Proxy-palvelun käyttöönotto Exam-asennukseen

Muutospäivämäärä	Muutoksen tekijä	Muutoksen kohde
13.07.2018	Matti Kakkinen	Asennusdokumentaation ensimmäinen versio
20.02.2020	Lauri Pohjanen	Lisätty alkuun maininta sivun tarkoituksesta ja ajantasaisuudesta

LISÄYS 20.02.2020: Tämä sivu ohjeistaa korkeakoulun oman Proxy-palvelimen asentamiseen ja käyttöönottoon mikä ei ole enää (2020) tarpeellista vaan korkeakoulussa voidaan ottaa käyttöön keskitetysti ylläpidetty kirjautumisvälityspalvelin, jonka käyttöönoton ohjeet täällä Kirja utumisvälityspalvelimen (proxy) käyttöönotto. Ao. sivun tiedot eivät enää ole kaikin osin ajantasaisia esim. haka.conf tiedoston sisältämässä IdP-palvelinten luettelossa on puutteita. (Ajantasainen tieto käytössä olevista IdP-palveluista löytyy Haka metadatasta.)

Tälle sivulle on dokumentoitu, kuinka Exam asennukseen voidaan ottaa käyttöön Squid-proxy, jonka kautta voidaan hallita tenttikoiden verkkoliikennettä.

1. Proxy-palvelu yleisesti
2. Proxy-palvelun arkkitehtuuri
3. Proxyn asennus Exam-palvelimelle
4. Proxyn käyttöönotto tenttikoneella

1. Proxy-palvelu yleisesti

Proxy-palvelun avulla voidaan rajata tenttikoneiden pääsyä verkkoon. Käytännössä tenttikoneiden verkkoliikenne asetetaan kulkemaan Squid-proxyn kautta, ja Squid-proxyssa on asetettu sallitut osoitteet.

Yleensä mikäli halutaan tenttikoneilla päästä vain oman korkeakoulun asennukseen, ei verkkoliikenteen rajaamisessa ole ongelmia, koska silloin riittää pääsy Exam-asennukseen ja korkeakoulun kirjatumispalvelimeen eli Shibboleth idP:hen. Ongelma tulee esiin silloin, jos halutaan ottaa käyttöön yhteiskäyttöisyyden ominaisuuksia, jolloin tulisi verkkoliikenne tulee sallia myös muiden korkeakoulujen idP:palvelimiin. Proxy mahdollistaa keskitetyn hallinnan korkeakoulujen idp-palvelimien osoitteille, jolloin ylläpito helpottuu.

Lisäksi proxy palvelun avulla voidaan seurata mitä verkkoliikennettä tenttikoneilla tapahtuu, ja tarvittaessa väärinkäyttötilanteissa on mahdollista selvittää miltä tenttikoneelta on missäkin käyty. Palvelu lokittaa tenttikoneen IP-osoitteen, aikaleimat sekä verkkosivut jonne pääsyä on yritetty. Varsinaisia henkilötietoja ei tallenneta, mutta nämä tiedot on tallennettu Examiin, joten tenttitilojen kulunvalvonnan avulla on henkilöiden tunnistaminen mahdollista.

2. Proxy-palvelun arkkitehtuuri

Proxy-palvelu on siis Exam-asennukseen halutessa lisättävä palvelu. Proxy voidaan asettaa minkä tahansa Exam-asennuksen eteen, joten sen käyttöönotto korkeakoulun asennukseen ei vaadi Exam-asennuksesta muutoksia. Seuraavassa kuvassa selvennetään kuinka palvelun verkkoliikenne toimii.

Kuva: Exam proxy ympäristö. Lähde: Jussi Talaskivi, Jyväskylän Yliopisto, 2018

Eli Squid-proxy asennetaan Exam-palvelimelle erillisenä palveluna, joilloin Examin käyttö onnistuu myös normaalisti.

3. Proxyn asennus Exam-palvelimelle

Palvelimella käytetään valmista Docker containeria: https://hub.docker.com/r/sameersbn/squid/ jolloin vältetään oman containerin ylläpitotarvetta.

Squid-proxy on otettu käyttöön old.exam.csc.fi palvelmella. Toteutus on tehty vastaavasti kuin muut Exam-palvelut, eli docker containeria varten on oma systemd service, jonka avulla voi käyttää palvelua.

Systemd-servicen sisältö on seuraava:

```
/etc/systemd/system/docker-squid.service

[Unit]
Description=Squid proxy
[Service]
ExecStartPre=-/usr/bin/docker rm squid
ExecStart=/usr/bin/docker run \
        --name squid \
         -i \
         -p 8080:8080 \
         -v /opt/exam/squid_proxy/haka.conf:/etc/squid3/haka.conf \
         -v /opt/exam/squid_proxy/squid.conf:/etc/squid3/squid.conf \
         -v /var/log/squid3:/var/log/squid3 \
         sameersbn/squid:3.3.8-23
ExecStop=-/usr/bin/docker stop squid
[Install]
WantedBy=multi-user.target
```

Eli squid proxy toimii portissa 8080, johon liikenne tulee ohjata tenttikoneelta mikäli halutaan käyttää proxyä.

Squid-proxyä varten on kaksi asetustiedostoa, jotka ovat polussa: /opt/exam/squid_proxy

Tiedostoista squid.conf sisältää Squid-proxy asetukset ja haka.conf sisältää osoitteet joihin saa ottaa yhteyttä proxyn välityksellä.

Lokit on host-koneen kansiossa /var/log/squid3

Tiedoston squid.conf sisältö on seuraavanlainen:

```
#
# Recommended minimum configuration:
#

# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
acl localnet src 10.0.0.0/8     # RFC1918 possible internal network
acl localnet src 172.16.0.0/12  # RFC1918 possible internal network
acl localnet src 192.168.0.0/16 # RFC1918 possible internal network
acl localnet src fc00::/7       # RFC 4193 local private network range
acl localnet src fe80::/10      # RFC 4291 link-local (directly plugged) machines
acl valamis src 79.141.147.136/24
#acl everyone src 0.0.0.0/0

acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT

include /etc/squid3/haka.conf

http_access deny !allowdomains

#
# Recommended minimum Access Permission configuration:
#
# Deny requests to certain unsafe ports
http_access deny !Safe_ports

# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports

# Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager

# We strongly recommend the following be uncommented to protect innocent
# web applications running on the proxy server who think the only
# one who can access services on "localhost" is a local user
http_access deny to_localhost

#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
http_access allow localnet
http_access allow localhost

#http_access allow everyone
http_access allow valamis
# ADD NETWORK HERE ====================
```

```
# And finally deny all other access to this proxy
http_access deny all

# Squid normally listens to port 3128
http_port 8080

# Uncomment and adjust the following to add a disk cache directory.
#cache_dir ufs /var/spool/squid 100 16 256
cache_dir null /tmp
cache deny all

# Leave coredumps in the first cache dir
coredump_dir /var/spool/squid

#
# Add any of your own refresh_pattern entries above these.
#
refresh_pattern ^ftp:           1440    20%     10080
refresh_pattern ^gopher:        1440    0%      1440
refresh_pattern -i (/cgi-bin/|\?) 0     0%      0
refresh_pattern .               0       20%     4320

cache_mgr exam-support@postit.csc.fi
visible_hostname old.exam.csc.fi
```

Mikäli Proxy halutaan asentaa toiselle palvelimelle, tulee muuttaa kohtia:

Näillä voidaan valita mistä osoitteista on sallittu ottaa yhteyttä Proxyyn. Ohessa sallittu Valamiksen ip:stä yhteydenotto, ja vapaa yhteydenotto mistä tahansa ip:stä on kommentoitu pois.

```
acl valamis src 79.141.147.136/24
#acl everyone src 0.0.0.0/0
```

Määritetyn verkon pääsy tulee vielä sallia, jotta yhteydenottaminen onnistuu. Nyt on sallittu verkon valamis yhteydentotto, mutta everyone on kommentoitu pois.

```
#http_access allow everyone
http_access allow valamis
```

Lopuksi virheilmoituksissa on näkyvissä asetettu yhteysosoite, ja palvelun url. Nämä voi asettaa haluamakseen.

```
cache_mgr exam-support@postit.csc.fi
visible_hostname old.exam.csc.fi
```

Toinen Squid-proxyn asetustiedosto on haka.conf. Tänne on tallennettu osoitteet joihin saa proxyn kautta ottaa yhteyttä. Ohessa esimerkki old.exam.csc.fi palvelimelta, josta sallittu yhteydenotto palvelimeen old.exam.csc.fi sekä korkeakoulujen shibboleth idp-palvelimiin. Mikäli rivejä halutaan lisätä, tulee vain lisätä rivi:

acl allowdomains dstdomain old.exam.csc.fi

Jossa ainoastaan viimeinen url tarvitsee muuttaa. Muut määritykset tulee jättää ennalleen.

haka.conf tiedosto kokonaisuudessaan:

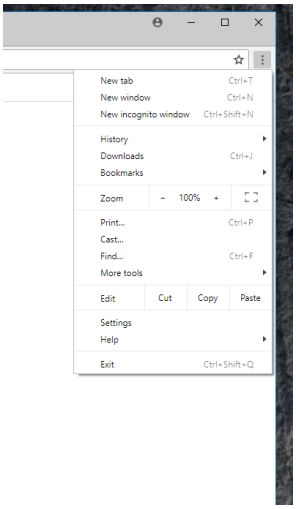
```
acl allowdomains dstdomain old.exam.csc.fi
acl allowdomains dstdomain testsp.funet.fi
acl allowdomains dstdomain testidp.funet.fi
acl allowdomains dstdomain crl.usertrust.com
acl allowdomains dstdomain kaviidp.vyv.fi
acl allowdomains dstdomain idp1.samk.fi
acl allowdomains dstdomain idp.shh.fi
acl allowdomains dstdomain login.helsinki.fi
acl allowdomains dstdomain tunnistus.thl.fi
acl allowdomains dstdomain xidp.xamk.fi
acl allowdomains dstdomain crl-3.trust.teliasonera.com
acl allowdomains dstdomain idp.lapinamk.fi
acl allowdomains dstdomain kamidp01.kamit.fi
acl allowdomains dstdomain idp.ulapland.fi
acl allowdomains dstdomain idp.uniarts.fi
acl allowdomains dstdomain tunnistus.laurea.fi
acl allowdomains dstdomain tunnistus.smedu.fi
acl allowdomains dstdomain login.jyu.fi
acl allowdomains dstdomain idp.oph.fi
acl allowdomains dstdomain idp2.jamk.fi
acl allowdomains dstdomain idp.tut.fi
acl allowdomains dstdomain idp2.epedu.fi
acl allowdomains dstdomain idp.tamk.fi
acl allowdomains dstdomain narcidp.vyv.fi
acl allowdomains dstdomain crl3.digicert.com
acl allowdomains dstdomain salpa.certia.fi
acl allowdomains dstdomain rap.humak.fi
acl allowdomains dstdomain idp.lut.fi
acl allowdomains dstdomain idp.metropolia.fi
acl allowdomains dstdomain idp.diak.fi
acl allowdomains dstdomain sso.utu.fi
acl allowdomains dstdomain idp.narc.fi
acl allowdomains dstdomain tunnistus.mpkkfu.fi
acl allowdomains dstdomain idp.haaga-helia.fi
acl allowdomains dstdomain sts.psshp.fi
acl allowdomains dstdomain shibbo.hamk.fi
acl allowdomains dstdomain tunnistus.pelastusopisto.fi
acl allowdomains dstdomain idp3.karelia.fi
acl allowdomains dstdomain tullbommen.arcada.fi
acl allowdomains dstdomain idp.uef.fi
acl allowdomains dstdomain haka.lpt.fi
acl allowdomains dstdomain idp.savonia.fi
acl allowdomains dstdomain idp.oamk.fi
acl allowdomains dstdomain login.uwasa.fi
acl allowdomains dstdomain idp.centria.fi
acl allowdomains dstdomain shibboleth.uta.fi
acl allowdomains dstdomain idp.abo.fi
acl allowdomains dstdomain idp1.turkuamk.fi
acl allowdomains dstdomain crl4.digicert.com
acl allowdomains dstdomain ocsp.digicert.com
acl allowdomains dstdomain idp.vamk.fi
acl allowdomains dstdomain login.oulu.fi
acl allowdomains dstdomain idp.saimia.fi
acl allowdomains dstdomain sipuli.fmi.fi
acl allowdomains dstdomain idp.csc.fi
acl allowdomains dstdomain idp1.novia.fi
acl allowdomains dstdomain ocsp.usertrust.com
acl allowdomains dstdomain ocsp.trust.telia.com
acl allowdomains dstdomain idp.aalto.fi
```

Tämän jälkeen proxy on käyttövalmis, ja seuraavat asetukset tulee tehdä tenttikoneelle.

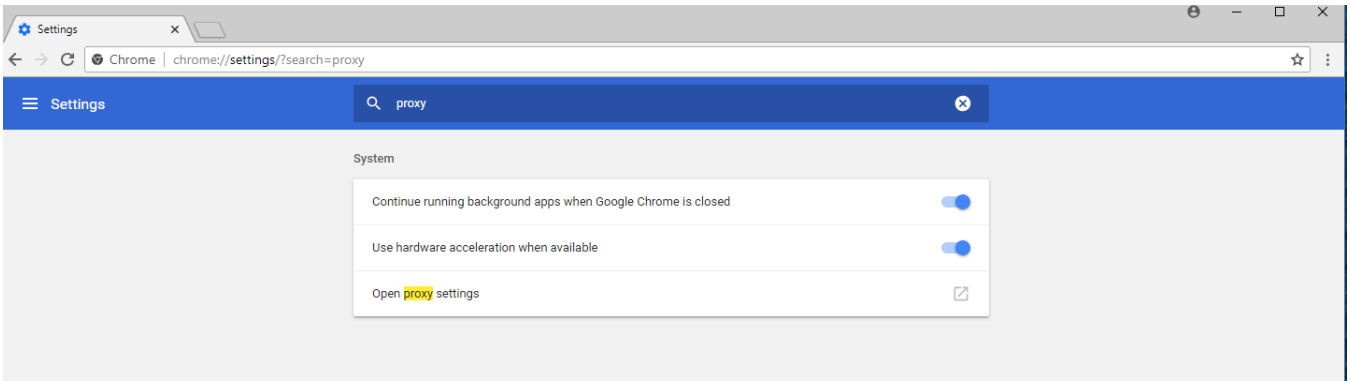
4. Proxyn käyttöönotto tenttikoneella

Seuraavassa esimerkissä on kerrottu kuinka proxy voidaan ottaa käyttöön Windows 10 + Chrome yhdistelmällä.

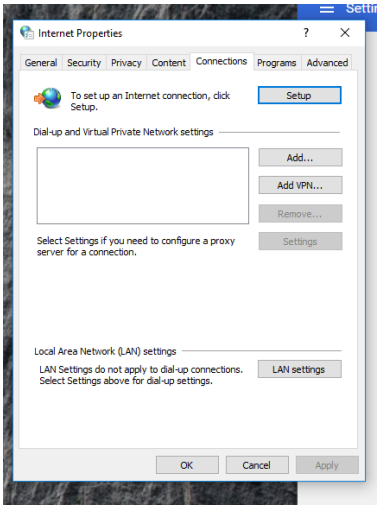
Avaa Chrome ja valitse settings asetusvalikosta oikealta:



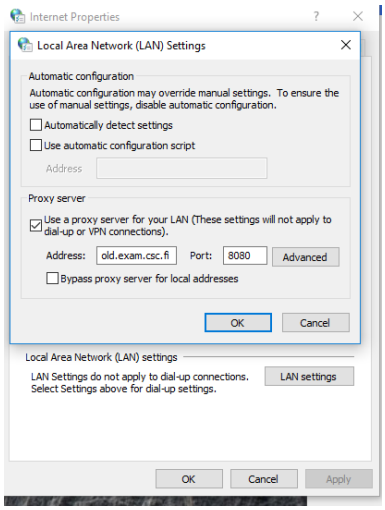
Seuraavaksi kirjoita hakukenttään sana "proxy", jolloin "open proxy settings" tulee näkyviin. Klikkaa kyseisestä asetuksesta.



Tämän jälkeen avautuu windows asetusikkuna "Internet Properties", klikkaa sieltä painiketta "LAN settings"

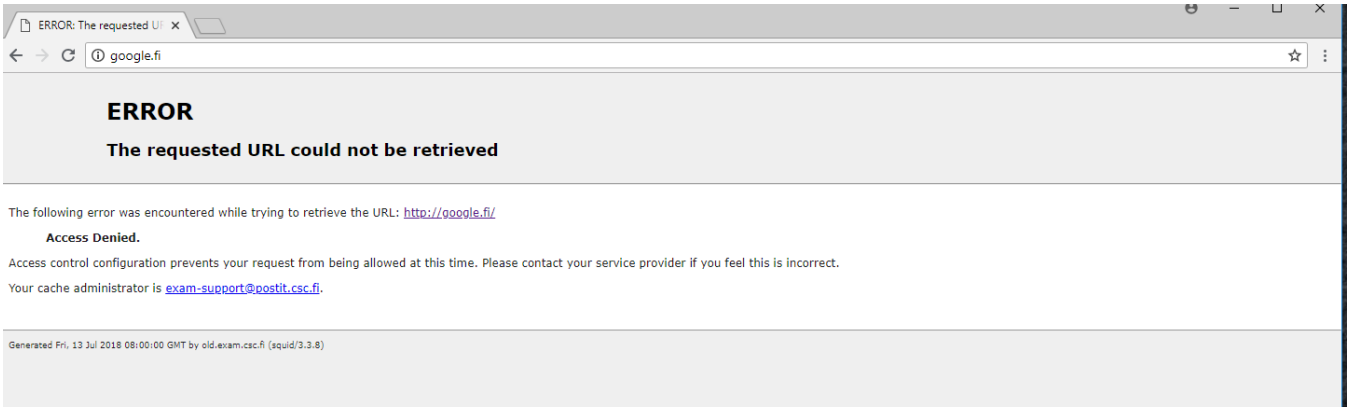


Nyt avoinna on "Local Area Network (LAN) Settings" syötä kenttiin oheiset asetukset "Proxy server kohtaan" ja valitse pois "Automatically detect settings".

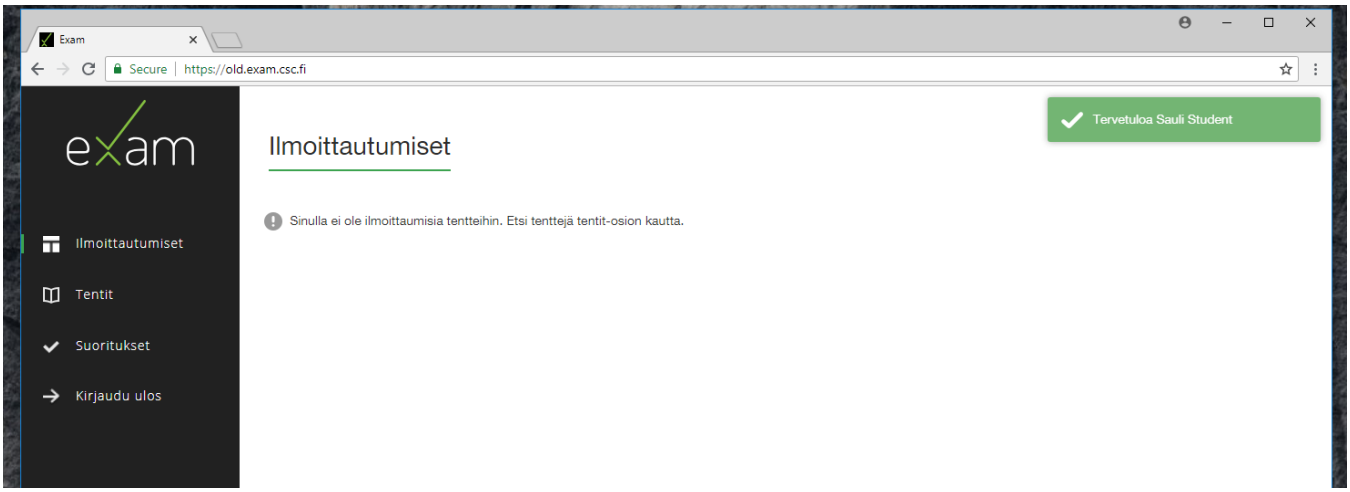


Lopuksi paina ok, ja Proxy on käytössä tenttikoneella. Voit varmentaa toiminnan siten, että kokeilet sivuja old.exam.csc.fi ja esimerkiksi google.fi.

Kun menet sivulle google.fi, tulee ilmoitus että pääsy on estetty, sekä yhteystiedot mikäli käyttäjällä on tarvetta olla yhteydessä proxy-palvelun ylläpitoon:



Vastaavasti kun käyttäjä menee old.exam.csc.fi, tulisi sivun avautua normaalisti:



Nyt proxy-palvelu on otettu käyttöön myös tenttikoneella ja asennus on valmis.