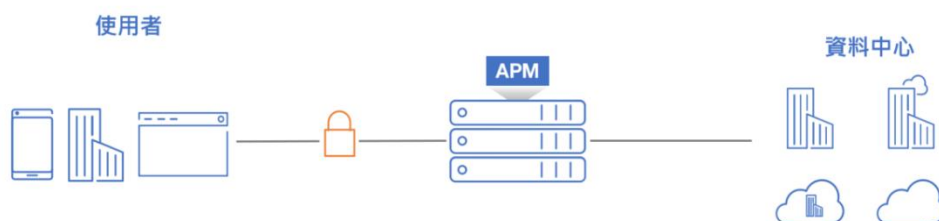


F5 APM SSL-VPN 簡易配置手冊

一、常見架構



二、基礎配置

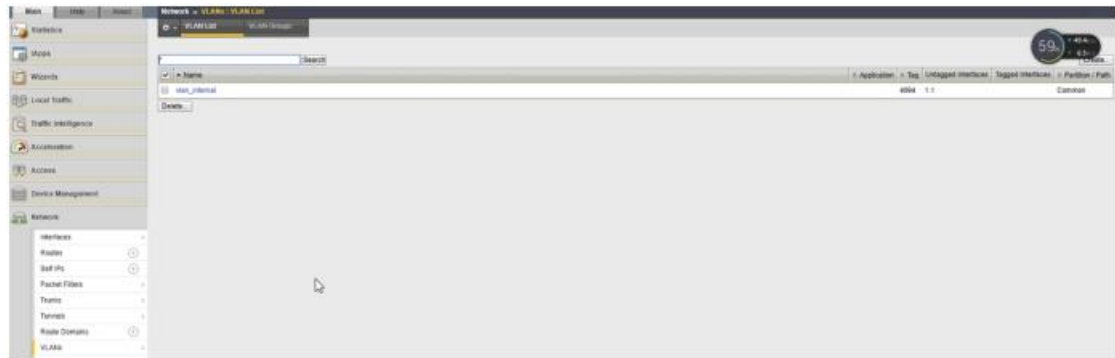
啟動 License

➤ 如下圖所示，啟動 APM 模組 license

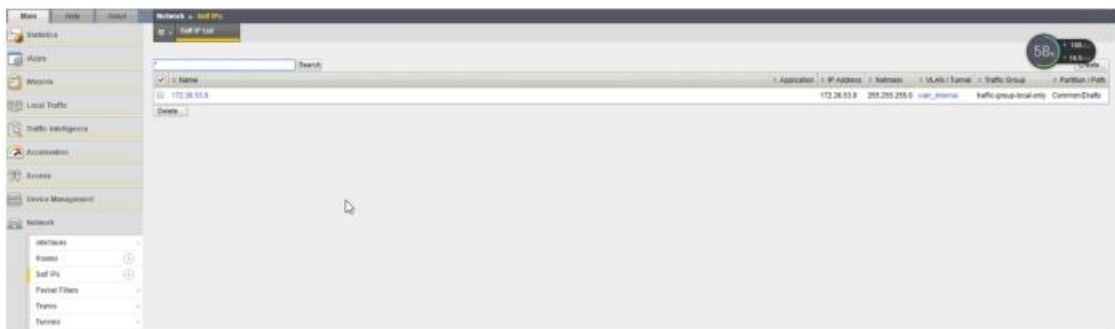
Module	Provisioning	License Status	Required Disk (GB)	Required Memory (MB)
Management (MOMT)	Small	N/A	0	1264
Carrier Grade NAT (CGNAT)	Disabled	Unlicensed	0	0
Local Traffic (LTM)	None	Unlicensed	0	1800
Application Security (ASM)	None	Unlicensed	20	1462
Fraud Protection Service (FPS)	None	N/A	12	544
Global Traffic (DNS)	None	Unlicensed	0	148
Link Controller (LC)	None	Unlicensed	0	148
Access Policy (APM)	IP Normal	Licensed	13	494
Application Visibility and Reporting (AVR)	None	Licensed	16	676
Policy Enforcement (PEM)	None	Unlicensed	16	1223
Advanced Firewall (AFM)	None	Unlicensed	16	1050
Application Acceleration Manager (AAM)	None	Unlicensed	32	2050
Secure Web Gateway (SWG)	None	Unlicensed	24	4056
Rules Language Extensions (RULEX)	None	Licensed	0	748
URLDB Mirror (URLDB)	None	Unlicensed	36	2048

網路配置

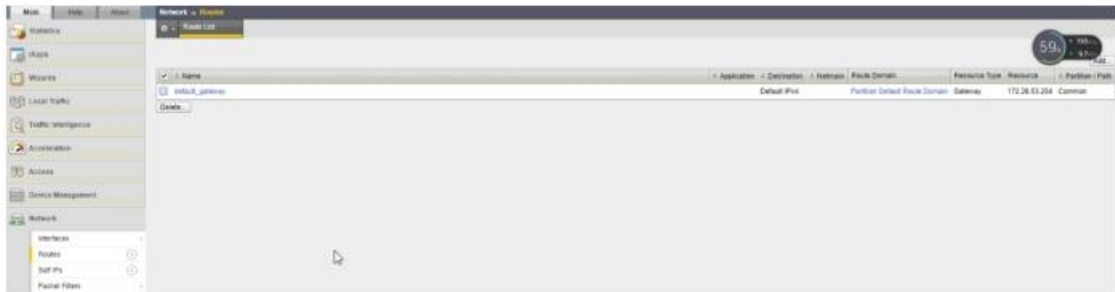
➤ 如下圖所示，配置 vlan



➤ 如下圖所示，配置 Selfip 介面位址



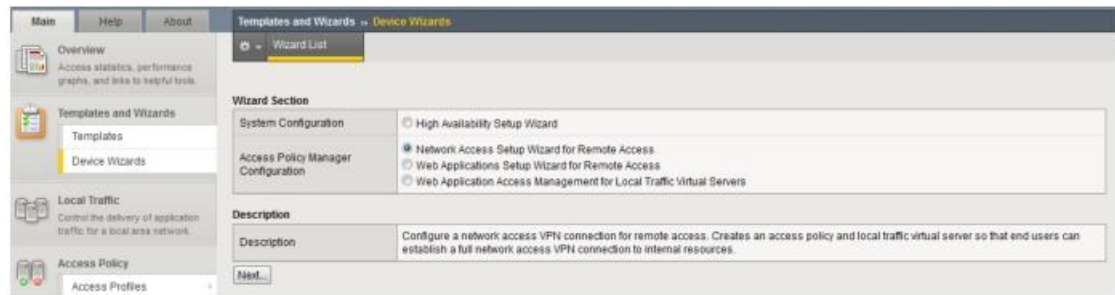
➤ 如下圖所示，配置預設路由



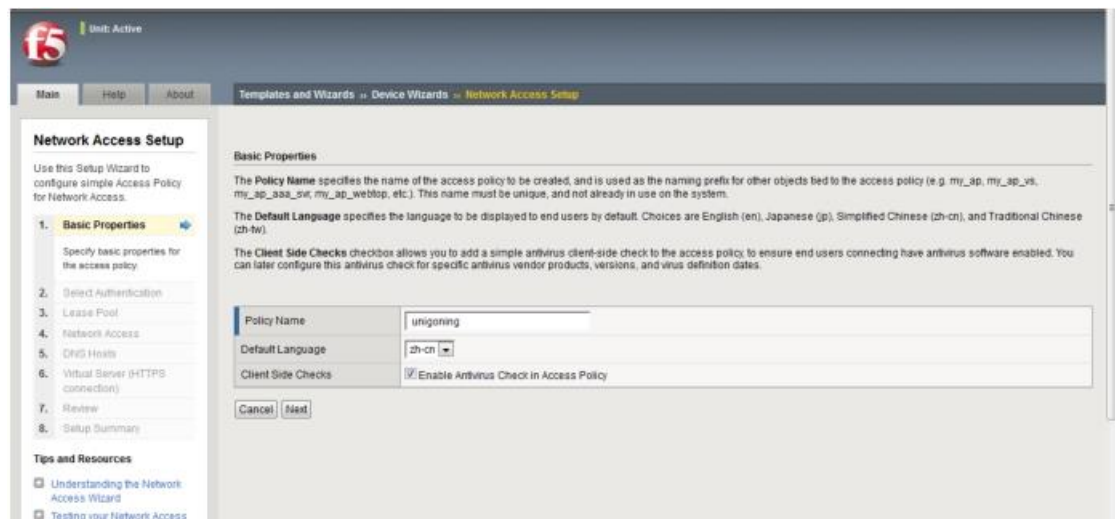
三、 通過範本實現 F5-APM SSLVPN 基本功能

在本例中我們將通過 F5-APM 的範本功能，簡單快速的搭建出一套可以實現 SSLVPN 基本功能的系統。

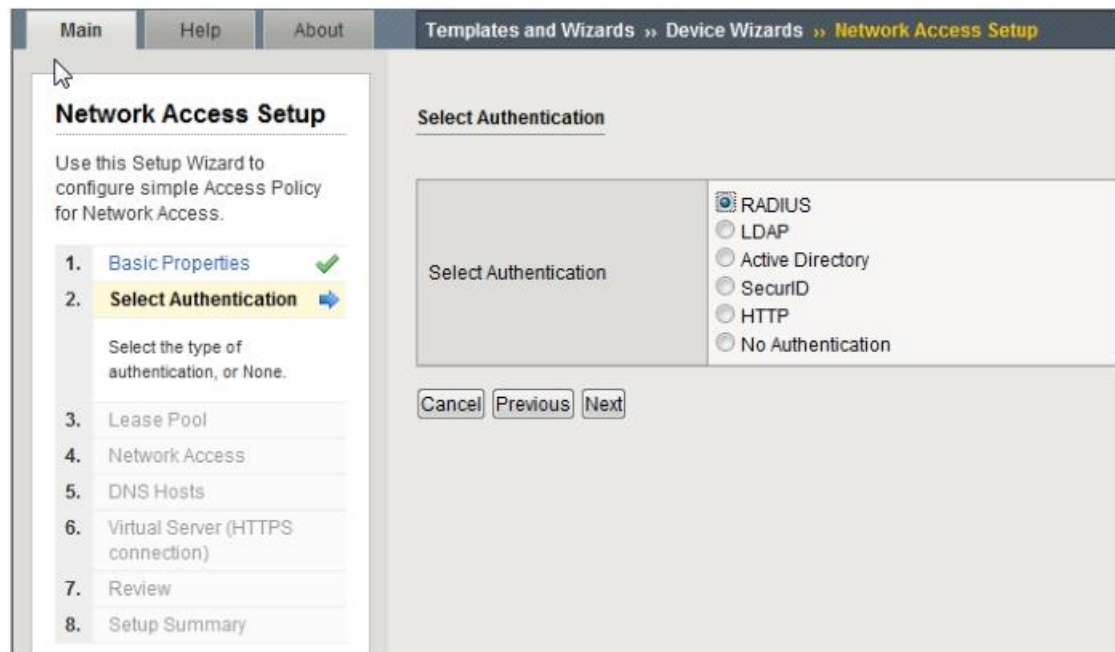
1、選擇 Access Policy Manager Configuration---Network Access Setup Wizard for Remote Access。



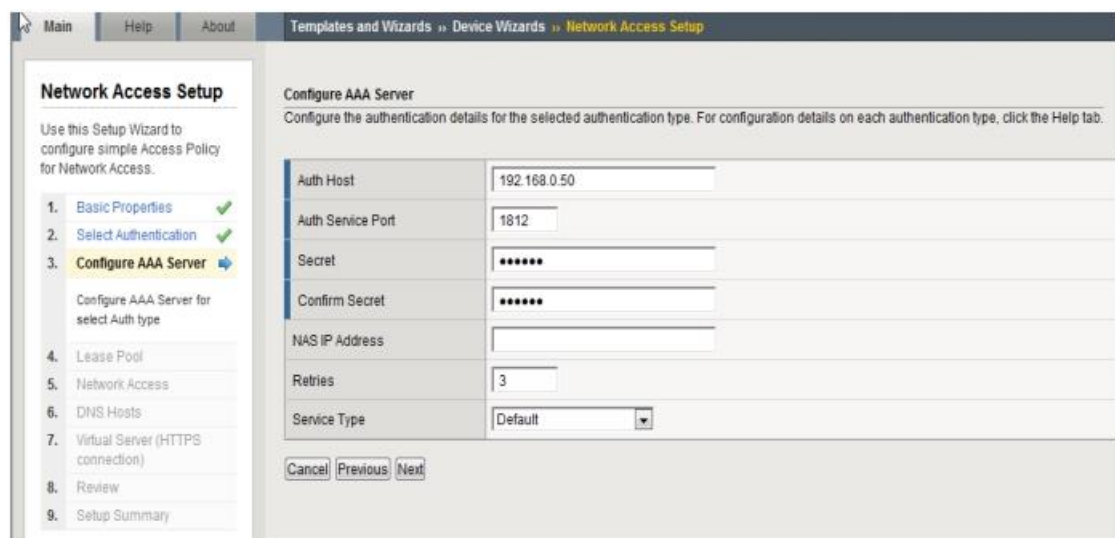
2、填寫 SSLVPN 名稱及語言類型，選擇是否用戶端檢查病毒檢查。



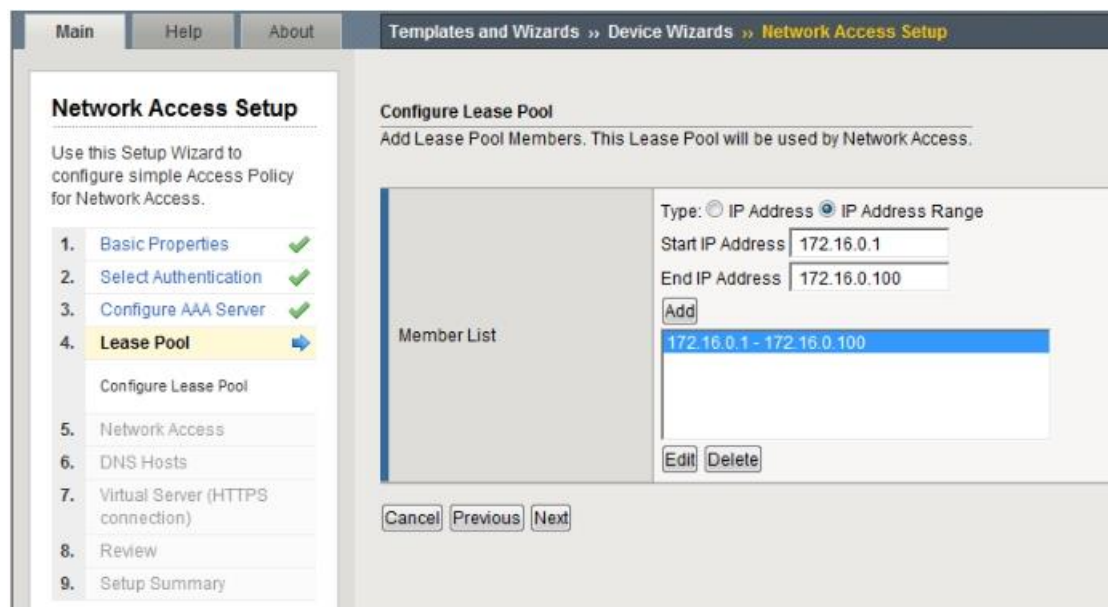
3、選擇所需的 AAA 認證方式。



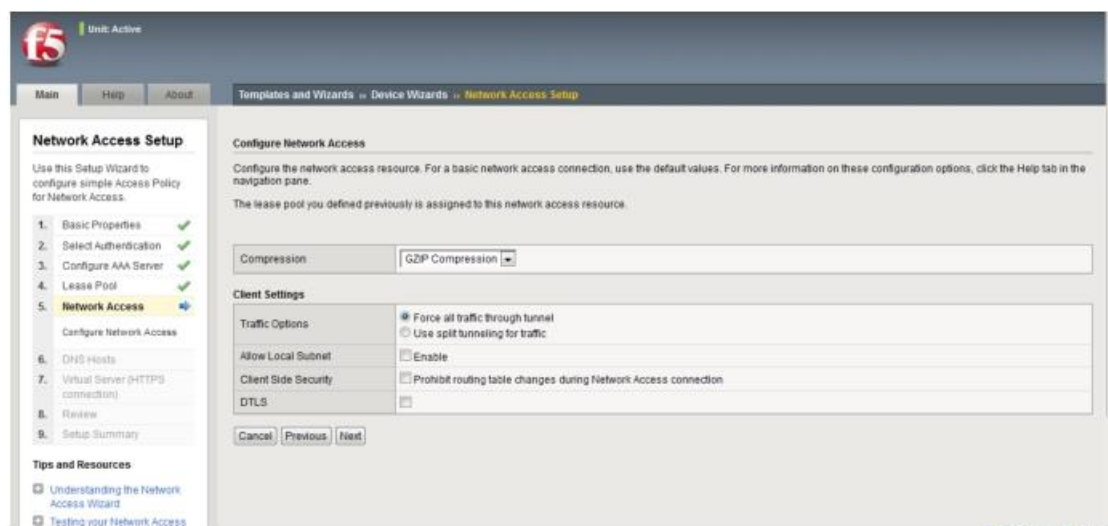
4、填寫 AAA 認證資訊。



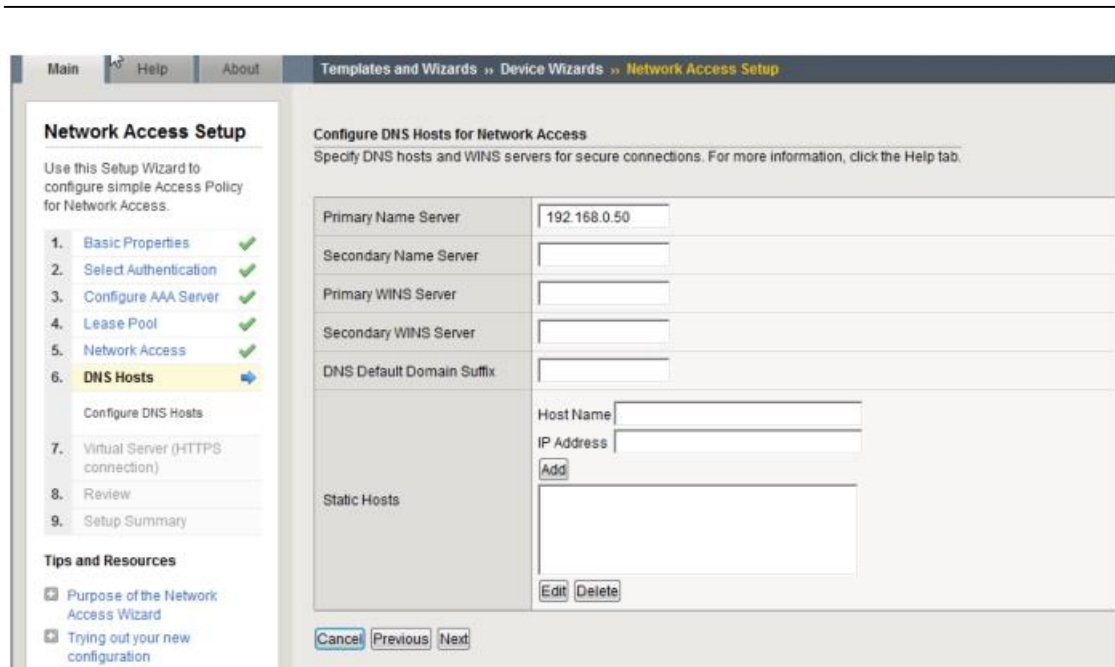
5、填寫 Lease pool 資訊



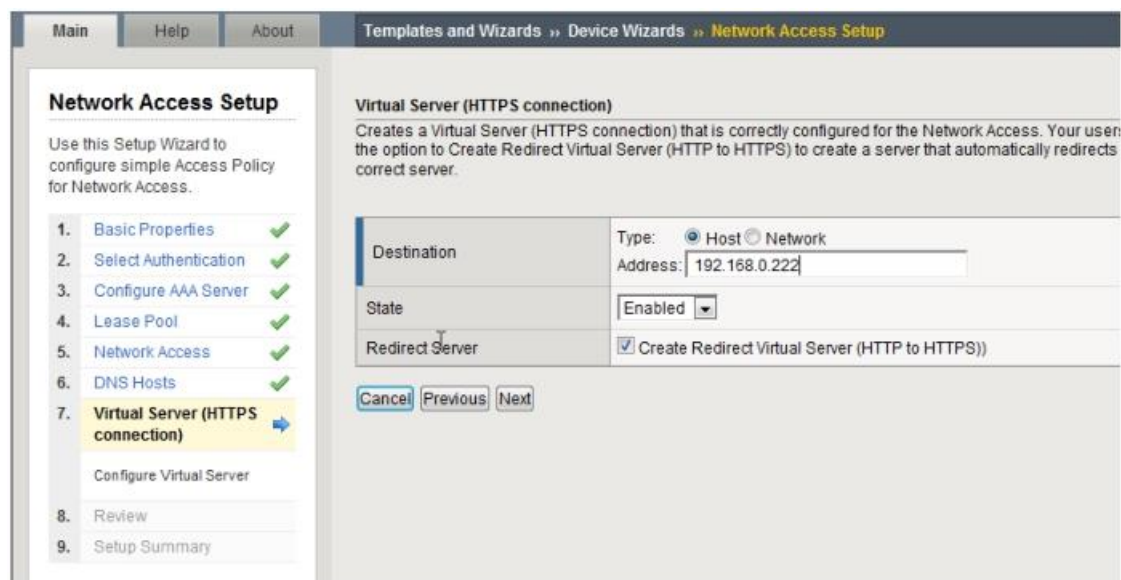
6、配置 Network Access 資訊。



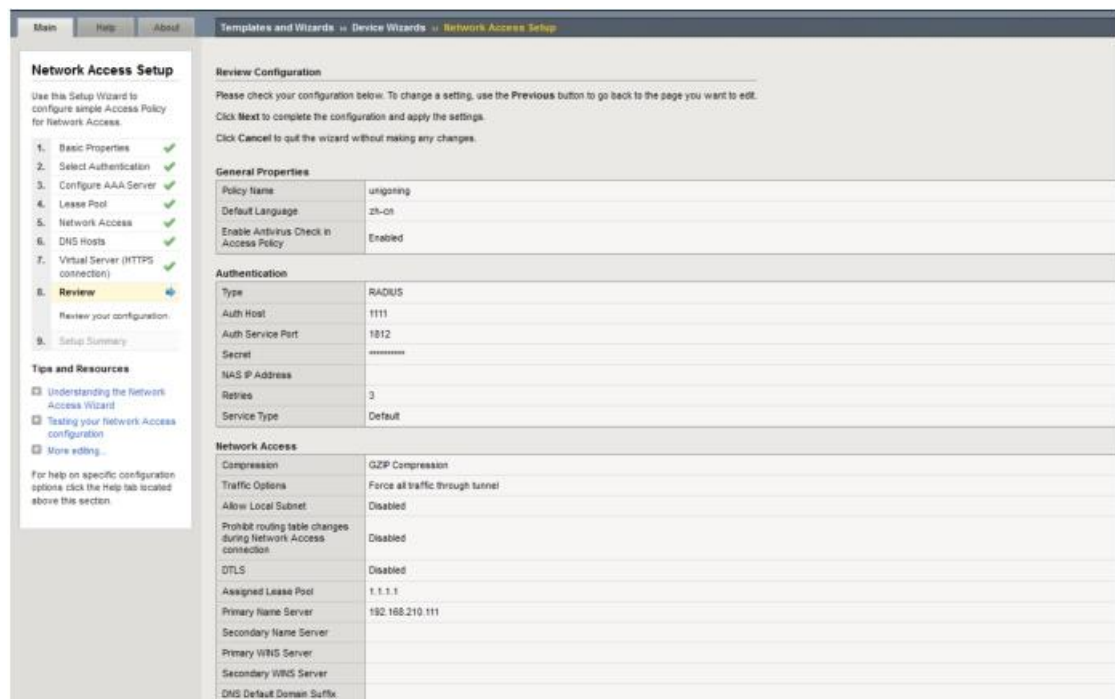
7、填寫 DNS 資訊。



8、配置 SSLVPN 相應 VS 資訊。



9、範本完成後，SSLVPN 資訊。



總結：

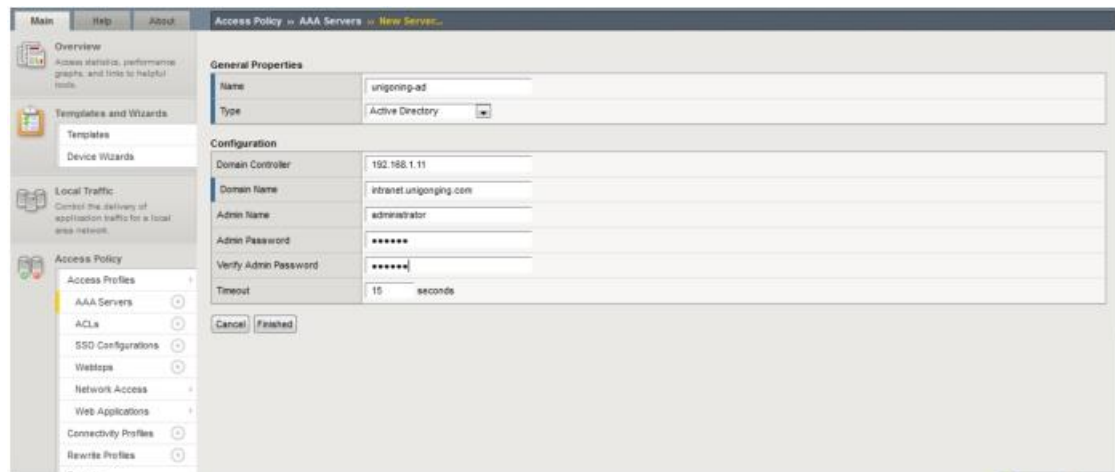
通過範本可簡單直觀的完成 APM 的 SSLVPN 的基礎搭建；實例中此時已可實現 RADIUS 單因子認證方式登錄。

二、F5-APM 雙因數認證

在本例中我們將通過配置 APM，實現通過雙因數認證方式訪問並使

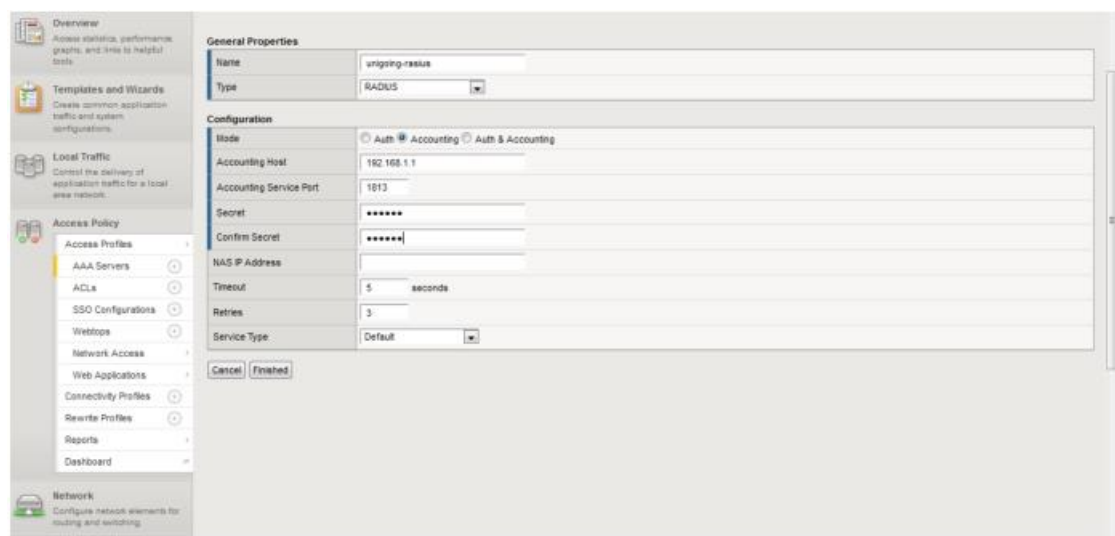
用 SSLVPN 資源。

1、填寫 AAA 認證 AD 域資訊。



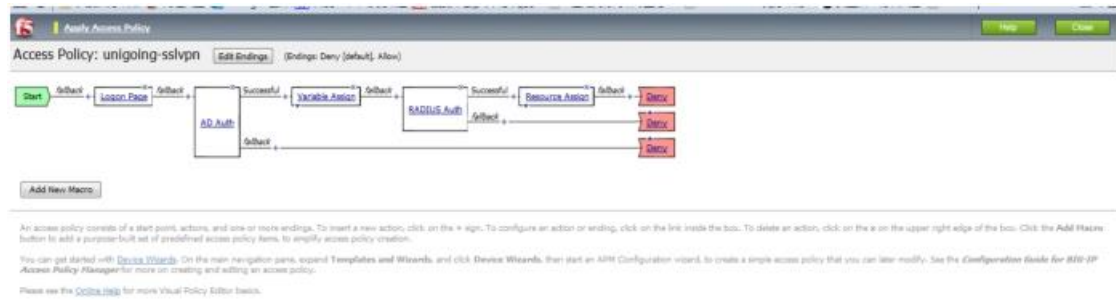
The screenshot shows the configuration page for a new AAA server. The left sidebar contains navigation options: Overview, Templates and Wizards, Local Traffic, Access Policy (with sub-items: Access Profiles, AAA Servers, ACLs, SSO Configurations, Webtops, Network Access, Web Applications, Connectivity Profiles, Rewrite Profiles), and Network. The main content area is titled 'Access Policy > AAA Servers > New Server...'. It is divided into 'General Properties' and 'Configuration' sections. The 'General Properties' section includes fields for Name (unigong-ad) and Type (Active Directory). The 'Configuration' section includes fields for Domain Controller (192.168.1.11), Domain Name (intranet.unigong.com), Admin Name (administrator), Admin Password (masked with asterisks), Verify Admin Password (masked with asterisks), and Timeout (15 seconds). At the bottom of the configuration area are 'Cancel' and 'Finished' buttons.

2、填寫 AAA 認證 RADIUS 資訊



The screenshot shows the configuration page for a new AAA server. The left sidebar is identical to the previous screenshot. The main content area is titled 'Access Policy > AAA Servers > New Server...'. It is divided into 'General Properties' and 'Configuration' sections. The 'General Properties' section includes fields for Name (unigong-radius) and Type (RADIUS). The 'Configuration' section includes radio buttons for Mode (Auth, Accounting, Auth & Accounting), with 'Auth' selected. Other fields include Accounting Host (192.168.1.1), Accounting Service Port (1813), Secret (masked with asterisks), Confirm Secret (masked with asterisks), NAS IP Address, Timeout (5 seconds), Retries (3), and Service Type (Default). At the bottom of the configuration area are 'Cancel' and 'Finished' buttons.

3、配置完成後的 Access policy 資訊。



4、配置 Logon Page 資訊，除預設設置外需要額外添加一條 Password 資訊，在 Post Variable Name 及 Session Variable Name 中填寫與 Variable Assign 中相對應的變數名。

Analyze Access Policy

Access Policy: unigoing-sslvpn (Endings: Deny (default), Allow)

Properties | [Expand Rules](#)

Name: Logon Page

Logon Page Agent			
Type	Post Variable Name	Session Variable Name	Read Only
1 text	Username	Username	No
2 password	password	password	No
3 password	Lpassword	Lpassword	No
4 none	field4	field4	No
5 none	field5	field5	No

Customization

Language: zh-cn [Reset all defaults](#)

Form Header Text: F5 Networks ebro 安全牆

Logon Page Input Field #1: 用戶名

Logon Page Input Field #2: 密碼

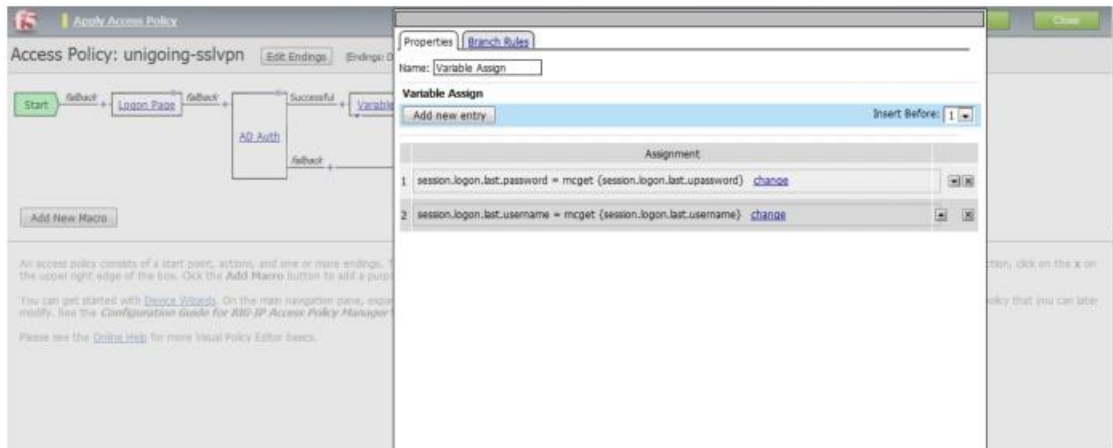
Logon Page Input Field #3: 驗證碼

Logon Page Input Field #4: 按鈕 4

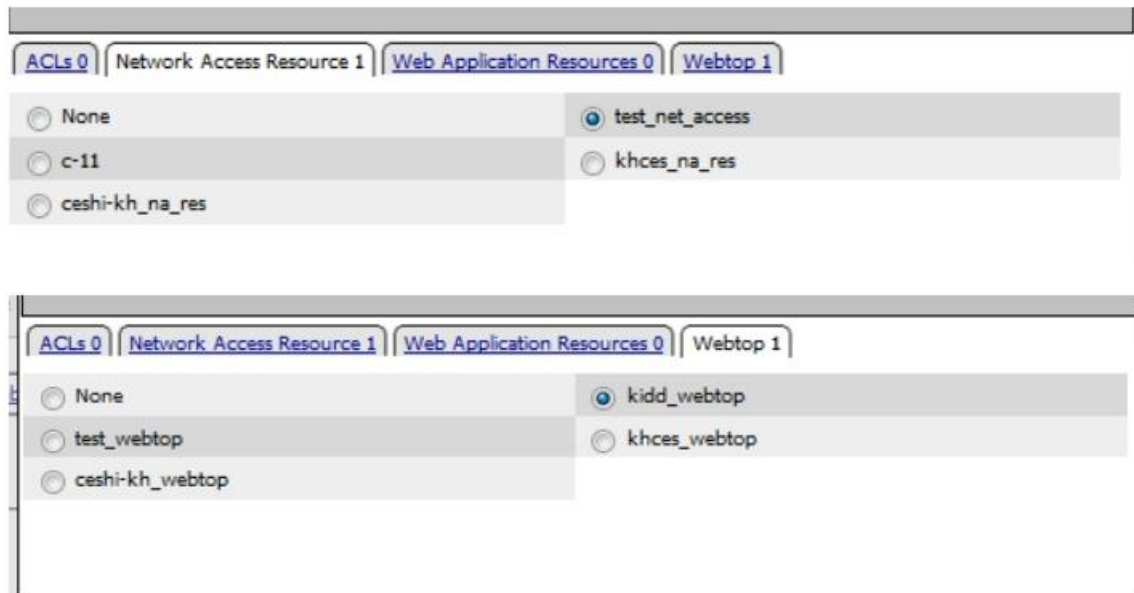
Logon Page Input Field #5: 按鈕 5

Cancel Save Help

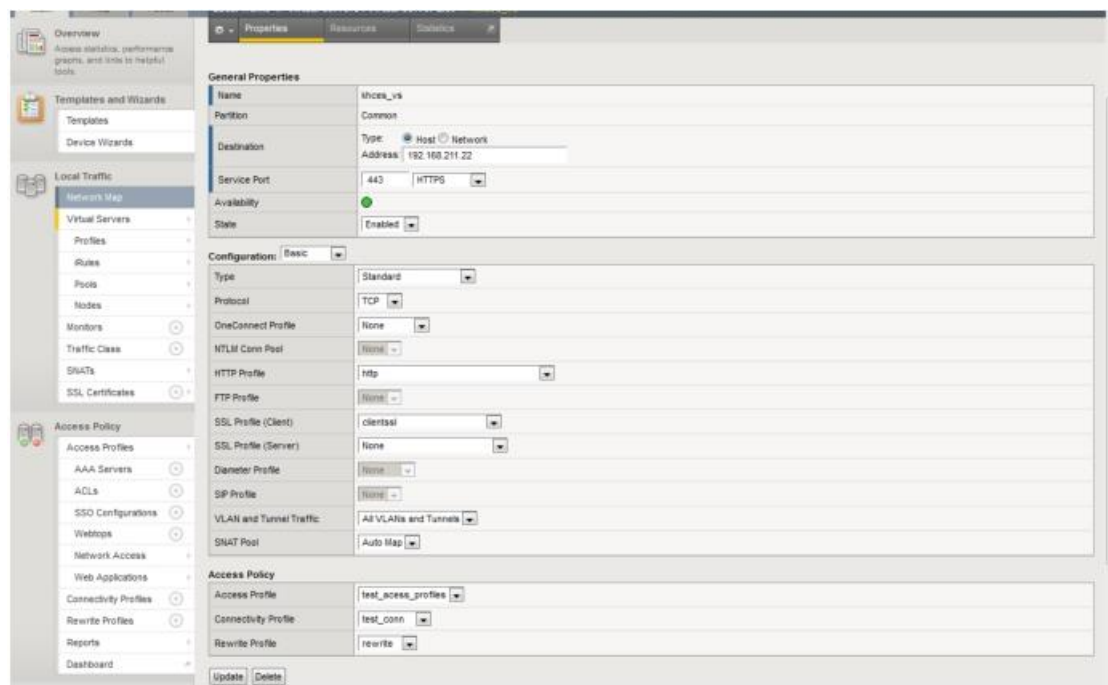
5、按照 Logon Page 中新建 Password 變數名，填寫 Variable Assign 中變數資訊。



6、選擇 Resource Assign 資訊



7、配置 SSLVPN VS 資訊。



8、配置完成後，APM 雙因數登陸介面。

總結

通過上述配置即可完成 APM 的雙因子登陸；實例中使用 AD 域及 RADIUS 認證方式完成雙因子認證登陸，其他認證方式配置方法基本相同。

