Firebox mobilevpn tavat

Mobilevpn tavat, joita WG tukee ja käyttää:

- Sslvpn — WG:n Win & Mac sslvpn client ja muut OS: OpenVPN client softa.
- IKEv2 — sisäänrakennettu Win/Mac/iOS. Androidiin pitää asentaa StrongSwan client.
- IPSec — sisäänrakennettu Mac/iOS/Android. Windowsin pitää asentaa IPSec client
- L2TP — sisäänrakennettu Win/Mac/iOS/Android
- Access Portal — clientless vpn, verkkoselain & HTML5 tekniikkaa.

Nykysuositus on käyttää IKEv2 vpn:ää:

- IKEv2 on paljon nopeampi kuin sslvpn ja tällä hetkellä näyttää siltä, että IKEv2 tulee olemaan preferoitu mobilevpn tapa.

- SSL-VPN on kaikista mobilevpn tavoista aina se ”hitain”. Suurin syy siihen on TLS, eli se käyttää samaa salaustekniikkaa kuin HTTPS, ja tämä salaustapa vaati tehoa sekä muurin että työaseman päässä.

Firebox mobilevpn lisenssit

Mobilevpn lisenssit lasketaan ns. kuinka monta yhtäaikaisia yhteyttä on päällä.

Esim. T40 muurissa on:

- 30 SSLVPN mobilevpn lisenssiä
- 30 IKEv2/IPSec mobilevpn lisenssiä
- 30 L2TP mobilevpn lisenssiä

Silloin muurissa voi olla yhtä aikaa päällä:

- 30 yhtäaikaista sslvpn mobilevpn yhteyttä
- 30 yhtäaikaista IKEv2 tai IPSec mobilevpn yhteyttä, (esim. 20 IKEv2 ja 10 IPSec yhteyttä)
- 30 yhtäaikaista L2TP mobilevpn yhteyttä
- **HUOM: T40 muuri on ensisijaisesti suunniteltu 30:lle mobilevpn käyttäjälle ja vaikka teoriassa saisit T40 muurin konffattua 90 mobilevpn (30 sslvpn + 30 IKEv2 + 30 L2TP) yhteyttä niin muurin tehot alkaa loppumaan ja kaikki liikenne muuri läpi menee todella hitaaksi!**

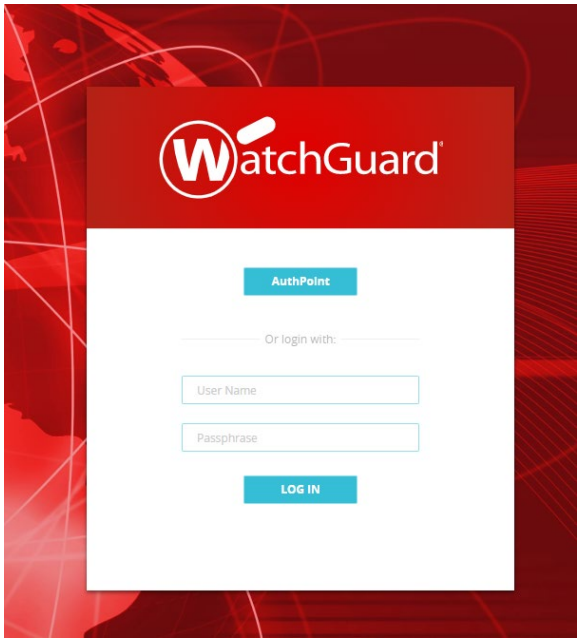
Muurien mobilevpn lisenssit ovat jo valmiiksi max tilassa, joten muureihin ei saa hankittua lisää mobilevpn lisenssejä. Ainut tapa saada enemmän mobilevpn lisenssejä on päivittää muuri uudempaan / isompaan.

Access Portal

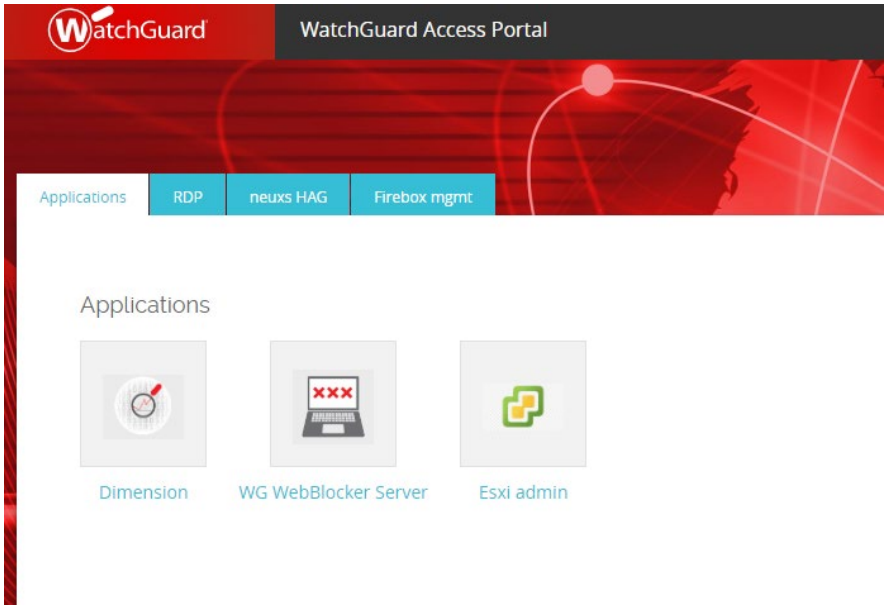
- vaati Firebox 12.5 tai uudemman version.
- M-sarja, (ei M200 tai M300) Firebox V ja Firebox Cloud muurit uudet T40 ja T80 muurit

- Perustuu Apache Guagamole softaan.
  clientless remote desktop gateway.
  pelkkä HTML5 netti-selain riittää
  ei tarvetta client softalle tai netti-selain plugin softille.

- RDP and SSH resurssit.
- Sisäiset webbi resurssit (reverse proxy)
- Ulkoiset webbi resurssit (SAML auth.)



Portaali autentikointi
Firebox-DB, Active Directory, Radius, SAML



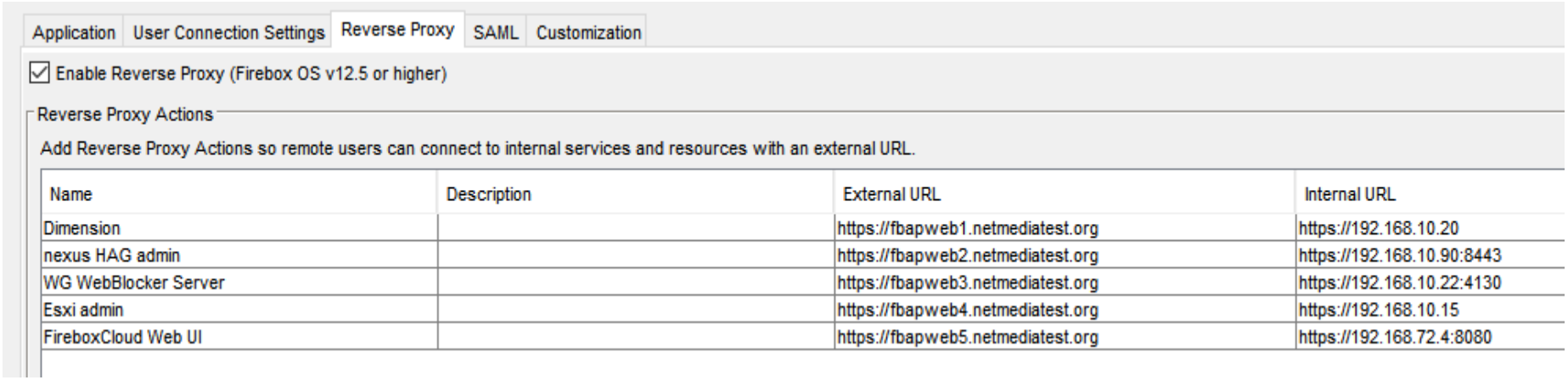
Current Estimates

Model	Max RDP Sessions*
M270	10
M370	15
M470	20
M570	50
M670	50
M4600	50
M5600	120

RDP sessions can use up to 100 Mb of Memory
*Not enforced. Usage may vary depending on session type

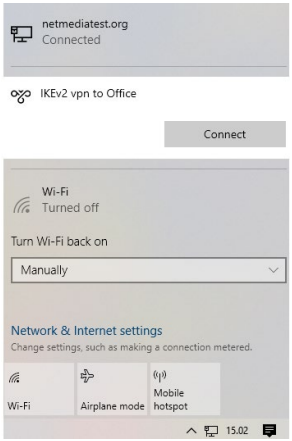
reverse proxy vaatimukset:

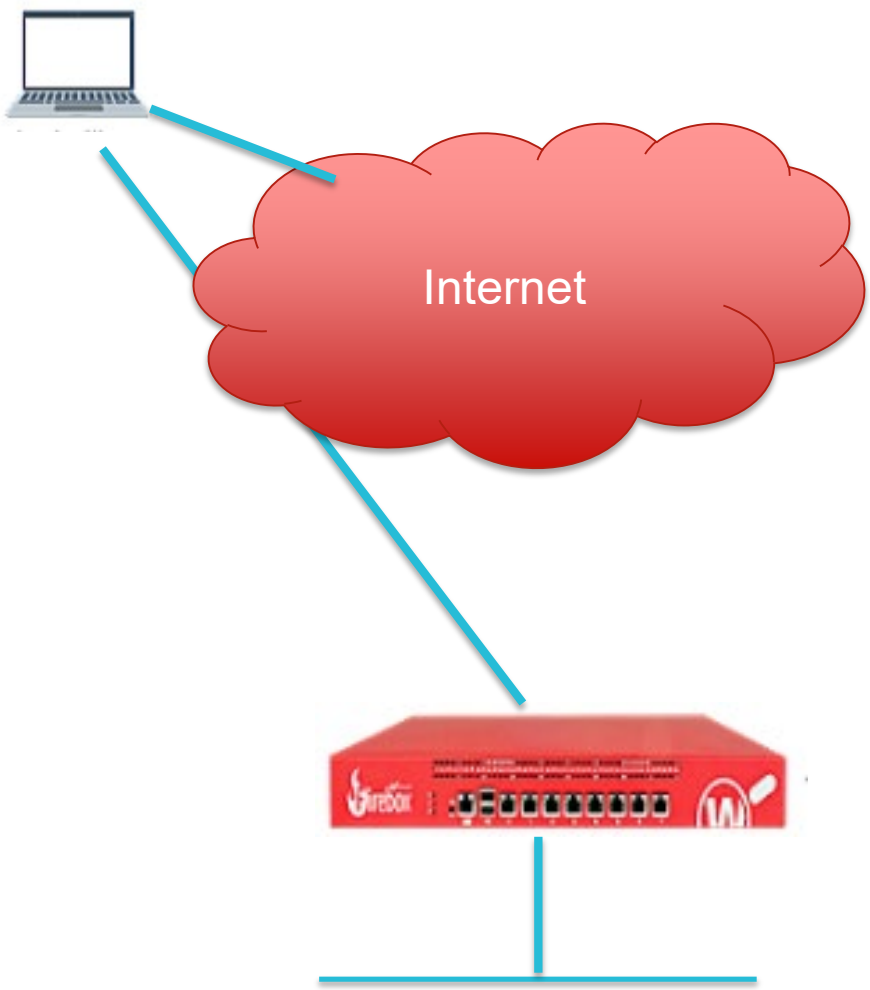
- Kirjautuminen Access Portaalin pitää tapahtua FQDN tavalla, ei IP osoitteella.
- Vaati wildcard, multi-domain tai SAN (Subject Alternative Name) sertin koska jokainen sisäinen webbi resurssi vaati oman FQDN.



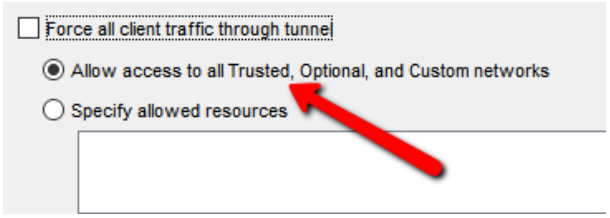
- Internal URL voi olla DNS nimi tai IP osoite.
- Portti käännös mahdollista (esim. https://192.168.10.1:8080)

Split vs Full tunnel



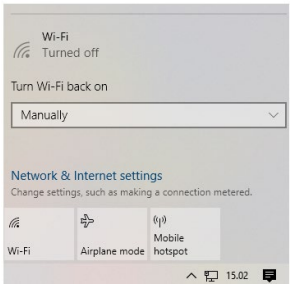


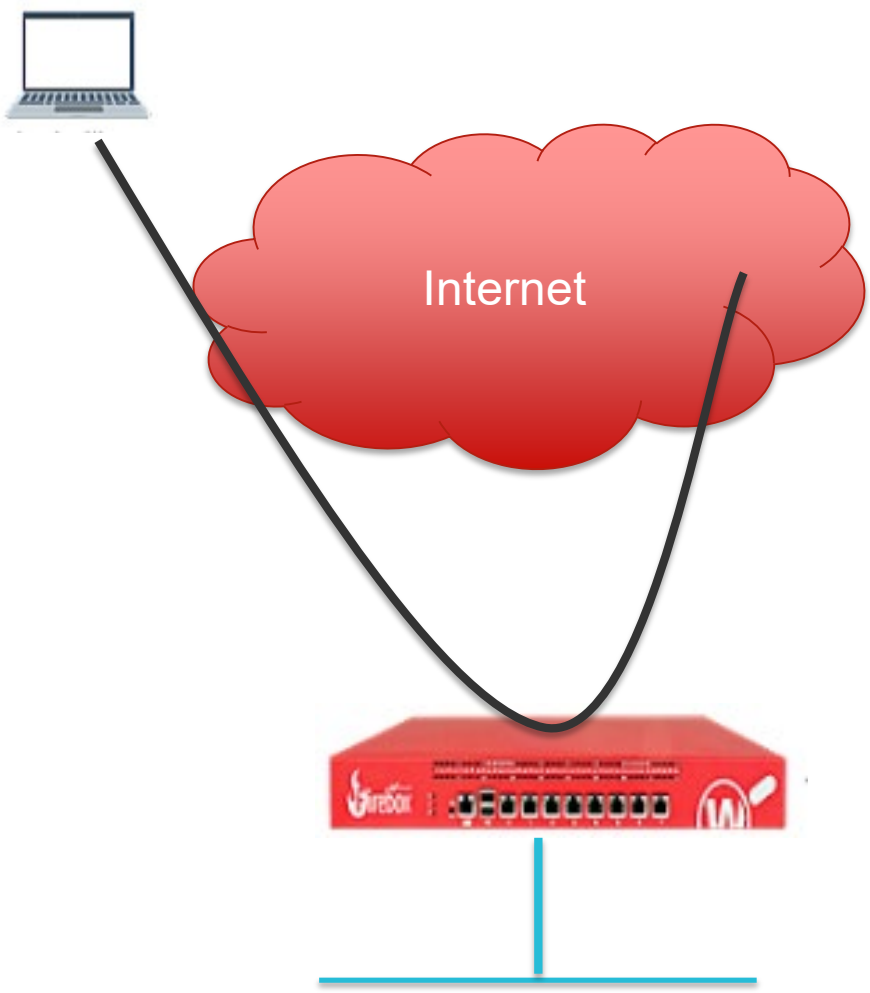
192.168.160.0/24 verkko



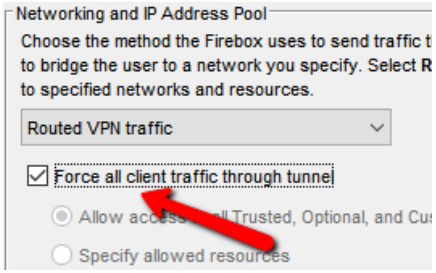
Split tavalla tunneliin menee vain toimiston 192.168.160.0/24 liikenne ja netti surffaus menee suoraan ulos työaseman netti liittymästä.

SSLVPN asetuksissa:
Allow access to all Trusted, Optional and Custom networks
tai Specify allowed resources



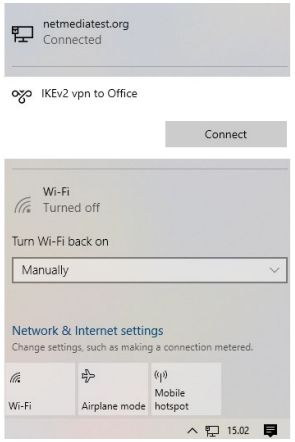


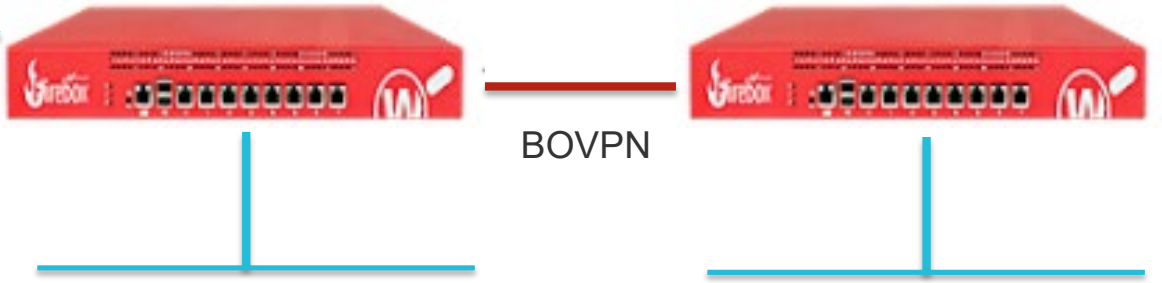
192.168.160.0/24 verkko

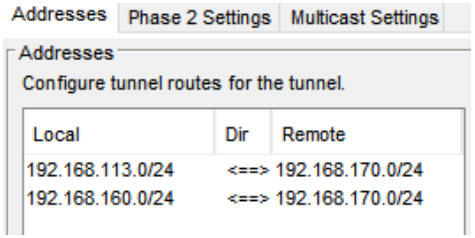


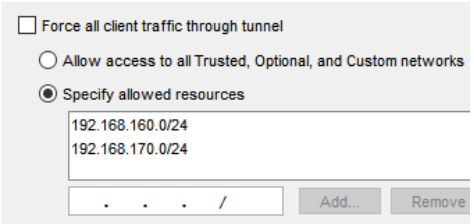
Full tavassa taas kaikki liikenne menee tunnelin, surffaus nettiin kiertää palomuurin kautta ulos. Työasema saa 0.0.0.0/0 reitin.

Sslvpn oletus tapa on nykyään Full (Force) tunnel.









Mobilevpn BOVPN reititys tavassa mobilevpn yhteyden Virtual IP Address Pool reitti kerrotaan myös BOVPN tunneli asetuksissa.

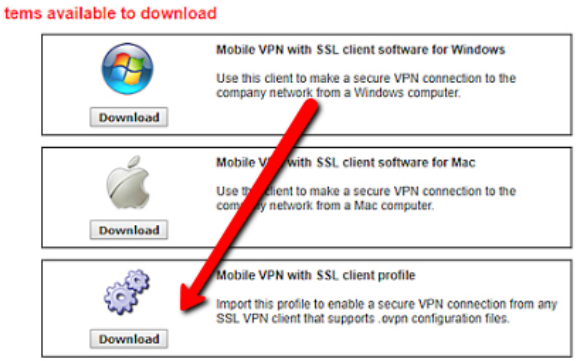
SSLVPN asetuksissa:
Specify allowed resources tai Force (0.0.0.0/0)

- WG:n sslvpn = OpenVPN (https://openvpn.net/)

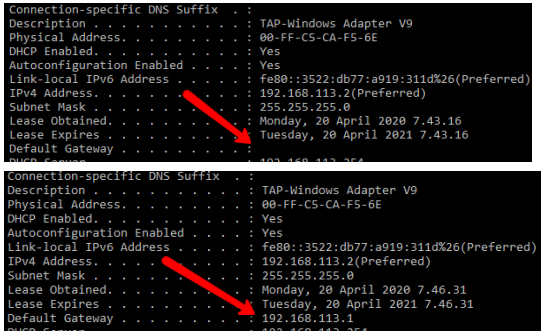
- iOS ja Android:
  OpenVPN Connect

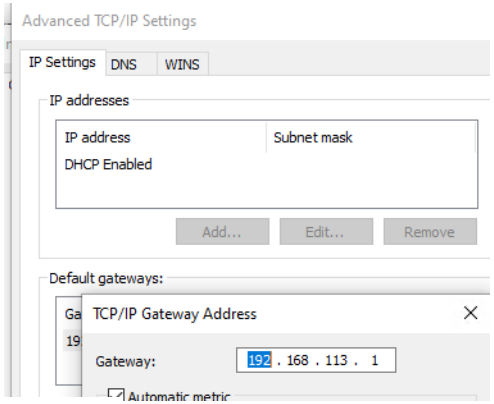
Download on the App Store

GET IT ON Google Play



- Office 365 ja sslvpn Full (Force) tunnel ongelma.
  (https://watchguardsupport.secure.force.com/publicKB?type=Known%20Issues&SFDCID=kA10H000000g3SPSAY&lang=en_US)

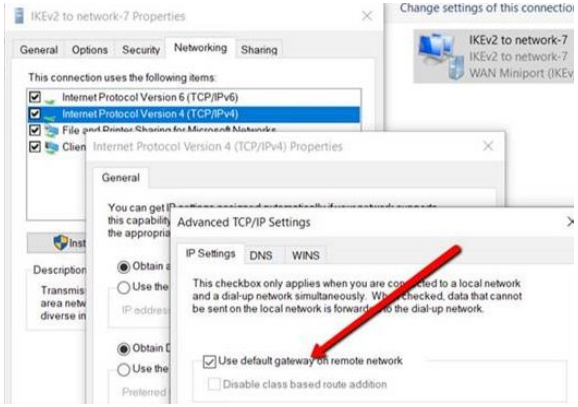





```
WG# config
WG(config)#policy
WG(config/policy)#sslvpn resource default-route-client
```

- Oletuksena IKEv2 tekee Force all traffic to tunnel. 0.0.0.0/0

  IKEv2 IPv4 asetuksissa ”Use default gateway…”



- Spilt tavalla IKEv2 ei saa automaattisesti muurista reittejä vaan ne pitää konfiguroida jokaisen IKEv2 työasemaan erikseen, esim. PowerShell, Intune avulla. (https://docs.microsoft.com/en-us/powershell/module/vpnclient/add-vpnconnectionroute?view=win10-ps)

```
PS C:\Users\user2> Set-VpnConnection "WG IKEv2" -SplitTunneling $true
PS C:\Users\user2> Add-VpnConnectionRoute "WG IKEv2" 192.168.0.0/16
PS C:\Users\user2> Add-VpnConnectionRoute "WG IKEv2" 10.0.0.0/8
```

- IKEv2 tukee Always on VPN tapaa. (Muuri tukee vain User Tunnel tapaa) (https://directaccess.richardhicks.com/always-on-vpn/) (https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/always-on-vpn/deploy/vpn-deploy-client-vpn-connections)

- Android vaati strongSwan VPN Client softan

GET IT ON Google Play

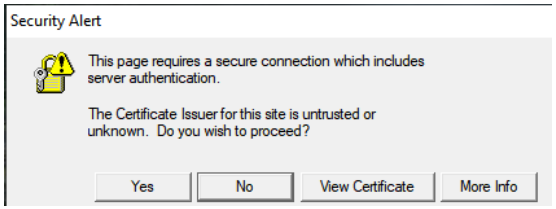
Sertifikaatit sslvpn ja IKEv2 mobilevpn kanssa.

- Muuri ei käytä sertifikaattia mobilevpn:ssä autentikointiin, vaan sillä luodaan salattu yhteys jonka sisällä voidaan antaa tunnukset. (idea on samanlainen kuin HTTPS surffauksen kanssa…)

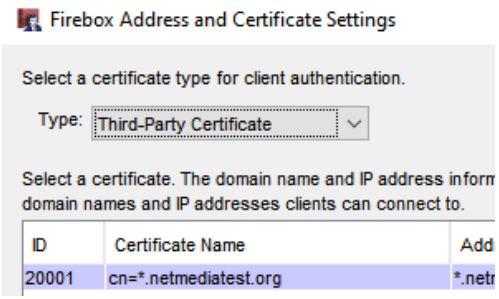
- Muurin viedään oma Web sertti.

Signed	2020-02-26 15:44	Web Client	RSA	o=WatchGuard ou=Fireware cn=Fireware web Client
Signed*	2020-03-04 11:28	Web Server	RSA	cn=*.netmediatest.org
Signed	2020-03-26 22:40	Proxy Authority	RSA	o=WatchGuard_Technologies ou=Fireware cn=Fireware

- sslvpn:ssä riittää että muuri käyttää tätä Web serttiä.



- IKEv2 pitää vaihtaa Firebox-Generated Certificate --> Third-Party Certificate.



- Jos käyttää virallista serttiä IKEv2:ssa silloin työasemaan ei tarvitse viedä muurista serttiä.

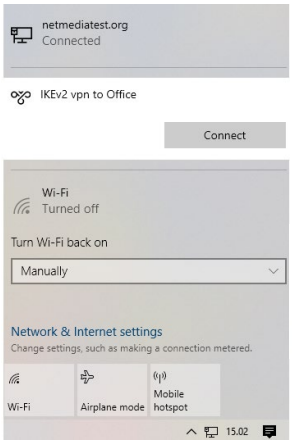
  Windows “certmgr.msc”

Firebox sslvpn ja IKEv2 AuthPoint MFA

sslvpn

MFA push viesti

AuthPoint cloud



ikev2 vpn

AD & NPS

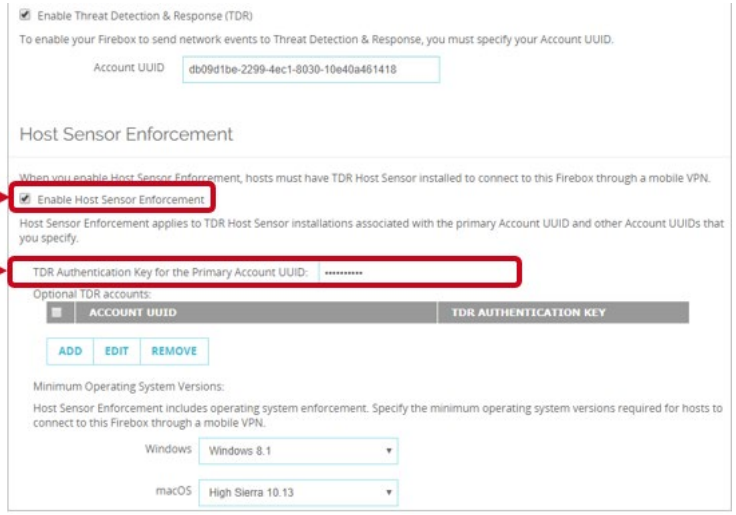
AuthPoint Gateway
LDAP agent
Radius server
Radius client to NPS for ikev2

Free AuthPoint and DNSWatchGO 60 DaysUp to 250 Users

TDR Host Sensor Enforcement

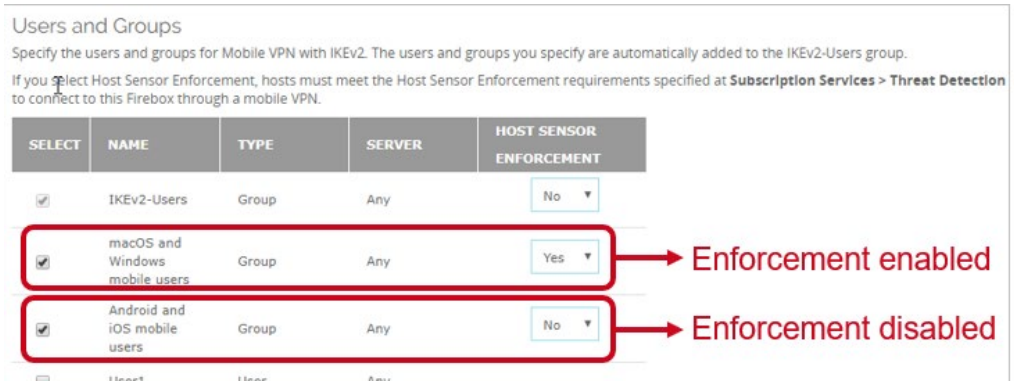
- TDR Host Sensor Enforcement adds integrity checks that limit mobile VPN connections to devices that follow corporate policy
- Your key corporate networks are more secure because only devices unlikely to be compromised by malware can connect.
- Host Sensor Enforcement supports Windows and macOS

Firebox configuration (Web UI)



Enable

Specify the TDR authentication key for the TDR account associated with this Firebox



Enforcement enabled

Enforcement disabled