Advanced ORPS RADSECProxy Configuration

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

For RadSecProxy 1.8.0 and above:

```
# 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:'1home.site

    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
}
```

```
# Upstream RADIUS proxy
server  roaming0.govroam.uk {
        host 212.219.190.139
        type udp
## Change XXXX to the supplied RADIUS secret.
        secret XXXX
        RewriteOut OutboundFilter
#This checks that status of the adjacent servers.
        statusServer minimal
}

# Upstream RADIUS proxy
server  roaming1.govroam.uk {
        host 212.219.209.43
        type udp
## Change XXXX to the supplied RADIUS secret.
        secret XXXX
        RewriteOut OutboundFilter
#This checks that status of the adjacent servers.
        statusServer minimal
}

# Upstream RADIUS proxy
server  roaming2.govroam.uk {
        host 212.219.247.59
        type udp
## Change XXXX to the supplied RADIUS secret.
        secret XXXX
        RewriteOut OutboundFilter
#This checks that status of the adjacent servers.
        statusServer minimal
}

# Upstream RADIUS proxy
server  roaming3.govroam.uk {
        host 195.194.21.203
        type udp
## Change XXXX to the supplied RADIUS secret.
        secret XXXX
        RewriteOut OutboundFilter
#This checks that status of the adjacent servers.
        statusServer minimal
}


# Local IdP which will do the authentication (Omit for Visited Only)
# Configure to match the RADIUS server to which auth requests for your local
realm will be sent.
server  localidp1 {
        host 10.10.10.21
```

```
        type udp
        secret XXXX
        statusServer auto
}


# RADIUS requests will also be received from the national proxies. (Omit for
Visited Only)
client  roaming0.govroam.uk {
        host 212.219.190.139
        type udp
## Change XXXX to the supplied RADIUS secret.
        secret XXXX
}
client  roaming1.govroam.uk {
        host 212.219.209.43
        type udp
## Change XXXX to the supplied RADIUS secret.
        secret XXXX

}
client  roaming2.govroam.uk {
        host 212.219.247.59
        type udp
## Change XXXX to the supplied RADIUS secret.
        secret XXXX

}
client  roaming3.govroam.uk {
        host 195.194.21.203
        type udp
## Change XXXX to the supplied RADIUS secret.
        secret XXXX

}

# Wireless system
# Configure this to match the wireless controller/controllers from which the
authentication requests are coming.
client  nas {
        host 10.10.10.10
        type udp
        secret XXXX
        fticksVISCOUNTRY GB
# Change 'home.site' to your realm
        fticksVISINST 1home.site
}

#Known local realm (Omit for Visited Only)
#Configure 'localnet' to be the name of the realm for your site and
'localidp1' to be the IDP mentioned above
```

```
realm localnet {
        server localidp1
}

### 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)"
}
```

For older versions of RadSecProxy (e.g. on Debian)

```
# 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:'1home.site
}


# Upstream RADIUS proxy
server  roaming0.govroam.uk {
        host 212.219.190.139
        type udp
## Change XXXX to the supplied RADIUS secret.
        secret XXXX
        RewriteOut OutboundFilter
#This checks that status of the adjacent servers.
        statusServer on
}

# Upstream RADIUS proxy
server  roaming1.govroam.uk {
        host 212.219.209.43
        type udp
## Change XXXX to the supplied RADIUS secret.
        secret XXXX
        RewriteOut OutboundFilter
#This checks that status of the adjacent servers.
        statusServer on
}

# Upstream RADIUS proxy
server  roaming2.govroam.uk {
        host 212.219.247.59
        type udp
## Change XXXX to the supplied RADIUS secret.
        secret XXXX
        RewriteOut OutboundFilter
#This checks that status of the adjacent servers.
        statusServer on
}

# Upstream RADIUS proxy
server  roaming3.govroam.uk {
        host 195.194.21.203
        type udp
## Change XXXX to the supplied RADIUS secret.
```

```
        secret XXXX
        RewriteOut OutboundFilter
#This checks that status of the adjacent servers.
        statusServer on
}


# Local IdP which will do the authentication (Omit for Visited Only)
# Configure to match the RADIUS server to which auth requests for your local
realm will be sent.
server  localidp1 {
        host 10.10.10.21
        type udp
        secret XXXX
        statusServer off
}


# RADIUS requests will also be received from the national proxies. (Omit for
Visited Only)
client  roaming0.govroam.uk {
        host 212.219.190.139
        type udp
## Change XXXX to the supplied RADIUS secret.
        secret XXXX
}
client  roaming1.govroam.uk {
        host 212.219.209.43
        type udp
## Change XXXX to the supplied RADIUS secret.
        secret XXXX

}
client  roaming2.govroam.uk {
        host 212.219.247.59
        type udp
## Change XXXX to the supplied RADIUS secret.
        secret XXXX

}
client  roaming3.govroam.uk {
        host 195.194.21.203
        type udp
## Change XXXX to the supplied RADIUS secret.
        secret XXXX

}

# Wireless system
# Configure this to match the wireless controller/controllers from which the
```

```
authentication requests are coming.
client  nas {
        host 10.10.10.10
        type udp
        secret XXXX
        fticksVISCOUNTRY GB
# Change 'home.site' to your realm
        fticksVISINST 1home.site
}

#Known local realm (Omit for Visited Only)
#Configure 'localnet' to be the name of the realm for your site and
'localidp1' to be the IDP mentioned above

realm localnet {
        server localidp1
}

### 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)"
}
```

From:
https://wiki.govroam.uk/dokuwiki/ - **Govroam**

Permanent link:
https://wiki.govroam.uk/dokuwiki/doku.php?id=siteadmin:advanced_orps_radsecproxy_configuration&rev=1628679625

Last update: **2021/08/11 11:00**