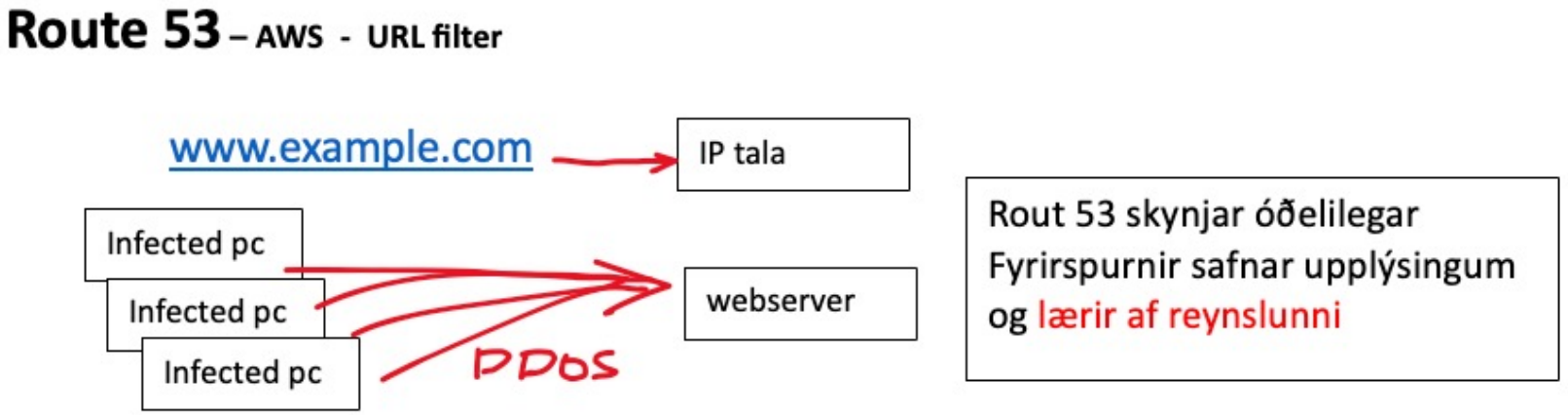
URL filter: Notum þjónustu

PaloAlto, þjónusta sem safnar upplýsingum um hvaða URL ber að forðast, nota machin learning
Webroot, cloudflare gera svipað

White list approach **Black list approach**

URL filter


Tölva
Pi Hole DNS
Ódýr lausn fyrir Heimili
Heldur lista yfir auglýsinga DNS o.fl.
internet


Route 53 – AWS - URL filter
www.example.com
IP tala
Infected pc
Infected pc
Infected pc
webserver
DDoS
Rout 53 skynjar óðelilegar
Fyrirspurnir safnar upplýsingum
og lærir af reynslunni

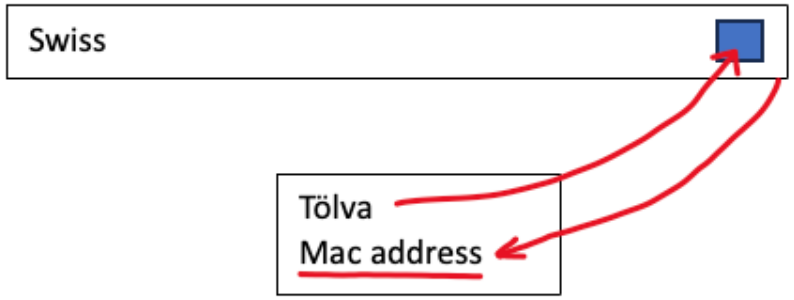
Port í svissum

Disable disconnected ports

Gera ónotuð port óvirk. => getur valdið óþæginum, valdið auka vinnu og tímabundnum vanda
En er öruggt

Enable Port Security

- Tölva tengist sviss
- Sviss skoða mac addressu
- Bara skráðar mac addressur leyfðar



Ekki hægt að setja eitthvað annað í samand við port sem var virkt

Innrásarprófanir - Penetration testing

- Ráðum öruggan aðila til að gera prófanir á öryggi okkar
- Kemst hann inn á netið
- Er hugbúnaður uppfærður
- Eru göt í eldvegg
- Kemst hann í gögn
- Gott fyrir gæða úttektir
- Nota mismunandi aðila til að gera þessi próf.

- Passa að er gera ekki þessi próf á cloud þjónustu án þess að láta þá vita