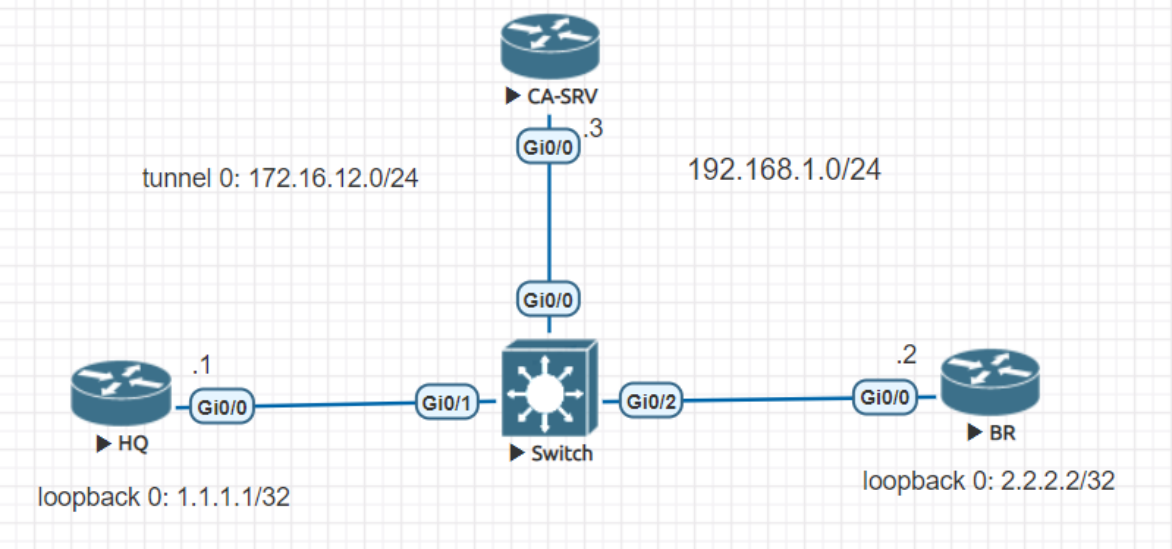
Cryptography
LAB – Cấu hình FlexVPN dùng Server CA trên Router

Sơ đồ:



Mô tả:

Sơ đồ Lab gồm 1 switch, 2 router và 1 router đóng vai trò server ca được đấu nối như hình.

Trên sơ đồ này, học viên sẽ thực tập cấu hình flexvpn sử dụng certificate được tạo ra trên server ca.

Yêu cầu:

1. Học viên thực hiện đấu nối các thiết bị và đặt địa chỉ IP cũng như các hostname của các thiết bị như được chỉ ra trên hình.
2. Sau khi thiết lập xong sơ đồ, học viên tiến hành cấu hình flexvpn trên router HQ và BR sử dụng phương thức Pre-shared key.
3. Thực hiện cấu hình server ca trên router CA-SRV để tự động tạo ra certificate, sau đó thêm phương thức xác thực sử dụng certificate được tạo trên server ca vào router HQ và BR.

Thực hiện:

Bước 1: Kết nối và cấu hình cơ bản:

Học viên thực hiện kết nối thiết bị và cấu hình cơ bản trên các thiết bị theo yêu cầu đặt ra.

Bước 2: Cấu hình flexvpn trên router HQ và BR:

Cấu hình:

Cấu hình ikev2 keyring trên router HQ:

```
HQ(config)#ip domain-name vnpro.com
HQ(config)#crypto ikev2 keyring IKE-RING
HQ(config-ikev2-keyring)#peer BR
HQ(config-ikev2-keyring-peer)#address 192.168.1.2
HQ(config-ikev2-keyring-peer)#pre-shared-key vnpro123
HQ(config-ikev2-keyring-peer)#exit
```

Cấu hình ikev2 profile trên router HQ:

```
HQ(config)#crypto ikev2 profile IKE-PROFILE
IKEv2 profile MUST have:
   1. A local and a remote authentication method.
   2. A match identity or a match certificate or match any statement.
HQ(config-ikev2-profile)#match identity remote address 192.168.1.2
255.255.255.0
HQ(config-ikev2-profile)#authentication local pre-share
HQ(config-ikev2-profile)#authentication remote pre-share
HQ(config-ikev2-profile)#keyring local IKE-RING
HQ(config-ikev2-profile)#dpd 60 2 on-demand
HQ(config-ikev2-profile)#exit
```

Lưu ý: dpd là câu lệnh để kiểm tra tình trạng peers ở bài này thì interval 60s và holdtime là 2 lần 60s.

Cấu hình ipsec profile trên router HQ:

```
HQ(config)#crypto ipsec profile IPSEC-PROFILE
HQ(ipsec-profile)#set ikev2-profile IKE-PROFILE
HQ(ipsec-profile)# exit
```

Cấu hình interface tunnel trên router HQ:

```
HQ(config)#interface tunnel 0
HQ(config-if)#ip address 172.16.12.1 255.255.255.0
HQ(config-if)#tunnel source g0/0
HQ(config-if)#tunnel destination 192.168.1.2
HQ(config-if)#tunnel protection ipsec profile IPSEC-PROFILE
HQ(config-if)#exit
```

Cấu hình tương tự trên router BR:

```
BR(config)#ip domain-name vnpro.com
```

```
BR(config)#crypto ikev2 keyring IKE-RING
BR(config-ikev2-keyring)#peer HQ
BR(config-ikev2-keyring-peer)#address 192.168.1.1
BR(config-ikev2-keyring-peer)#pre-shared-key vnpro123
BR(config-ikev2-keyring-peer)#exit
BR(config-ikev2-keyring)#exit
BR(config)#crypto ikev2 profile IKE-PROFILE
IKEv2 profile MUST have:
   1. A local and a remote authentication method.
   2. A match identity or a match certificate or match any statement.
BR(config-ikev2-profile)#match identity remote address 192.168.1.1
255.255.255.0
BR(config-ikev2-profile)#authentication local pre-share
BR(config-ikev2-profile)#authentication remote pre-share
BR(config-ikev2-profile)#keyring local IKE-RING
BR(config-ikev2-profile)#dpd 60 2 on-demand
BR(config-ikev2-profile)#exit
BR(config)#crypto ipsec profile IPSEC-PROFILE
BR(ipsec-profile)#set ikev2-profile IKE-PROFILE
BR(ipsec-profile)# exit
BR(config)#interface tunnel 0
BR(config-if)#ip address 172.16.12.2 255.255.255.0
BR(config-if)#tunnel source g0/0
BR(config-if)#tunnel destination 192.168.1.1
BR(config-if)#tunnel protection ipsec profile IPSEC-PROFILE
BR(config-if)#exit
```

Lưu ý: Phải cấu hình định tuyến để các địa chỉ loopback của các router có thể ping được nhau thông qua interface tunnel.

Kiểm tra:

Ping loopback0 của router HQ sang loopback0 của router BR:

```
HQ#ping 2.2.2.2 source 1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
```

```
Packet sent with a source address of 1.1.1.1

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms
```

Kiểm tra ikv2 session trên router HQ:

```
HQ#show crypto ikev2 session
 IPv4 Crypto IKEv2 Session


Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1


Tunnel-id Local                 Remote                fvrf/ivrf
Status
1         192.168.1.1/500       192.168.1.2/500       none/none
READY
      Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth
sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/12 sec
Child sa: local selector  192.168.1.1/0 - 192.168.1.1/65535
          remote selector 192.168.1.2/0 - 192.168.1.2/65535
          ESP spi in/out: 0xFD71C36F/0x8CD44616


 IPv6 Crypto IKEv2 Session
```

Lúc này ta thấy Auth sign và Auth verify đang để PSK là đang ở dạng pre-shared key.

Bước 3: Cấu hình server ca và thay đổi phương thức pre-shared key sang dùng certificate:

Cấu hình:

Đầu tiên ta phải cấu hình ntp để đồng bộ thời gian của 3 router vì khi router HQ và BR lấy certificate từ server ca thì thầy gian phải nằm trong start valid certificate ở router CA-SRV.

Cấu hình server ca trên router CA-SRV:

```
CA-SRV(config)#ip domain-name vnpro.com
CA-SRV(config)#ip http server
CA-SRV(config)#crypto pki server CA-SRV
CA-SRV(cs-server)#issuer-name cn="CA-SRV"
CA-SRV(cs-server)#grant auto
% The CA was already configured to automatically grant certificates
```

```
CA-SRV(cs-server)#no shutdown
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit
Password:

Re-enter password:
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

% Certificate Server enabled.
CA-SRV(cs-server)#
Nov 29 07:06:24.061: %SSH-5-ENABLED: SSH 1.99 has been enabled
Nov 29 07:06:25.040: %PKI-6-CS_ENABLED: Certificate server now enabled.
CA-SRV(cs-server)#exit
```

Thay đổi phương thức Auth sign và Auth verify:

Trên router HQ cấu hình trustpoint:

```
HQ(config)#crypto pki trustpoint CA-SRV
HQ(ca-trustpoint)#enrollment url http://192.168.1.3:80
HQ(ca-trustpoint)#subject-name cn=HQ.vnpro.com
HQ(ca-trustpoint)#exit
```

Trên router HQ cấu hình pki authentication:

```
HQ(config)#crypto pki authenticate CA-SRV
Certificate has the following attributes:
       Fingerprint MD5: 852F07BC 48EA88B1 B292AB69 5F1E5629
      Fingerprint SHA1: 55982CB0 AA5681F4 099397BA 72D002CD 78E22D8C

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
```

Cấu hình enroll trên router HQ:

```
HQ(config)#crypto pki enroll CA-SRV
```

```
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.

Password:
Re-enter password:

% The subject name in the certificate will include: cn=HQ.vnpro.com
% The subject name in the certificate will include: HQ.vnpro.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose CA-SRV' commandwill show the
fingerprint.

HQ(config)#
*Nov 29 07:27:37.153: CRYPTO_PKI:  Certificate Request Fingerprint MD5:
8316C965 832B8903 D69309AF 071AC60B
*Nov 29 07:27:37.155: CRYPTO_PKI:  Certificate Request Fingerprint SHA1:
84446996 99AF16D6 2A30DCF3 C268D8F4 F2E91540
*Nov 29 07:27:37.975: %PKI-6-CERTRET: Certificate received from Certificate
Authority
HQ(config)#exit
```

Thay đổi ikev2 profile trên router HQ:

```
HQ(config)#crypto ikev2 profile IKE-PROFILE
HQ(config-ikev2-profile)#authentication local rsa-sig
HQ(config-ikev2-profile)#identity local dn
HQ(config-ikev2-profile)#pki trustpoint CA-SRV
HQ(config-ikev2-profile)#exit
```

Kiểm tra certificate trên router HQ:

```
HQ#show crypto pki certificates verbose CA-SRV
Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 02
  Certificate Usage: General Purpose
  Issuer:
    cn=CA-SRV
  Subject:
    Name: HQ.vnpro.com
    hostname=HQ.vnpro.com
    cn=HQ.vnpro.com
  Validity Date:
    start date: 14:27:37 GMT Nov 29 2020
    end   date: 14:27:37 GMT Nov 29 2021
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (512 bit)
  Signature Algorithm: SHA1 with RSA Encryption
  Fingerprint MD5: 19F2DA37 95B91FE9 1EF2BE4D F17C5501
  Fingerprint SHA1: 9033C963 D2B8D5D5 7777C62F 38F9582D 9B9E51E3
  X509v3 extensions:
    X509v3 Key Usage: A0000000
      Digital Signature
      Key Encipherment
    X509v3 Subject Key ID: 126707CD F3D95581 2AC483D9 05D3B632 C3A0F434
    X509v3 Authority Key ID: 93A2E50B 8F5010C7 510B39BA 3EFD88B9 51EC98E0
    Authority Info Access:
  Associated Trustpoints: CA-SRV
  Key Label: HQ.vnpro.com

CA Certificate
  Status: Available
  Version: 3
```

```
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=CA-SRV
  Subject:
    cn=CA-SRV
  Validity Date:
    start date: 14:06:24 GMT Nov 29 2020
    end   date: 14:06:24 GMT Nov 29 2023
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
  Signature Algorithm: MD5 with RSA Encryption
  Fingerprint MD5: 852F07BC 48EA88B1 B292AB69 5F1E5629
  Fingerprint SHA1: 55982CB0 AA5681F4 099397BA 72D002CD 78E22D8C
  X509v3 extensions:
    X509v3 Key Usage: 86000000
      Digital Signature
      Key Cert Sign
      CRL Signature
    X509v3 Subject Key ID: 93A2E50B 8F5010C7 510B39BA 3EFD88B9 51EC98E0
    X509v3 Basic Constraints:
        CA: TRUE
    X509v3 Authority Key ID: 93A2E50B 8F5010C7 510B39BA 3EFD88B9 51EC98E0
    Authority Info Access:
  Associated Trustpoints: CA-SRV
```

Trên router BR cấu hình trustpoint:

```
BR(config)#crypto pki trustpoint CA-SRV
BR(ca-trustpoint)#enrollment url http://192.168.1.3:80
BR(ca-trustpoint)#revocation-check none
BR(ca-trustpoint)#exit
```

Cấu hình pki authentication trên router BR:

```
BR(config)#crypto pki authenticate CA-SRV
```

```
Certificate has the following attributes:
       Fingerprint MD5: 852F07BC 48EA88B1 B292AB69 5F1E5629
      Fingerprint SHA1: 55982CB0 AA5681F4 099397BA 72D002CD 78E22D8C

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
```

Cấu hình certificate map trên router BR:

```
BR(config)#crypto pki certificate map CA-MAP 10
BR(ca-certificate-map)#issuer-name eq cn=CA-SRV
BR(ca-certificate-map)#exit
```

Cấu hình thay đổi ikev2 profile trên router BR:

```
BR(config)#crypto ikev2 profile IKE-PROFILE
BR(config-ikev2-profile)#match certificate CA-MAP
BR(config-ikev2-profile)#authentication remote rsa-sig
BR(config-ikev2-profile)#exit
```

Kiểm tra:

Shutdown và no shutdown interface tunnel trên router HQ:

```
HQ(config)#int tunnel 0
HQ(config-if)#sh
Nov 29 07:39:59.441: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0,
changed state to down
Nov 29 07:39:59.442: %LINK-5-CHANGED: Interface Tunnel0, changed state to
administratively down
HQ(config-if)#no shut
Nov 29 07:40:05.324: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
Nov 29 07:40:05.326: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Nov 29 07:40:07.316: %LINK-3-UPDOWN: Interface Tunnel0, changed state to up
```

Kiểm tra lại phương thức Auth sign và Auth verify:

Trên router HQ:

```
HQ#show crypto ikev2 sa de
 IPv4 Crypto IKEv2  SA
```

```
Tunnel-id Local                 Remote                fvrf/ivrf
Status
2         192.168.1.1/500       192.168.1.2/500       none/none
READY
      Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth
sign: RSA, Auth verify: PSK
      Life/Active Time: 86400/141 sec
      CE id: 1039, Session-id: 2
      Status Description: Negotiation done
      Local spi: 819B30AF922A70BC       Remote spi: 0255C23F4EDA3502
      Local id: hostname=HQ.vnpro.com,cn=HQ.vnpro.com
      Remote id: 192.168.1.2
      Local req msg id:  2              Remote req msg id:  0
      Local next msg id: 2              Remote next msg id: 0
      Local req queued:  2              Remote req queued:  0
      Local window:      5              Remote window:      5
      DPD configured for 60 seconds, retry 2
      Fragmentation not  configured.
      Extended Authentication not configured.
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Initiator of SA : Yes


 IPv6 Crypto IKEv2  SA
```

Trên router BR:

```
BR#show crypto ikev2 sa de
 IPv4 Crypto IKEv2  SA


Tunnel-id Local                 Remote                fvrf/ivrf
Status
1         192.168.1.2/500       192.168.1.1/500       none/none
READY
      Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth
sign: PSK, Auth verify: RSA
      Life/Active Time: 86400/202 sec
```

```
      CE id: 1039, Session-id: 2
      Status Description: Negotiation done
      Local spi: 0255C23F4EDA3502       Remote spi: 819B30AF922A70BC
      Local id: 192.168.1.2
      Remote id: hostname=HQ.vnpro.com,cn=HQ.vnpro.com
      Local req msg id:  0              Remote req msg id:  2
      Local next msg id: 0              Remote next msg id: 2
      Local req queued:  0              Remote req queued:  2
      Local window:      5              Remote window:      5
      DPD configured for 60 seconds, retry 2
      Fragmentation not  configured.
      Extended Authentication not configured.
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Initiator of SA : No

IPv6 Crypto IKEv2  SA
```