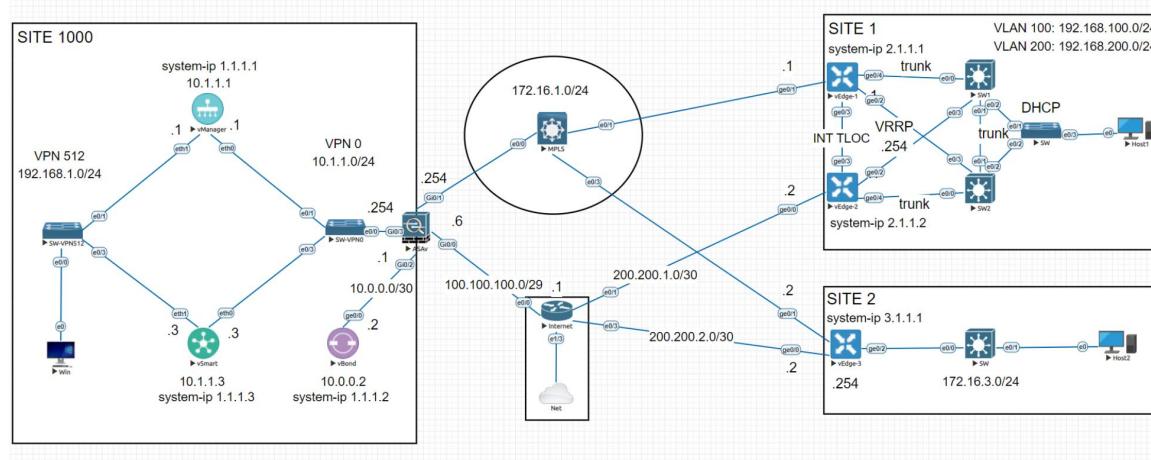


LAB: CONTROLLERS BEHIND NAT

I. Sơ đồ



Tên thiết bị	Username	Password	Version
vManage	admin	Admin	20.10.1
vBond	admin	Admin	20.10.1
vSmart	admin	Admin	20.10.1
vEdge	admin	Admin	20.10.1
PC		Test123	Windows 10

II. Yêu cầu

Kết nối và cấu hình địa chỉ IP thiết bị theo mô hình, để đảm bảo các địa chỉ IP WAN ở các site có thể thấy nhau.

Cấu hình bring-up SD-WAN controller: vManage, vBond, vSmart.

III. Thực hiện:

3.1. Cấu hình các thiết bị để đảm bảo để bảo các địa chỉ IP WAN ở các site có thể thấy nhau

Cấu hình vManage:

```
config ter
system
```

```
host-name vmanage
system-ip 11.1.1.1
site-id 1000
organization-name VnPro
vbond 100.100.100.3
vpn 0
interface eth0
no shutdown
ip address 10.1.1.1/24
tunnel-interface
allow-service all
color private1
ip route 0.0.0.0/0 10.1.1.254
vpn 512
interface eth1
no shutdown
ip add 192.168.1.1/24
commit and-quit
```

Cấu hình vSmart:

```
config ter
system
host-name vsmart
system-ip 11.1.1.3
site-id 1000
organization-name VnPro
vbond 100.100.100.3
vpn 0
interface eth0
no shutdown
ip address 10.1.1.3/24
tunnel-interface
allow-service all
```

```
color private1
ip route 0.0.0.0/0 10.1.1.254
vpn 512
int eth1
no shutdown
ip add 192.168.1.3/24
commit and-quit
```

Cấu hình vBond:

```
config ter
system
host-name vbond
system-ip 11.1.1.2
site-id 1000
organization-name VnPro
vbond 100.100.100.3 local vbond-only
vpn 0
interface ge0/0
no shutdown
ip address 10.0.0.2/30
tunnel-interface
encapsulation ipsec
allow-service all
ip route 0.0.0.0/0 10.0.0.1
vpn 512
int eth0
no shutdown
ip address 192.168.1.2/24
commit and-quit
```

Cấu hình vEdge 1:

```
conf ter
system
```

```
host-name vedge1
system-ip 1.1.1.1
site-id 1
organization-name VnPro
vbond 100.100.100.3
vpn 0
no int ge0/0
int ge0/1
no shutdown
ip add 172.16.1.1/24
tunnel-interface
encapsulation ipsec
color mpls
allow-service all
ip route 0.0.0.0/0 172.16.1.254
exit
vpn 512
int eth0
no shutdown
commit and-quit
```

Cấu hình vEdge 2:

```
conf ter
system
host-name vedge2
system-ip 1.1.1.2
site-id 1
organization-name VnPro
vbond 100.100.100.3
vpn 0
int ge0/0
no shutdown
ip add 200.200.1.2/30
tunnel-interface
encapsulation ipsec
```

```
color biz-internet
allow-service all
ip route 0.0.0.0/0 200.200.1.1
exit
vpn 512
int eth0
no shutdown
commit and-quit
```

Câu hình vEdge 3:

```
conf ter
system
host-name vedge3
system-ip 2.1.1.1
site-id 2
organization-name VnPro
vbond 100.100.100.3
vpn 0
int ge0/0
no shutdown
ip add 200.200.2.2/30
tunnel-interface
encapsulation ipsec
allow-service all
color biz-internet
ip route 0.0.0.0/0 200.200.2.1
vpn 512
int eth0
no shutdown
commit and-quit
```

Câu hình ASA v:

```
conf ter
hostname ASA v
int g0/0
```

```
ip add 100.100.100.6 255.255.255.248
nameif outside
security-level 0
no shutdown
exit
int g0/1
ip add 172.16.1.254 255.255.255.0
nameif MPLS
security-level 0
no shutdown
exit
int g0/2
ip add 10.0.0.1 255.255.255.252
nameif DMZ
security-level 50
no shutdown
exit
int g0/3
ip add 10.1.1.254 255.255.255.0
nameif inside
security-level 100
no shutdown
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
object network vmanage
host 10.1.1.1
nat (inside,outside) static 100.100.100.2
exit
object network vbond
host 10.0.0.2
nat (DMZ,outside) static 100.100.100.3
exit
object network vsmart
host 10.1.1.3
nat (inside,outside) static 100.100.100.4
```

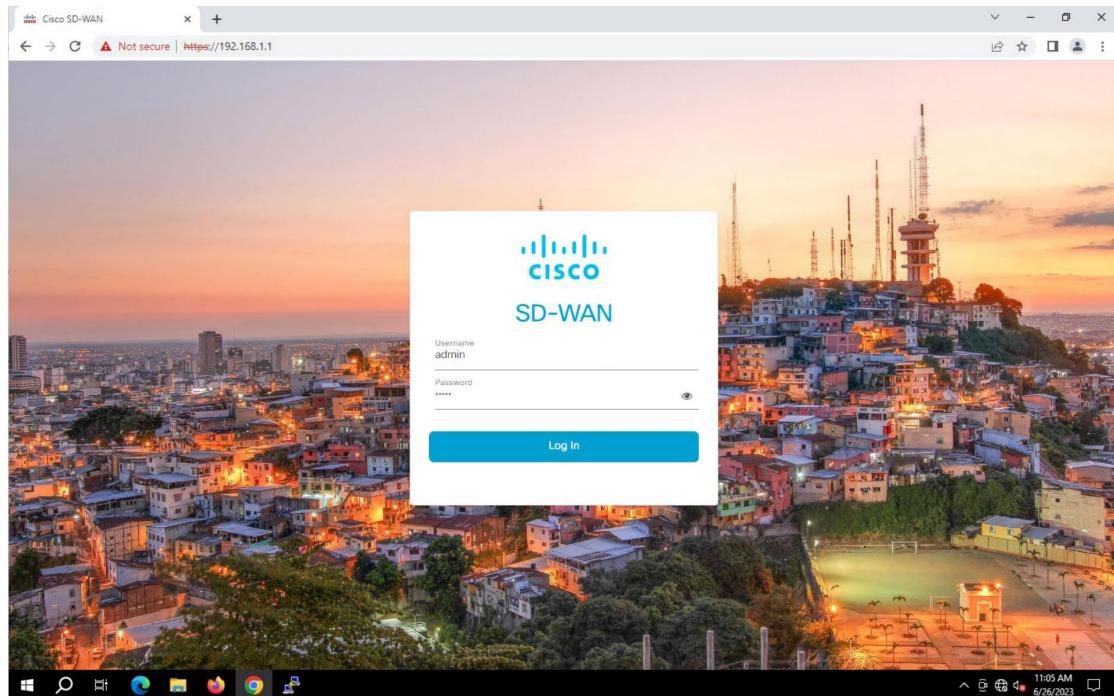
```
exit
access-list controller extended permit ip any any
access-group controller in interface outside
access-group controller out interface outside
access-group controller in interface MPLS
access-group controller out interface MPLS
access-group controller in interface DMZ
access-group controller out interface DMZ
access-group controller in interface inside
access-group controller out interface inside
icmp permit any outside
icmp permit any MPLS
icmp permit any DMZ
icmp permit any inside
route outside 0.0.0.0 0.0.0.0 100.100.100.1
object network out_vmanage
host 100.100.100.2
exit
object network out_vbond
host 100.100.100.3
exit
object network out_vsmart
host 100.100.100.4
exit
object network MPLS
subnet 172.16.1.0 255.255.255.0
exit
nat (inside,DMZ) source static vsmart out_vsmart destination static out_vbond vbond
nat (DMZ,inside) source static vbond out_vbond destination static out_vsmart vsmart
nat (inside,DMZ) source static vmanage out_vmanage destination static out_vbond vbond
nat (DMZ,inside) source static vbond out_vbond destination static out_vmanage vmanage
nat (DMZ,DMZ) source static vbond out_vbond destination static out_vbond vbond
nat (DMZ,MPLS) source static vbond out_vbond destination static MPLS MPLS
nat (inside,MPLS) source static vsmart vsmart destination static MPLS MPLS
nat (inside,MPLS) source static vmanage vmanage destination static MPLS MPLS
```

```
policy-map global_policy
class inspection_default
inspect icmp
end
copy run start
```

3.2. Cấu hình bring-up SD-WAN controller: vManage, vBond, vSmart.

Sau khi đã cấu hình cơ bản cho cả 3 thành phần controller trong SD-WAN fabric ta tiến hành promote vManage lên thành CA(Certificate Authority)

- Dùng trình duyệt trên pc (trong sơ đồ lab) login vào vManage: <https://192.168.1.1> với username: admin và password: Admin



IV. Kiểm tra:

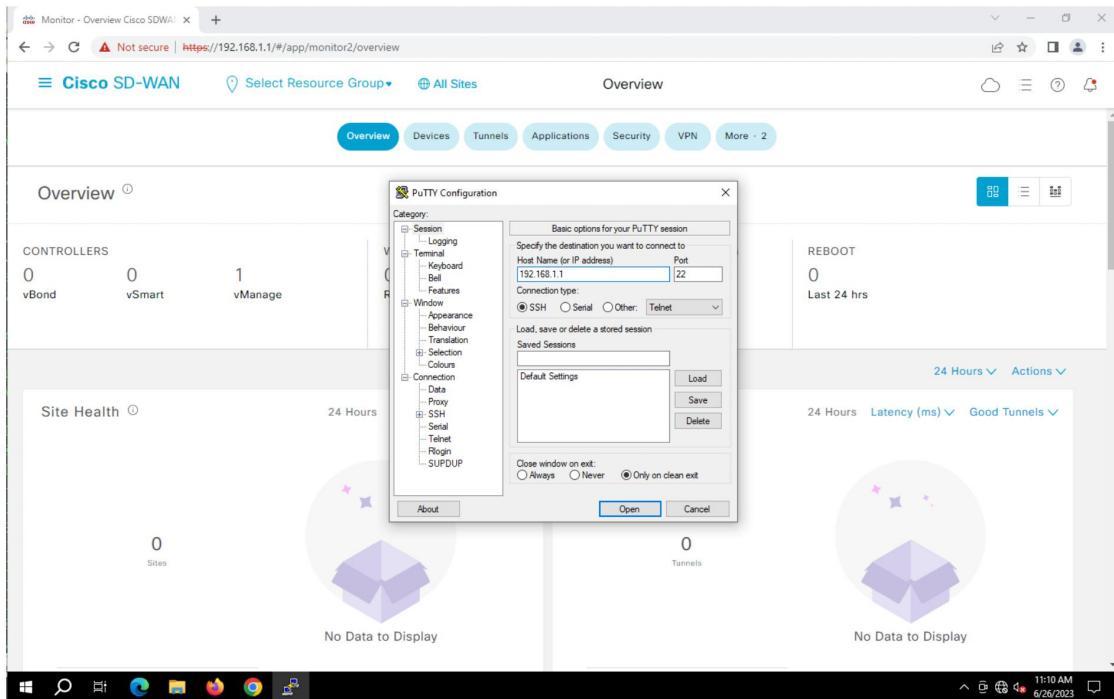
Kết nối thành công vào vManage.

Ở bài lab này chúng ta sẽ dùng vManage làm server chứng thực. Dùng openssl để tạo và ký certificates từ vshell

- Sau khi kết nối thành công vManage ta sẽ tiến hành promote vManage lên thành CA: dùng terminal console trên vManage:
 - + Gõ lệnh vshell để vào Shell mode cấu hình openssl: “**vshell**”
 - + Tiếp theo generate key RSA 2048 ta gõ lệnh : “**openssl genrsa -out ROOTCA.key 2048**”
 - + Sau khi đã có key ta sẽ generate 1 ROOTCA ta gõ lệnh: “**openssl req -x509 -new -nodes -key ROOTCA.key -sha256 -days 2000 -out ROOTCA.pem**”
 - + Tiếp theo ta gõ theo tùy chọn, còn không gõ gì thì cứ enter cho qua

```
-----
Country Name (2 letter code) [AU]:VN
State or Province Name (full name) [Some-State]:HCM
Locality Name (eg, city) []:HCM
Organization Name (eg, company) [Internet Widgits Pty Ltd]:VNPRO
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
vmanage:~$
```

- Tiếp theo vào PC (trong sơ đồ lab) SSH vào vmanage với ip: *192.168.1.1*



+ Ta vào shell mode với lệnh **vshell** gõ lệnh: **cat ROOTCA.pem** để đọc chứng chỉ số, sau đó ta copy chứng chỉ số đó từ begin đến end

```

vmanage# vshell
vmanage:~$ cat ROOTCA.pem
-----BEGIN CERTIFICATE-----
MIIDbTCCA1WgAwIBAgIUVdzgMAJuD7ihLQtfDnzHjOHF56cwDQYJKoZIhvcNAQEL
BQAwRjELMAkGA1UEBhMCVk4xDAAKbgNVBAgMA0hDTTEMMAoGA1UEBwwDSENNMQ4w
DAYDVQQKDAVWT1BStzELMAkGA1UECwwCSVQwHhcNMjMwNjI2MTEwODUwWhcNMjgx
MjE2MTEwODUwWjBGMQswCQYDVQQGEwJWtjemMAoGA1UECAwDSENNMQwwCgYDVQQH
DANIQ00xDjAMBgNVBAoMBVZOUFJPMQswCQYDVQQLDAJJVDCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBAlOMekQofTWgRNmZGfMwTrXk0Uv6mAfJHXWiI6jc
Xzkm9x3X9930bk9KDhn3FHjMwQj63o4kHdNcBzHNgdjid6S7yeIa8VD+EflNpyON
jZ6AFzxydvnZkyMK6ScyzIfwlqhDEJYQmP4Vk5AckcXC1hU6fAk1fWxeNTjaheE
bx3b2XrtkH6jVgfqRnFPXd9wIo1TQuDWDVd8Q1Aql8hnOKo2D02ABoAspXa5Nf
BT47jDyHQYBz9b8B8xMQUxrceUpe4asJe1+BHiTe9KIIGiAb60cG9PYfH1TJFx8e
/S8yOGHzQjrrtT4eQ4EtrfFtRkPR/lp49P+Rb3WMOKyjLBECAwEAAAaNTMFEwHQYD
VR0OBByEFHxVS/dKjRXVujsF+HkuHAodqiPqmB8GA1UdIwQYMBaAFHxVS/dKjRXV
ujsF+HkuHAodqiPqmB8GA1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEB
AE5sYblrNNsdtC1+rHA04pzMaW9i05yl1n1Io0/WLKPj2jX+FW9sQjUhIha/anRwP
qQU6Igleb/LZWRBRMIGPaC6/F+NzXgXI//AKjVaQ17P16N5tRYUWE9CFk3+tK3/
Wgia/HlsRv0WXAHQ8jc0mDN1bm6/LfJXOJMUsWzHbCG8cJ/P8GFcaNFY638Wzp3
kVg+TQzo/m5rmxJrLKGK8bCpaZYpXRvJQX5hP/KyudG+BeT4xWYSYyNrv+3lwPe2
Rnf1j10kSdhGFGsJxw7GoIYUfgHgnwvlvLF4ntIuxoTngRKP/wgvBFJCcHjcSGuA
z9Jq4b9I1CNLHjGbm+JPnTQ=
-----END CERTIFICATE-----
vmanage:~$ 
```

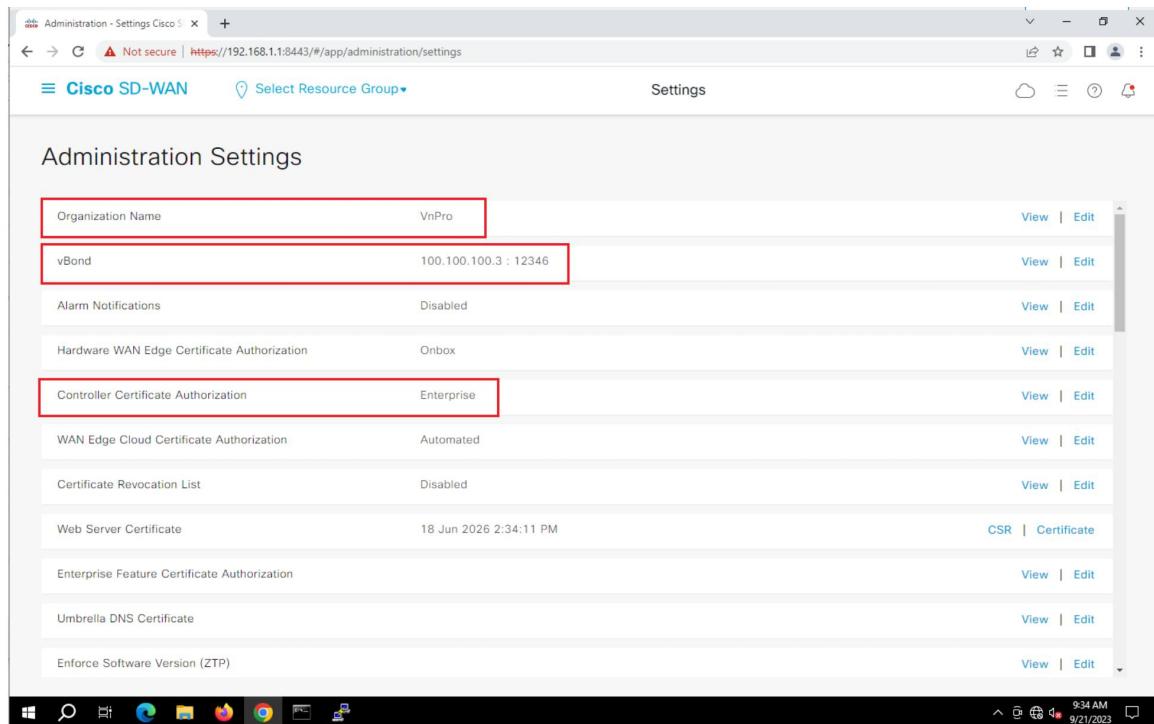
- Sau đó ta vào **Administration → Setting → Controller Certificate Authorization** → chọn **Enterprise Root Certificate** rồi paste vào Certificate chọn **Import & Save**

The screenshot shows the Cisco SD-WAN Administration Settings window. In the left sidebar, the 'Administration' section is highlighted with a red box. The main pane displays the 'Overview' dashboard with sections for Certificate Status (0 Certificates, 1 Warning), Licensing (0 Assigned, 0 Invalid), and Reboot (0 Reboots, Last 24 hrs). Below this is a 'Tunnel Health' summary showing 0 tunnels and a message 'No Data to Display'. The bottom half of the window is a large text area for 'Controller Certificate Authorization' under the 'Cisco' tab. It shows certificate signing options: Cisco (Recommended), Digicert, Manual, and Enterprise Root Certificate (selected). A large text box contains a complex certificate signing request (CSR) string. At the bottom are 'Import & Save' and 'Cancel' buttons.

Ta chỉnh lại :

+ Organization name: “VnPro”

+ vBond: “ 100.100.100.3”



The screenshot shows the Cisco SD-WAN Administration Settings page. The 'vBond' row is highlighted with a red box, displaying the IP address 100.100.100.3 : 12346. Other settings listed include Organization Name (VnPro), Alarm Notifications (Disabled), Hardware WAN Edge Certificate Authorization (Onbox), Controller Certificate Authorization (Enterprise), WAN Edge Cloud Certificate Authorization (Automated), Certificate Revocation List (Disabled), Web Server Certificate (CSR | Certificate, issued on 18 Jun 2026 2:34:11 PM), Enterprise Feature Certificate Authorization, Umbrella DNS Certificate, and Enforce Software Version (ZTP). The browser status bar at the bottom indicates it's not secure.

==> vManage đã được promote lên thành CA

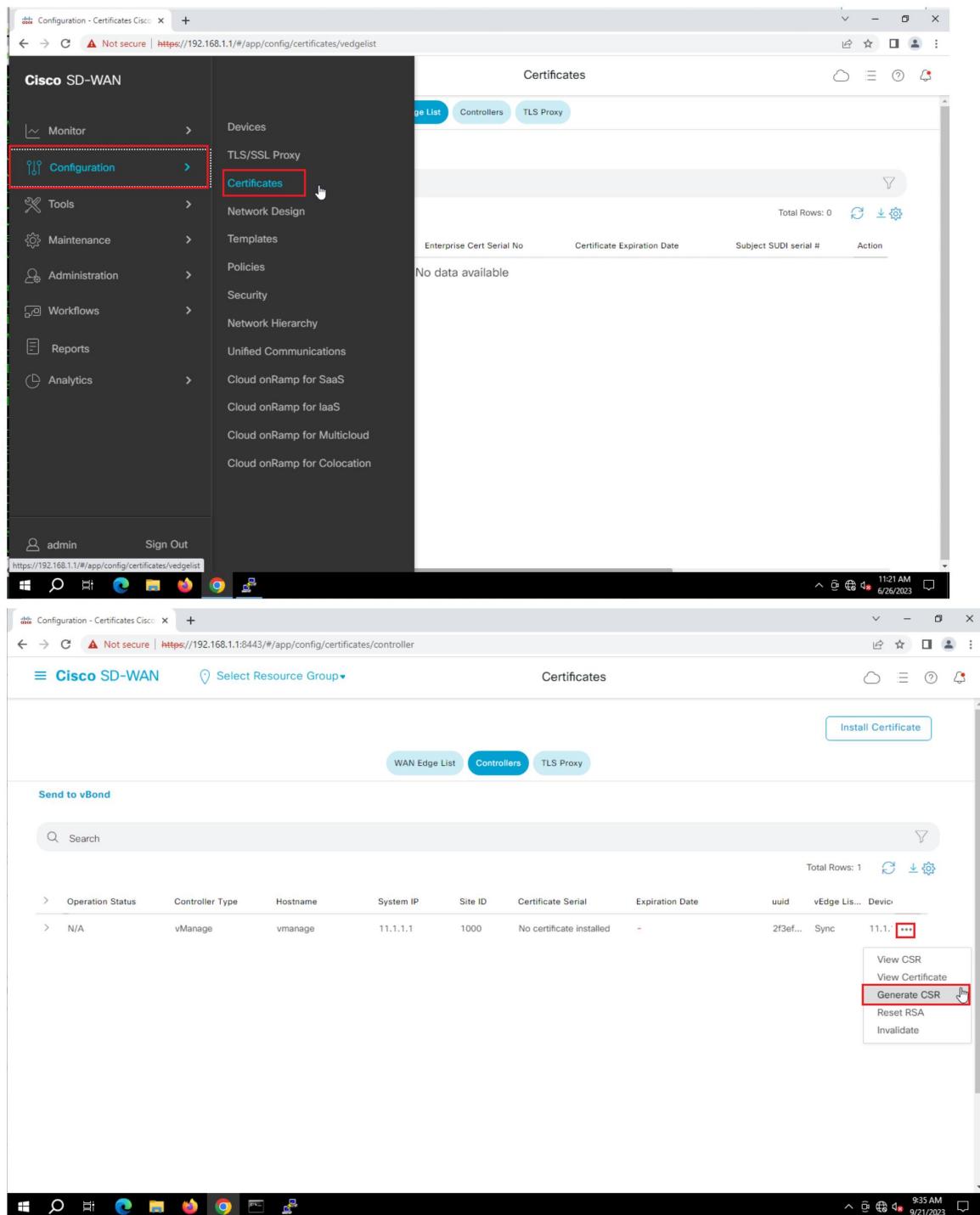
- Dùng vManage để ký chứng thực cho vManage, vSmart, vBond.

Vmanage

+ Truy cập vào giao diện web để tạo một yêu cầu ký chứng thực

+ Configuration → Certificates → Controllers → vManage → Generate CSR để tạo file

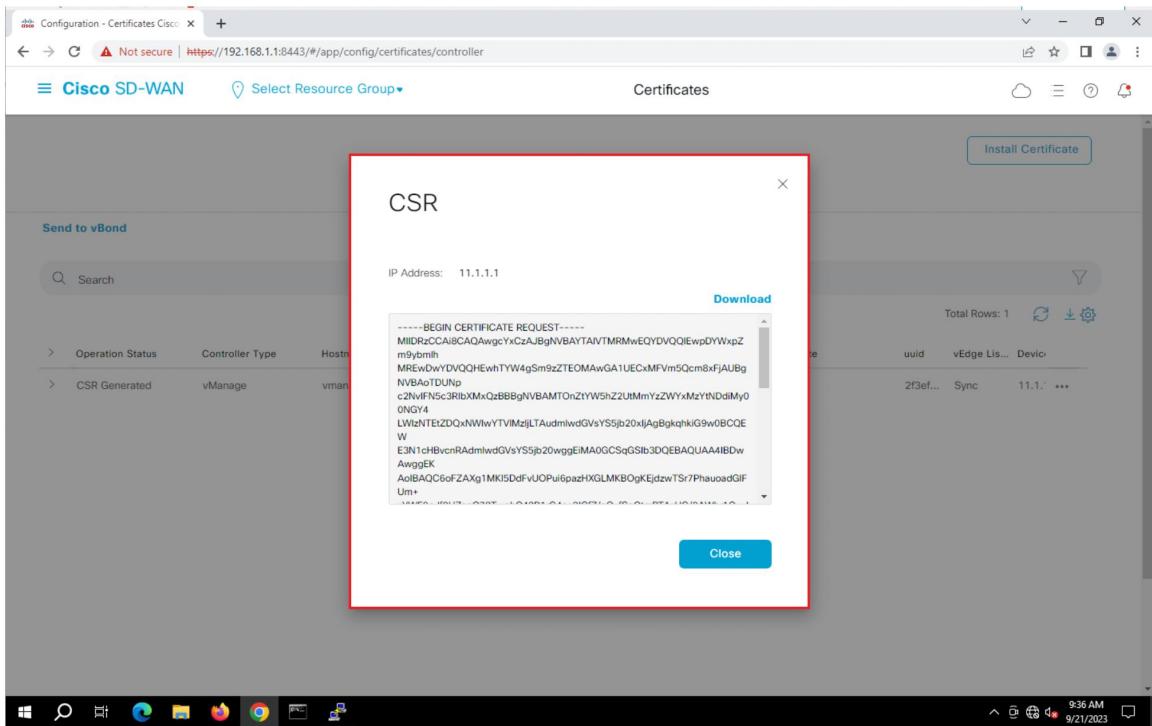
`vmanage_csr`



The screenshot shows two windows of the Cisco SD-WAN Configuration interface. Both windows have the URL <https://192.168.1.1/#/app/config/certificates/vedgeList>.

Left Window: The title bar says "Cisco SD-WAN". The left sidebar has a red box around the "Configuration" item under "Monitor". The main content area is titled "Certificates" with tabs for "vEdge List", "Controllers", and "TLS Proxy". It displays a table with columns: Enterprise Cert Serial No, Certificate Expiration Date, Subject SUDI serial #, and Action. The message "No data available" is shown.

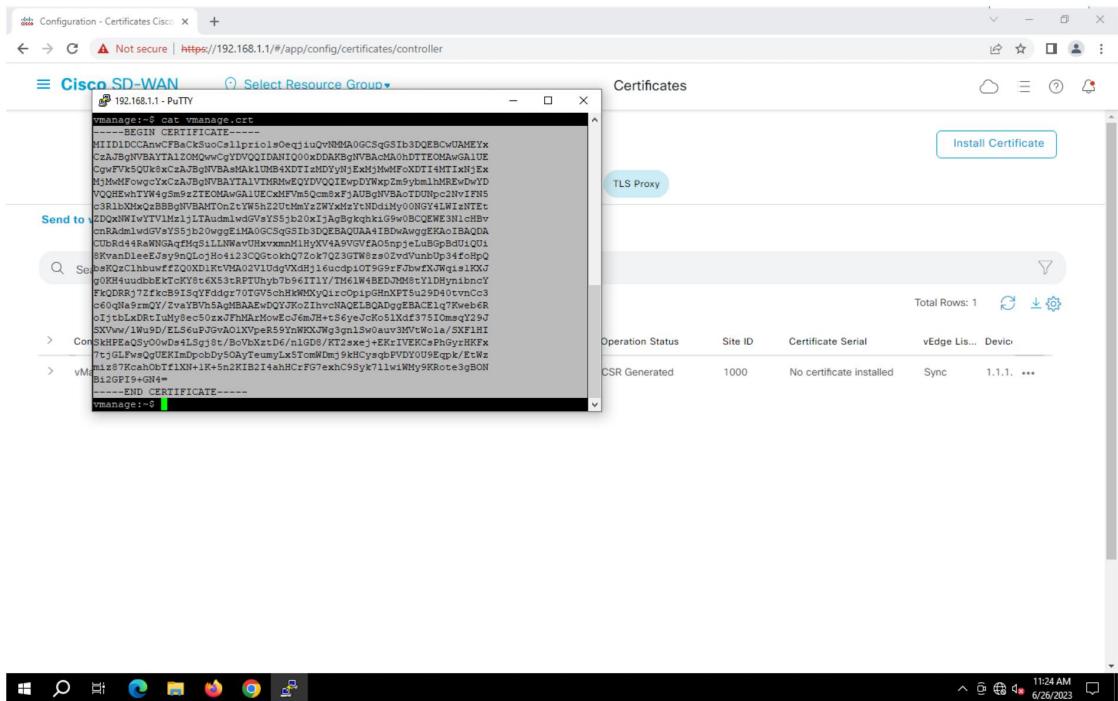
Right Window: The title bar says "Cisco SD-WAN". The left sidebar has a red box around the "Certificates" item under "Devices". The main content area is titled "Certificates" with tabs for "WAN Edge List", "Controllers", and "TLS Proxy". It shows a table with one row of data. The "Action" column for this row contains a context menu with options: "View CSR", "View Certificate", "Generate CSR" (which is highlighted with a red box), "Reset RSA", and "Invalidate".



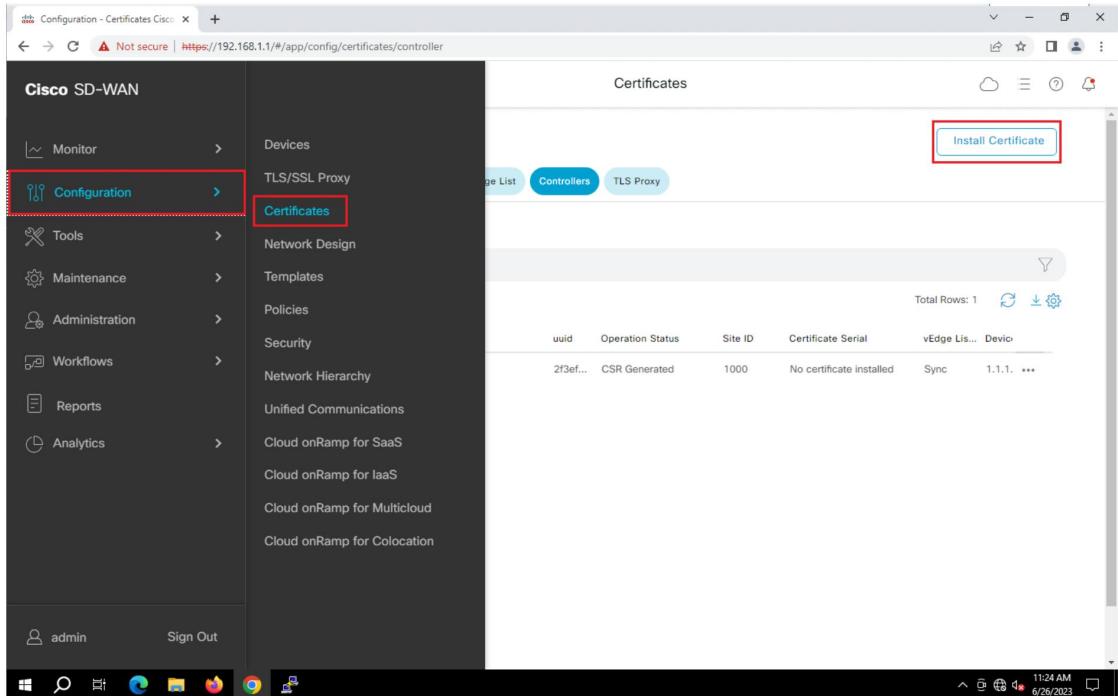
- Sau khi tạo xong file csr, ta dùng khóa ROOTCA.key để ký file vmanage_csr ta vừa tạo ra với câu lệnh như sau: **openssl x509 -req -in vmanage_csr -CA ROOTCA.pem -CAkey ROOTCA.key -CAcreateserial -out vmanage.crt -days 2000 -sha256** ==> tạo file vmanage.crt
Kiểm tra kết quả là: đã ký thành công

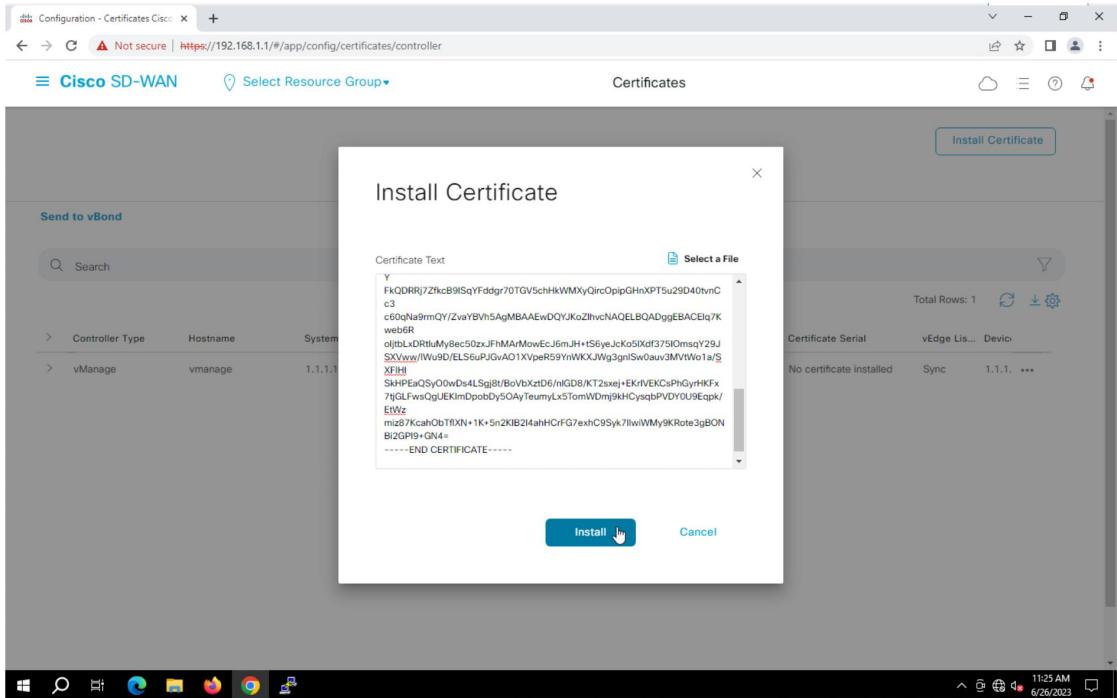
```
vmanage:~$ openssl x509 -req -in vmanage_csr -CA ROOTCA.pem -CAkey
Acreateserial -out vmanage.crt -days 2000 -sha256
Signature ok
subject=C = US, ST = California, L = San Jose, OU = VnPro, O = Cisc
o Systems, CN = vmanage-2f3ef136-47b3-44f8-b351-d415b0a5e39c-0.vipt
ela.com, emailAddress = support@viptela.com
Getting CA Private Key
vmanage:~$
```

- Ta vào trong PC (trong sơ đồ lab) vào putty gõ địa chỉ **192.168.1.1** rồi SSH Dùng lệnh **cat vmanage.crt** để đọc file vmanage.crt

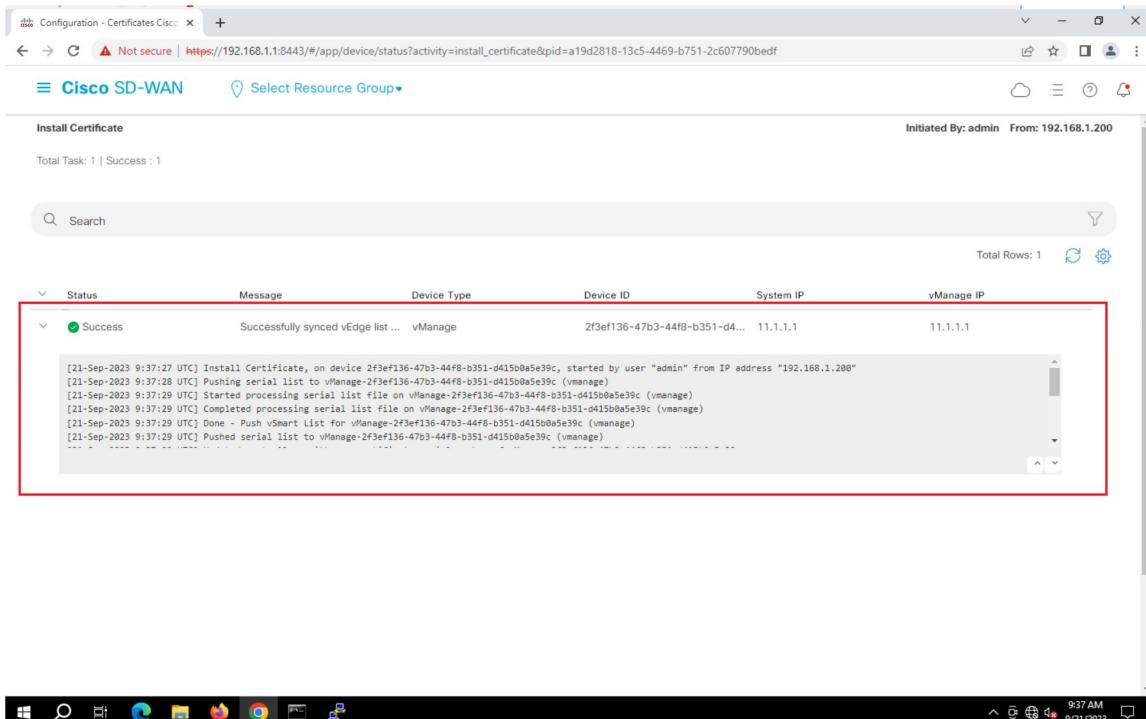


- Và cài đặt chứng thực trên giao diện web: Configuration → Certificates → Controllers → Install Certificate:





Kiểm Tra: Đã xác thực thành công vManage



vBond

Vào Configuration → Device → Controller → Add controller

The screenshot shows the Cisco SD-WAN Configuration interface. On the left, there is a navigation sidebar with the following items:

- Monitor
- Configuration** (highlighted with a red box)
- Tools
- Maintenance
- Administration
- Workflows
- Reports
- Analytics

Below the sidebar, there are two user accounts: admin and Sign Out.

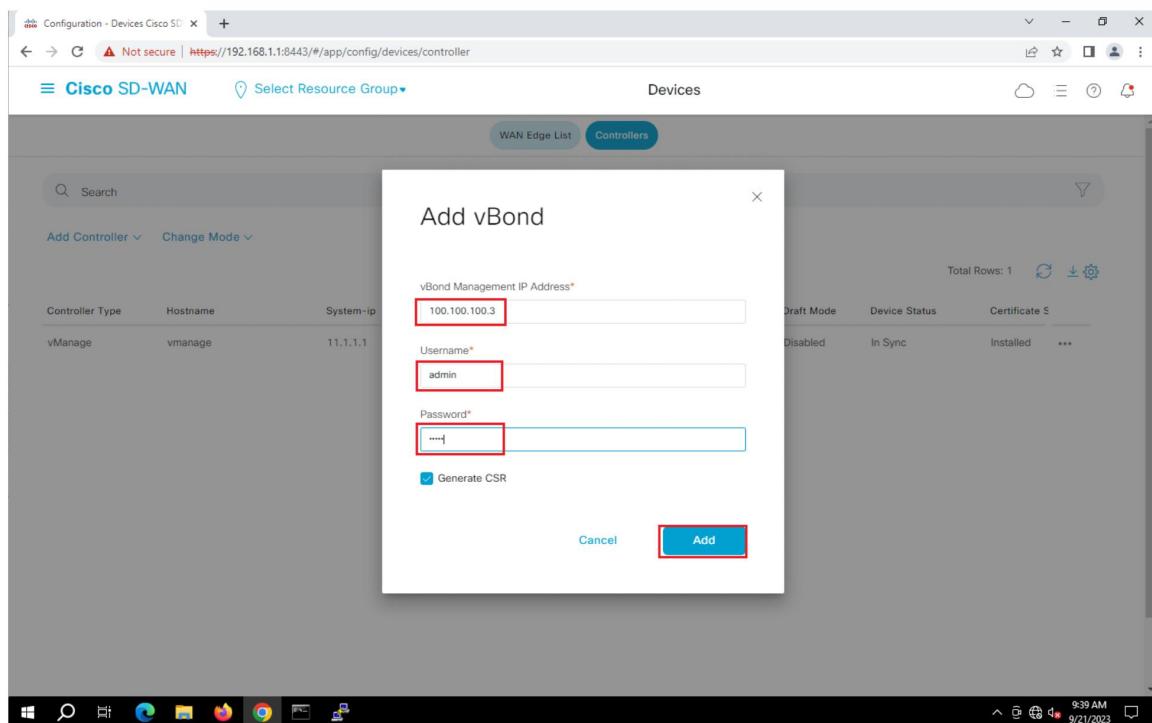
The main content area has tabs: **WAN Edge List** (selected) and **Controllers**. The WAN Edge List tab shows a table with the following columns: ID, Region ID, Mode, Device Status, Assigned Config Group, and Assigned Template. The table displays the message "No data available".

Screenshot 2:

This screenshot shows the same interface but with the **Controllers** tab selected. The navigation sidebar remains the same. The main content area shows a table with the following columns: Controller Type, Hostname, System-ip, Site ID, Region ID, Mode, Assigned Template, Draft Mode, Device Status, and Certificate S. There is one entry in the table:

Controller Type	Hostname	System-ip	Site ID	Region ID	Mode	Assigned Template	Draft Mode	Device Status	Certificate S
vManage	vmanage	11.1.1.1	1000	-	CLI	-	Disabled	In Sync	Installed

- Cấu hình vBond Management ip address: 100.100.100.3, username: admin, password: Admin



Kiểm tra: xuất hiện vBond

Controller Type	Hostname	System-ip	Site ID	Region ID	Mode	Assigned Template	Draft Mode	Device Status	Certificate S
vBond	-	-	-	-	CLI	-	Disabled	Not Installed	***
vManage	vmanage	1.1.1.1	1000	-	CLI	-	Disabled	In Sync	Installed

- Trên console vBond ta vào mode vshell dùng lệnh **vshell**

Tiếp theo dùng lệnh **scp vbond_csr admin@100.100.100.2:/home/admin/vbond_csr**

Lệnh này dùng scp để truyền file vbond_csr từ vbond qua vmanage

```
vbond# vshell
vbond:~$ scp vbond_csr admin@100.100.100.2:/home/admin/vbond_csr
The authenticity of host '100.100.100.2 (100.100.100.2)' can't be established.
ECDSA key fingerprint is SHA256:bzT/seGP8nUR2ilFB2V4vCzTQ9e//ZJWWBlZgIs9Ge
s.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '100.100.100.2' (ECDSA) to the list of known hosts.
viptela 20.10.1

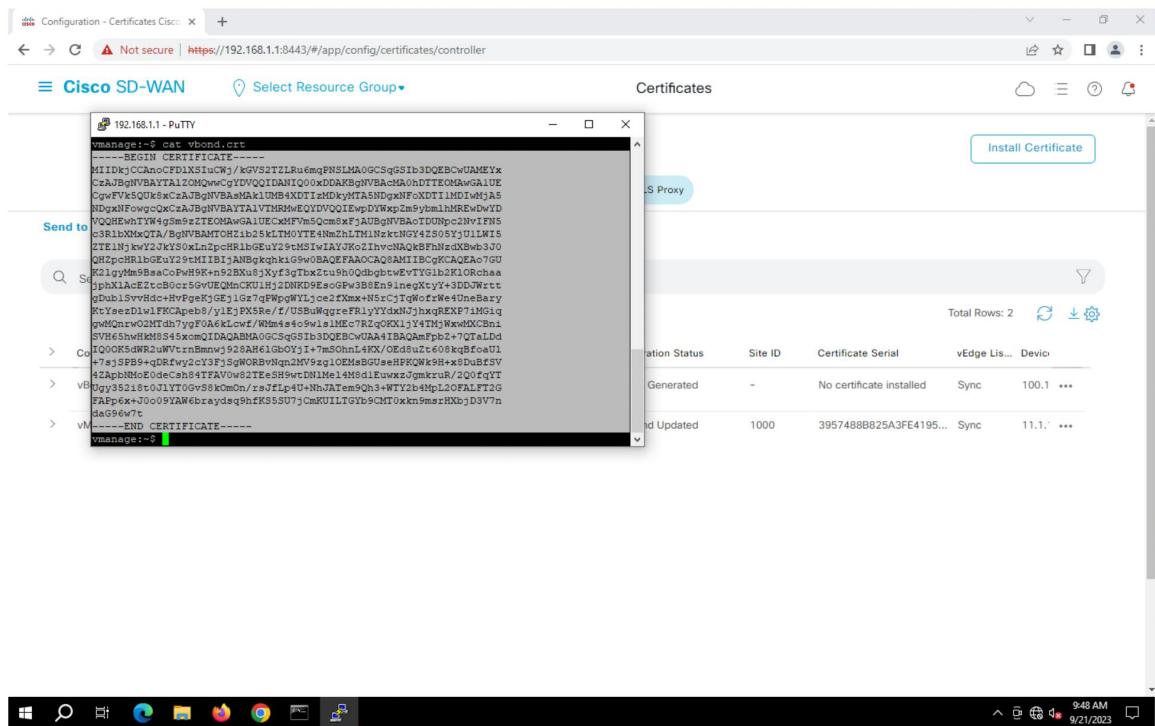
Password:                                     0%   0      0.0KB/s  ---:
vbond_csr                                     100% 1212    58.0KB/s  00:0
0
vbond:~$
```

- Tiếp tục ở console vmanage dùng câu lệnh: “**openssl x509 -req -in vbond_csr -CA ROOTCA.pem -CAkey ROOTCA.key -CAcreateserial -out vbond.crt -days 500 -sha256**” để chuyển file vbond_csr sang vbond.crt

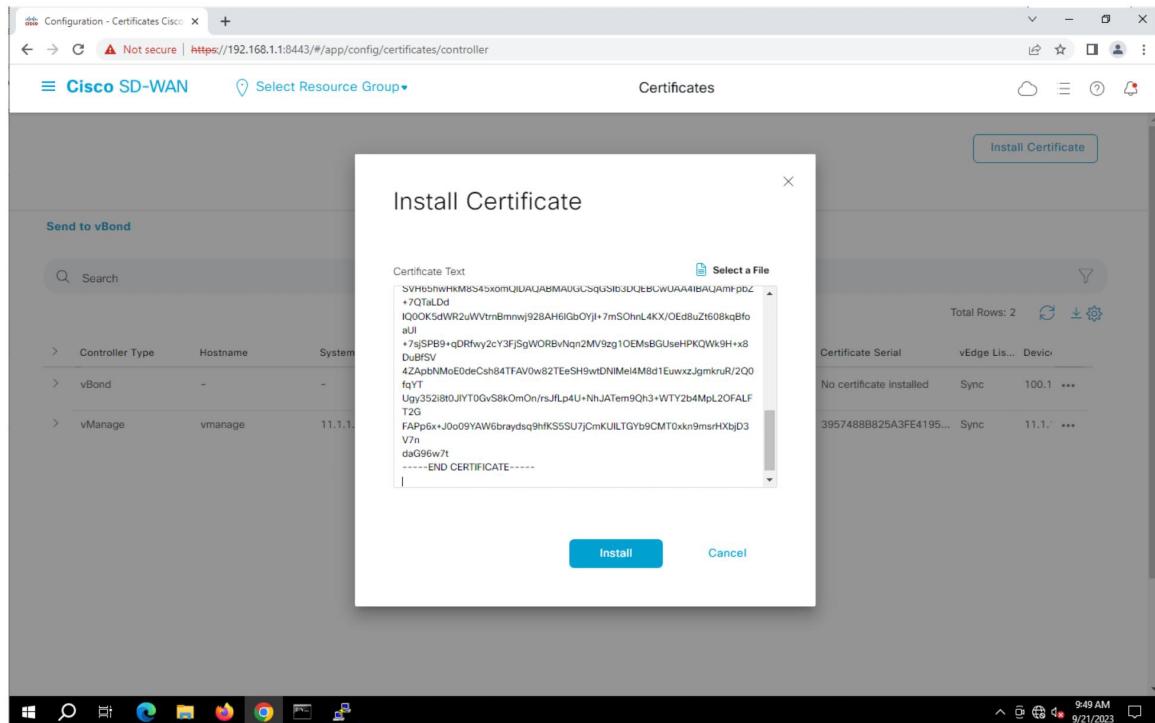
```
vmanage:~$ openssl x509 -req -in vbond_csr -CA ROOTCA.pem -CAkey RO
reateserial -out vbond_crt -days 500 -sha256
Signature ok
subject=C = US, ST = California, L = San Jose, OU = VnPro, O = Cisc
o Systems, CN = vbond-34a186fa-3579-4f8e-9b55-b9e15690cbda-1.viptel
a.com, emailAddress = support@viptela.com
Getting CA Private Key
vmanage:~$
```

```
vmanage:~$ ls -l
total 32
-rw----- 1 admin admin 1700 Jun 26 11:08 ROOTCA.key
-rw----- 1 admin admin 1249 Jun 26 11:08 ROOTCA.pem
-rw----- 1 admin admin    41 Jun 26 11:40 ROOTCA.srl
-rw-r--r-- 1 admin admin  566 Jun 26 10:03 archive_id_rsa.pub
-rw----- 1 admin admin 1298 Jun 26 11:40 vbond_crt
-rw----- 1 admin admin 1212 Jun 26 11:40 vbond_csr
-rw----- 1 admin admin 1302 Jun 26 11:23 vmanage.crt
-rw-r--r-- 1 root  root 1212 Jun 26 11:22 vmanage_csr
vmanage:~$
```

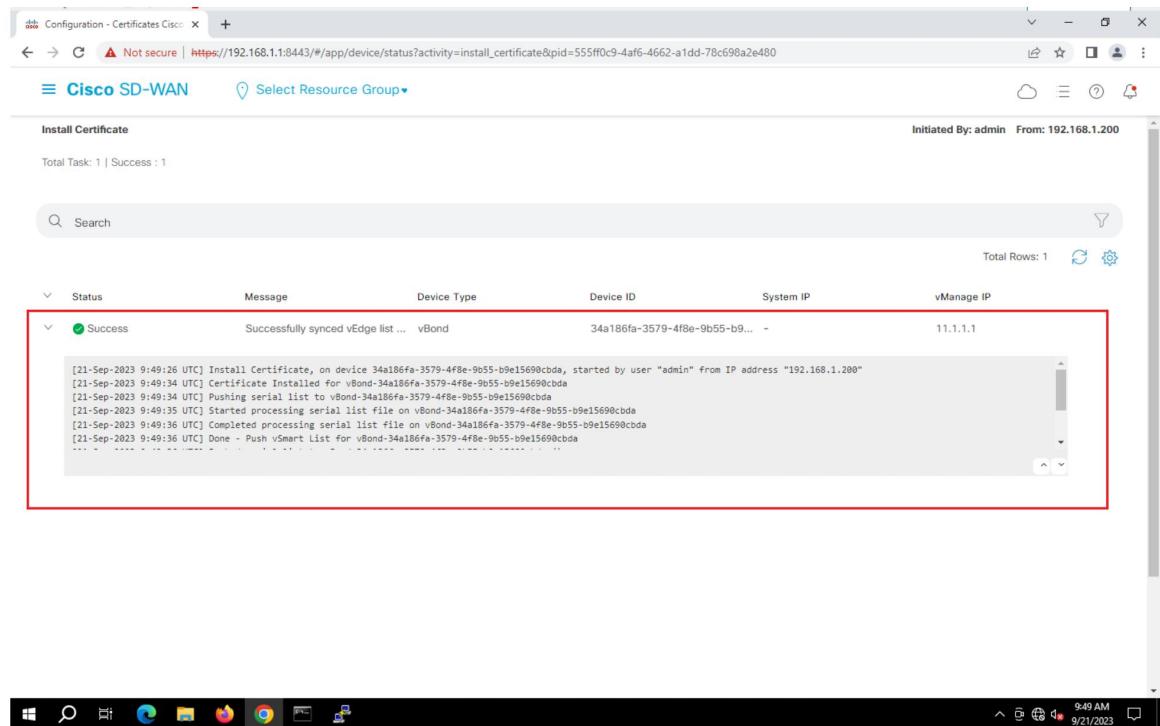
- Vào PC (trong sơ đồ lab) ssh vào vmanage, dùng **cat vbond.crt** để copy chứng chỉ số



- Sau đó vào giao diện trên web vmanage chọn Install Certificate



Kiểm tra kết quả: thành công

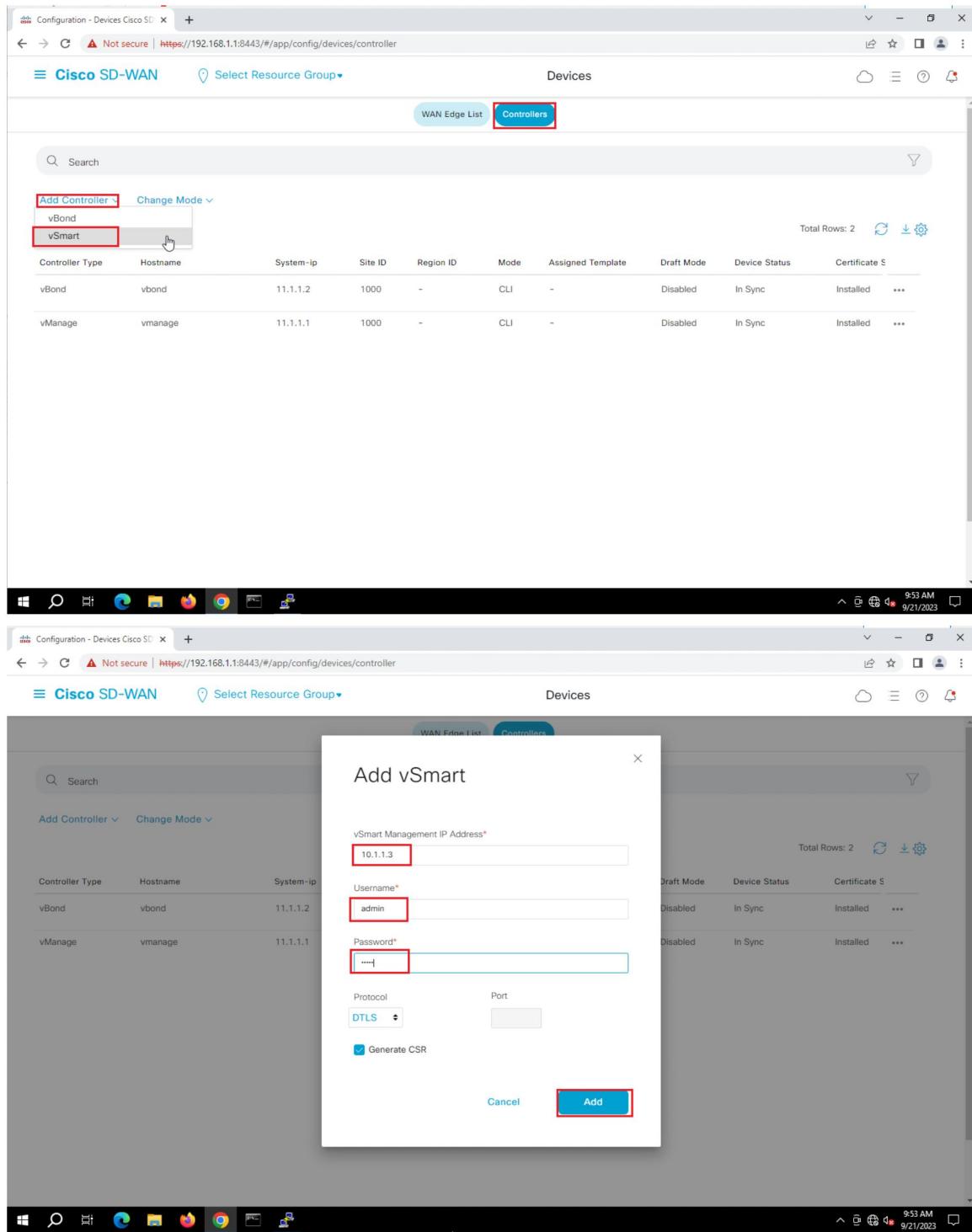


The screenshot shows a browser window titled "Configuration - Certificates Cisco" with the URL https://192.168.1.1:8443/#/app/device/status?activity=install_certificate&pid=555ff0c9-4af6-4662-a1dd-78c698a2e480. The page header includes "Cisco SD-WAN" and "Select Resource Group". The main content area is titled "Install Certificate" and displays a table with one row. The table columns are: Status, Message, Device Type, Device ID, System IP, and vManage IP. The single row shows a "Success" status with the message "Successfully synced vEdge list ... vBond". The "Message" column contains a detailed log of the process:

```
[21-Sep-2023 9:49:36 UTC] Install Certificate, on device 34a186fa-3579-4f8e-9b55-b9...  
[21-Sep-2023 9:49:34 UTC] Certificate Installed for vBond-34a186fa-3579-4f8e-9b55-b9e15690cbda  
[21-Sep-2023 9:49:34 UTC] Pushing serial list to vBond-34a186fa-3579-4f8e-9b55-b9e15690cbda  
[21-Sep-2023 9:49:35 UTC] Started processing serial list file on vBond-34a186fa-3579-4f8e-9b55-b9e15690cbda  
[21-Sep-2023 9:49:36 UTC] Completed processing serial list file on vBond-34a186fa-3579-4f8e-9b55-b9e15690cbda  
[21-Sep-2023 9:49:36 UTC] Done - Push vSmart List for vBond-34a186fa-3579-4f8e-9b55-b9e15690cbda
```

vSmart: tương tự vBond

- Cấu hình vSmart Management ip address: 10.1.1.3, username: admin, password: Admin



The screenshot shows two windows from the Cisco SD-WAN configuration interface.

Top Window (Controller List):

- Header: Cisco SD-WAN, Select Resource Group, Devices, WAN Edge List, Controllers.
- Search bar: Search.
- Buttons: Add Controller (dropdown), Change Mode (dropdown).
- Table Headers: Controller Type, Hostname, System-ip, Site ID, Region ID, Mode, Assigned Template, Draft Mode, Device Status, Certificate S.
- Table Data:

Controller Type	Hostname	System-ip	Site ID	Region ID	Mode	Assigned Template	Draft Mode	Device Status	Certificate S
vBond	vbond	11.1.1.2	1000	-	CLI	-	Disabled	In Sync	Installed
vManage	vmanage	11.1.1.1	1000	-	CLI	-	Disabled	In Sync	Installed
- Total Rows: 2, with icons for Refresh, Download, and Settings.

Bottom Window (Add vSmart Dialog):

- Header: Cisco SD-WAN, Select Resource Group, Devices, WAN Edge List, Controllers.
- Form Fields:

vSmart Management IP Address*	10.1.1.3
Username*	admin
Password*	1234
Protocol	DTLS
<input checked="" type="checkbox"/> Generate CSR	
- Buttons: Cancel, Add.
- Table Headers (faded background): Draft Mode, Device Status, Certificate S.
- Table Data (faded background):

Draft Mode	Device Status	Certificate S
Disabled	In Sync	Installed
Disabled	In Sync	Installed

- Trên console vSmart ta vào mode vshell dùng lệnh **vshell**

Tiếp theo dùng lệnh **scp vsmart_csr admin@10.1.1.1:/home/admin/vsmart_csr**

Lệnh này dùng scp để truyền file vsmart_csr từ vsmart qua vmanage

```
vsmart# vshell
vsmart:~$ scp vsmart_csr admin@10.1.1.1:/home/admin/vsmart_csr
The authenticity of host '10.1.1.1 (10.1.1.1)' can't be established.
ECDSA key fingerprint is SHA256:bzT/seGP8nUR2ilFB2V4vCzTQ9e//ZJWWBlZgIs9Ge
s.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.1.1.1' (ECDSA) to the list of known hosts.
viptela 20.10.1

Password:                                     0%   0      0.0KB/s  --- -
vsmart_csr                                     100% 1212    1.8MB/s  00:0
0
vsmart:~$
```

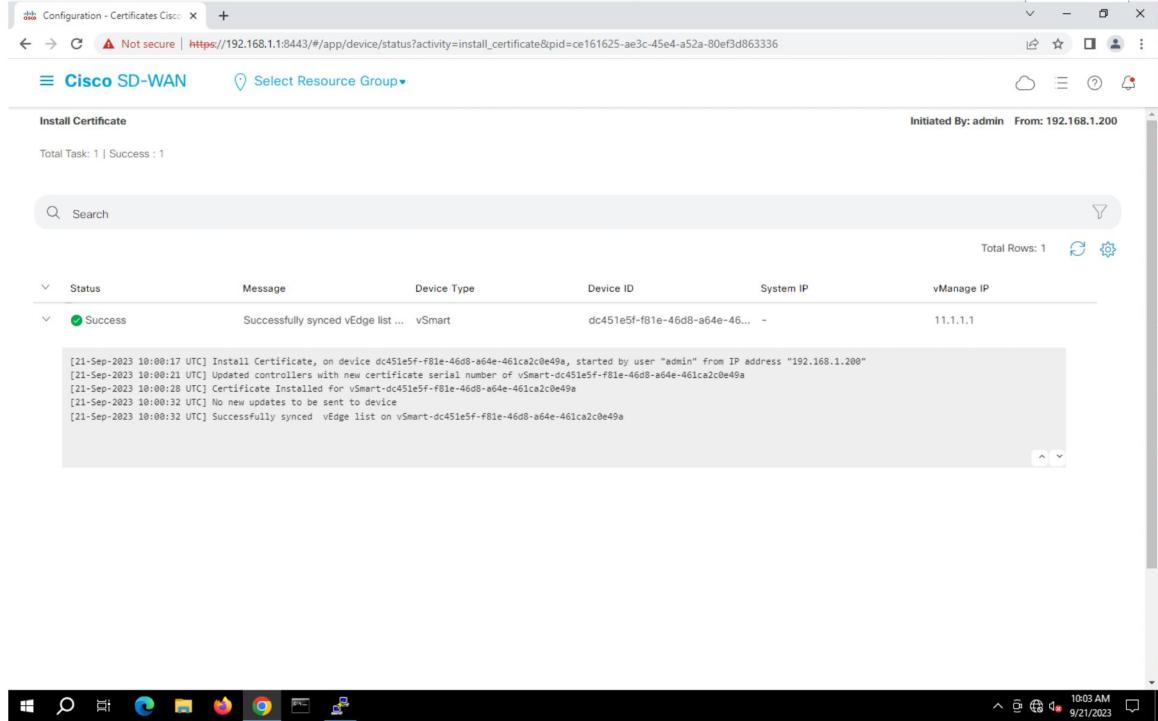
- Tiếp tục ở console vmanage dùng câu lệnh: “**openssl x509 -req -in vsmart_csr -CA ROOTCA.pem -CAkey ROOTCA.key -CAcreateserial -out vsmart.crt -days 500 -sha256**” để chuyển file *vsmart_csr* sang *vsmart.crt*

```
vmanage:~$ openssl x509 -req -in vsmart_csr -CA ROOTCA.pem -CAkey R
createserial -out vsmart.crt -days 500 -sha256
Signature ok
subject=C = US, ST = California, L = San Jose, OU = VnPro, O = Cisc
o Systems, CN = vsmart-dc451e5f-f81e-46d8-a64e-461ca2c0e49a-1.vipte
la.com, emailAddress = support@viptela.com
Getting CA Private Key
vmanage:~$
```

- Vào PC (trong sơ đồ lab) ssh vào vManage, dùng **cat vsmart.crt** để copy chứng chỉ số

- Sau đó vào giao diện trên web vManage chọn Install Certificate

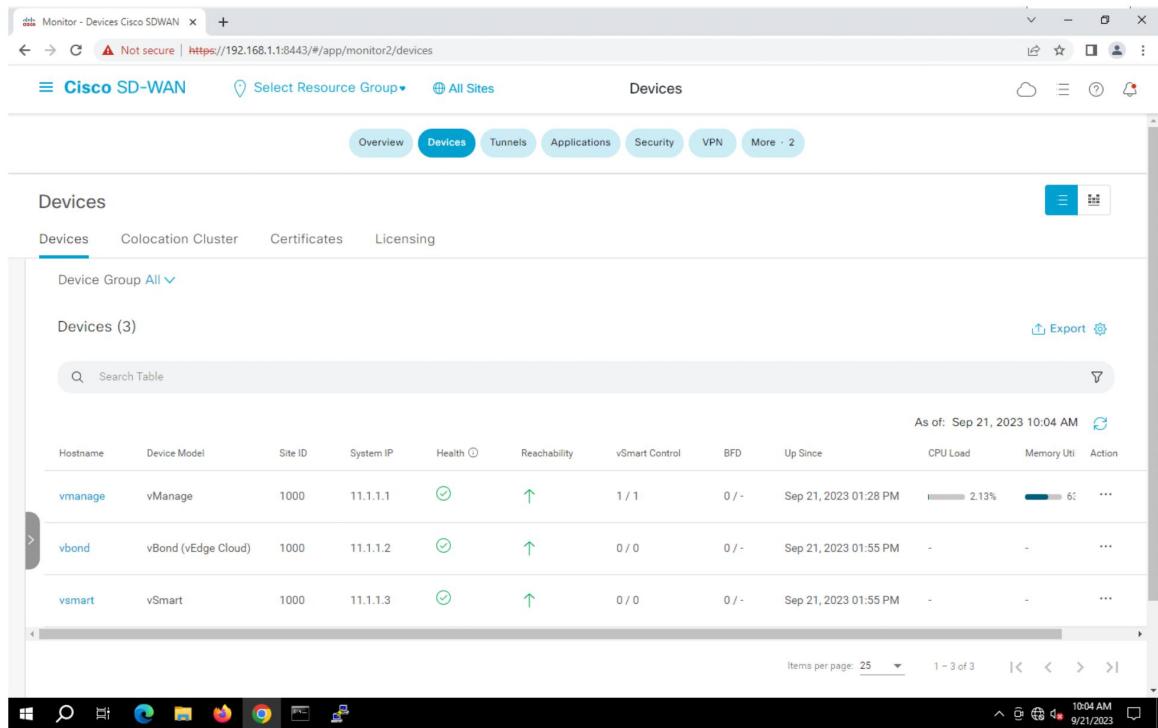
- Kết quả thành công:



The screenshot shows a browser window titled "Configuration - Certificates Cisco SD-WAN". The URL is https://192.168.1.1:8443/#/app/device/status?activity=install_certificate&pid=ce161625-ae3c-45e4-a52a-80ef3d863336. The page displays a table titled "Install Certificate" with one row of data. The table columns are: Status, Message, Device Type, Device ID, System IP, and vManage IP. The data row is: Success, Successfully synced vEdge list ..., vSmart, dc451e5f-f81e-46d8-a64e-46..., ~, 11.1.1.1. A log message box shows the following entries:

```
[21-Sep-2023 10:00:17 UTC] Install Certificate, on device dc451e5f-f81e-46d8-a64e-461ca2c0e49a, started by user "admin" from IP address "192.168.1.200"  
[21-Sep-2023 10:00:21 UTC] Updated controllers with new certificate serial number of vSmart-dc451e5f-f81e-46d8-a64e-461ca2c0e49a  
[21-Sep-2023 10:00:28 UTC] Certificate Installed for vSmart-dc451e5f-f81e-46d8-a64e-461ca2c0e49a  
[21-Sep-2023 10:00:32 UTC] No new updates to be sent to device  
[21-Sep-2023 10:00:32 UTC] Successfully synced vEdge list on vSmart-dc451e5f-f81e-46d8-a64e-461ca2c0e49a
```

- vManage, vSmart, vBond đã bring-up thành công



The screenshot shows the Cisco SD-WAN Monitor interface. At the top, there's a header bar with tabs for Overview, Devices (which is selected), Tunnels, Applications, Security, VPN, and More. Below the header, a sub-header says "Devices". Underneath that, there are tabs for Devices, Colocation Cluster, Certificates, and Licensing. A sub-sub-header "Device Group All" is shown. The main area displays a table titled "Devices (3)". The table columns include Hostname, Device Model, Site ID, System IP, Health, Reachability, vSmart Control, BFD, Up Since, CPU Load, Memory Util, and Action. The data rows are:

Hostname	Device Model	Site ID	System IP	Health	Reachability	vSmart Control	BFD	Up Since	CPU Load	Memory Util	Action
vmanage	vManage	1000	11.1.1.1	Green checkmark	Up arrow	1 / 1	0 / -	Sep 21, 2023 01:28 PM	2.13%	60%	...
vbond	vBond (vEdge Cloud)	1000	11.1.1.2	Green checkmark	Up arrow	0 / 0	0 / -	Sep 21, 2023 01:55 PM	-	-	...
vsmart	vSmart	1000	11.1.1.3	Green checkmark	Up arrow	0 / 0	0 / -	Sep 21, 2023 01:55 PM	-	-	...

At the bottom of the interface, there's a toolbar with icons for search, refresh, and other navigation functions.

3.3. Thiết lập thiết bị vEdge vào hệ thống Cisco SD-WAN

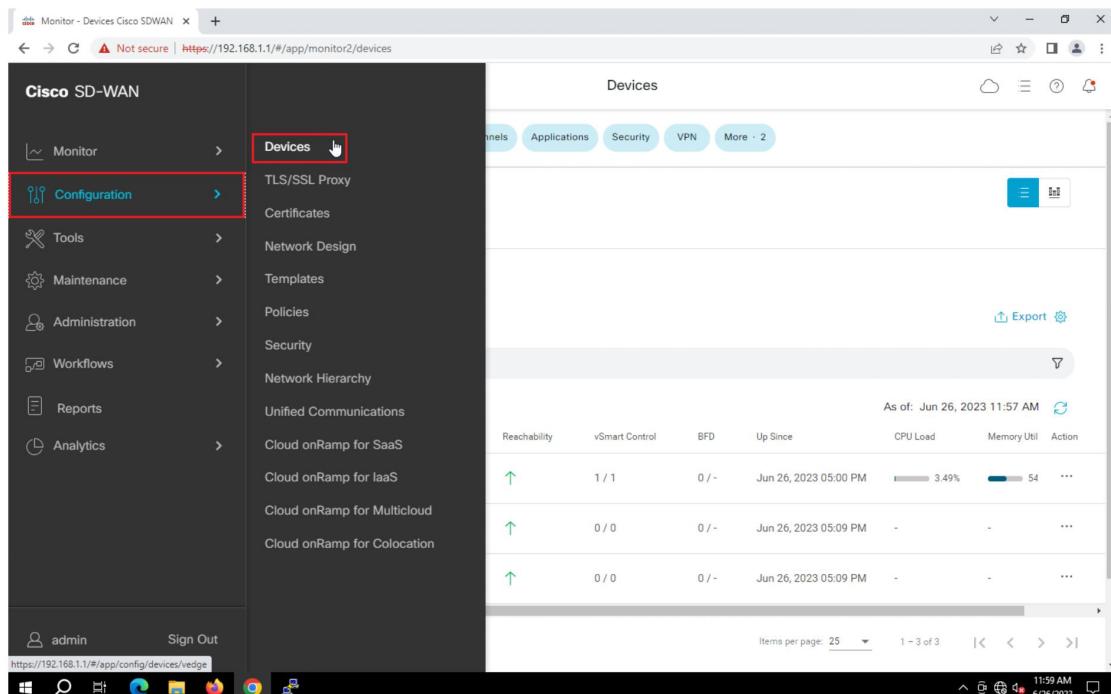
Cấu hình license vEdge

Để có được file (serialFile.viptela) thì ta phải có một smart account hoặc có thể download nó tại đây:

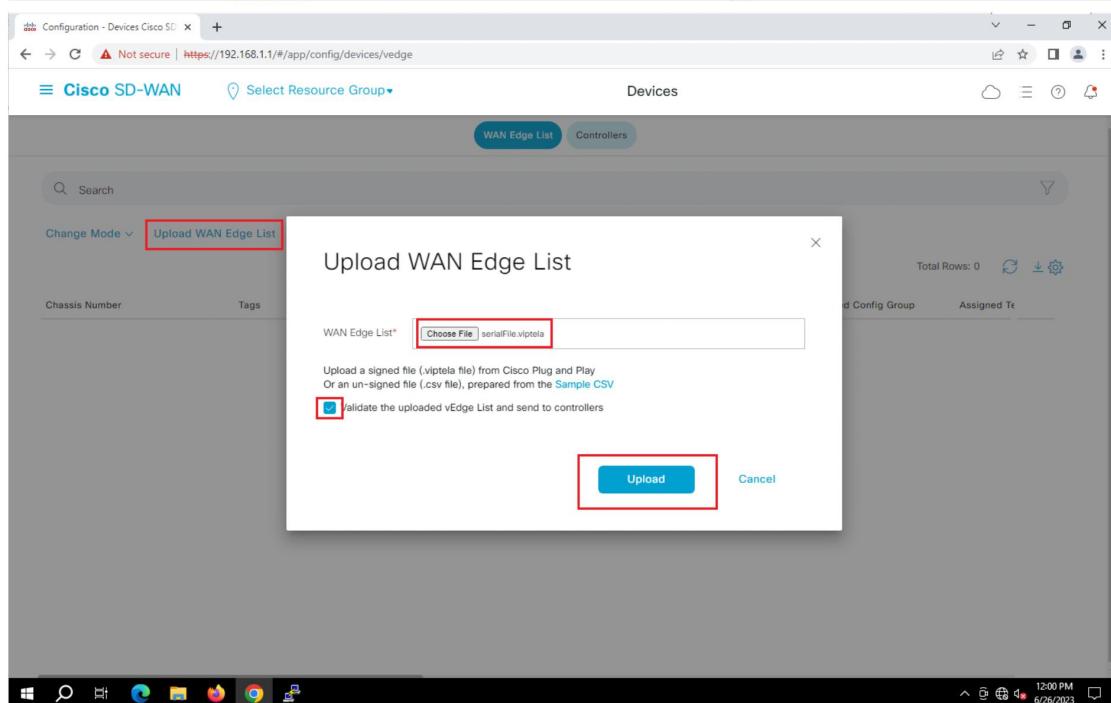
https://drive.google.com/file/d/1rEcGj2ufgs_lqkK_PO-mZe7MmZqQcYFf/view?usp=sharing

(cần chỉnh lại organization name trong phần cấu hình các thiết bị là: **VnPro** để có thể upload được file này)

Chọn **Configuration->Devices->Upload WAN Edge List** và chọn file trong phần download (**serialFile.viptela**)



The screenshot shows the Cisco SD-WAN interface. On the left, a sidebar menu is open with several options: Monitor, Configuration (which is highlighted with a red box), Tools, Maintenance, Administration, Workflows, Reports, and Analytics. The main content area displays a table titled 'Devices' with columns for Reachability, vSmart Control, BFD, Up Since, CPU Load, Memory Util, and Action. There are three entries in the table, all showing 'Up' status and 'Jun 26, 2023 05:09 PM' as the last update. At the bottom of the table, there are buttons for 'Items per page' (set to 25), '1 – 3 of 3', and navigation arrows.



The screenshot shows a modal dialog box titled 'Upload WAN Edge List'. It has a 'WAN Edge List*' input field with a 'Choose File' button and a file path 'serialFile.viptela'. Below the input field is a note: 'Upload a signed file (.viptela file) from Cisco Plug and Play Or an un-signed file (.csv file), prepared from the [Sample CSV](#)'. There is a checked checkbox labeled 'Validate the uploaded vEdge List and send to controllers'. At the bottom of the dialog are two buttons: 'Upload' (highlighted with a red box) and 'Cancel'.

Upload WAN Edge List

WAN Edge List* serialFile.viptela

Upload a signed file (.viptela file) from Cisco Plug and Play
Or an un-signed file (.csv file), prepared from the [Sample CSV](#)

Validate the uploaded vEdge List and send to controllers

Are you sure you want to upload serialFile.viptela ?

Upload WAN Edge List

vEdge list uploaded successfully

- Number of vEdges uploaded successfully: 10

The screenshot shows a web-based configuration interface for Cisco SD-WAN. The top navigation bar includes tabs for 'Devices' and 'Controllers'. Below the navigation is a search bar and a menu with options like 'Change Mode', 'Upload WAN Edge List', 'Export Bootstrap Configuration', 'Sync Smart Account', and 'Add PAYG WAN Edges'. A table lists ten WAN edges, each with columns for Chassis Number, Tags, Hostname, Site ID, Region ID, Mode, Device Status, Assigned Config Group, and Assigned Tx. The table header indicates 'Total Rows: 10'. The bottom of the screen shows a standard Windows taskbar with icons for Start, Search, Task View, File Explorer, Edge, Google Chrome, Task Manager, and a clock showing 12:03 PM on 6/26/2023.

- Trên console vManage ta vào mode vshell dùng lệnh **vshell**

Tiếp theo dùng lệnh **scp ROOTCA.pem admin@172.16.1.1:/home/admin/R0OTCA.PEM**

Lệnh này dùng scp để truyền file ROOTCA.pem từ vmanage qua vedge

```
vmanage# vshell
vmanage:~$ scp ROOTCA.pem admin@172.16.1.1:/home/admin/R0OTCA.PEM
The authenticity of host '172.16.1.1 (172.16.1.1)' can't be established.
ECDSA key fingerprint is SHA256:aunoAbDXNHsXkm6R1DMLagsvHwcG64seS0qKQhhEnU
4.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.16.1.1' (ECDSA) to the list of known hosts
.
viptela 20.10.1

Password:
ROOTCA.pem                                         0%   0      0.0KB/s  --:-
ROOTCA.pem                                         100% 1249     60.0KB/s  00:0
0
vmanage:~$
```

Trên console vedge chúng ta request license

request root-cert-chain install /home/admin/R0OTCA.PEM

```
vedge1# request root-cert-chain install /home/admin ROOTCA.PEM
Uploading root-ca-cert-chain via VPN 0
Copying ... /home/admin/ROOTCA.PEM via VPN 0
Updating the root certificate chain..
Successfully installed the root certificate chain
vedge1#
```

Vào web vManage chọn **Configuration -> Certificates** chọn **chassis number** và **token**

Chassis Number	Site ID	Device Status	Hostname	Device Model	Serial No./Token	Reachability	Certific	...
0b0f3c75-47c5-5e73-a557-9cf97c754274	-	-	vEdge Cloud	Token - 1681d823ec0948d2bd35dab0bad29d4c	-			...
168a2add-2c4f-fcb1-6139-1d99df86e22e	-	-	vEdge Cloud	Token - 77a1c50e16774259a73df97179951fad	-			...
5316bef9-7742-d0c9-1048-df6288bb4e56	-	-	vEdge Cloud	Token - 4810508e40b144f2b63b3623d1c62109	-			...
57569bb0-0758-89a6-37e7-1f8e62ced210	-	-	vEdge Cloud	Token - 0778de671a4114437bcb0a06da1fb1312	-			...
80060207-b2bd-a5fa-691f-72386930a34e	-	-	vEdge Cloud	Token - c4478875cb94561ab498883ac6c64d7	-			...
84c6527e-45e6-c5a8-c33c-fff9d8ad42a4	-	-	vEdge Cloud	Token - 598a2ec1fc14166a8e0426bc013fcdd	-			...
a95df91b-578a-e6a2-8da8-589f1106758	-	-	vEdge Cloud	Token - 5ddc8587bc884c5583d415f5203d0a9	-			...
be5ba729-6684-943c-1e91-7d6ff296e97b	-	-	vEdge Cloud	Token - 5ca1046d258d42b1a2c16e63380a8156	-			...
ecfb966f-55f0-b701-b9df-717fe3ca0fd0	-	-	vEdge Cloud	Token - 87e96a7a10044cd78af3b061e4559705	-			...

Vào lại Putty và gõ lệnh **request vedge-cloud activate chassis-number chassis-number token token**

(chassis number và token đã chọn trong mục certificate)

```
vedge1# request vedge-cloud activate chassis-number
Value for 'chassis-number' (<Chassis number/uuid of the device>): 0
b0f3c75-47c5-5e73-a557-9cf97c754274
Value for 'token' (<Serial number of the device>): 1681d823ec0948d2
bd35dab0bad29d4c
vedge1#
```

Trên hai vedge còn lại, chúng ta làm tương tự.

IV. Kiểm tra

```
vedge1# show control connections
          PEER
PEER   PEER PEER      SITE      DOMAIN PEER
          PUB
TYPE   PROT SYSTEM IP   ID      ID      PRIVATE IP
          PORT  ORGANIZATION      LOCAL COLOR
          PROXY STATE UPTIME     ID
-----
```

vsmart	dtls	11.1.1.3	1000	1	10.1.1.3	mpls	No	12446	10.1.1.3	0
			12446					connect		
vbond	dtls	0.0.0.0	0	0	100.100.100.3	mpls	-	12346	100.100.10	0
0.3			12346	VnPro				up	0:00:01:26	0
vmanage	dtls	11.1.1.1	1000	0	10.1.1.1	mpls	No	12846	10.1.1.1	0
			12846	VnPro				up	0:00:01:05	0

```
vedge1# 
```



```
vedge2# show control connections
          PEER
PEER   PEER PEER      SITE      DOMAIN PEER
          PUB
TYPE   PROT SYSTEM IP   ID      ID      PRIVATE IP
          PORT  ORGANIZATION      LOCAL COLOR
          PROXY STATE UPTIME     ID
-----
```

vsmart	dtls	11.1.1.3	1000	1	10.1.1.3	biz-internet	No	12346	100.100.10	0
0.4			12346	VnPro				up	0:00:46:01	0
vbond	dtls	0.0.0.0	0	0	100.100.100.3	biz-internet	-	12346	100.100.10	0
0.3			12346	VnPro				up	0:00:46:01	0
vmanage	dtls	11.1.1.1	1000	0	10.1.1.1	biz-internet	No	12346	100.100.10	0
0.2			12346	VnPro				up	0:00:46:01	0

```
vedge2# 
```



```
vedge3# show control connections
          PEER
PEER   PEER PEER      SITE      DOMAIN PEER
          PUB
TYPE   PROT SYSTEM IP   ID      ID      PRIVATE IP
          PORT  ORGANIZATION      LOCAL COLOR
          PROXY STATE UPTIME     ID
-----
```

vsmart	dtls	11.1.1.3	1000	1	10.1.1.3	biz-internet	No	12346	100.100.10	0
0.4			12346	VnPro				up	0:00:44:25	0
vbond	dtls	0.0.0.0	0	0	100.100.100.3	biz-internet	-	12346	100.100.10	0
0.3			12346	VnPro				up	0:00:48:07	0
vmanage	dtls	11.1.1.1	1000	0	10.1.1.1	biz-internet	No	12946	100.100.10	0
0.2			12946	VnPro				up	0:00:43:17	0

```
vedge3# 
```

