

Advanced ORPS RADSECProxy Configuration

This should be representative of the configuration used in production. It contains the appropriate logging and filtering.

```
# Some basic logging
LogLevel 3
LogDestination          x-syslog:///LOG_DAEMON

# Prevents RADIUS servers from causing a loop by sending requests back
again.
LoopPrevention          On
# FTICKS is a standardised way of logging authentication attempts.
FTicksSyslogFacility LOG_LOCAL0
FTicksReporting Full
FTicksMAC VendorKeyHashed
FTicksKey arandomsalt

rewrite OutboundFilter {
    # Operator-Name
    RemoveAttribute 126
    AddAttribute 126:'lexample.ac.uk

    WhitelistMode on
    # User-Name
    WhitelistAttribute 1
    # EAP-Message
    WhitelistAttribute 79
    # Message-Authenticator
    WhitelistAttribute 80
    # State
    WhitelistAttribute 24
    # Proxy-State
    WhitelistAttribute 33
    # Operator-Name
    WhitelistAttribute 126
    # Class
    WhitelistAttribute 25
    # Calling-Station-Id
    WhitelistAttribute 31
    # Called-Station-Id
    WhitelistAttribute 30
    # Chargeable-User-Identity
    WhitelistAttribute 89
}

### Catch a load of common misconfigurations
realm /^$/ {
    replymessage "Misconfigured client: empty realm!"
```

```
}

realm
/((myabc|gmail|googlemail|hotmail|live|outlook|yahoo|unimail).com|(.*\.)?3g
ppnetworks?.org|yahoo.cn) {
    replymessage "Misconfigured client: govroam realm not permitted"
}

realm /@(.*\.(ax\.uk|ax\.edu|sc\.uk|ac\.edu|ac\.u|local)|ac\.uk)$ {
    replymessage "Misconfigured client: govroam realm invalid (typo?)"
}

realm /@\. {
    replymessage "Misconfigured client: govroam realm invalid (leading '.')"
}

realm /@[^\.]+$ {
    replymessage "Misconfigured client: govroam realm invalid (incomplete)"
}

### Check it's a syntactically correct realm and proxy if ok
realm /@[0-9a-zA-Z\.]+\.[0-9a-zA-Z\.]+$ {
    server roaming0.govroam.uk
    server roaming1.govroam.uk
    server roaming2.govroam.uk
    server roaming3.govroam.uk
}

### Otherwise reject it
realm * {
    replymessage "Misconfigured client: govroam realm invalid (syntax
error)"
}

# Upstream RADIUS proxy (Omit for Visited Only)
server roaming0.govroam.uk {
    host 212.219.190.139
    type udp
    secret XXXX
    RewriteOut OutboundFilter
    statusServer on #This checks that status of the adjacent servers.
}

# Upstream RADIUS proxy (Omit for Visited Only)
server roaming1.govroam.uk {
    host 212.219.209.43
    type udp
    secret XXXX
    RewriteOut OutboundFilter
```

```
        statusServer on    #This checks that status of the adjacent servers.
    }

# Upstream RADIUS proxy (Omit for Visited Only)
server roaming2.govroam.uk {
    host 212.219.247.59
    type udp
    secret XXXX
    RewriteOut OutboundFilter
    statusServer on    #This checks that status of the adjacent servers.
}

# Upstream RADIUS proxy (Omit for Visited Only)
server roaming3.govroam.uk {
    host 195.194.21.203
    type udp
    secret XXXX
    RewriteOut OutboundFilter
    statusServer on    #This checks that status of the adjacent servers.
}

# Local IdP which will do the authentication (Omit for Visited Only)
server localidp1 {
    host 10.10.10.21
    type udp
    secret XXXX
    statusServer on
}

# RADIUS requests will also be received from the national proxies.
client nrps1 {
    host 212.219.190.139
    type udp
    secret XXXX
}
client localidp1 {
    host 10.10.10.21
    type udp
    secret XXXX
}

# Wireless system (Omit for Visited Only)
client nas {
    host 10.10.10.10
    type udp
    secret XXXX
    fticksVISOUNTRY GB
    fticksVISINST lhome.site    # Adding information to the logs
    about this client.
}
```

```
}  
  
#Known local realm (Omit for Visited Only)  
realm localnet {  
    server localidp1  
}  
  
#Default destination for unknown realms  
realm * {  
    server roaming0.govroam.uk  
}
```

From: <https://wiki.govroam.uk/dokuwiki/> - Govroam

Permanent link: https://wiki.govroam.uk/dokuwiki/doku.php?id=siteadmin:advanced_orps_radsecproxy_configuration&rev=1615302258

Last update: **2021/03/09 15:04**

