

vpn ikev2 anyconnect with freeradius

Introduction

Configuring and deploying Cisco IOS certificate server

```
conf t
```

First define the new CA.

```
ip http server

crypto pki server ca-server
  database level names
  no database archive
  hash sha512
  lifetime certificate 3650
  lifetime ca-certificate 7305 23 59
  eku server-auth client-auth
  auto-rollover 365
  database url flash:ca
exit
```

Now we have a CA operating, we need to generate a certificate for our router to identify itself to clients.

```
crypto key generate rsa general modulus 2048 exportable label ca-server
do crypto pki server ca-server start

crypto key generate rsa general modulus 2048 exportable label router

crypto pki trustpoint router
  enrollment url http://<ip address>:80
  ip-address <ip address>
  fqdn <DNS entry pointing to router>
  subject-name CN=<site name>,OU=user-vpn,O=<company name>
  revocation-check crl
  rsakeypair router
  auto-enroll regenerate
  hash sha512
exit

crypto pki authenticate router
crypto pki enroll router
```

The certificate server should now have a pending request.

Last update: 25/05/2018 atelier:chantier:vpn-ikev2-anyconnect-with-freeradius http://debian-facile.org/atelier:chantier:vpn-ikev2-anyconnect-with-freeradius
11:44

```
do show crypto pki server ca-server requests
do crypto pki server ca-server grant <request number>
```

The request number is often 1

Client Related Configuration

```
crypto key generate rsa general modulus 2048 exportable label anyconnect

crypto pki trustpoint anyconnect
  enrollment url http://<ip address>:80
  serial-number none
  fqdn none
  ip-address none
  subject-name CN=<site name>,OU=user-vpn,O=<company name>
  revocation-check none
  rsakeypair anyconnect

crypto pki authenticate anyconnect
crypto pki enroll anyconnect
```

The certificate server should now have a pending request.

```
do show crypto pki server ca-server requests
do crypto pki server ca-server grant <request number>
```

The request number is often 1

Export And Install Certificates For Client

```
crypto pki export anyconnect pem terminal
```

Crypto Configuration

```
aaa new-model
aaa group server radius freeradius

server-private <freeradius ip> auth-port 1812 acct-port 1813 key cisco12
aaa authentication login win7 group freeradius

aaa accounting network default start-stop group freeradius

crypto ikev2 profile default
```

```
match identity remote key-id anyconnect_remote_access
match identity remote key-id cisco.com
identity local dn
authentication remote eap query-identity
authentication local rsa-sig
pki trustpoint anyconnect
dpd 60 2 on-demand
aaa authentication eap win7
aaa authorization user eap cached
aaa accounting eap default
virtual-template 1
```

```
crypto ipsec transform-set default esp-aes 256 esp-sha-hmac
mode tunnel
```

```
crypto ipsec profile default
set ikev2-profile default
```

```
interface Virtual-Template1 type tunnel
ip unnumbered Loopback0
tunnel mode ipsec ipv4
tunnel protection ipsec profile default
```

```
ip local pool mypool 192.168.1.3
```

```
access-list 99 permit any
```

```
a
```

```
ggggg
```

```
a
```

```
ggggg
```

```
a
```

```
gggggg
```

```
a
```

Introduction

Introduction

From:
<http://debian-facile.org/> - Documentation - Wiki



Permanent link:
<http://debian-facile.org/atelier:chantier:vpn-ikev2-anyconnect-with-freeradius>

Last update: **25/05/2018 11:44**