

Xem thêm tại <https://hainguyenit.edubit.vn>

CẤU HÌNH F5 LTM TỪ ĐẦU CHO NEWBIE

1. Tải software làm lab
2. Kích hoạt license free 30 ngày
3. Cài web server trên Ubuntu để test
4. Đặt IP cho cổng LAN và WAN
5. Cấu hình cân bằng tải 2 webserver qua HTTP
6. Cấu hình HTTP redirect sang HTTPS
7. Import Certificate vào F5
8. Cấu hình Persistent Session
9. Giải thích automap và Snat
10. One-arm mode: chỉ cần 1 interface LAN
11. Cấu hình HA cluster F5

Xem thêm tại <https://hainguyenit.edubit.vn>

1. Tải software về làm lab và xin license

Vào trang <https://www.f5.com/trials/big-ip-virtual-edition> tạo 1 account miễn phí, rồi tải software **BIGIP-16.1.3-0.0.12.ALL.qcow2.zip** (hoặc version khác nhưng dạng filename **ALL.qcow2.zip** là được) xin license 30 ngày (sẽ được gửi về mail của bạn).

1. Login or register

You will need to use your F5 support ID to login in and request your trial key. Don't have one? No problem, click the link below and go through the steps to create your support account.

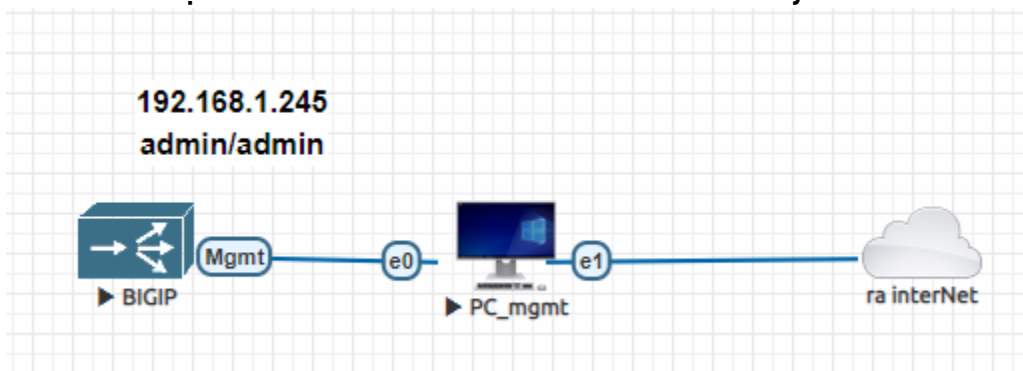


2. Request your key

Once you're logged in, you'll be prompted to pick the trial type and number of licenses you want. Your order will be delivered via the email you used to create your support account.

2. Login vào thiết bị để active license

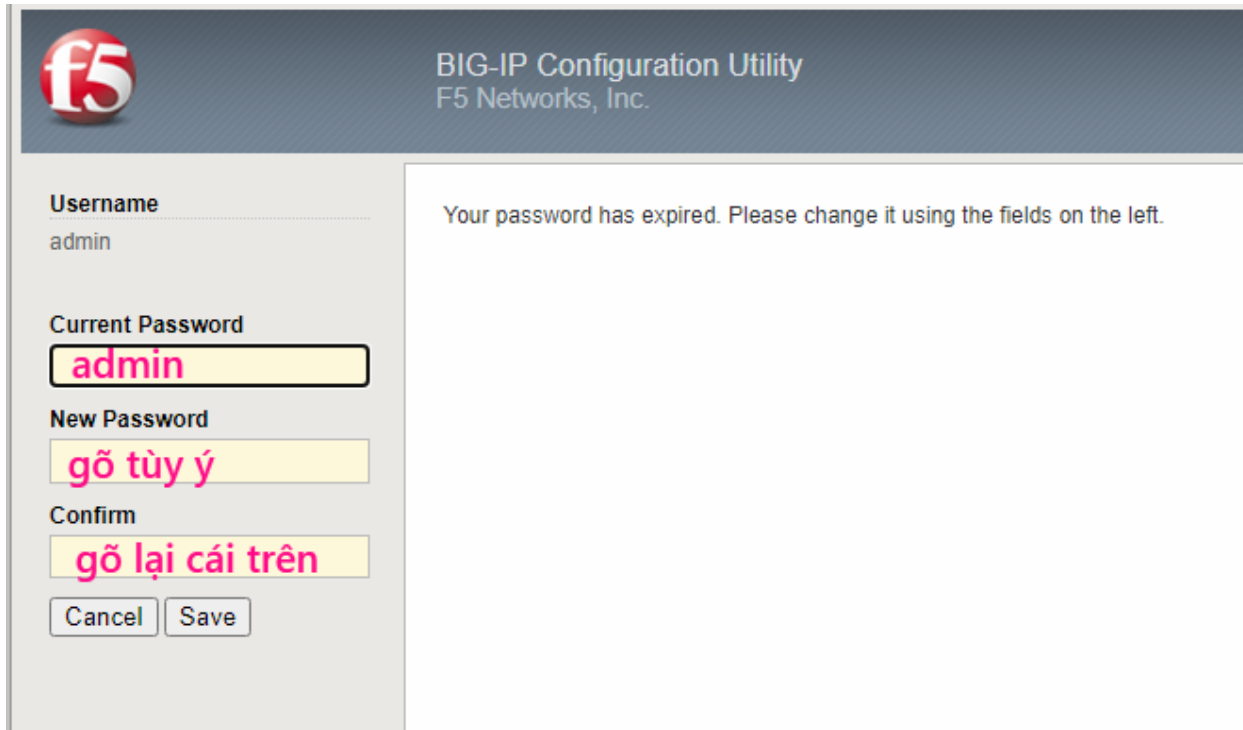
Add thiết bị lên EVE-NG và kéo mô hình như này



Mặc định cổng Mgmt có IP là 192.168.1.245 (admin/admin)

Ta từ con PC truy cập qua web gui vào để đổi pass

Xem thêm tại <https://hainguyenit.edubit.vn>



f5 BIG-IP Configuration Utility
F5 Networks, Inc.

Username
admin

Current Password
admin

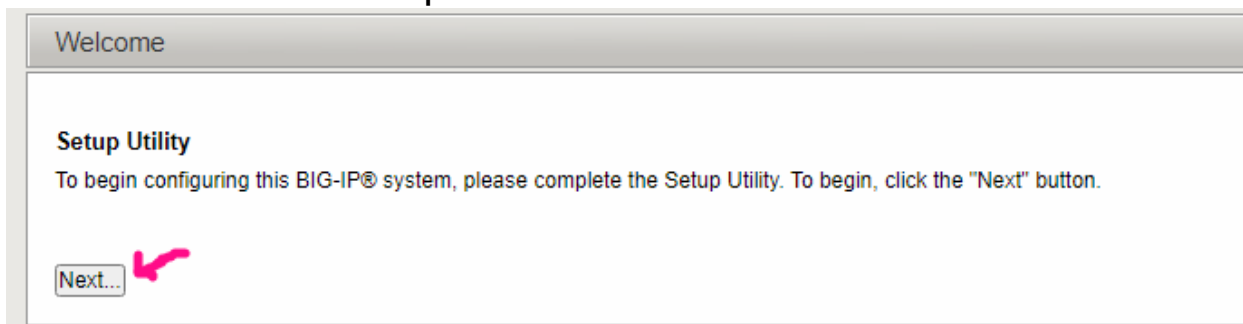
New Password
gõ tùy ý

Confirm
gõ lại cái trên

Cancel Save

Your password has expired. Please change it using the fields on the left.

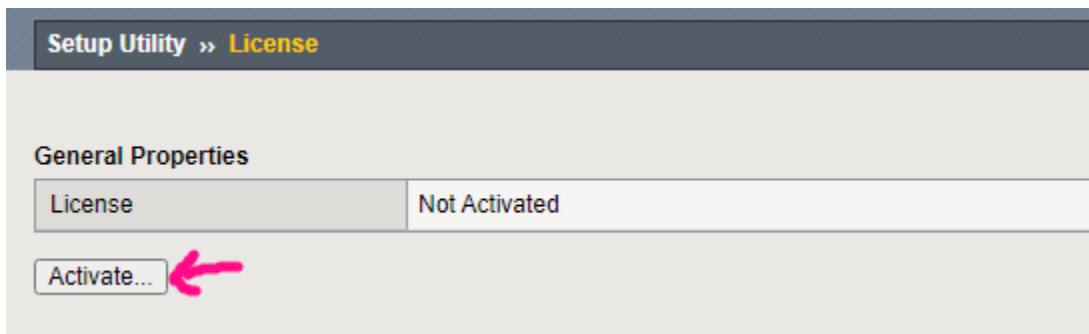
Sau đó sẽ vào first setup:



Welcome

Setup Utility
To begin configuring this BIG-IP® system, please complete the Setup Utility. To begin, click the "Next" button.

Next...



Setup Utility >> License

General Properties

License	Not Activated
---------	---------------

Activate...

Mở mail đã nhận key ra, điền key vào:

Xem thêm tại <https://hainguyenit.edubit.vn>

General Properties

Base Registration Key	RIP-XUUYW-FSHSR-ACELL-WIXLWBM <input type="button" value="Revert"/>
Add-On Registration Key List	Add-On Key <input type="text"/> <input type="button" value="Add"/>
	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Activation Method	<input type="radio"/> Automatic (requires outbound connectivity) <input checked="" type="radio"/> Manual
License Comparison	<input type="checkbox"/> Enable License Comparison

Bấm NEXT sẽ được, như dưới, kích vào ô khoanh như dưới:

Copy/Paste Text Download/Upload File

```
0e38119698868dd93e44c879e83bf845ca2c4dff1603469a57ef0093c941285f51b23623c64b73be  
d3b409d3fb228d00657b788f8ca3514059166cf281c3b17bdf99345c9bdc41cc17a3c994a4b97f28  
c222c09518f167dff9f4ad17e5bf8d9dabbd517600ba2a3f4b392bbd594f520509edbb2920984288  
f9590a163b4474a90d001f51766dd1d3ec8725eb3a7fd319b779d18631ca3051ec8a94482a91f2d8  
9d410661fc66e9f0cf814ee82f9805352b1705cb5d410b77c84714dbdb898e158a01d1765dbd48fk  
0c2ff4d658f93482ac25a2a66648b899a91779ad7c99e045879c81c6e72a35bb6288793b07b001d0  
6b4bb0e6b50e0cb57a52faafc6931d3947ad59faad038f832b3111136f1134b3ea30dbcc0d1e76ce  
02a8ed6fc49a8445e886a8a4f27719a5f0163b5a04b8eb9beb7a292f7bfc12c3355daaa6d322a221  
86fe6b3832ba8580a0bf060d093a2820d85a8339b0b037c3f736752ea93c9888b74899cf98f3953c  
a42231e5598683f1b5c58a5553048126fdc9964852ef5655fb06d22ee28779be81704639933004bc
```

[Click here to access F5 Licensing Server](#)

Sau đó ra trang web F5 và paste phần text ở trên vào đây rồi bấm NEXT:

Xem thêm tại <https://hainguyenit.edubit.vn>

Activate F5 Product

Use this license activation page for current F5 products. **Paste phần text ở trên vào đây**

Enter Your Dossier

```
305909d25937365a2e56aeac5ee221735016a72d2afdb033f97ee52f2ed8d32e19425f902256878d90213b
7765055d0ec4a33dc3bc1e8424ba04df1ebb9243d01e6c122aadf4a43ddec1d9e125c76fdb5cbe58488587d
a6b6d2f887f2885ea1e2c5c383f8248e5077b100b010766ed1f398e6421edd450cd99bc61c8a48ccb9ffb66
96ba22314adc7cb4e01ddcd795c48da9fb1e1e6bb74de6df95bd2bdf744d5e719b74431872ae9c143e9bcd8
1039ae7a79688a4e74b870e11bd7a957eeee2ae25aeb95195fb8d97d8854ce643ae7310f16aada8dc52ca35
ff3b1b110feed69764f1536814bb2fa3c7beec17d36740041e315bb5bcc6641ee812b367d5d4697eceb2b6
95b952e6b3d12cae6df2e03471a96dad41909ca66404aeef758161357bf117750caae7a272c48d5eab87571
4b44967a5b4f7d45c8b2c757639ef5866070c2f57245dcad285e46ab8b97c5c39cdd6a7871fd36ff7a860f
1463bfe63210d238c2107d1737f9e354584bdb17cf587c50ddac117c4fb109926a2b00dbfe87dabb19b4796
b6337f78463fef9d433c802e50b2bfc7e3daeb7c88a87fd63b2055050653314704a7c5fb558e6914c75260c
242fccb5cc0e0a6d49251250a14247f8bd46e033abda334a69e53065c48c433e4defc8e5051f0216b2d1e6
33ceb0f5648051f43f587dfffcc0171b6a973aeefa5cafbba83e882a346c15c813bf1010c794dfbea60977
4a3ca36c70089ab25e26fdc7b977637041cc7b16a943711ee39ac211b0a438c5ca5d483d606d9f75e1bfc96
0ad39d24f70f7e33a42410ddf57b49a5bdf641d66084937a9b6b8b52013bb7c3a7e605baa003fdd31817704
8743492f155e540d203bcce46d65109b024db02717801638395744ffff65da9d8bbf821e26bf0706b9839a0
```

ctr A để copy toàn bộ chỗ text này

```
#
# Module List
#
active module : BIG-IP, VE Trial|FZUTGJK-VPEOFMF|Rate Shaping|External
Interface and Network HSM, VE|SDN Services, VE|SSL, Forward Proxy, VE|BIG-IP VE,
Multicast Routing|APM, Limited|SSL, VE|DNS (1K QPS), VE|Routing Bundle, VE|ASM,
VE|Crypto Offload, VE, Tier 1 (25M - 200M)|Max Compression, VE|AFM, VE|Advanced Web
Application Firewall, VE|DNSSEC|Anti-Virus Checks|Base Endpoint Security
Checks|Firewall Checks|Network Access|Secure Virtual Keyboard|APM, Web
Application|Machine Certificate Checks|Protected Workspace|Remote Desktop|App
Tunnel|VE, Carrier Grade NAT (AFM ONLY)|PSM, VE
#
# Accumulated Tokens for Module
# DNS (1K QPS), VE gtm_rate_fallback 1000 key FZUTGJK-VPEOFMF
#
# Accumulated Tokens for Module
# DNS (1K QPS), VE gtm_rate_limit 1000 key FZUTGJK-VPEOFMF
#
# Accumulated Tokens for Module
```

Rồi paste vào ô License bên webgui của thiết bị F5:

Step 3: License

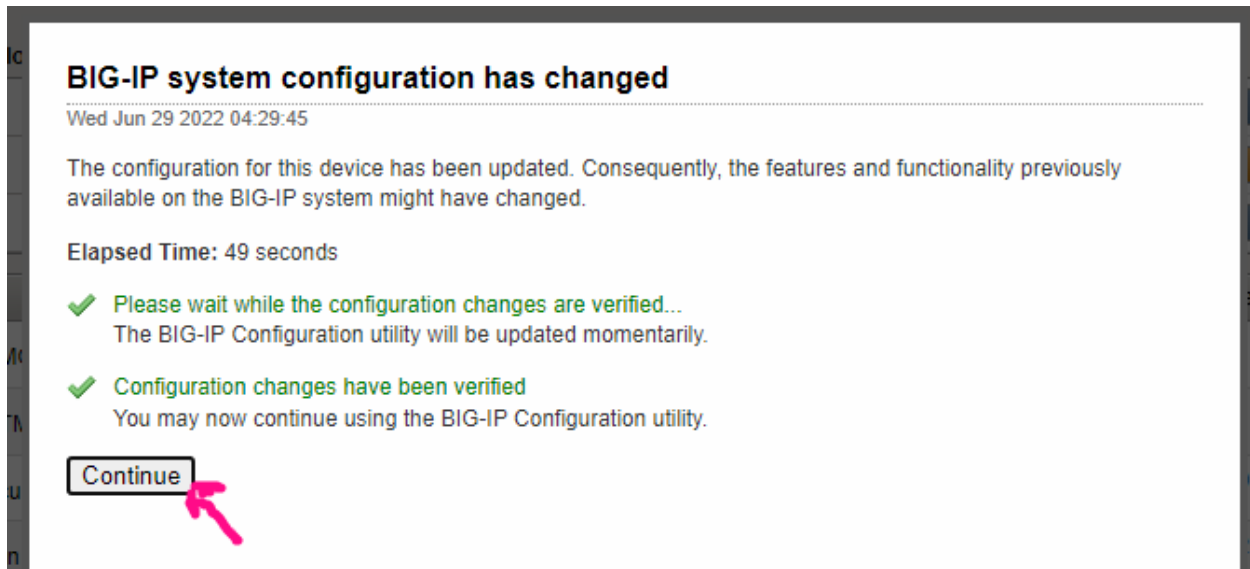
```
#
# Outbound License Authorization Signature
#
Authorization : b519c788f588c6b4fa4906e2afc34e32f22cc5dccc37f4c479f050118de
#
# -----
# Copyright 1996-2022, F5 Networks, Inc.
# All rights reserved.
# -----
```

Dán vào đây rồi next

Next...

Xem thêm tại <https://hainguyenit.edubit.vn>

Sau đó đợi tầm 5 phút :



Thấy LTM đã có license là OK (License này dùng được 30 ngày)

Module	Provisioning	License Status	F
Management (MGMT)	Small	N/A	0
Local Traffic (LTM)	<input checked="" type="checkbox"/> Nominal	Licensed	0

Bấm Next tiếp và điền 1 số thông số:

Xem thêm tại <https://hainguyenit.edubit.vn>

Setup Utility » Platform

General Properties

Management Config IPv4	<input type="radio"/> Automatic (DHCP) <input checked="" type="radio"/> Manual
IPv4 Config Details	IP Address[/prefix]: <input type="text" value="192.168.1.245"/>
	Network Mask: <input type="text" value="255.255.255.0"/> /24
	Management Route: <input type="text"/>
Management Config IPv6	<input checked="" type="radio"/> Automatic (DHCP) <input type="radio"/> Manual
Host Name	<input type="text" value="f5-01.local"/>
Host IP Address	<input type="text" value="Use Management Port IP Address"/>
Time Zone	<input type="text" value="Asia/Hong Kong"/>

User Administration

Root Account	<input type="checkbox"/> Disable login
	Password: <input type="password" value="....."/>
	Confirm: <input type="password" value="....."/>
SSH Access	<input checked="" type="checkbox"/> Enabled
SSH IP Allow	<input type="text" value="* All Addresses"/>

Điền IP mới nếu cần đổi

Điền pass mới nếu cần đổi

Sau đó bấm finish luôn.

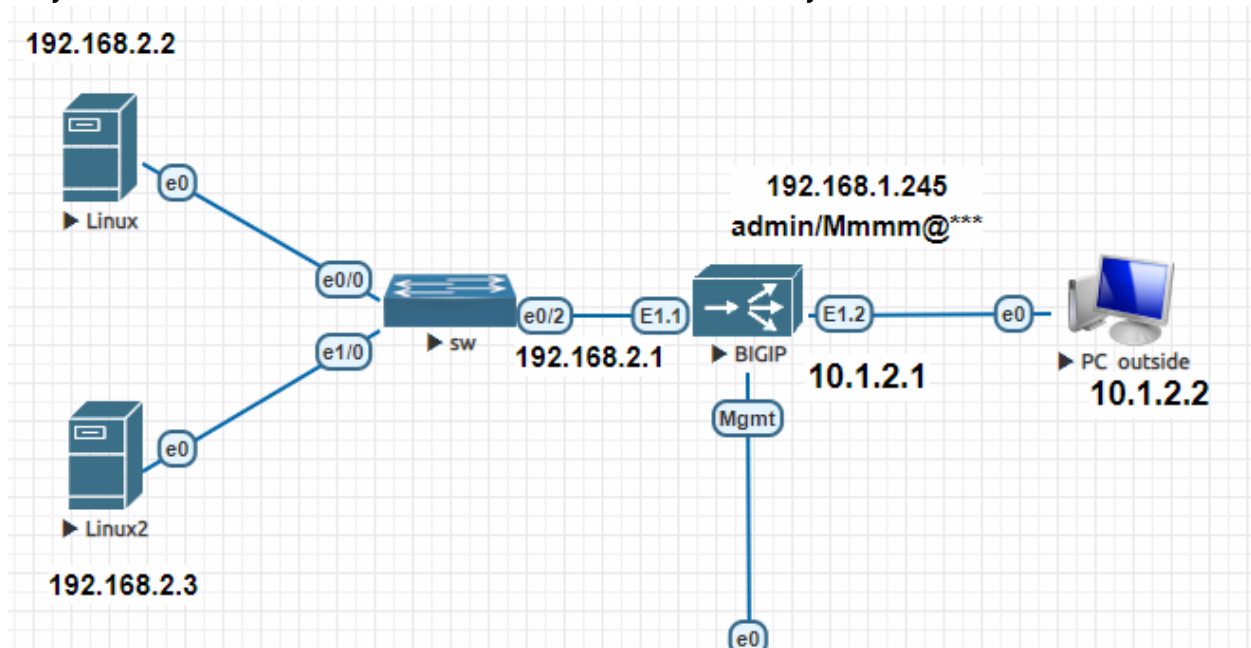
Advanced Network Configuration

Create advanced device configurations by clicking **Finished** and navigating to the Main tab of the Configuration Utility.

Xem thêm tại <https://hainguyenit.edubit.vn>

3. Setup webserver trên ubuntu 18

Lấy 2 node ubuntu ra cho thành mô hình như này:



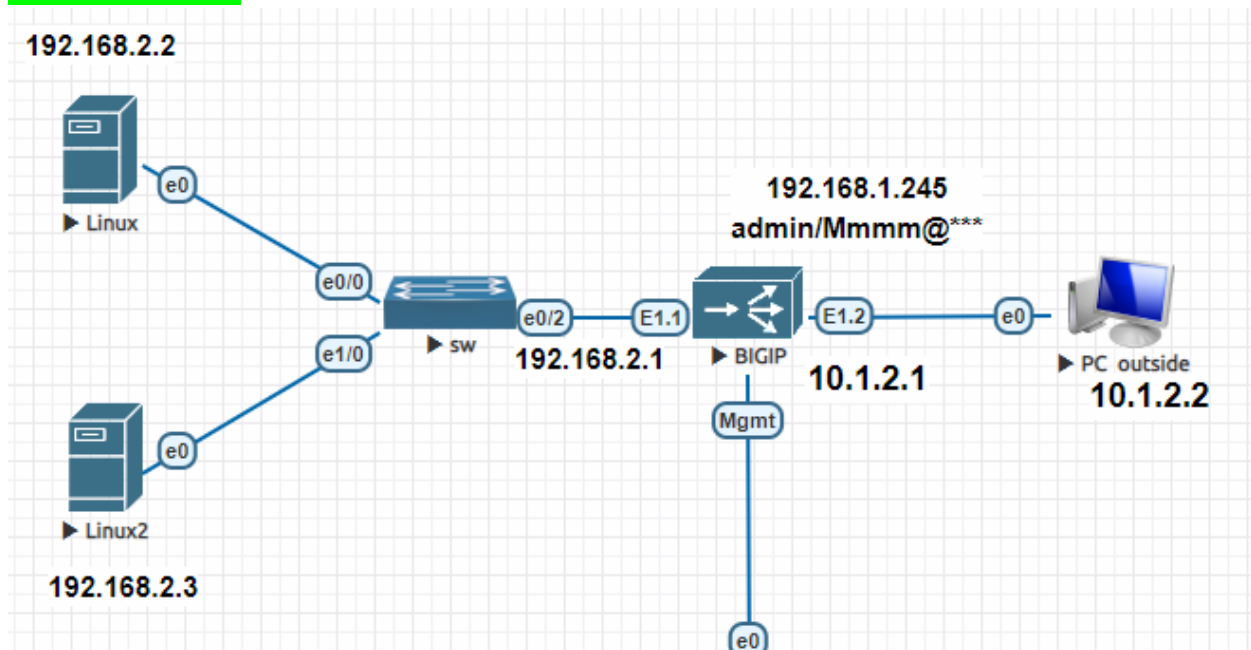
Sau đó cài Apache trên 2 node Ubuntu theo hướng dẫn trên mạng, ví dụ ở trang này:

<https://www.digitalocean.com/community/tutorials/how-to-install-the-apache-web-server-on-ubuntu-18-04-quickstart>

Sau khi cài xong **telnet localhost 80** thử xem cổng 80 đã thông chưa? Và từ ubuntu này gõ `http:<ip của ubuntu kia>` xem hiện ra trang web chưa là được.

4. Cấu hình IP cho cổng WAN và LAN

4.1 IP LAN E1.1



- Trên F5 không có kiểu đặt IP thẳng vào port như router. Thay vào đó sẽ cần tạo ra vlan, rồi gán port đó vào vlan, rồi đặt IP cho vlan đó. (Tương tự SVI trong CCNA)
- Trong bài này ta đã cấu hình switch cổng trunk e0/2, allow vlan 100 và trên F5 sẽ tagging tương ứng vlan 100 vào E1.1

Bước 1: Tạo vlan tên là NOI-B0 (nội bộ) và Gán port E1.1 vào vlan NOI-B0

Bước 2: Gán IP cho vlan NOI-B0 192.168.2.1/24

Bước 3: Ping thử về server 192.168.2.2 và 192.168.2.3 xem ok chưa

Chi tiết:

Bước 1: Vào Vlan > Vlan list > Create , điền như dưới:

Xem thêm tại <https://hainguyenit.edubit.vn>

General Properties

Name	NOIBO
Partition / Path	Common
Description	
Tag	100

Resources

Interface: 1.2
Tagging: Select...
Add
1.1 (tagged)
Edit Delete

Configuration: Basic

Source Check	<input type="checkbox"/>
MTU	1500
Auto Last Hop	Default

Bước 2: Vào Self IPs > Create

Network >> Self IPs >> IP-LAN

Properties

Configuration

Name	IP-LAN
Partition / Path	Common
IP Address	192.168.2.1
Netmask	255.255.255.0
VLAN / Tunnel	NOIBO
Port Lockdown	Allow None
Traffic Group	<input type="checkbox"/> Inherit traffic group from current partition / path traffic-group-local-only (non-floating)

Xem thêm tại <https://hainguyenit.edubit.vn>

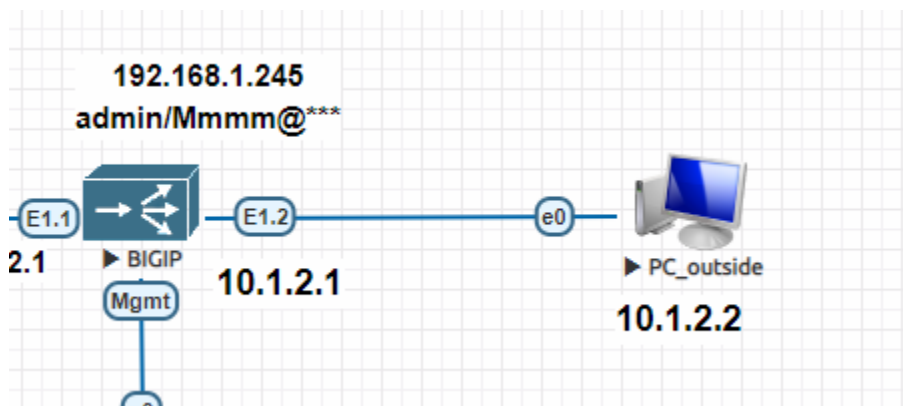
Bước 3: Ping từ F5 đến 2 server xem thông chưa

Mở màn hình cli lên; gõ ping 192.168.2.2 và ping 192.168.2.3

```
[root@f5-01:Active:Standalone] config # ping 192.168.2.2
PING 192.168.2.2 (192.168.2.2) 56(84) bytes of data.
64 bytes from 192.168.2.2: icmp_seq=1 ttl=64 time=2.43 ms
64 bytes from 192.168.2.2: icmp_seq=2 ttl=64 time=1.16 ms
64 bytes from 192.168.2.2: icmp_seq=3 ttl=64 time=1.32 ms

--- 192.168.2.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 200lms
rtt min/avg/max/mdev = 1.165/1.638/2.430/0.565 ms
[root@f5-01:Active:Standalone] config # ping 192.168.2.3
PING 192.168.2.3 (192.168.2.3) 56(84) bytes of data.
64 bytes from 192.168.2.3: icmp_seq=1 ttl=64 time=1.64 ms
64 bytes from 192.168.2.3: icmp_seq=2 ttl=64 time=1.06 ms
64 bytes from 192.168.2.3: icmp_seq=3 ttl=64 time=0.980 ms
```

4.2 Đặt IP cho cổng WAN E1.2



Cũng vào VLAN > Create và tạo vlan cho OUTSIDE như dưới:

Xem thêm tại <https://hainguyenit.edubit.vn>

Network >> VLANs : VLAN List >> New VLAN...

General Properties

Name	OUT
Description	
Tag	

Resources

Interface: 1.2
Tagging: Untagged
Add
Interfaces
Edit Delete

Rồi vào Self IPs > Create để đặt IP WAN cho F5:

Configuration

Name	IP-WAN
IP Address	10.1.2.1
Netmask	255.255.255.0
VLAN / Tunnel	OUT
Port Lockdown	Allow None
Traffic Group	<input type="checkbox"/> Inherit traffic group from current partition / path traffic-group-local-only (non-floating)
Service Policy	None

Cancel Repeat Finished

Xem thêm tại <https://hainguyenit.edubit.vn>

Test lại ping từ F5 ra PC outside

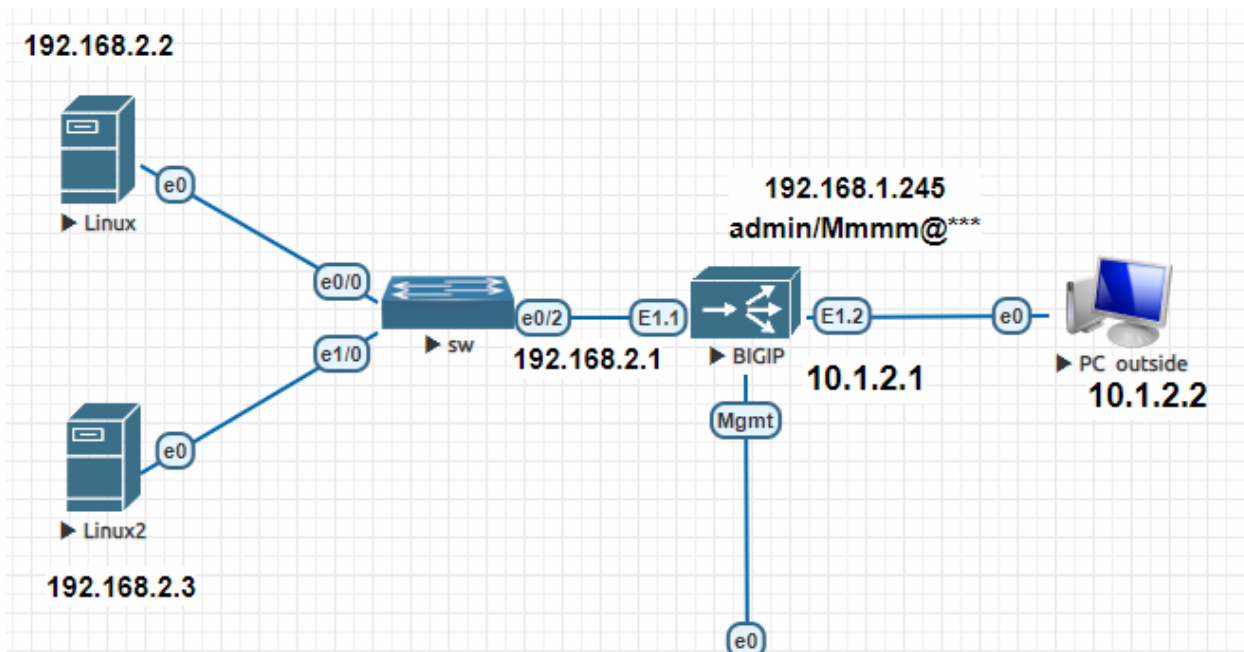
```
[root@f5-01:Active:Standalone] config # ping 10.1.2.2
PING 10.1.2.2 (10.1.2.2) 56(84) bytes of data.
64 bytes from 10.1.2.2: icmp_seq=1 ttl=128 time=1.86 ms
64 bytes from 10.1.2.2: icmp_seq=2 ttl=128 time=3.78 ms
64 bytes from 10.1.2.2: icmp_seq=3 ttl=128 time=0.958 ms
64 bytes from 10.1.2.2: icmp_seq=4 ttl=128 time=0.728 ms
64 bytes from 10.1.2.2: icmp_seq=5 ttl=128 time=0.845 ms
```

Từ PC outside ping vào cũng OK

```
PS C:\Users\Administrator> ping 10.1.2.1
Pinging 10.1.2.1 with 32 bytes of data:
Reply from 10.1.2.1: bytes=32 time<1ms TTL=255
Reply from 10.1.2.1: bytes=32 time<1ms TTL=255
Reply from 10.1.2.1: bytes=32 time<1ms TTL=255
Reply from 10.1.2.1: bytes=32 time<1ms TTL=255
```

DONE

5. Cấu hình cân bằng tải giữa 2 webserver



Traffic http từ ngoài PC_outside sẽ gọi đến IP đại diện (10.1.2.100) , sau đó F5 sẽ phân phối lần lượt đến 2 server 192.168.2.2 và 192.168.2.3 theo giải thuật round-robin (vòng tròn)

Xem thêm tại <https://hainguyenit.edubit.vn>

Trên F5 khai báo các khái niệm cơ bản sau:

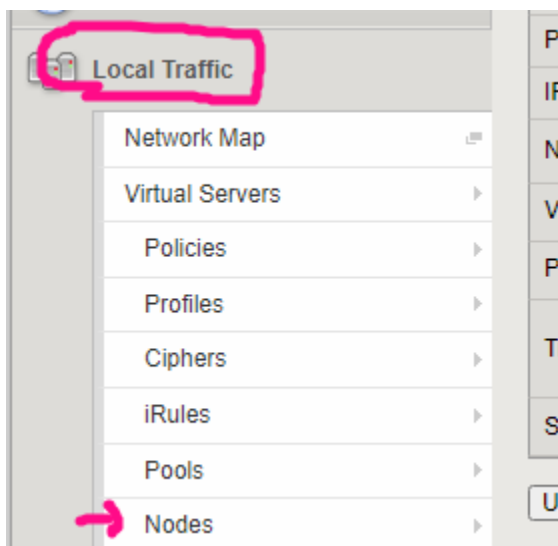
>> Node: là IP của các server LAN, kèm port dịch vụ của server đó, ví dụ 2 webserver chạy http thì Node = IP+port 80

>> Pool: là tập hợp các Node trên vào 1 nhóm, F5 sẽ lần lượt điều hướng request từ ngoài vào 2 Node này theo giải thuật mình chọn (default là round-robin)

>> Virtual Server: Là 1 process của F5 để thực hiện load balancing. Được đại diện bằng 1 IP. Từ ngoài gọi vào IP này.

5.1 Khai báo NODE

Vào Local Traffic > Node > Create



Sau đó điền IP và chọn Health Monitor là ICMP, được như này (lưu ý chấm xanh là online OK, đỏ-xanh dương là chưa được)

<input checked="" type="checkbox"/>	Status	Name	Description	Application	Address
<input type="checkbox"/>	●	Node-01			192.168.2.2
<input type="checkbox"/>	●	Node-02			192.168.2.3

Enable | Disable | Force Offline | Delete...

Xem thêm tại <https://hainguyenit.edubit.vn>

5.2 Khai báo POOL

Vào Local Traffic > Pool > Create

Configuration: Basic

Name: Pool-website

Description:

Health Monitors:

- Active: /Common, http
- Available: /Common, gateway_icmp, http2, http2_head_f5, http_head_f5

Resources:

Load Balancing Method: Round Robin

Priority Group Activation: Disabled

New Members:

- New Node New FQDN Node Node List
- Node Name: Node-01 (Optional)
- Address: 192.168.2.2
- Service Port: 80 HTTP
- Add

Node Name	Address/FQDN	Service Port	Auto Populate	Priority
No members to display.				

Edit Delete

Thấy Pool xanh lên như này là OK

Local Traffic >> Pools : Pool List

Pool List Statistics

* Search

<input checked="" type="checkbox"/>	Status	Name
<input type="checkbox"/>	●	Pool-website

Delete...

Xem thêm tại <https://hainguyenit.edubit.vn>

5.3 Khai báo VIRTUAL SERVER

Vào Local Traffic > Virtual Server > Create

Điền như dưới:

General Properties	
Name	VS1
Partition / Path	Common
Description	
Type	Standard
Source Address	<input checked="" type="radio"/> Host <input type="radio"/> Address List 0.0.0.0/0 ← Allow all source IP
Destination Address/Mask	<input checked="" type="radio"/> Host <input type="radio"/> Address List 10.1.2.100 ← IP của virtual server mà từ ngoài gọi
Service Port	<input checked="" type="radio"/> Port <input type="radio"/> Port List 80 HTTP
Notify Status to Virtual Address	<input checked="" type="checkbox"/>

SMTP Profile	None
TDR Profile	None
VLAN and Tunnel Traffic	All VLANs and Tunnels ←
Source Address Translation	Auto Map ← Giải thích bài sau

Content Rewrite

Rewrite Profile	+ None
-----------------	--------

Còn các chỗ khác để mặc định

Sang tab Resource để trở vào Pool vừa tạo ở bước trước

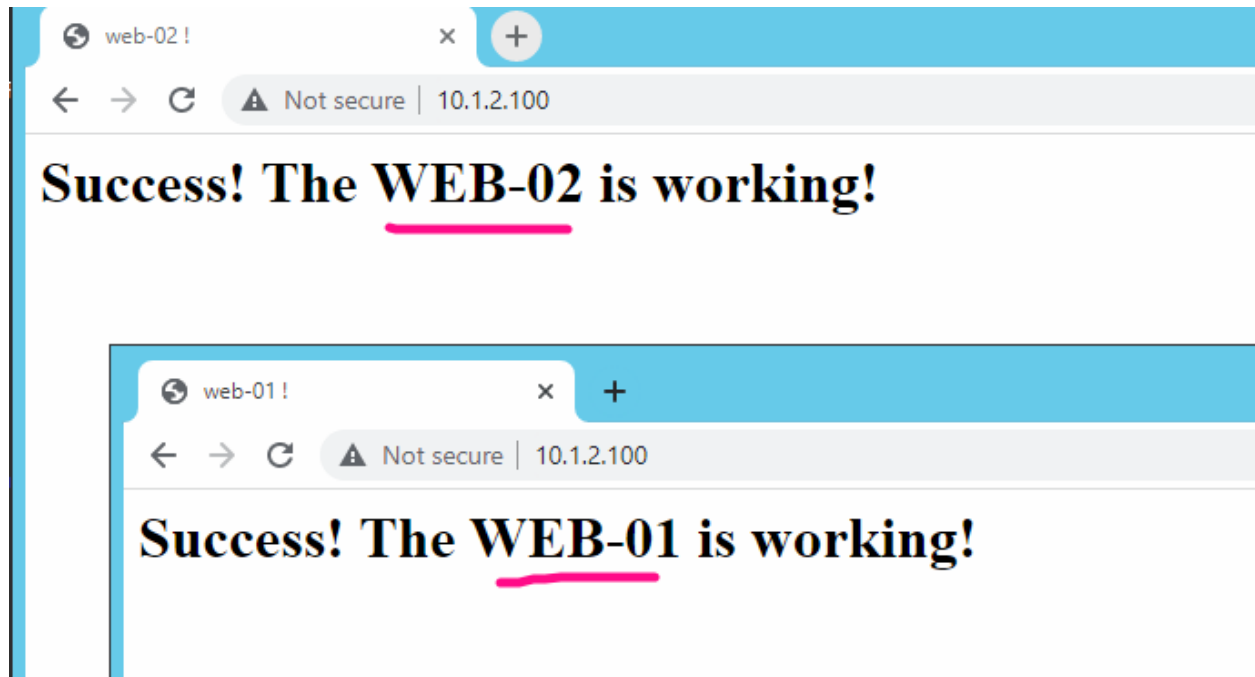
Local Traffic >> Virtual Servers : Virtual Server List >> VS1

Settings	Properties	Resources	Security	Statistics
Load Balancing				
Default Pool		Pool-website ←		
Default Persistence Profile		None		
Fallback Persistence Profile		None		

Xem thêm tại <https://hainguyenit.edubit.vn>

Test lại: Từ PC_Outside gõ `http://10.1.2.100`, rồi bấm F5 để refresh.

Thấy lúc thì vào web01, lúc vào web02 => vậy đã chia tải thành công.



6. HTTPS redirection

Khi người dùng gõ `http://10.1.2.100` như bài trên, ta đã cấu hình ok. Tuy nhiên trong thực tế nếu để http thì thông tin mật khẩu sẽ bị lộ khi bắt gói bằng wireshark => vì vậy nhu cầu là cần chạy giao thức https giữa người dùng và F5 để mã hóa dữ liệu.

Khi F5 nhận được https, sẽ giải mã thành http và thực hiện phân phối request đến 2 server như bình thường.

=> Trong bài này sẽ cấu hình để người dùng dù gõ http cũng biến thành https

Bước 1: Tạo thêm virtual server port 443

Bước 2: Vào Virtual Server port 80 để chỉnh irule trở sang 443

Bước 3: tạo profile SSL và apply vào Virtual server 443

Bước 4: Test lại gõ `http://10.1.2.100` xem có redirect sang https không?

Xem thêm tại <https://hainguyenit.edubit.vn>

Bước 1: Tạo thêm virtual server port 443

Tương tự như bài 5 ; chỉ khác chỗ chọn port là 443 (vẫn giữ nguyên VS-80 ở bài trước)

Service Port	<input checked="" type="radio"/> Port <input type="radio"/> Port List
	<input type="text" value="443"/> <input type="text" value="HTTPS"/>
Notify Status to Virtual Address	<input checked="" type="checkbox"/>

Tạo xong thì được 02 virtual server UP như này:

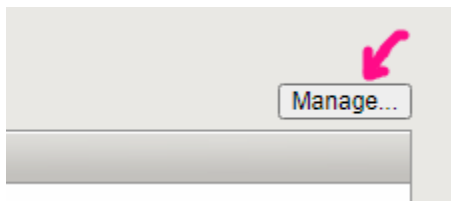
<input checked="" type="checkbox"/>	Status	Name
<input type="checkbox"/>	●	VS-443
<input type="checkbox"/>	●	VS1

Bước 2: Vào Virtual Server port 80 để chỉnh iRule trở sang 443

Vào Virtual Server 80, chọn profile HTTP như hình

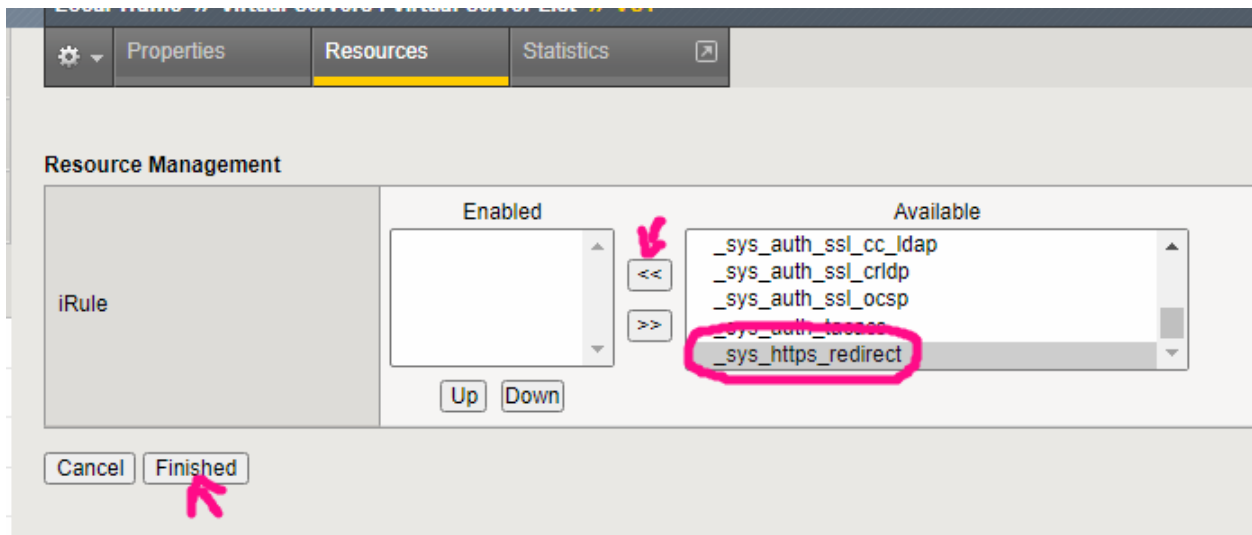
Configuration:	Basic
DoH Profile Type	None
Protocol	TCP
Protocol Profile (Client)	tcp
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile (Client)	http
HTTP Profile (Server)	(Use Client Profile)

Sau đó bấm vào tab Resource , nhìn thấy chữ iRule bên trái, bấm vào Manage bên phải tương ứng:



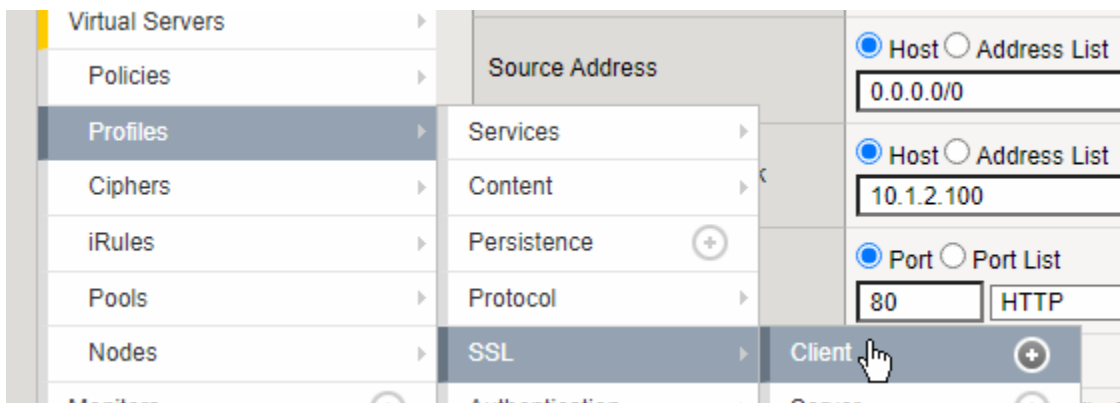
Xem thêm tại <https://hainguyenit.edubit.vn>

Chọn https redirect như hình

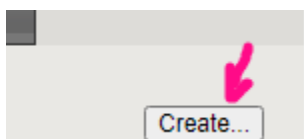


Bước 3: tạo profile SSL và apply vào Virtual server 443

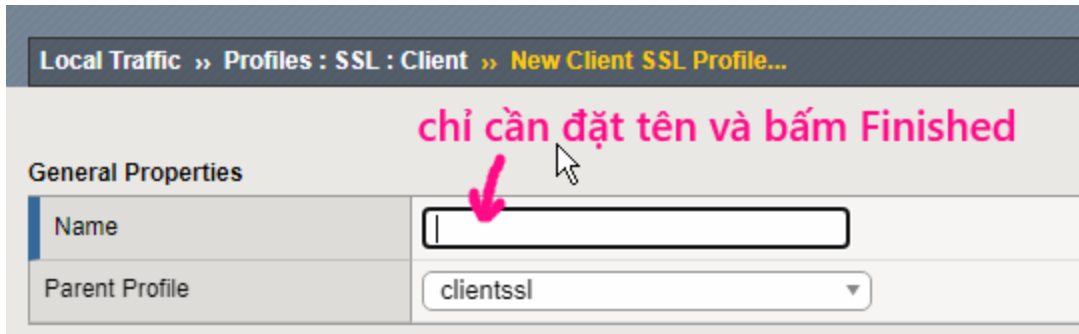
Vào Profiles > SSL > Client



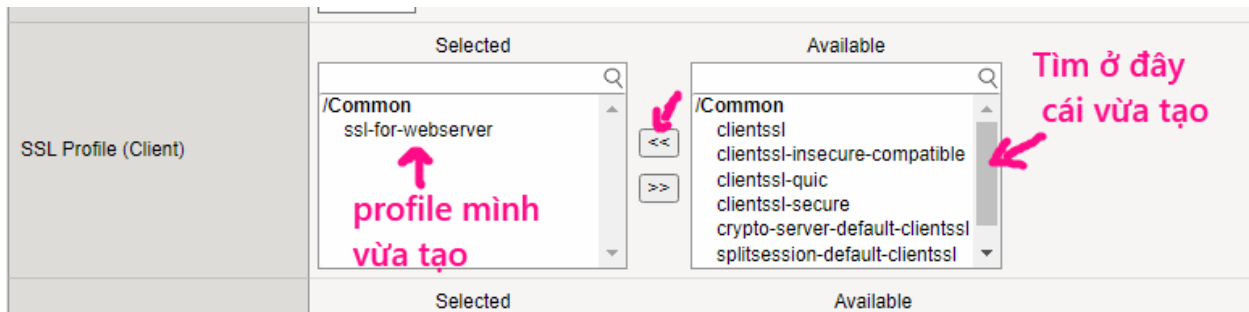
Bấm Create



Xem thêm tại <https://hainguyenit.edubit.vn>



Vào virtual server 443 và apply ssl profile vào



Bấm update

Bước 4: Test lại gõ <http://10.1.2.100> xem có redirect sang https không?



Xem thêm tại <https://hainguyenit.edubit.vn>

7. Import Certificate vào F5

Trong bước trên ta đã cấu hình https khi truy cập vào F5. Tuy nhiên cert bị báo lỗi. Trong bài này ta sẽ thực hiện import certificate xịn vào F5.

Step 1: Mua SSL certificate từ các nhà cung cấp uy tín

Ta sẽ giả lập cert xịn bằng cách tự generate từ linux ra

Dùng lệnh:

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/F5test.key -out /etc/ssl/certs/F5test.crt
```

Vào thư mục /etc/ssl/private/ thấy file key bí mật đã được tạo ra

```
-rw----- 1 root root 1704 Jul 6 13:16 F5test.key
```

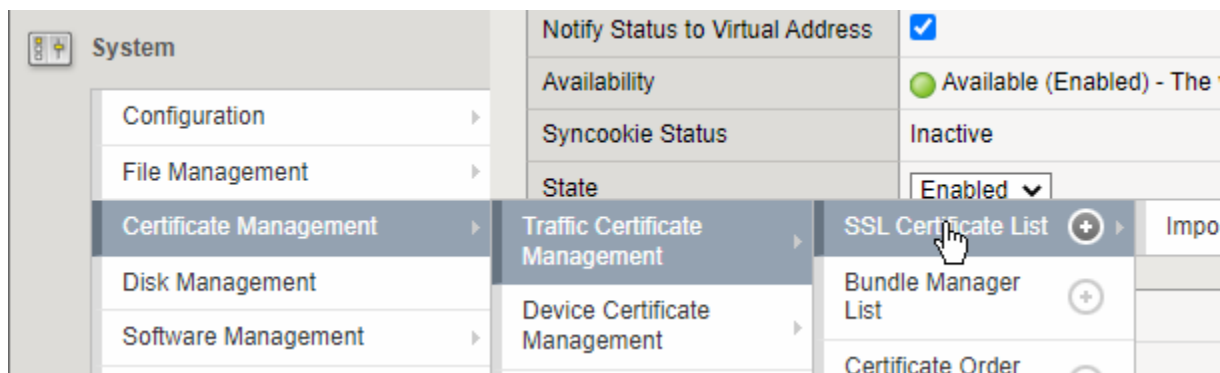
Vào thư mục /etc/ssl/certs thấy cert đã được tạo:

```
-rw-r--r-- 1 root root 1444 Jul 6 13:16 F5test.crt
```

=> Copy 2 file này ra con máy Mgmt để import vào F5

Step 2: Import 2 file key và cert trên vào F5

Vào System >... như ảnh dưới



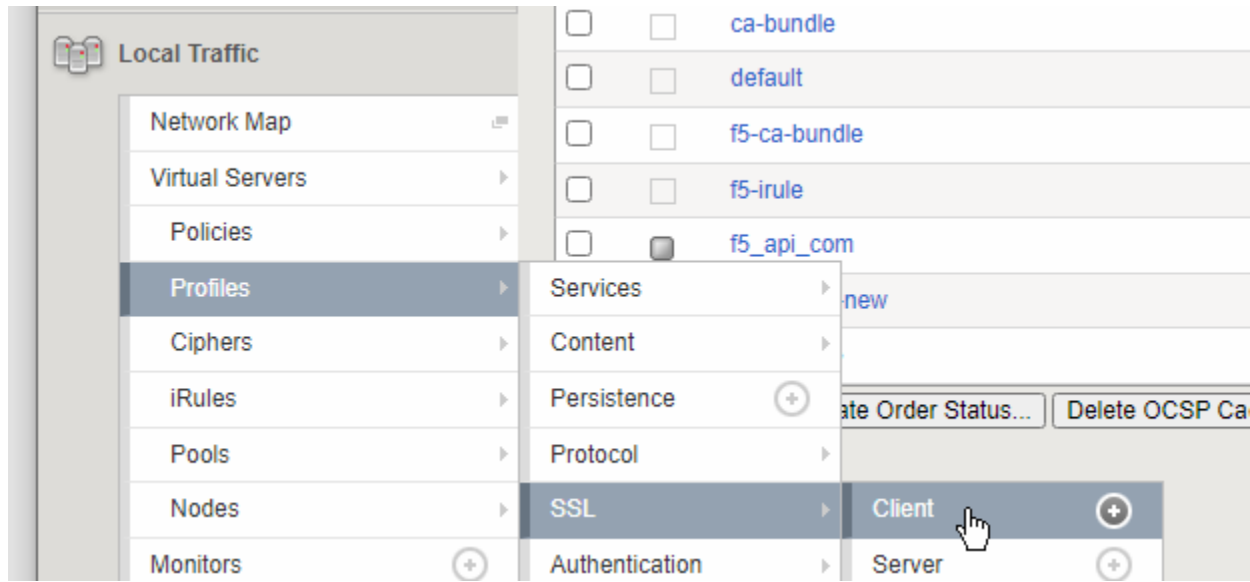
Xem thêm tại <https://hainguyenit.edubit.vn>

Sau đó chọn Import lần lượt 2 file key và cert vào, và được như này

<input type="checkbox"/>	<input type="checkbox"/>	my-hainm-new	RSA Certificate	hainm
<input type="checkbox"/>	<input type="checkbox"/>	my-key-F	RSA Key	Normal

Step 3: Tạo SSL profile trở đến 2 file key và cert mới

Vào Local Traffic >...như ảnh dưới



Chọn **Create** và điền:

Điền tên

General Properties

Name:

Parent Profile: clientssl

Configuration: Basic Custom

Certificate Key Chain: Add Edit Delete

OCSP Stapling: Add lần lượt file key và file cert

Notify Certificate Status to Virtual Server:

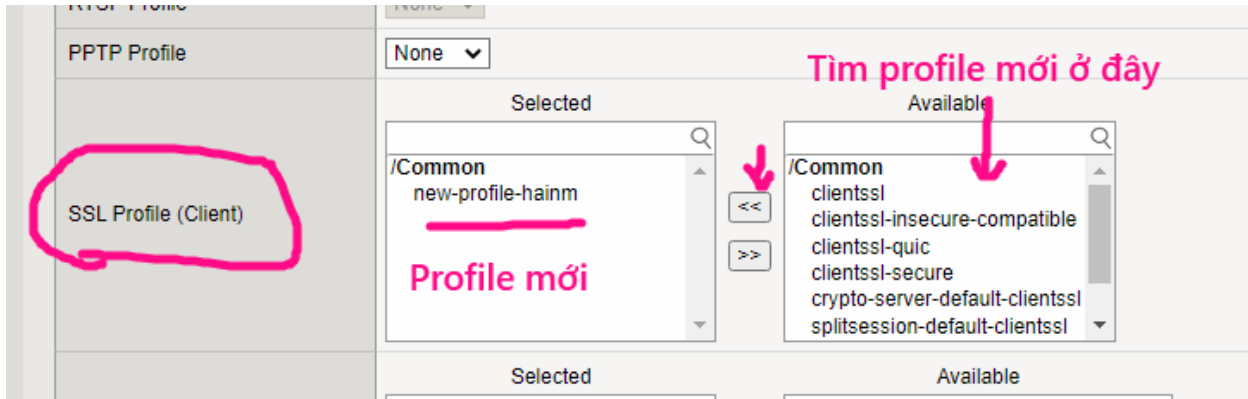
Proxy SSL:

Proxy SSL Passthrough:

Xem thêm tại <https://hainguyenit.edubit.vn>

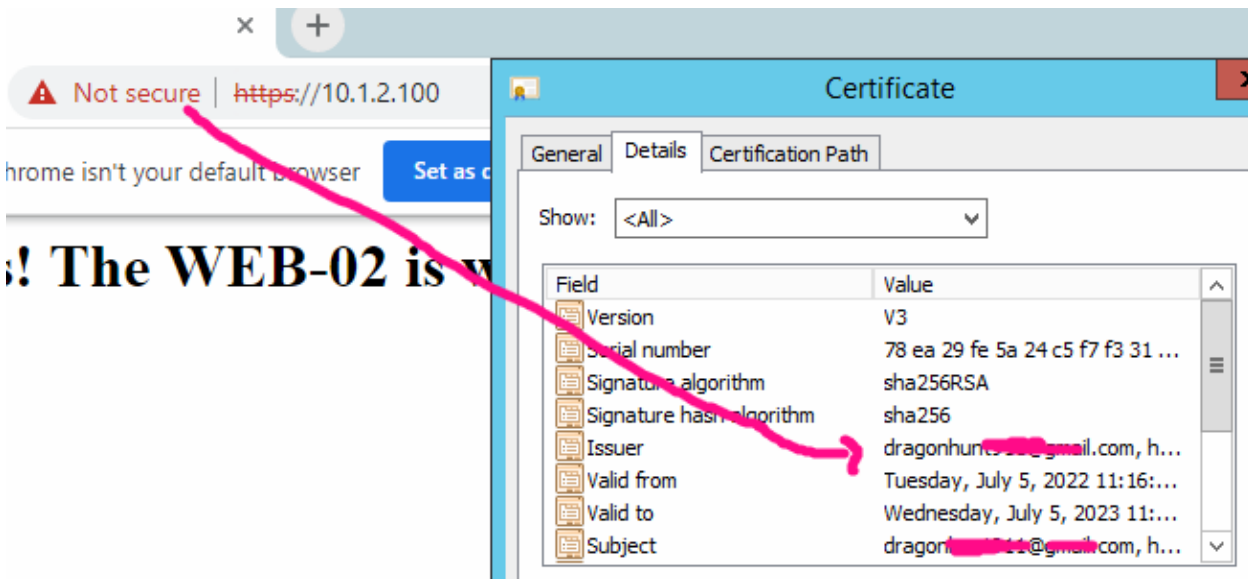
Step 4: Apply profile vừa tạo vào Virtual Server 443

Vào VS443, tìm đến mục SSL Profile(Client), tìm profile vừa tạo



Bấm Update để cập nhật

Sau đó test lại từ PC_Outside vào lại. Xem đã thấy các thông tin chứng chỉ mới chưa



Xem thêm tại <https://hainguyenit.edubit.vn>

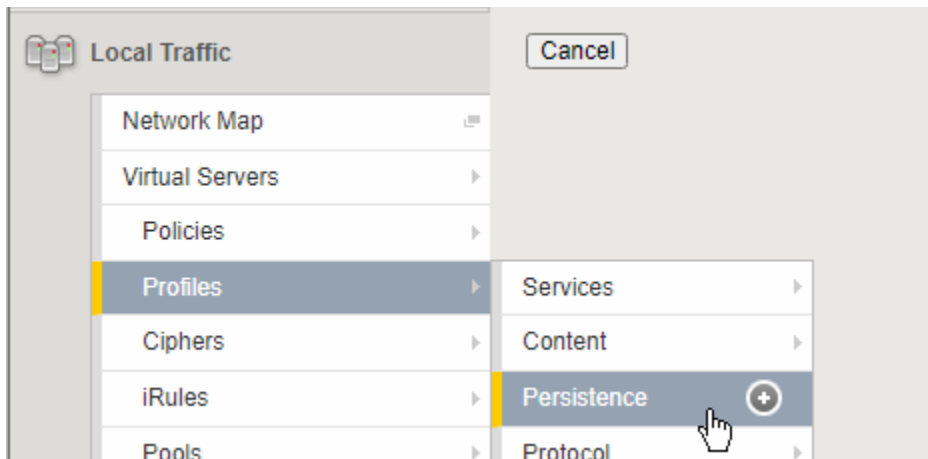
8. Persistent Session

Ví dụ 1 user đang kết nối vào webserver-01, sau đó user này tắt trình duyệt đi, rồi lại kết nối lại, thì nếu để mặc định, có thể F5 sẽ phân phối vào webserver-02.

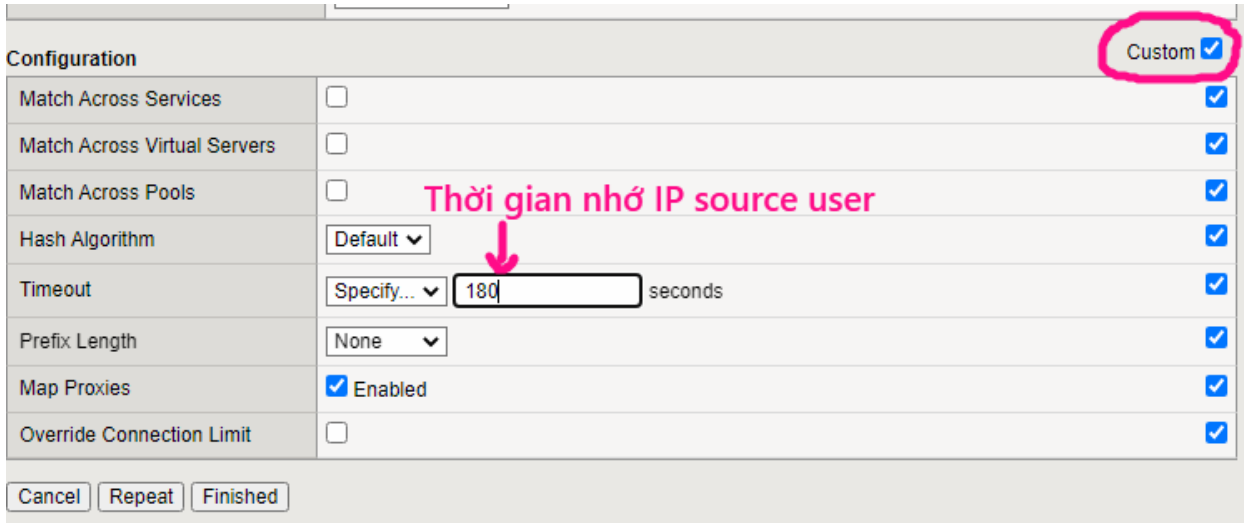
=> Điều này có thể gây gián đoạn giao dịch => Nên F5 có cơ chế nhớ session cũ (trong khoảng thời gian đặt sẵn) để khi user kết nối lại sẽ phân phối vào đúng webserver-01 ban đầu.

Step 1: Làm bài 7 đã chạy

Step 2: Vào Profiles > Persistent > Create

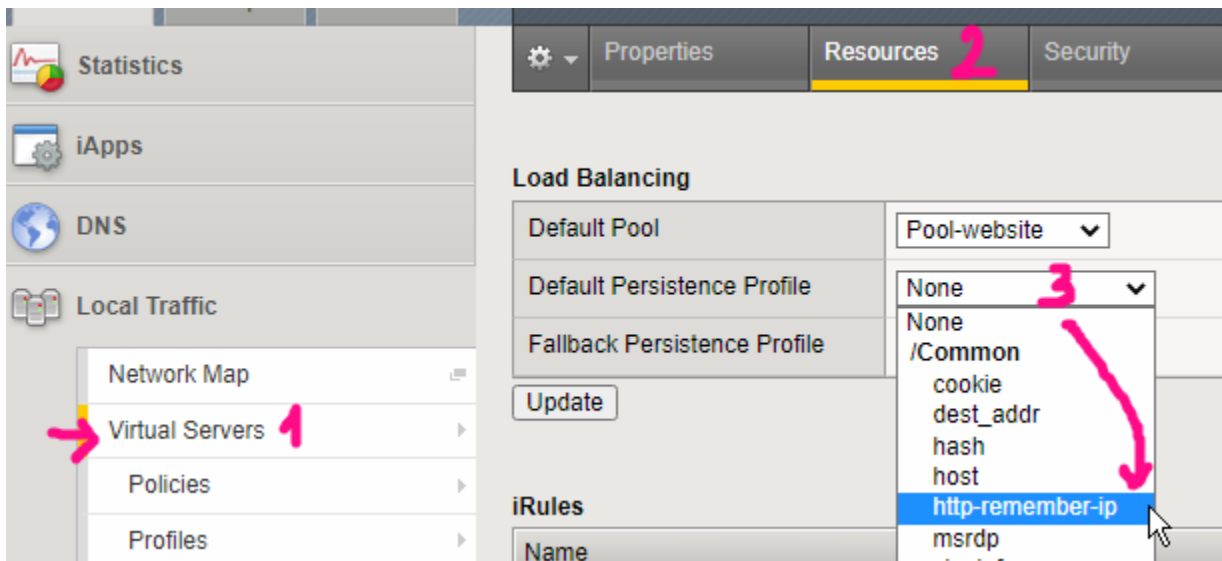


Xem thêm tại <https://hainguyenit.edubit.vn>



Bấm Finished

Step 3: Vào Virtual Server 443 sau đó chọn như hình:



Step 4: Test lại: từ PC_outside, truy cập <http://10.1.2.100> sau đó tắt trình duyệt đi đợi 10 giây; lại vào lại, refresh nhiều lần để thấy chỉ vào 1 webserver thôi.

Xem thêm tại <https://hainguyenit.edubit.vn>

9. Giải thích khác nhau Automap và SNAT

Như bài 5.3 ta đã chọn Automap thay vì Snat, bài này phân biệt giữa AutoMap và Snat.

>> **AUTOMAP**: là khi gói tin (SRC: IP user ngoài net, DST: IP Virtual Server) qua F5

sẽ được biến đổi thành (SRC: **IP LAN của F5-192.168.2.1**; DST: IP của WEBSEBER 01 hoặc 02)

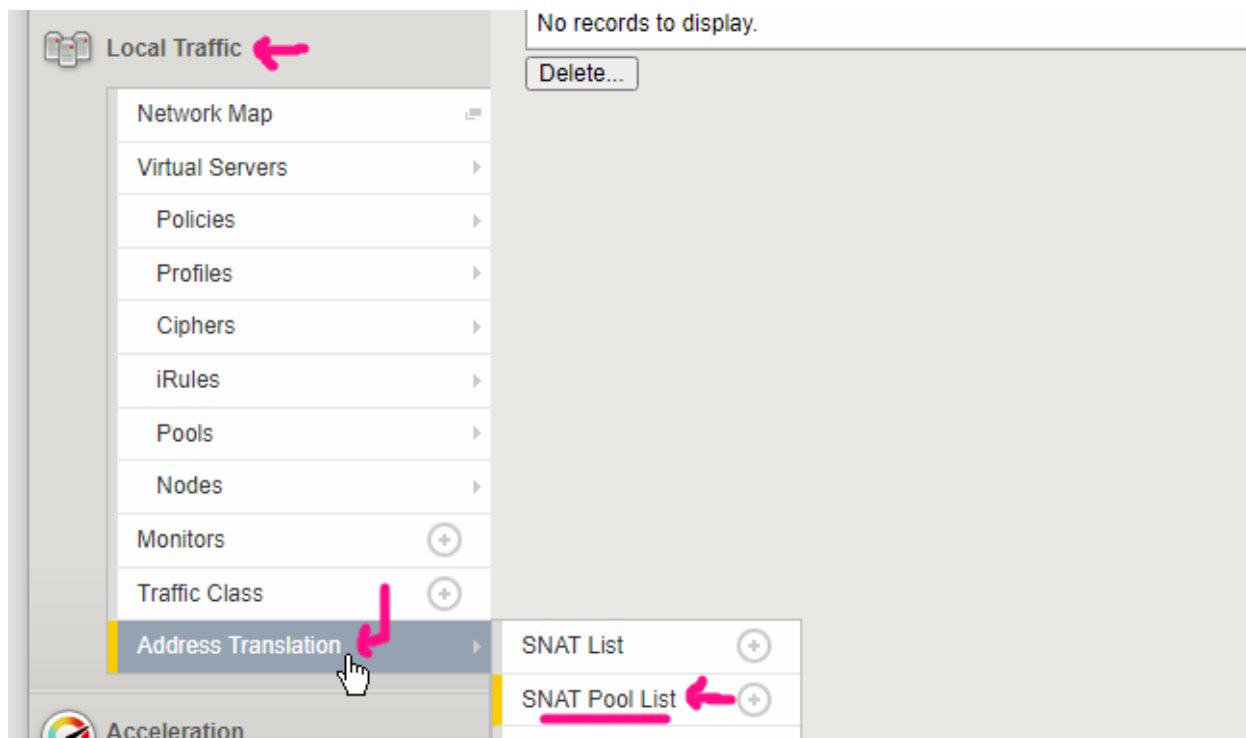
>> **SNAT**: Chỗ bôi đỏ bên trên được biến thành IP do mình chủ động đặt ra.

Ứng dụng: Nếu dùng Automap mà có trên 65335 connection đồng thời thì sẽ bị quá tải, do không đủ mỗi port cho 1 connection

Còn dùng SNAT ta có thể tạo ra nhiều IP , tránh được quá tải.

Ở đây ta sẽ test phần SNAT (tạo ra IP 192.168.2.10)

Vào Local Traffic > Address Translation > SNAT Pool List > Create



Xem thêm tại <https://hainguyenit.edubit.vn>

The screenshot shows a configuration window with two main sections: 'General Properties' and 'Configuration'. In 'General Properties', the 'Name' field contains 'snat-new-pool'. In 'Configuration', the 'IP Address' field contains '192.168.2.10'. Below this is an 'Add' button with a checkmark, followed by an empty 'Member List' table with 'Edit' and 'Delete' buttons. At the bottom, there are 'Cancel', 'Repeat', and 'Finished' buttons, with 'Finished' being highlighted by a pink arrow.

Vào Virtual Server 443 > và chọn SNAT và pool vừa tạo:

The screenshot shows a configuration window for a Virtual Server. It has three rows of settings: 'VLAN and Tunnel Traffic' set to 'All VLANs and Tunnels', 'Source Address Translation' set to 'SNAT', and 'SNAT Pool' set to 'snat-new-pool'.

Từ PC_Outside truy cập http:10.1.2.100

Kết quả đã thấy IP 192.168.2.10 được dùng

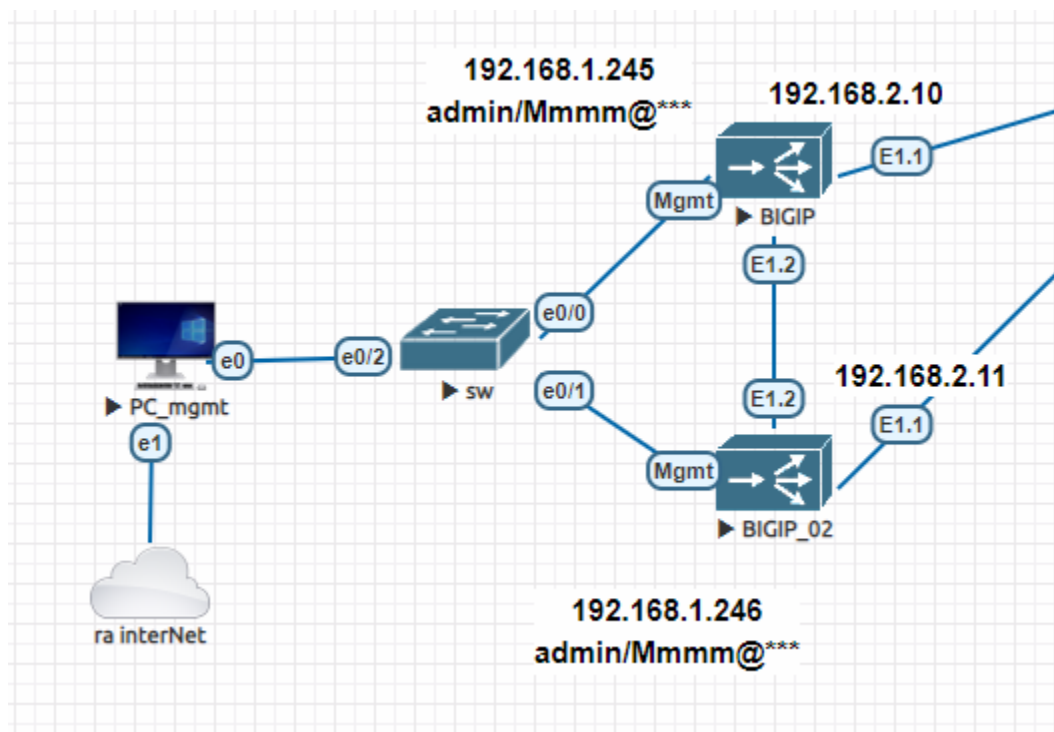
192.168.2.10	192.168.2.3	TCP	60
192.168.2.10	192.168.2.3	TCP	60
192.168.2.3	192.168.2.10	TCP	58
192.168.2.10	192.168.2.3	TCP	70
192.168.2.3	192.168.2.10	TCP	70
192.168.2.10	192.168.2.3	TCP	60
192.168.2.10	192.168.2.3	HTTP	739
192.168.2.3	192.168.2.10	TCP	58
192.168.2.3	192.168.2.10	HTTP	506
192.168.2.10	192.168.2.3	TCP	60
192.168.2.3	192.168.2.10	TCP	58

Xem thêm tại <https://hainguyenit.edubit.vn>

Step 3: Test lại: từ PC_outside truy cập <http://192.168.2.100>



11. Cấu hình HA cluster



Giả sử F5-01 đang có cấu hình từ bài trước và đang chạy, ta cần tích hợp F5-02 (chưa có cấu hình) vào để thành cluster.

Xem thêm tại <https://hainguyenit.edubit.vn>

Step 1: F5-01: Check đã Tạo vlan HA 999 và đặt IP cho nó là 1.1.1.1/30, gán vào cổng E1.2 chưa?

Tương tự F5-02, ta đặt IP Vlan HA là 1.1.1.2/30 gán vào E1.2 và vlan NOI-B0 192.168.2.11/24 gán cổng E1.1 (Đặt cả cổng mgmt là 192.168.1.246/24 nữa)

Step 2: Trên F5-01 : Bấm vào logo F5 và chọn Setup HA



Sau đó chọn:

Setup Utility

Run the Setup Utility again to make changes to basic device settings and standard network configuration.

- [Run the Setup Utility](#)
- [Run Config Sync/HA Utility](#)

Standard Network Configuration

Create a standard network configuration by configuring these features:

- Redundancy
- VLANs
- NTP
- DNS
- Config Sync
- Failover
- Mirroring
- Peer Device Discovery (for Redundant Configurations)

Next...

Redundant Device Wizard Options

Config Sync

Display configuration synchronization options

High Availability

Display failover and mirroring options

Failover Method: Network

Cancel

Next...

Xem thêm tại <https://hainguyenit.edubit.vn>

internal chính là dải LAN vừa tạo

Internal Network Configuration

Internal VLAN	<input type="radio"/> Create VLAN internal <input checked="" type="radio"/> Select existing VLAN
Select VLAN	NOIBO
Self IP	Address: 192.168.2.10 Netmask: 255.255.255.0 Port Lockdown: Allow Default
Floating IP	Address: 192.168.2.99 Port Lockdown: Allow Default

Điền IP cùng dải

Mô hình này không có external interface nên chọn “External Network” cũng là vlan NỘI-BỘ luôn.

External Network Configuration

External VLAN	<input type="radio"/> Create VLAN external <input checked="" type="radio"/> Select existing VLAN
Select VLAN	NOIBO
Self IP	Address: 192.168.2.10 Netmask: 255.255.255.0 Port Lockdown: Allow Default
Default Gateway	
Floating IP	Address: 192.168.2.99 Port Lockdown: Allow Default

BẤM NEXT

Xem thêm tại <https://hainguyenit.edubit.vn>

Tiếp đến là mục HA

High Availability Network Configuration

High Availability VLAN	<input type="radio"/> Create VLAN HA <input checked="" type="radio"/> Select existing VLAN
Select VLAN	VLAN-HA
Self IP	Address: 1.1.1.1 Netmask: 255.255.255.252

High Availability VLAN Configuration

VLAN Name	VLAN-HA
VLAN Tag ID	999
Interfaces	VLAN Interfaces: 1.1 Tagging: Select... Add 1.2 (tagged) Edit Delete

Cancel Next...

NTP:

Network Time Protocol Configuration

Điền NTP nếu có, không thì next

Address:	
Add	


DNS: Điền vào, mục nào không có thì để trống, và next tiếp

Xem thêm tại <https://hainguyenit.edubit.vn>

ConfigSync Configuration

Local Address	1.1.1.1 (VLAN-HA) ▼
---------------	---------------------

Cancel Next...



Đồng bộ config qua IP HA

Management Failover Unicast Configuration

Address Family Mode	IPv4 & IPv6 ▼
---------------------	---------------

Failover Unicast Configuration


<input checked="" type="checkbox"/> ▲ Local Address
<input type="checkbox"/> 1.1.1.1
<input type="checkbox"/> Management Address

Delete

Failover Multicast Configuration

Use Failover Multicast Address	<input type="checkbox"/> Enabled
--------------------------------	----------------------------------


Cancel Next...



Mirroring Configuration

Primary Local Mirror Address	1.1.1.1 (VLAN-HA) ▼
Secondary Local Mirror Address	None ▼

Cancel Next...




Standard Pair Configuration

Establish an Active/Standby pair by discovering another device.

After discovering the other device, the system performs the following actions:

- Establishes trust between this device and the peer or subordinate device
- Creates a device group that contains this device and the peer or subordinate device
- Creates a traffic group that supports an active/standby configuration

Next...



Xem thêm tại <https://hainguyenit.edubit.vn>

Discover Configured Peer or Subordinate Device

If you have already configured a peer or subordinate device for this active/standby pair high availability, and create a traffic group that supports active/standby configuration.

Next...

Retrieve Device Credentials (Step 1 of 3)

Device Type	Peer
Device IP Address	1.1.1.2
Administrator Username	admin
Administrator Password

Cancel Retrieve Device Information

IP HA của con số 2

user/pass của nó

Verify Device Certificate (Step 2 of 3)

Subject	/C=--/ST=WA/L=Seattle/O=MyCompar
Management IP Address	1.1.1.2
Expiration	Sun Jul 05 10:23:52 HKT 2032
Serial Number	9864a216d83c9c32
Signed	Yes
SHA-1	8236e05e5752fbe9a2303e636303152
MD5	a0b3a26be092df6f2a0b7d417d84598t

Cancel Device Certificate Matches

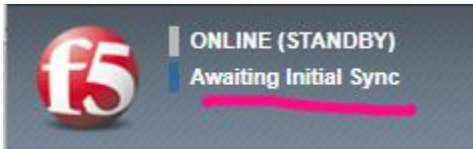
Add Device (Step 3 of 3)

Device Name	f5-02.local
Sync-Failover Group Name	device-group-failover-3801b27e3605

Cancel Add Device

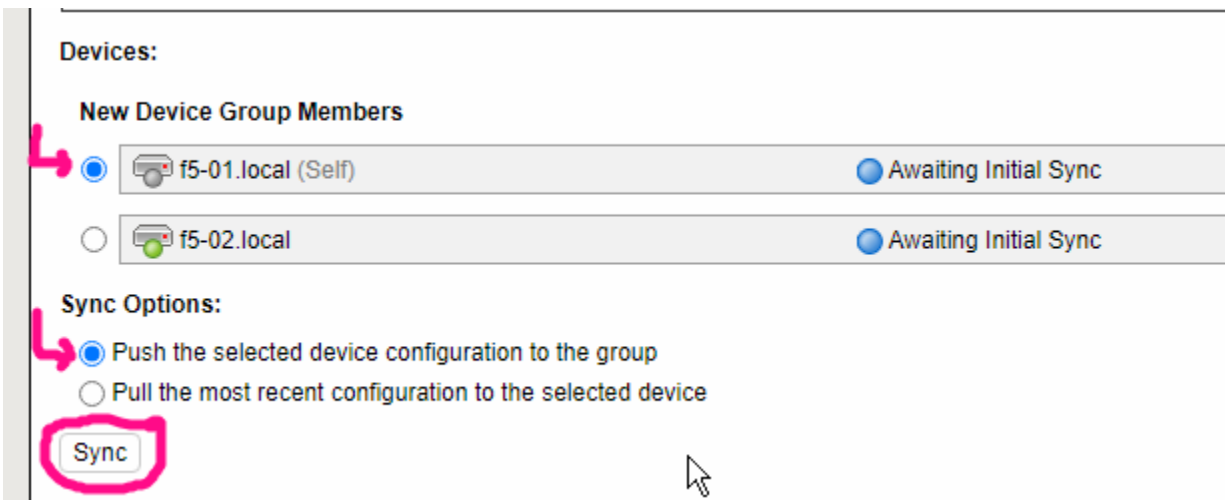
Xem thêm tại <https://hainguyenit.edubit.vn>

Sau đó thấy 2 thiết bị F5 hiện như này, chờ ta nhấn đồng bộ cấu hình:



Để đồng bộ cấu hình, trên **F5 nào active**, ta vào **Device Management > Overview**

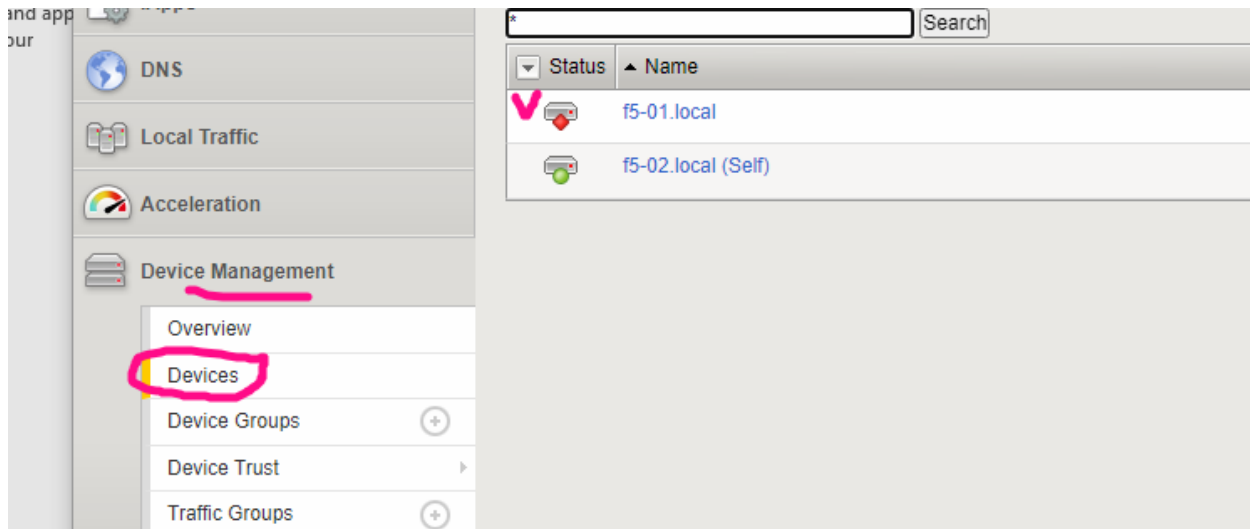
Sau đó chọn F5-01 và push cấu hình sang F5-02,



DONE, CHECK CẤU HÌNH 2 BÊN ĐÃ ĐỒNG BỘ.

NOTE: Làm trên lab ảo thấy bị hiện tượng: F5-02 luôn coi F5-01 là offline (dù ping ok), và F5-02 luôn là active; kể cả force standby thì chỉ 1 lúc sau F5-02 lại lên active (ko biết vì sao, ở ngoài thật thì không bị)

Xem thêm tại <https://hainguyenit.edubit.vn>



- >> Các virtual server(VS) tạo trên F5-01 ban đầu; khi F5-02 làm active thì user bên ngoài không vào được. Chỉ vào được khi off F5-02 đi
- >> Các VS tạo mới trên F5-02 thì user vào ok