



# OpenVPN with Mikrotik RouterBOARD

Anthony, Duong Nguyen

Sales Director

Mobile: +84 9 7117 5115 - Email: [duongnt@adtek.vn](mailto:duongnt@adtek.vn)

# About Us



# Our Company

- ▶ Company Name: AD.TEK Joint Stock Company
- ▶ Brand name: Advanced Networks Technology
- ▶ Head quarter: No.9 Building 10, Lane 95 Chua Boc st., Dong Da dist., Hanoi
- ▶ Founded: November 2010
- ▶ Resources: 30+ employees with 10+ Technical engineers
- ▶ Business: Datacenter and Enterprise Network solutions and products distribution
- ▶ Contact: [sales@adtek.vn](mailto:sales@adtek.vn) [www.adtek.vn](http://www.adtek.vn)

| Hanoi                                                                      | Ho Chi Minh City                                                               | Nha Trang City                                                             |
|----------------------------------------------------------------------------|--------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| 45/140 Khuat Duy Tien st.<br>Thanh Xuan, Hanoi<br>Hotline: +84 98 672 8080 | 26F/11 Le Quoc Hung st.<br>Ward 12, Dist. 4, HCMC.<br>Hotline: +84 98 652 8080 | 25 Nguyen Van Bay st.<br>Phuoc Long, Nha Trang<br>Hotline: +84 97 235 8080 |

# Our Solutions

- ▶ DataCenter: Cable Routing & Pathway system, Structured Cabling System, Network infrastructure, Network Routing & Switching, Cloud Storage, DCIM, UPS, Rack & Cabinet
- ▶ Enterprise: Structured Cabling system, Routing & Switching, Server & Storage, Security, Wireless Solution, Video Surveillance, UPS, Rack & Cabinet
- ▶ Wireless: Carrier grade Wireless PTP, PMP, Wifi Access Point, Hotspot & Billing solutions

# Our Vertical Market



## Our Partners

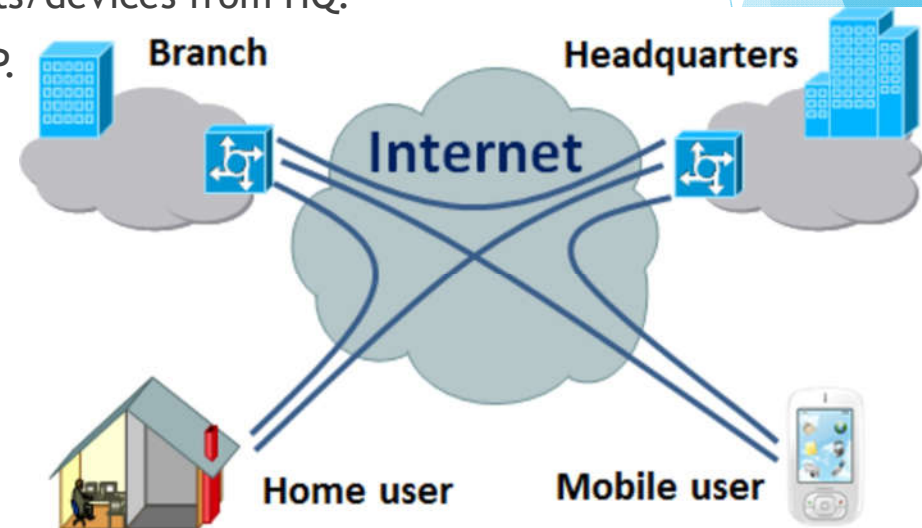




# OpenVPN with Mikrotik RouterOS

# Challenges

- ▶ Corporate with Head Quarter and multiple branch/offices need to sharing data between sites
- ▶ Corporate with mobile users working out of office and connect to Private/Local Applications system
- ▶ Central managed for IT networking equipments/devices from HQ.
- ▶ Over budget for leasedline/MPLS VPN from ISP.



# Prerequisites

- ▶ Equipments
  - ▶ HQ networks (LAN, Servers) and Mikrotik Gateway router
  - ▶ Branch networks with Mikrotik Gateway router
- ▶ Technical skill
  - ▶ Networking basic: TCP/IP, NAT, IPSec, VPN, SSL knowledge based
  - ▶ RouterOS features, Webfig/Winbox, RouterOS CLI

# What is OpenVPN?

- ▶ Open Source software application implements VPN (virtual private network) for creating secure point-to-point or site-to-site connection.
- ▶ Written by Jame Yonan and published under GNU General Public License (GPL)
- ▶ Support routed or bridged mode and remote access topology
- ▶ Used custom security protocol utilized SSL/TSL for key exchange
- ▶ Allow peers to authenticate each other using pre-shared secret key, certificates or username/password.
- ▶ Uses the OpenSSL encryption library, as well as the SSLv3/TLSv1 protocol, and contains many security and control features.
- ▶ Has been ported and embedded to several systems like DD-WRT (GNU/Linux-based firmware for wireless routers and access points), Mikrotik RouterOS, SoftEther VPN,...

# Architecture

## ► Encryption

- OpenVPN uses the OpenSSL library to provide encryption of both the data and control channels. It lets OpenSSL do all the encryption and authentication work, allowing OpenVPN to use all the ciphers available in the OpenSSL package
- Can support the HMAC (Hash-based message authentication code) packet authentication feature to add an additional layer of security to the connection
- Also support hardware acceleration to get better encryption performance

## ► Authentication

- Support pre-shared keys, certificate-based, and username/password-based authentication

## ► Security

- 256 bits encryption through OpenSSL library
- Custom protocol based on SSL and TLS support IKE, IPSec, L2TP or PPTP.

## ► Networking

- Support over both UDP or TCP
- Support IPv6 (version 2.3.x)
- Support working through proxy servers (including HTTP proxy server)
- Support working through NAT
- Support TUN (layer 2) or TAP (layer 3) interface
- IANA official port: 1194

# Mikrotik RouterOS and OpenVPN

## ▶ Support

- ▶ TCP
- ▶ Bridging (TAP interface)
- ▶ Routing (TUN interface)
- ▶ Certificates
- ▶ P2P mode

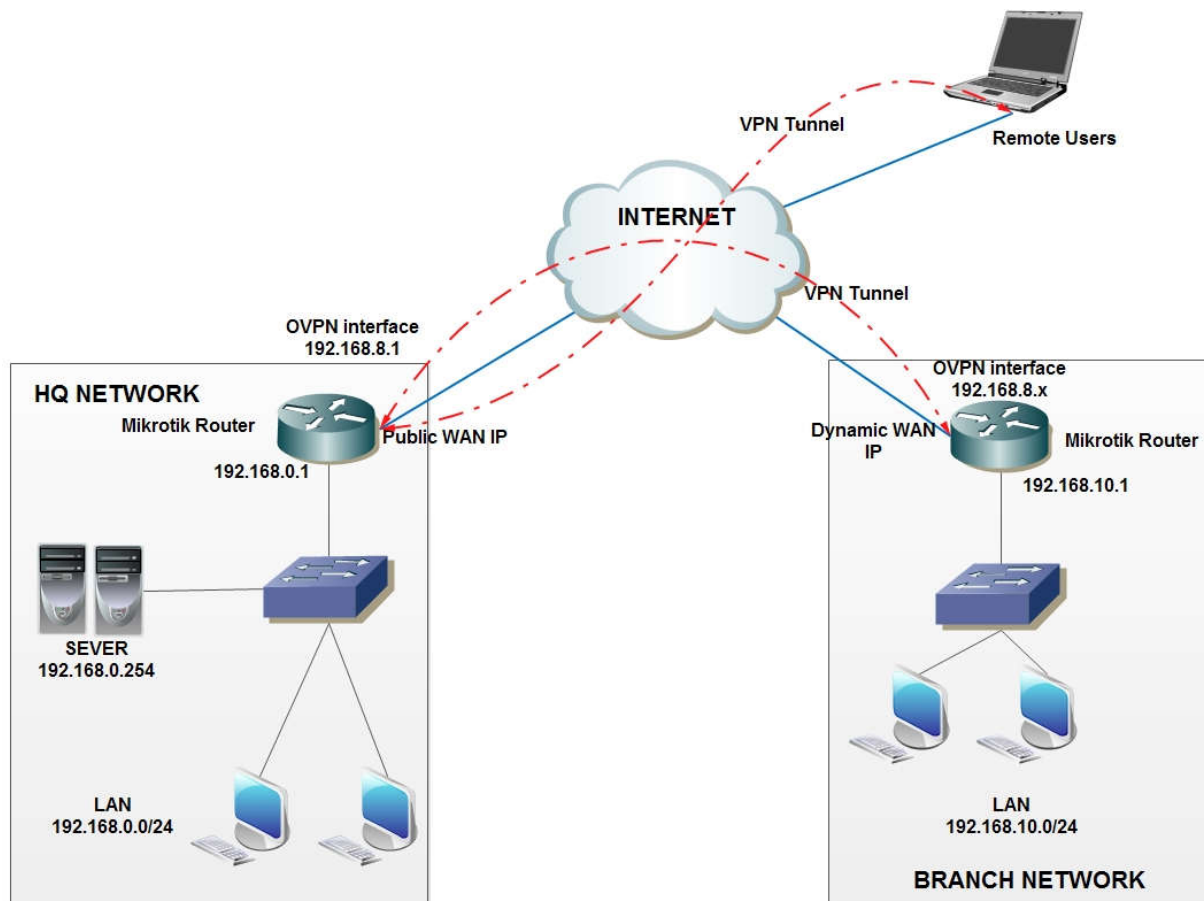
## ▶ Naming Linux/Windows vs. RouterOS

- ▶ TUN - RouterOS: IP
- ▶ TAP - RouterOS: ethernet

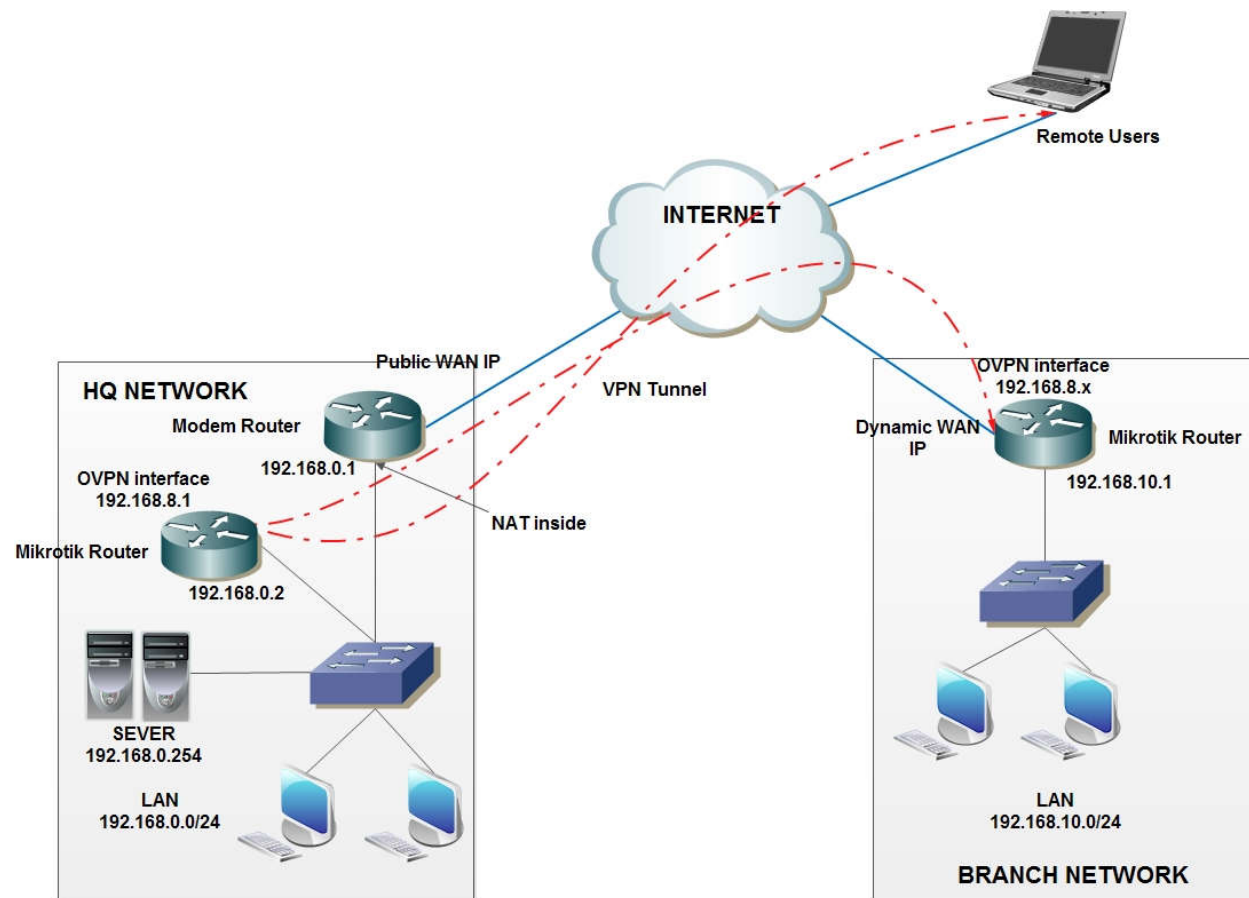
## ▶ Unsupport

- ▶ UDP
- ▶ LZO Compression

# Topology



# Topology



# How to?

- ▶ 1. Certificate Generation
- ▶ 2. Server site VPN gateway setup
- ▶ 3. Branch site VPN Client setup
- ▶ 4. Routing & Check connection



# Certificates generation

- ▶ ssh/telnet to HQ Mikrotik gateway, create your own certificate authority (CA) named myCA and.

```
admin@HQ-MikrotikGW] /certificate> add name=myCa common-name=myCa key-usage=key-cert-sign,crl-sign
admin@HQ-MikrotikGW] /certificate>
admin@HQ-MikrotikGW] /certificate>
admin@HQ-MikrotikGW] /certificate> sign myCa ca-crl-host=192.168.1.1 name=myCa
```

- ▶ 192.168.1.1 is LAN interface
- ▶ export the CA certificate

```
adm: [admin@HQ-MikrotikGW] /certificate> export-certificate myCa
```

- ▶ Create a private and public key pair for the VPN Server and another key pair for the VPN Client.

```
[admin@HQ-MikrotikGW] /certificate> add name=OVPNserver common-name=server
[admin@HQ-MikrotikGW] /certificate> add name=OVPNbranch common-name=branch
```

# Certificates generation (cont.)

- ▶ Sign both public keys with new CA

```
#/certificate sign OVPNserver ca=myCA name=server
```

```
#/certificate sign OVPNbranch ca=myCA name=branch
```

- ▶ Export the VPN branch's private key and public key+certificate files.

```
[admin@HQ-MikrotikGW] /certificate> export-certificate export-passphrase=yourpassword branch
```

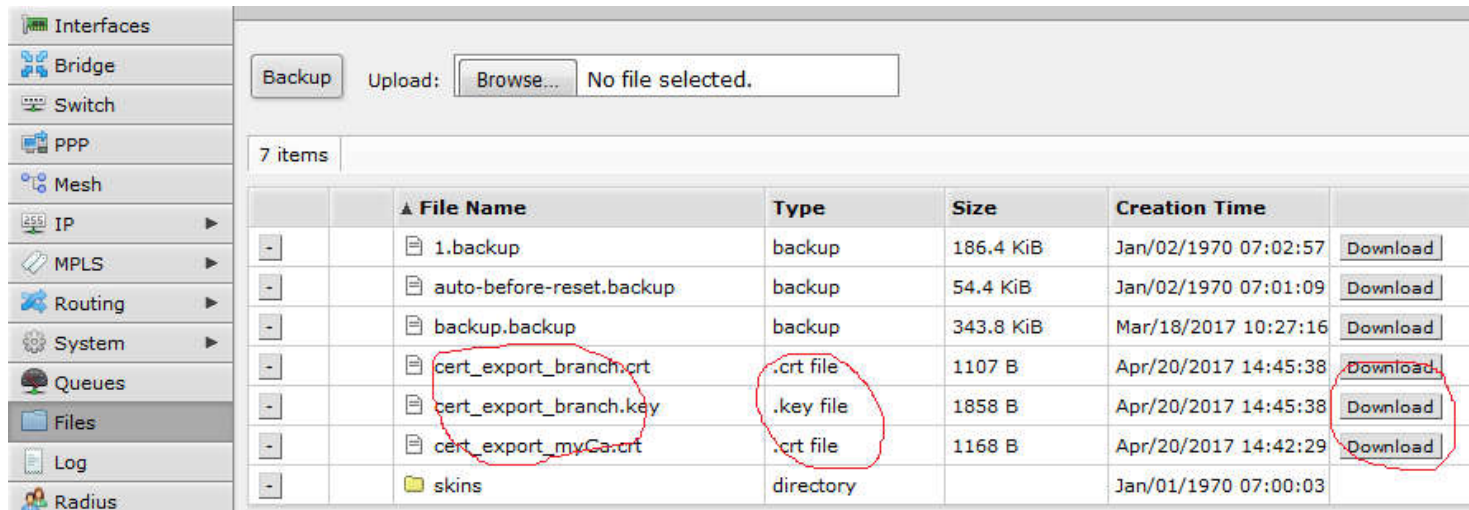
```
[admin@HQ-MikrotikGW] /certificate> print
Flags: K - private-key, D - dsa, L - crt, C - smart-card-key, A - authority,
I - issued, R - revoked, E - expired, T - trusted
#      NAME      CO.. SUBJECT-ALT-NAME      FI..
0 K L A T myCa    myCa                      a4..
1 K I  server    se..                      da..
2 K I  branch    br..                      b1..
[admin@HQ-MikrotikGW] /certificate>
```

- ▶ Check your files:

```
[admin@HQ-MikrotikGW] > file print
# NAME                                TYPE                                SIZE CREATION-TIME
0 skins                               directory                           jan/01/1970 07:00:03
1 auto-before-reset.backup            backup                             54.4KiB jan/02/1970 07:01:09
2 1.backup                            backup                             186.4KiB jan/02/1970 07:02:57
3 cert_export_branch.crt              .crt file                           1107 apr/20/2017 14:45:38
4 cert_export_myCa.crt               .crt file                           1168 apr/20/2017 14:42:29
5 cert_export_branch.key              .key file                           1858 apr/20/2017 14:45:38
6 backup.backup                      backup                             343.8KiB mar/18/2017 10:27:16
[admin@HQ-MikrotikGW] >
```

# Certificates generation (cont.)

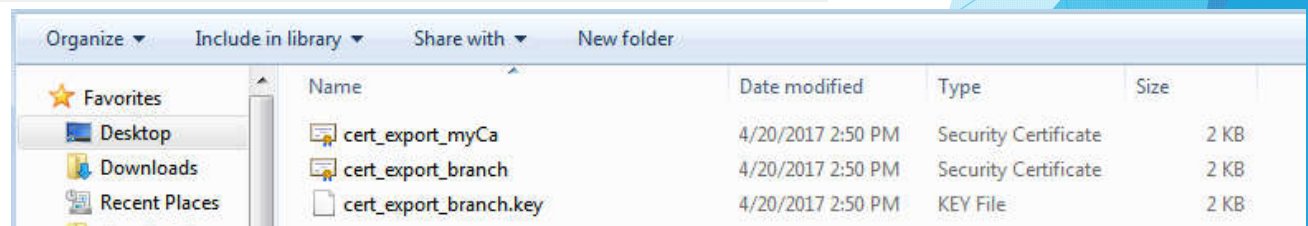
- Download branch's certificate files, using sftp/winbox or webfig.



Backup Upload:  No file selected.

7 items

|   | File Name                | Type      | Size      | Creation Time        |                                         |
|---|--------------------------|-----------|-----------|----------------------|-----------------------------------------|
| - | 1.backup                 | backup    | 186.4 KiB | Jan/02/1970 07:02:57 | <input type="button" value="Download"/> |
| - | auto-before-reset.backup | backup    | 54.4 KiB  | Jan/02/1970 07:01:09 | <input type="button" value="Download"/> |
| - | backup.backup            | backup    | 343.8 KiB | Mar/18/2017 10:27:16 | <input type="button" value="Download"/> |
| - | cert_export_branch.crt   | .crt file | 1107 B    | Apr/20/2017 14:45:38 | <input type="button" value="Download"/> |
| - | cert_export_branch.key   | .key file | 1858 B    | Apr/20/2017 14:45:38 | <input type="button" value="Download"/> |
| - | cert_export_myCa.crt     | .crt file | 1168 B    | Apr/20/2017 14:42:29 | <input type="button" value="Download"/> |
| - | skins                    | directory |           | Jan/01/1970 07:00:03 |                                         |



| Name                   | Date modified     | Type                 | Size |
|------------------------|-------------------|----------------------|------|
| cert_export_myCa       | 4/20/2017 2:50 PM | Security Certificate | 2 KB |
| cert_export_branch     | 4/20/2017 2:50 PM | Security Certificate | 2 KB |
| cert_export_branch.key | 4/20/2017 2:50 PM | KEY File             | 2 KB |

# Server site VPN gateway setup

- ▶ VPN parameters:
  - ▶ HQ LAN networks: 192.168.0.0/24; Branch LAN network: 192.168.10.0/24
  - ▶ VPN Network: 192.168.8.0/24, VPN Gateway: 192.168.8.1
  - ▶ IP Range for VPN Clients/Branch: 192.168.8.10-192.168.8.20
  - ▶ Server Certificate = yes
  - ▶ Auth = SHA1
  - ▶ Cipher = AES256
  - ▶ VPN TCP port = 1194
  - ▶ Client Certificate = Yes
  - ▶ Mode = IP (Layer 3 routing)

# Server site VPN gateway setup (cont.)

- ▶ Create the PPP profile and IP address pool

```
[admin@HQ-MikrotikGW] > /ip pool add name=ovpn-pool range=192.168.8.10-192.168.8.20
[admin@HQ-MikrotikGW] >
[admin@HQ-MikrotikGW] > /ppp profile add name=ovpn local-address=192.168.8.1 remote-address=ovpn-pool
```

- ▶ Check your configuration

```
[admin@HQ-MikrotikGW] > ip pool print
```

| # | NAME       | RANGES                    |
|---|------------|---------------------------|
| 0 | dhcp_pool1 | 192.168.0.2-192.168.0.254 |
| 1 | ovpn-pool  | 192.168.8.10-192.168.8.20 |

```
[admin@HQ-MikrotikGW] > /ppp profile print
```

Flags: \* - default

|   |                                                                                                                                                                                                                   |
|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0 | * name="default" use-mpfs=default use-compression=default use-vj-compression=default use-encryption=default only-one=default change-tcp-mss=yes address-list=""                                                   |
| 1 | name="ovpn" local-address=192.168.8.1 remote-address=ovpn-pool use-mpfs=default use-compression=default use-vj-compression=default use-encryption=default only-one=default change-tcp-mss=default address-list="" |

## Server site VPN gateway setup (cont.)

- ▶ Add “**branch**” user with second factor secret and check your configure

```
[admin@HQ-MikrotikGW] > /ppp secret add name=branch password=yourpassword profile=ovpn
[admin@HQ-MikrotikGW] >
[admin@HQ-MikrotikGW] >
[admin@HQ-MikrotikGW] > ppp secret print
Flags: X - disabled
#  NAME          SERVICE CALLER-ID  PASSWORD          PROFILE           REMOTE-ADDRESS
0  branch        any                yourpassword      ovpn
[admin@HQ-MikrotikGW] > █
```

- ▶ Replace **yourpassword** by your own password. This password must match both HQ and Branch configure.

## Server site VPN gateway setup (cont.)

- Create OVPN interface in the HQ-MikrotikGW using certificate, authentication SHA1, cipher AES256, port 1194, mode IP.

```
[admin@HQ-MikrotikGW] > /interface ovpn-server server set enabled=yes certificate=server auth=sha1 cipher=aes256
port=1194 netmask=24 require-client-certificate=yes mode=ip
[admin@HQ-MikrotikGW] >
[admin@HQ-MikrotikGW] >
[admin@HQ-MikrotikGW] >
[admin@HQ-MikrotikGW] > interface ovpn-server server print
      enabled: yes
      port: 1194
      mode: ip
      netmask: 24
      mac-address: FE:27:4D:08:0E:4B
      max-mtu: 1500
      keepalive-timeout: 60
      default-profile: default
      certificate: server
      require-client-certificate: yes
      auth: sha1
      cipher: aes256
[admin@HQ-MikrotikGW] >
```

# Branch site VPN Client setup

- Import certificate downloaded before to Branch Mikrotik Router using sftp/webfig/winbox

| Organize ▾             | Include in library ▾ | Share with ▾         | New folder |
|------------------------|----------------------|----------------------|------------|
| ★ Favorites            |                      |                      |            |
| Desktop                |                      |                      |            |
| Downloads              |                      |                      |            |
| Recent Places          |                      |                      |            |
| Name                   | Date modified        | Type                 | Size       |
| cert_export_myCa       | 4/20/2017 2:50 PM    | Security Certificate | 2 KB       |
| cert_export_branch     | 4/20/2017 2:50 PM    | Security Certificate | 2 KB       |
| cert_export_branch.key | 4/20/2017 2:50 PM    | KEY File             | 2 KB       |

Wireless

Interfaces

Bridge

Switch

PPP

Mesh

IP

MPLS

Routing

System

Queues

Files

Log

Radius

LCD

Backup

Upload:

Browse...

No file selected.

41 items

|   | ▲ File Name              | Type      | Size     | Creation Time        |          |
|---|--------------------------|-----------|----------|----------------------|----------|
| - | 111.rsc                  | script    | 73 B     | Mar/30/2017 13:52:17 | Download |
| - | 999.rsc                  | script    | 1900 B   | Mar/30/2017 13:54:41 | Download |
| - | activedone               | file      | 11 B     | Jan/02/1970 07:00:44 | Download |
| - | adtek.rsc                | script    | 73 B     | Mar/30/2017 13:50:25 | Download |
| - | auto-before-reset backup | backup    | 24.8 KiB | Dec/17/2016 07:41:47 | Download |
| - | cert_export_branch.crt   | .crt file | 1107 B   | Apr/20/2017 15:03:30 | Download |
| - | cert_export_branch.key   | .key file | 1858 B   | Apr/20/2017 15:03:34 | Download |
| - | cert_export_myCa.crt     | .crt file | 1168 B   | Apr/20/2017 15:03:18 | Download |
| - | disk1                    | disk      |          | Dec/13/2016 09:47:53 |          |

## Branch site VPN Client setup (cont.)

- Import certificates. Using your own password created before for passphrase

```
[admin@BR-MikrotikGW] /certificate> import file-name=cert_export_branch.crt
passphrase: *****
certificates-imported: 1
private-keys-imported: 0
files-imported: 1
decryption-failures: 0
keys-with-no-certificate: 0

[admin@BR-MikrotikGW] /certificate> import file-name=cert_export_branch.key
passphrase: *****
certificates-imported: 0
private-keys-imported: 1
files-imported: 1
decryption-failures: 0
keys-with-no-certificate: 0
```

```
[admin@BR-MikrotikGW] /certificate> import file-name=cert_export_myCa.crt
passphrase: *****
certificates-imported: 1
private-keys-imported: 0
files-imported: 1
decryption-failures: 0
keys-with-no-certificate: 0
```

- Check your imported certificates:

```
[admin@BR-MikrotikGW] > certificate print
Flags: K - private-key, D - dsa, L - crt, C - smart-card-key, A -
#      NAME                                COMMON-NAME
0 K    T cert_export_branch.crt_0         branch
1 L A  T cert_export_myCa.crt_0          myCa
[admin@BR-MikrotikGW] >
```

## Branch site VPN Client setup (cont.)

- ▶ Add VPN client interface.

```
[admin@BR-MikrotikGW] > interface ovpn-client \  
\... add name=ovpn-out1 connect-to=HQWAN-IP port=1194 mode=ip \  
\... user=branch password=yourpassword profile=default \  
\... certificate=cert_export_branch.crt_0 cipher=aes256 add-default-route=no
```

- ▶ Note:

- ▶ Change **HQWAN-IP** to your HQ Public IP address of HQ-MikrotikGW. If you are using dynamic IP address, please enable cloud and using domain name.
- ▶ Change yourpassword to your own password

# Routing & Check connection

- Check VPN Connection.

```
[admin@HQ-MikrotikGW] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
#   ADDRESS          NETWORK    INTERFACE
0   192.168.0.1/24     192.168.0.0 bridge1
1 D [REDACTED]         [REDACTED] pppoe-out1
2 D 192.168.8.1/32     192.168.8.20 <ovpn-branch>
[admin@HQ-MikrotikGW] >
```

```
[admin@HQ-MikrotikGW] > interface ovpn-server print
Flags: X - disabled, D - dynamic, R - running
#   NAME              USER      MTU CLIENT-ADDRESS      UPTIME   ENCODING
0   DR <ovpn-branch>   branch     1500 [REDACTED]          2h15m6s AES-256-CBC/SHA1
[admin@HQ-MikrotikGW] >
```

```
[admin@BR-MikrotikGW] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
#   ADDRESS          NETWORK    INTERFACE
0   ;;; defconf       192.168.10.1/24 192.168.10.0 bridge
1   ;;; hotspot network 10.5.50.1/24 10.5.50.0 hpdemo
2 D [REDACTED]         [REDACTED] pppoe-out1
3 D 192.168.8.20/32     192.168.8.1 ovpn-out1
[admin@BR-MikrotikGW] >
```

```
[admin@BR-MikrotikGW] > interface ovpn-client print
Flags: X - disabled, R - running
0   R name="ovpn-out1" mac-address=FE:09:3B:34:42:AE max-mtu=1500
    connect-to=[REDACTED] port=1194 mode=ip user="branch"
    password="yourpassword" profile=default
    certificate=cert_export_branch.crt_0 auth=sha1 cipher=aes256
    add-default-route=no
[admin@BR-MikrotikGW] >
```

## Routing & Check connection (cont)

```
[admin@HQ-MikrotikGW] > ping 192.168.8.20
```

| SEQ | HOST         | SIZE | TTL | TIME | STATUS |
|-----|--------------|------|-----|------|--------|
| 0   | 192.168.8.20 | 56   | 64  | 26ms |        |
| 1   | 192.168.8.20 | 56   | 64  | 22ms |        |
| 2   | 192.168.8.20 | 56   | 64  | 23ms |        |
| 3   | 192.168.8.20 | 56   | 64  | 23ms |        |

sent=4 received=4 packet-loss=0% min-rtt=22ms avg-rtt=23ms max-rtt=26ms

```
[admin@HQ-MikrotikGW] >
```

```
[admin@BR-MikrotikGW] >> ping 192.168.8.1
```

| SEQ | HOST        | SIZE | TTL | TIME | STATUS |
|-----|-------------|------|-----|------|--------|
| 0   | 192.168.8.1 | 56   | 64  | 23ms |        |
| 1   | 192.168.8.1 | 56   | 64  | 26ms |        |

sent=2 received=2 packet-loss=0% min-rtt=23ms avg-rtt=24ms max-rtt=26ms

# Routing & Check connection (cont.)

## ► On HQ Router:

```
[admin@HQ-MikrotikGW] >
[admin@HQ-MikrotikGW] > ip route add dst-address=192.168.10.0/24 gateway=192.168.8.20
[admin@HQ-MikrotikGW] >
```

## ► On Brand Router:

```
[admin@BR-MikrotikGW] > ip route add dst-address=192.168.0.0/24 \
\... gateway=192.168.8.1
```

## ► Check Routing

```
[admin@BR-MikrotikGW] >> ping 192.168.0.254
```

| SEQ | HOST          | SIZE | TTL | TIME | STATUS |
|-----|---------------|------|-----|------|--------|
| 0   | 192.168.0.254 | 56   | 63  | 25ms |        |
| 1   | 192.168.0.254 | 56   | 63  | 23ms |        |
| 2   | 192.168.0.254 | 56   | 63  | 23ms |        |

```
sent=3 received=3 packet-loss=0% min-rtt=23ms avg-rtt=23ms max-rtt=25ms
[admin@BR-MikrotikGW] >>
```

# Routing & Check connection (cont.)

- From Laptop in Branch, connect to HQ Server

```
C:\Windows\system32\cmd.exe
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 23ms, Maximum = 37ms, Average = 29ms

C:\Users\Anthony>
C:\Users\Anthony>
C:\Users\Anthony>
C:\Users\Anthony>tracert 192.168.0.254

Tracing route to MYSERVER [192.168.0.254]
over a maximum of 30 hops:
  0  118 ms    74 ms    1 ms    192.168.10.1
  1  24 ms     24 ms    24 ms    192.168.8.1
  2  30 ms     33 ms    32 ms    MYSERVER [192.168.0.254]

Trace complete.

C:\Users\Anthony>
```

```
C:\Windows\system32\cmd.exe
Default Gateway . . . . . :
Tunnel adapter Teredo Tunneling Pseudo-Interface:
    Connection-specific DNS Suffix  . :
    IPv6 Address. . . . . : 2001:0:9d38:6abd:347f:1e1:3f57:f5f8
    Link-local IPv6 Address . . . . . : fe80::347f:1e1:3f57:f5f8%14
    Default Gateway . . . . . :

C:\Users\Anthony>ping 192.168.0.254

Pinging 192.168.0.254 with 32 bytes of data:
Reply from 192.168.0.254: bytes=32 time=37ms TTL=62
Reply from 192.168.0.254: bytes=32 time=27ms TTL=62
Reply from 192.168.0.254: bytes=32 time=23ms TTL=62
Reply from 192.168.0.254: bytes=32 time=29ms TTL=62

Ping statistics for 192.168.0.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 23ms, Maximum = 37ms, Average = 29ms

C:\Users\Anthony>
C:\Users\Anthony>
```



# THANK YOU

**Anthony, Duong Nguyen**

*Sales Director*

Email: [duongnt@adtek.vn](mailto:duongnt@adtek.vn)

Mobile: +84 97 117 5115 / +84 93 448 6969 (Whatsapp/Zalo/Vibers)

Skype: duongnt37

## ADVANCED NETWORKS TECHNOLOGY – AD.TEK JSC

Email: [sales@adtek.vn](mailto:sales@adtek.vn)

Website: <http://www.adtek.vn>

### **Hanoi**

45/140 Khat Duy Tien st.,  
Thanh Xuan dist., Hanoi  
Hotline: +84 98 672 8080

### **Ho Chi Minh City**

26F/11 Le Quoc Hung st.,  
Ward 12, District 4, HCMC  
Hotline: +84 98 652 8080

### **Nha Trang City**

25 Nguyen Van Bay st.,  
Phuoc Long, Nha Trang City  
Hotline: +84 97 235 8080