OpenVPN

Integrating OpenVPN with RADIUS

Below is the culmination of at least a month working with OpenVPN.

I recently discovered a bug in the Mikrotik OpenVPN server implementation that prevents users from being informed that they entered invalid credentials. (This bug was resolved in RouterOS 7.4.) The project I'm working on requires Azure MFA be part of the equation for VPN authentication. Azure ADDS will lock a user account after three failed authentication attempts. Because of this Mikrotik bug, a user who accidentally mistypes a password has about nine seconds before Azure ADDS locks there account.

I submitted a bug report to Mikrotik, but as much as I am a Mikrotik fanboy, I know they're not going to fix it anytime soon (which they surprisingly did in RouterOS 7.4, but didn't back-port the fix into the ROS v6 release tree.) I can't be the first person to inform them of this bug, and their OpenVPN Server has always left much to be desired and not gotten much attention from them, so I don't expect it to be resolved anytime soon. I also wasn't about to deploy a VPN solution to a user base that was going to be constantly resulting in calls to the helpdesk because of account lockouts.

I wanted to use the Mikrotik router because its very easy to implement firewall policies that are based on the user's group returned from RADIUS.

The goal of this exercise was learning how to integrate RADIUS authentication with MFA PUSH requirements and be able to service similar group based firewall policies.

I have not yet gotten around to the firewall policies implementation, but I do have a good idea of how it can be done.

The configuration below uses the following authentication strategies:

- Private CA created with EasyRSAv3, complete with CRL distribution endpoints. This is not detailed here.
- The Private CA was created an an Intermediate CA signed by another well used CA that I did not want to use for client certificates.
- Server certificates generated by the above Private CA
- User certificates generated by the above Private CA
- The following factors are required for a successful login:
  - A valid user certificate. The CN must match the username of the person logging into the OpenVPN server.

    - Username and password supplied by the user is authentication against a RADIUS server.
        - Using RADIUS allows any number of 2FA/MFA solutions to be leveraged for a third factor such as an MFA PUSH notification via Azure MFA or DUO.
        - The OpenVPN radius plugin does not support radsec, so radsecproxy was also used to provide secure RADIUS queries across the Internet to redundant cloud hosted servers.

If you know what you're doing, you can use the configs and scripts listed below to implement the same solution. □□

Installing OpenVPN and the OpenVPN plugin in Ubuntu

```
apt -y install openvpn openvpn-auth-radius


mkdir -p /etc/openvpn/client /etc/openvpn/server /etc/openvpn/server-ccd
```

/etc/openvpn/server/server.conf

```
server 192.168.168.0 255.255.255.0
proto udp
port 1194
dev tun1
topology subnet

;user nobody
;group nogroup

cipher AES-256-GCM
auth SHA256

management 127.0.0.1 61194 /etc/openvpn/server/pw-file

duplicate-cn

;client-cert-not-required
verify-client-cert require
;username-as-common-name

;auth-user-pass-verify
```

```
ca         /etc/openvpn/server/ca-chained.crt
crl-verify /etc/openvpn/server/crl.pem
cert       /etc/openvpn/server/server.crt
key        /etc/openvpn/server/server.key
dh none
ecdh-curve secp521r1

tls-auth /etc/openvpn/server/tls-auth.key 0
tls-version-min 1.2

verb 1
log               /var/log/openvpn/openvpn.log
status            /var/log/openvpn/openvpn-status.log
client-config-dir /etc/openvpn/server-ccd

script-security 2
tls-verify            /etc/openvpn/server/script-tls-verify
auth-user-pass-verify /etc/openvpn/server/script-auth-user-pass-verify via-env
plugin                /usr/lib/openvpn/radiusplugin.so /etc/openvpn/server/radiusplugin.cnf
client-connect        /etc/openvpn/server/script-client-connect

ifconfig-pool-persist /var/log/openvpn/ipp.txt

push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 8.8.4.4"
;push "dhcp-option DNS 192.168.168.1"
push "dhcp-option DOMAIN ovpn.loc"

; Do you want the default gateway redirected? There's a few ways to do it:
push "redirect-gateway"
;push "redirect-gateway autolocal"
;push "redirect-gateway def1 bypass-dhcp"

; Pick other routes you want to push to the clients:
;push "route 10.0.0.0 255.0.0.0"
;push "route 172.16.0.0 255.240.0.0"
;push "route 192.168.0.0 255.255.0.0"
;push "route 100.64.0.0 255.192.0.0"

keepalive 10 120
```

```
persist-key
persist-tun

;mute 20
;explicit-exit-notify 1
```

/etc/openvpn/server/radiusplugin.cnf

```
# The NAS identifier which is sent to the RADIUS server
# The service type which is sent to the RADIUS server
# The framed protocol which is sent to the RADIUS server
# The NAS port type which is sent to the RADIUS server
# The NAS IP address which is sent to the RADIUS server
NAS-Identifier=something-that-is-meaningful
Service-Type=2
Framed-Protocol=1
NAS-Port-Type=5
NAS-IP-Address=192.168.1.1

# Path to the OpenVPN configfile. The plugin searches there for
# client-config-dir PATH   (searches for the path)
# status FILE                      (searches for the file, version must be 1)
# client-cert-not-required (if the option is used or not)
# username-as-common-name  (if the option is used or not)
OpenVPNConfig=/etc/openvpn/server/server.conf



# Support for topology option in OpenVPN 2.1
# If you don't specify anything, option "net30" (default in OpenVPN) is used.
# You can only use one of the options at the same time.
# If you use topology option "subnet", fill in the right netmask, e.g. from OpenVPN option "--
server NETWORK NETMASK"
subnet=255.255.255.0
# If you use topology option "p2p", fill in the right network, e.g. from OpenVPN option "--
server NETWORK NETMASK"
# p2p=10.8.0.1



# Allows the plugin to overwrite the client config in client config file directory,
```

```
# default is true
overwriteccfiles=true

# Allows the plugin to use auth control files if OpenVPN (>= 2.1 rc8) provides them.
# default is false
useauthcontrolfile=true



# Path to a script for vendor specific attributes.
# Leave it out if you don't use an own script.
#vsascript=/etc/openvpn/server/vsascript.pl

# Path to the pipe for communication with the vsascript.
# Leave it out if you don't use an own script.
#vsanamedpipe=/tmp/vsapipe

# A radius server definition, there could be more than one.
# The priority of the server depends on the order in this file. The first one has the highest
priority.
server
{
        acctport=1813
        authport=1812
        retry=0
        wait=30
        name=127.0.0.1
        sharedsecret=ChangeMe
}
```

/etc/openvpn/server/script-auth-user-pass-verify

The script below is used currently to make sure that the username and the user certificate name match, otherwise, deny the login request.

Unfortunately, OpenVPN runs the RADIUS plugin in a different thread, so if you're using RADIUS to do PUSH notifications to Azure MFA, DUO, Okta, etc., the user will most likely receive a PUSH notification if they have entered correct credentials, even though there may be a certificate mismatch since these two processes are running in parallel.

```
#!/bin/bash
DUMPFILE=/var/log/openvpn/dump.all
```

```
echo "script-auth-user-pass-verify" >> $DUMPFILE
date >> $DUMPFILE
echo "==========" >> $DUMPFILE
for arg in "$@"; do
        echo "ARG: $arg" >> $DUMPFILE
done
echo "==========" >> $DUMPFILE
env >> $DUMPFILE
echo "==========" >> $DUMPFILE
echo "Pulled from environment:" >> $DUMPFILE
echo "common_name: $common_name" >> $DUMPFILE
echo "username:    $username" >> $DUMPFILE
if [ "$common_name" = "$username" ]; then
        echo "Names match!!! Allowing connection!"
        echo "==========" >> $DUMPFILE
        echo "" >> $DUMPFILE
        echo "" >> $DUMPFILE
        echo "" >> $DUMPFILE
else
        echo "$untrusted_ip:$untrusted_port script-auth-user-pass-verify: common_name and
username do not match... denying connection!!!"
        echo "common_name and username do not match... denying connection!!!" >> $DUMPFILE
        echo "==========" >> $DUMPFILE
        echo "" >> $DUMPFILE
        echo "" >> $DUMPFILE
        echo "" >> $DUMPFILE
        exit 1
fi
```

/etc/openvpn/server/script-client-connect

This script doesn't do anything currently but log available environment variables to the dump.all file. It can be used to push additional configuration details to the OpenVPN server for the user that is logging in.

```
#!/bin/bash
DUMPFILE=/var/log/openvpn/dump.all

echo "script-client-connect" >> $DUMPFILE
```

```
date >> $DUMPFILE
echo "==========" >> $DUMPFILE
for arg in "$@"; do
        echo "ARG: $arg" >> $DUMPFILE
done
echo "==========" >> $DUMPFILE
env >> $DUMPFILE
echo "==========" >> $DUMPFILE
echo "" >> $DUMPFILE
echo "" >> $DUMPFILE
echo "" >> $DUMPFILE
```

OpenVPN Client Configuration

```
setenv FRIENDLY_NAME "Meaningful name"
setenv USERNAME "actual.username@some.domain.com"
setenv ALLOW_PASSWORD_SAVE 0

remote vpn.your.domain.here.com 1194

client
proto udp
dev tun1

connect-retry 300
connect-retry-max 0
ping 20

remote-cert-tls server
auth-user-pass
auth-retry interact
cipher AES-256-GCM
auth SHA256

nobind
persist-key
persist-tun
reneg-sec 0

<ca>
```

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
</ca>

key-direction 1

<tls-auth>
-----BEGIN OpenVPN Static key V1-----
-----END OpenVPN Static key V1-----
</tls-auth>

<key>
-----BEGIN PRIVATE KEY-----
-----END PRIVATE KEY-----
</key>

<cert>
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
</cert>
```

OpenVPN Connect Client - Profile Update

The latest versions of OpenVPN Connect deprecated a few configuration options. The following configuration option that was previously acceptable has been deprecated and needs to be changed to the two separate options. If using udp instead of tcp, just change the options appropriately.

```
proto tcp-client

# needs to be changed to

client
```

```
proto tcp
```

#end

Revision #7
Created 2022-05-12 23:10:46 UTC by bluecrow76
Updated 2023-10-18 19:19:38 UTC by bluecrow76