



國家高速網路與計算中心

TWAREN SSL-VPN建置與使用說明

報告人：林孟璋 6/10/2010

大綱

- 前言
- TWAREN SSL-VPN系統架構
- Cisco ASA-5550系統
- Juniper SA-6500系統
- 使用說明
- 管理者介面與SSL-VPN for iOS

前言

SSL-VPN使用時機

- 出差時，連回校內讀取圖書資源(ex：電子期刊)
- 校本部與分校的校園網路連接
- 專屬網路建置(ex：防災網路、Native IPv6 網路)
- 校園IP 不足時利用SSL-VPN 做IP 動態的分配
- ...

前言

TWAREN SSL-VPN建置日誌

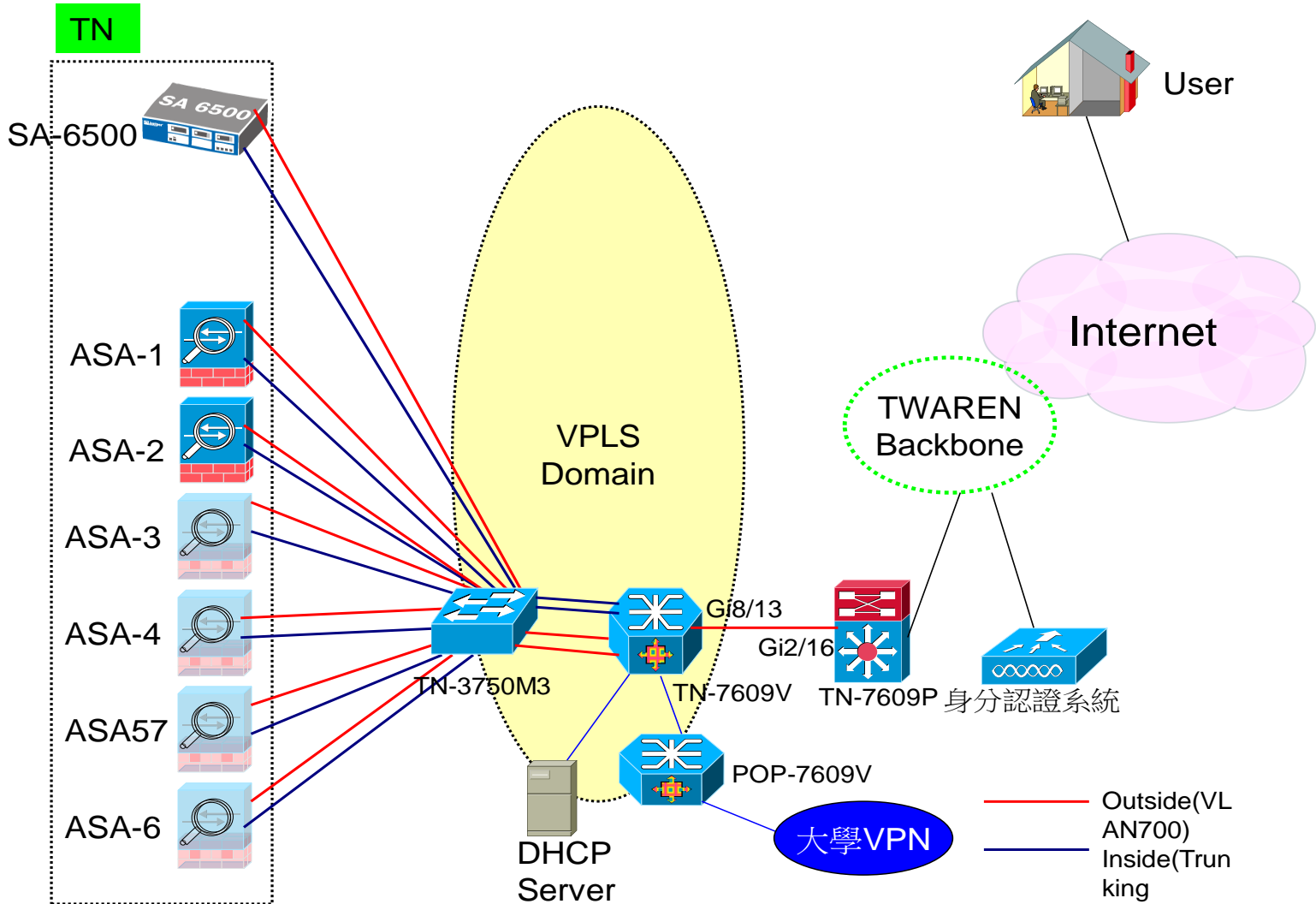
■ 2009/01 Cisco ASA-5550對外服務

系統由8部Cisco ASA 5550設備所組成，其中TWAREN南科機房有6部，TWAREN竹科機房有2部，設定為Cluster架構以提高系統之可用率。

■ 2010/08 Juniper SA-6500對外服務

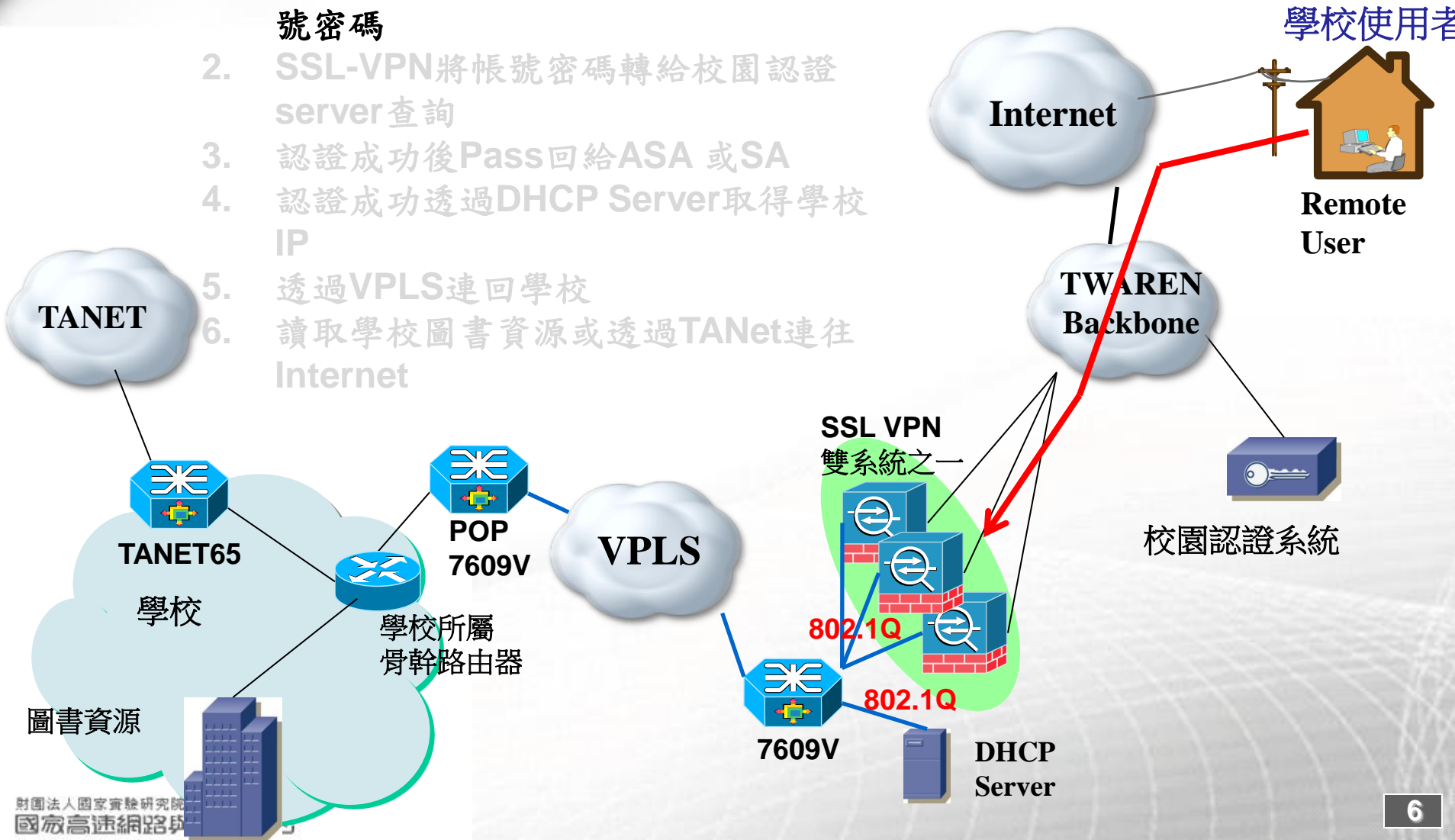
為提升服務品質與日漸增加連線單位需求，新建置1台可提供5000人使用之SA-6500，並提供良好的管理與設定介面。

TWAREN SSL-VPN系統架構



連線單位使用SSL-VPN服務-1

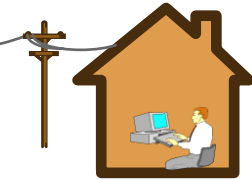
1. RemoteUser先連入SSL-VPN輸入帳號密碼
2. SSL-VPN將帳號密碼轉給校園認證server查詢
3. 認證成功後Pass回給ASA 或SA
4. 認證成功透過DHCP Server取得學校IP
5. 透過VPLS連回學校
6. 讀取學校圖書資源或透過TANet連往Internet



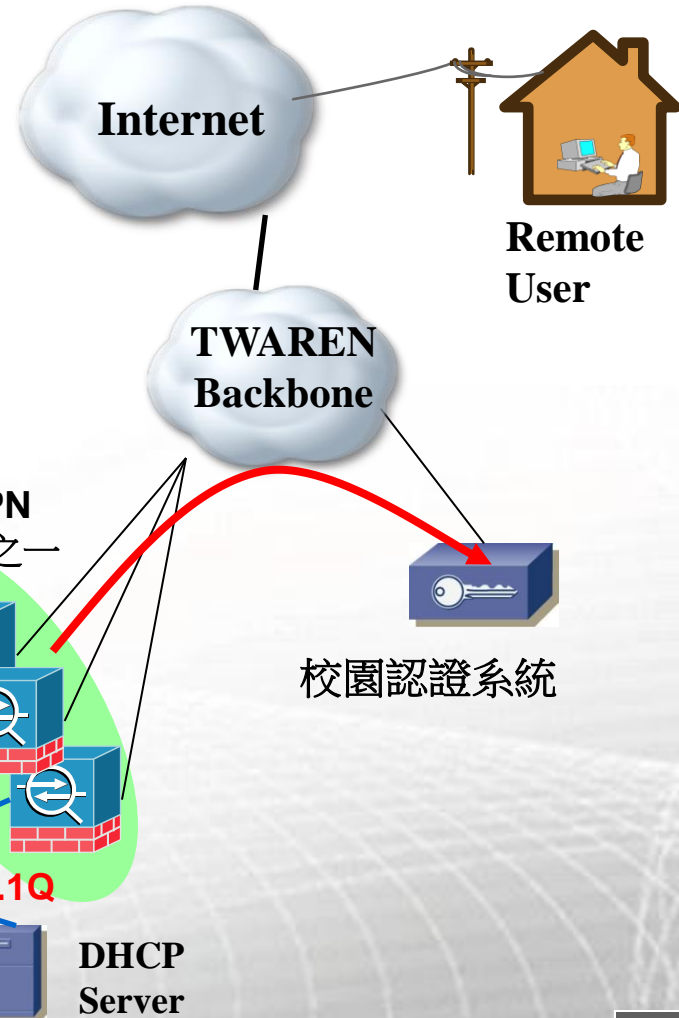
連線單位使用SSL-VPN服務-2

1. RemoteUser先連入SSL-VPN輸入帳號密碼
2. **SSL-VPN將帳號密碼轉給校園認證server查詢**
3. 認證成功後Pass回給ASA 或SA
4. 認證成功透過DHCP Server取得學校IP
5. 透過VPLS連回學校
6. 讀取學校圖書資源或透過TANet連往Internet

學校使用者



Remote User



Internet

TWAREN Backbone

SSL VPN 雙系統之一

校園認證系統

802.1Q

802.1Q

7609V

DHCP Server

TANET

TANET65

學校

圖書資源

POP 7609V

學校所屬
骨幹路由器

VPLS

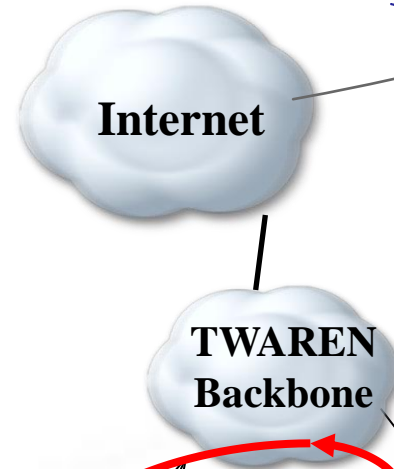
連線單位使用SSL-VPN服務-3

1. RemoteUser先連入SSL-VPN輸入帳號密碼
2. SSL-VPN將帳號密碼轉給校園認證server查詢
3. 認證成功後Pass回給ASA 或SA
4. 透過VPLS連回學校
5. 讀取學校圖書資源或透過TANet連往Internet

學校使用者

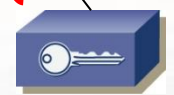


Remote User



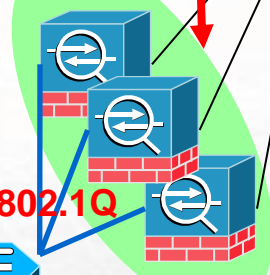
Internet

TWAREN Backbone



校園認證系統

SSL VPN
雙系統之一



802.1Q

802.1Q



7609V



DHCP Server



VPLS



POP
7609V

學校所屬
骨幹路由器



TANET



TANET65

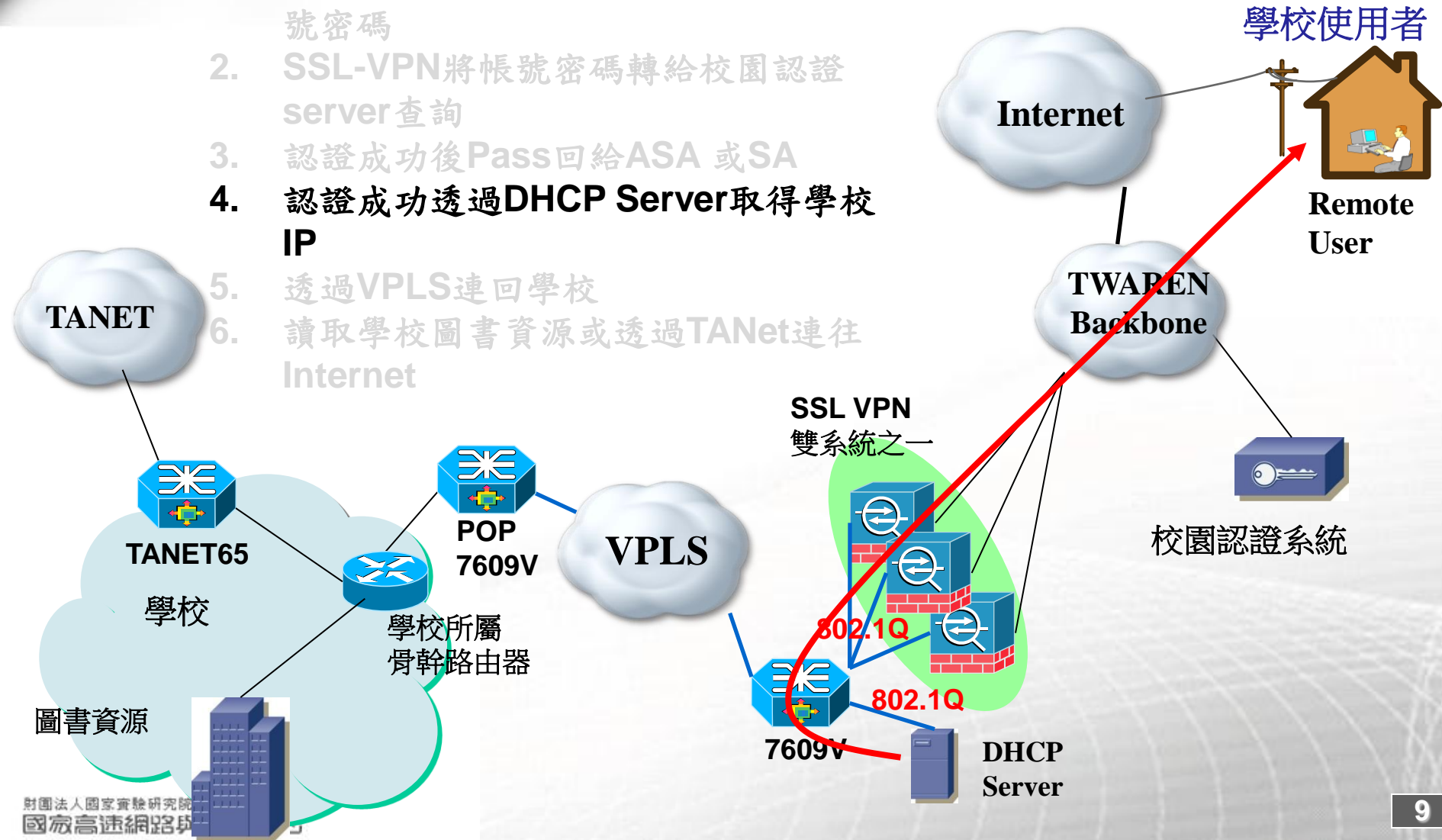
學校

圖書資源



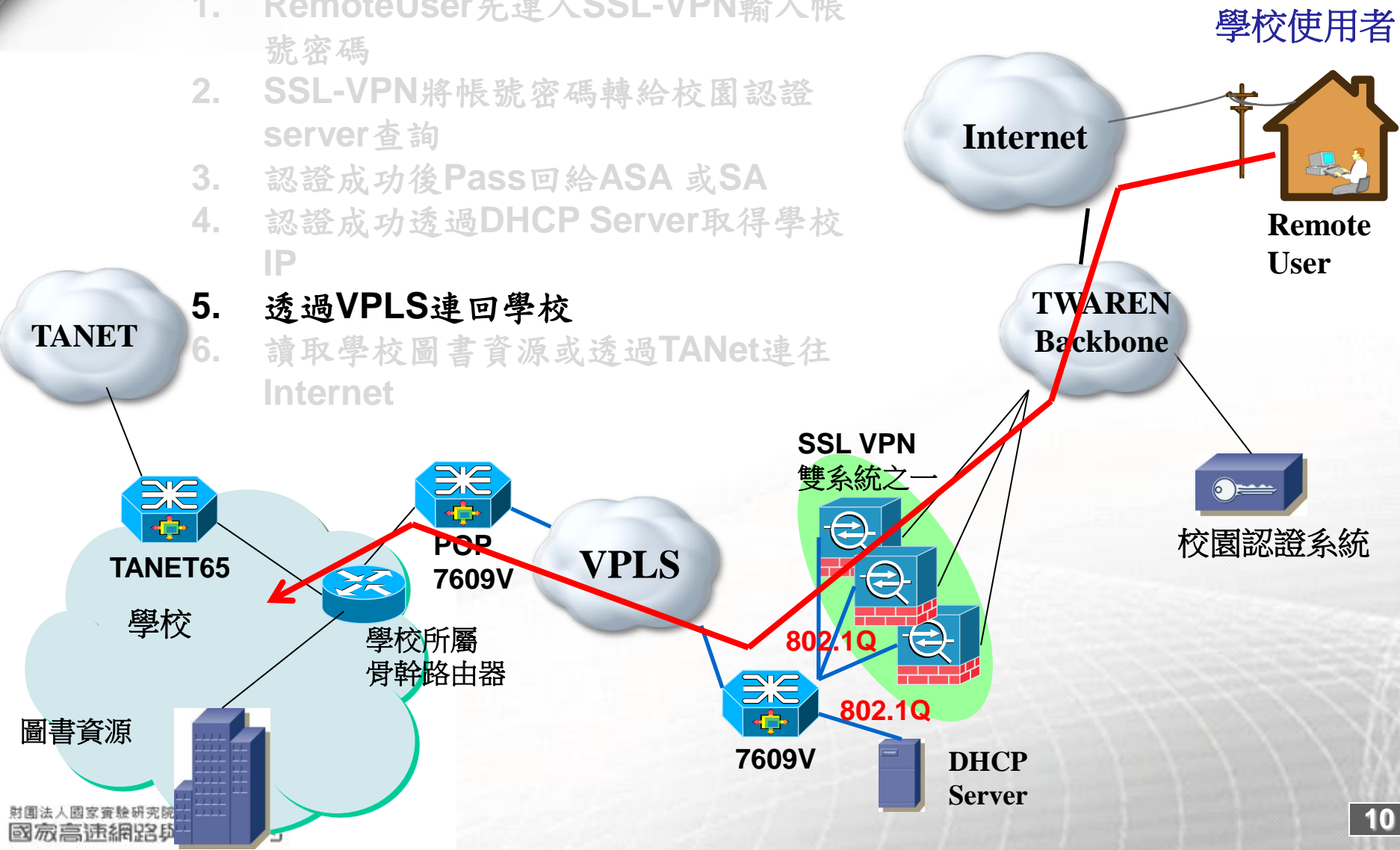
連線單位使用SSL-VPN服務-4

1. RemoteUser先連入SSL-VPN輸入帳號密碼
2. SSL-VPN將帳號密碼轉給校園認證server查詢
3. 認證成功後Pass回給ASA 或SA
4. 認證成功透過DHCP Server取得學校IP
5. 透過VPLS連回學校
6. 讀取學校圖書資源或透過TANet連往Internet



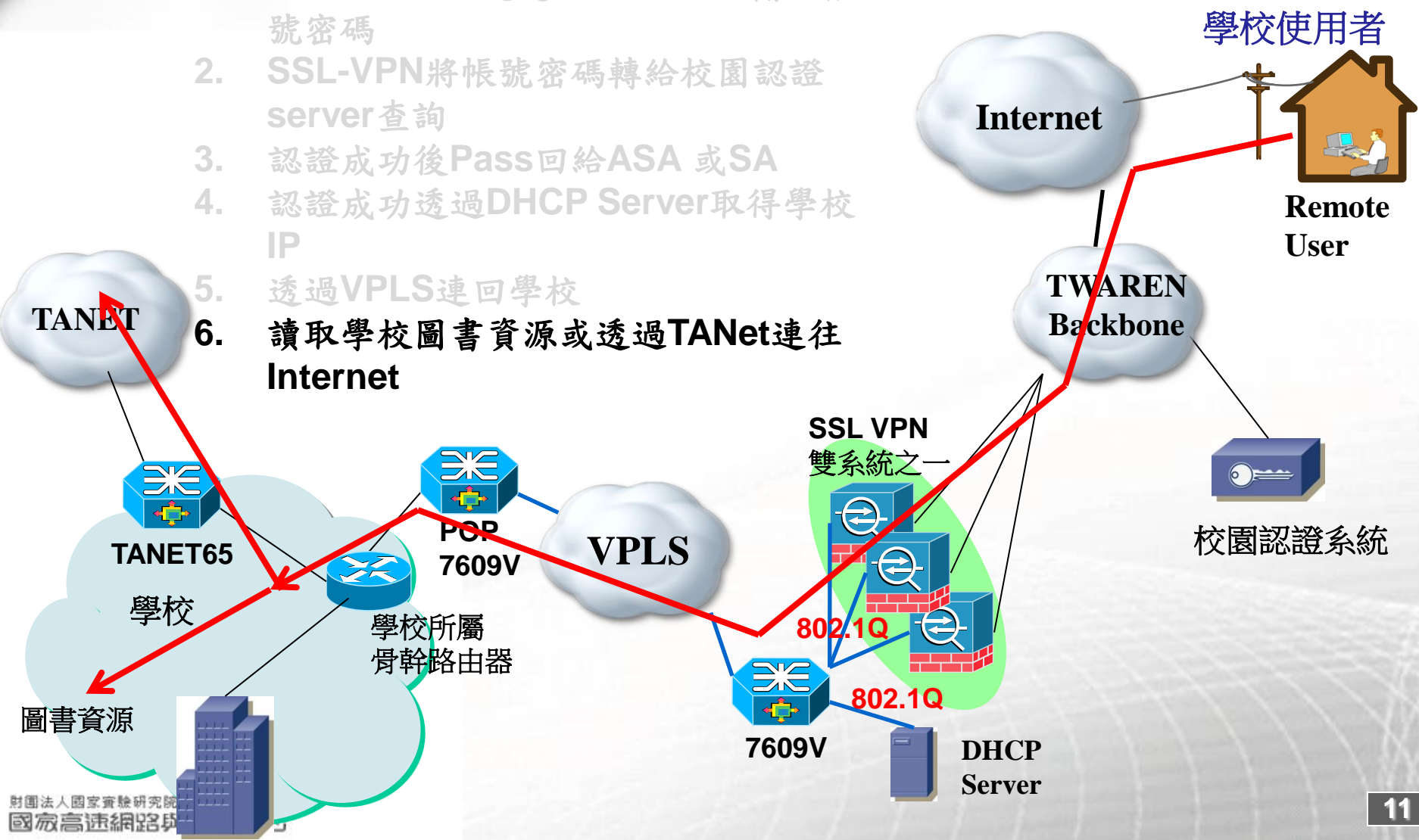
連線單位使用SSL-VPN服務-5

1. RemoteUser先連入SSL-VPN輸入帳號密碼
2. SSL-VPN將帳號密碼轉給校園認證server查詢
3. 認證成功後Pass回給ASA 或SA
4. 認證成功透過DHCP Server取得學校IP
5. 透過VPLS連回學校
6. 讀取學校圖書資源或透過TANet連往Internet



連線單位使用SSL-VPN服務-6

1. RemoteUser先連入SSL-VPN輸入帳號密碼
2. SSL-VPN將帳號密碼轉給校園認證server查詢
3. 認證成功後Pass回給ASA 或SA
4. 認證成功透過DHCP Server取得學校IP
5. 透過VPLS連回學校
6. 讀取學校圖書資源或透過TANet連往Internet



Cisco ASA-5550 系統

1. 欲申請服務之單位，需具備不與全國無線漫遊之認證伺服器。
2. 可接受多種之認證伺服器，例如Radius、LDAP、Tacacs+。
3. Cisco ASA-5550透過Cluster所組成，加強了容錯與提高了可用率。
4. User 登入網址：<https://sslvpn.twaren.net>



SSL-VPN 網頁驗證

身份認證採用校園無線漫遊機制的使用者名稱及密碼
請輸入正確格式：[xxx@xxx.edu.tw](#)

使用者名稱:

使用者密碼:

Juniper SA-6500系統

1. Juniper SA6500系統透過了IVE(Instant Virtual Extranet)技術(註)提供了高穩定度的SSL-VPN環境平台。
2. 亦可接受多種之認證伺服器，例如Radius、LDAP、AD/NT。
3. 擁有後端的管理介面，供管理人員查詢。
4. User登入網址:<https://sslvpn9.twaren.net/xxx> (xxx為學校縮寫)



Welcome to the
NCHC SSL VPN (Please use EMAIL account to login :

username

password

Realm

Please sign in to t

Sign In

註 The IVE is a hardened network operating system that acts as the platform for all Juniper Networks Secure Access products. These appliances provide a range of enterprise-class scalability, high availability, and security features that extend secure, remote access to network resources.

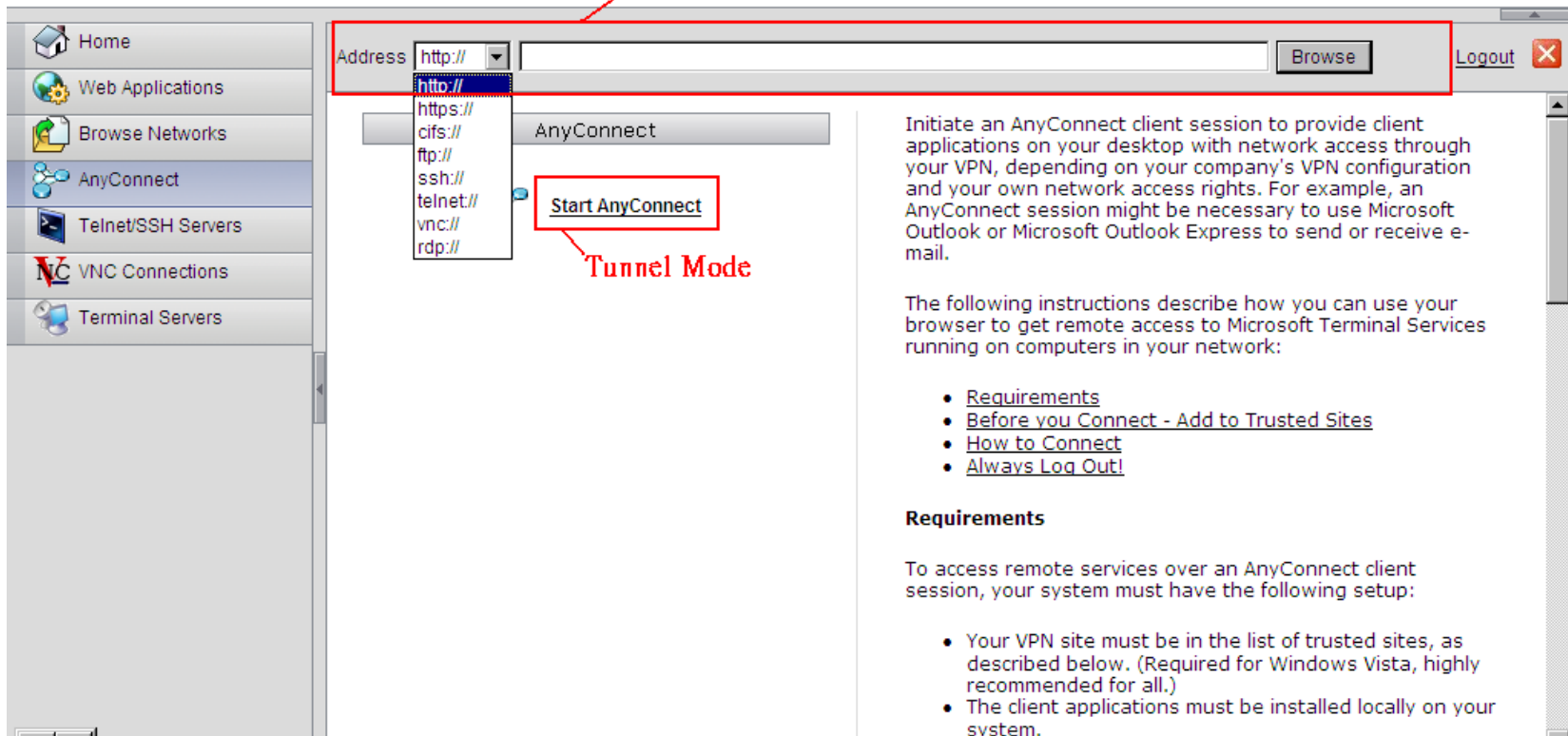
使用說明

■ Cisco ASA-5550

1. 登入網址<https://sslvpn.twaren.net>，輸入E-mail帳號、密碼。
2. 登入成功，出現如下頁畫面，分別有Clientless mode與Tunnel mode工作選項。
3. Tunnel mode為執行Cisco所提供的SSL-VPN Client應用程式AnyConnect，並取得學校所配置的IP。
4. Clientless mode，不需使用者在其電腦上安裝Client端軟體，只要有瀏覽器的電腦就可以允許使用者存取網路資源(例如FTP,RDP..)。
5. 左邊為各種可執行之應用程式。

使用說明

Cisco ASA-5550



The screenshot shows the Cisco ASA-5550 web interface. On the left is a navigation menu with options: Home, Web Applications, Browse Networks, AnyConnect (highlighted), Telnet/SSH Servers, VNC Connections, and Terminal Servers. The main content area is titled "Clientless Mode" and features a "Start AnyConnect" button. Below this, a dropdown menu is open, listing protocols: http://, https://, cifs://, ftp://, ssh://, telnet://, vnc://, and rdp://. A red box highlights the "Start AnyConnect" button, with a red arrow pointing to it from the label "Tunnel Mode". The right side of the page contains text explaining how to initiate an AnyConnect client session and provides a list of requirements and instructions for remote access.

Clientless Mode

Address

AnyConnect

Start AnyConnect

Tunnel Mode

Initiate an AnyConnect client session to provide client applications on your desktop with network access through your VPN, depending on your company's VPN configuration and your own network access rights. For example, an AnyConnect session might be necessary to use Microsoft Outlook or Microsoft Outlook Express to send or receive e-mail.

The following instructions describe how you can use your browser to get remote access to Microsoft Terminal Services running on computers in your network:

- [Requirements](#)
- [Before you Connect - Add to Trusted Sites](#)
- [How to Connect](#)
- [Always Log Out!](#)

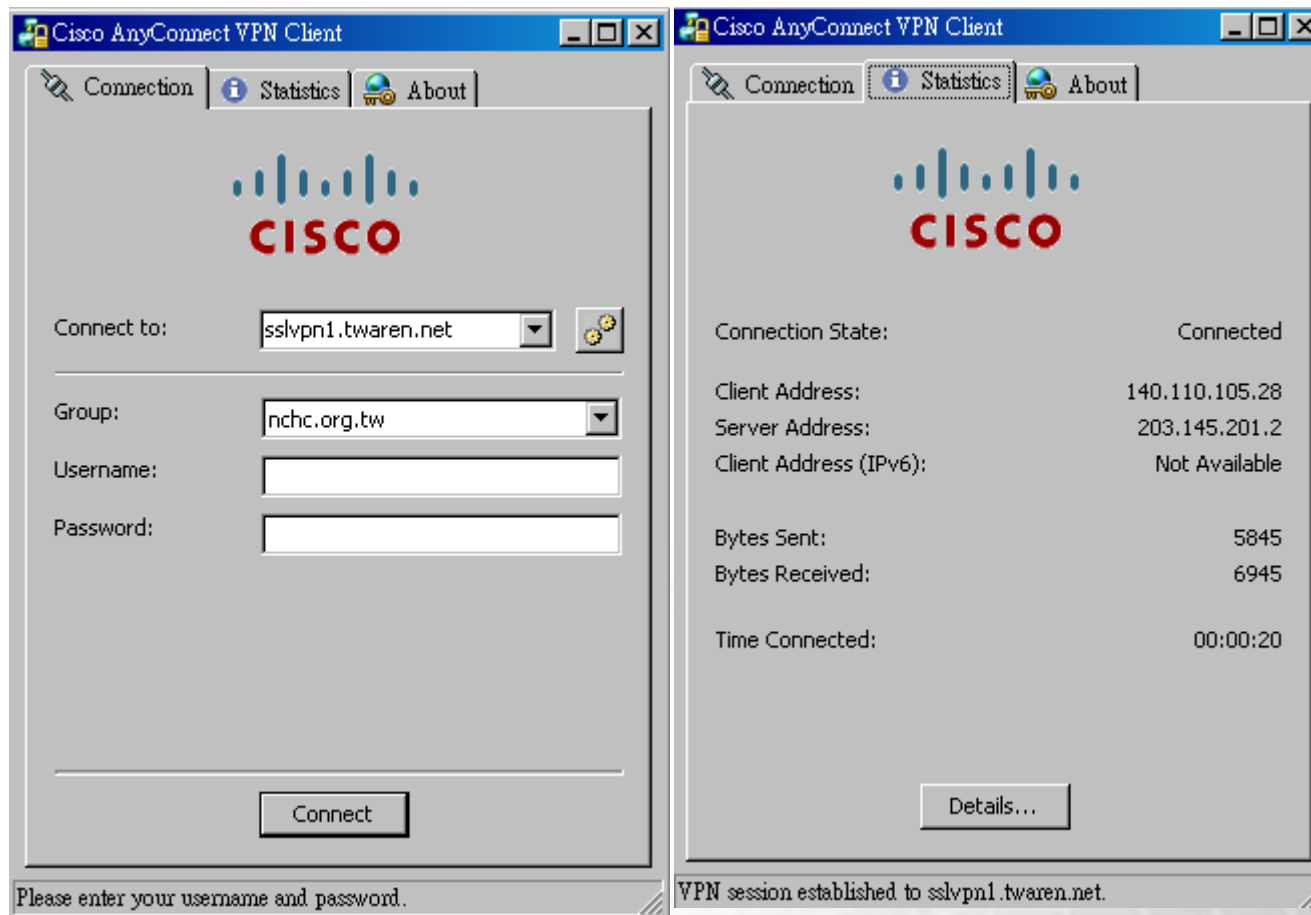
Requirements

To access remote services over an AnyConnect client session, your system must have the following setup:

- Your VPN site must be in the list of trusted sites, as described below. (Required for Windows Vista, highly recommended for all.)
- The client applications must be installed locally on your system.

使用說明

Tunnel mode , AnyConnect登入與執行時畫面



使用說明

■ Juniper SA-6500

1. 登入網址 <https://sslvpn9.twaren.net/xxx>，輸入E-mail帳號與密碼(XXXX為申請學校縮寫)，以國網中心為例，該縮寫為nchc(註)，整個URL為https://sslvpn9.twaren.net/nchc
2. 登入成功，出現如下畫面，第一次執行時，要求安裝SSL-VPN Client端軟體Network Connect的相關步驟。
3. 如果輸入不是nchc的帳號，會跳出請輸入正確e-mail帳號的提示資訊。
4. 下方為Juniper SA-6500提供的SSL-VPN Client端軟體啟動按鈕。

註:該縮寫，供連線單位自行命名

使用說明

■ Juniper SA-6500 登入畫面



The screenshot shows the login interface for the NCHC SSL VPN. At the top left is the NCHC logo and the text: 財團法人國家實驗研究院, 國家高速網路與計算中心, National Center for High-Performance Computing, and Better HPC Better Living. The main heading reads: Welcome to the NCHC SSL VPN (Please use EMAIL account to login : XXX@NCHC.ORG.). Below this are input fields for 'username', 'password', and 'Realm' (set to 'Radius_Users'). A 'Login' button is at the bottom left. A CAPTCHA section is located below the password field, with the instruction '請輸入下方驗證碼' and the code '10 10 9 1 5 7 10'. Two red annotations with arrows point to the username and CAPTCHA fields, providing instructions in Chinese.

財團法人國家實驗研究院
國家高速網路與計算中心
National Center for High-Performance Computing
Better HPC Better Living

Welcome to the
NCHC SSL VPN (Please use EMAIL account to login : XXX@NCHC.ORG.)

Please sign in to begin your secure session

username

password

Realm

請輸入下方驗證碼

10 10 9 1 5 7 10

Login

請輸入帶有@nchc.org.tw的E-mail
帳號

加強輸入驗證碼機制,防制
Robot輸入猜測帳號密碼

使用說明

Juniper SA-6500 登入成功後畫面



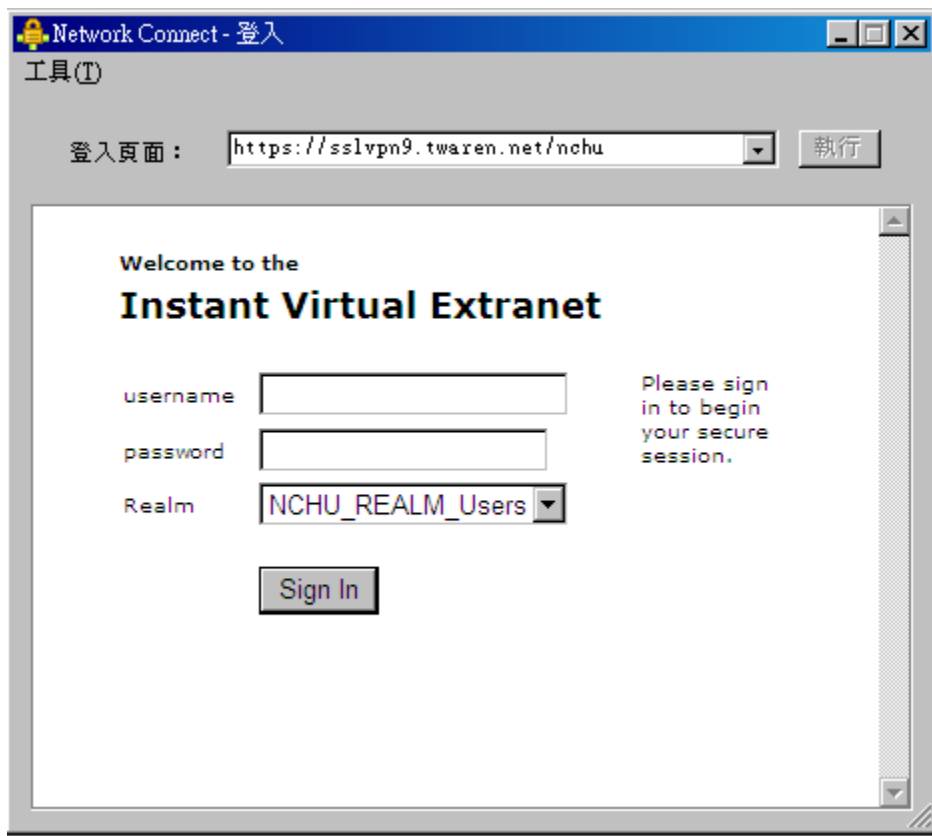
The screenshot shows the Juniper Networks web interface for the Secure Access SSL VPN. The header includes the Juniper Networks logo and navigation links: 首頁 (Home), 喜好設定 (Preferences), 說明 (Help), and 登出 (Logout). The main content area displays a welcome message: "Welcome to the Secure Access SSL VPN, nchuvpn@nchu.edu.tw." Below this, there are four expandable sections: "Web 標籤" (Web Tabs) with the message "您完全沒有 Web 標籤。" (You have no web tabs.); "檔案" (Files) with "您未將任何檔案加入書籤。" (You have not added any files to bookmarks.); "終端機工作階段" (Terminal Sessions) with "您完全沒有終端機工作階段。" (You have no terminal sessions.); and "用戶端應用程式工作階段" (Client Application Sessions), which is highlighted with a red border and contains a "Network Connect" entry with a "開始" (Start) button.

Copyright © 2001-2009 Juniper Networks, Inc.
All rights reserved.

Juniper your Net.

使用說明

Juniper Network Connect 登入與執行畫面



管理者介面

Cisco ASA-5550與Juniper SA-6500 皆提供後端管理者介面供查詢

The screenshot shows the TWAREN (Taiwan Advanced Research & Education Network) management interface. The header includes the TWAREN logo and the text "台灣高品質學術研究網路". Below the header, there is a "Logout" link. On the left side, there is a navigation menu with options: Home, Inquire, Report, and Change Password. The main content area displays a table titled "The Result" with the following columns: Session Start, Session Stop, User Name, Location, DHCP Start, DHCP IP, and Duration. The table contains seven rows of session data.

The Result						
Session Start	Session Stop	User Name	Location	DHCP Start	DHCP IP	Duration
2010-08-22 22:45:02	2010-08-22 22:45:31	5697121@nchc.edu.tw	140.110.175.155			0h:00m:29s
2010-08-22 22:45:41	2010-08-23 02:49:06	5697121@nchc.edu.tw	140.110.175.155			4h:03m:23s
2010-08-22 22:45:41	2010-08-23 17:39:17	5697121@nchc.edu.tw	140.110.175.155			2h:08m:11s
2010-08-23 21:44:52	2010-08-23 22:39:13	5697121@nchc.edu.tw	140.110.175.155			0h:54m:21s
2010-08-25 12:14:06	2010-08-25 12:22:59	5697121@nchc.edu.tw	140.110.175.155	2010-08-25 12:15:59	140.110.105.175	0h:08m:53s
2010-07-05 17:26:54	2010-08-25 18:06:36	5697121@nchc.edu.tw	140.110.175.155	2010-07-05 17:27:35	10.66.7.138	0h:58m:08s

Cisco 查詢使用者Log畫面

管理者介面

Logs

User Access Admin Access Sensors Client Logs

Log Settings Filters

View by filter: Standard:Standard (default) Show 200 items

Edit Query:

Update

Reset Query

Save Query...

Save Log As...

Clear Log

Filter: Standard (default)

Date: Oldest to Newest

Query:

Export Format: Standard

Severity	ID	Message
Info	AUT23315	2010-09-05 15:08:41 - SA6500 - [127.0.0.1] NCHC::System()[] - Radius Accounting: Successfully sent radius accounting USER session stop request for [REDACTED](Radius_Users)[Radius_Users]
Info	NWC23465	2010-09-05 15:08:41 - SA6500 - [REDACTED] NCHC::0912015@narl.org.tw(Radius_Users)[Radius_Users] - Network Connect: Session ended for user with IP 140.110.105.28
Info	AUT23315	2010-09-05 15:08:41 - SA6500 - [127.0.0.1] NCHC::System()[] - Radius Accounting: Successfully sent radius accounting NC session stop request for [REDACTED](Radius_Users)[Radius_Users]
Info	ERR24670	2010-09-05 15:08:41 - SA6500 - [REDACTED] NCHC::0912015@narl.org.tw(Radius_Users)[Radius_Users] - Network Connect: ACL count = 0.
Info	JAV20023	2010-09-05 15:08:41 - SA6500 - [REDACTED] NCHC::0912015@narl.org.tw(Radius_Users)[Radius_Users] - Closed connection to TUN-VPN port 443 after 3606 seconds, with 1211 bytes read (in 6 chunks) and 7701 bytes written (in 20 chunks)

Juniper SA-6500管理者端畫面

SSL-VPN for iOS



View In iTunes

Free
Category: [Business](#)
Updated: 08 September 2010
Current Version: 1.0.0.7121
1.0.0.7121
1.0 MB
Language: English
Developer: Juniper Networks
© 2010 Juniper Networks, Inc.
[Rated 4+](#)
Requirements: Compatible with iPhone and iPod touch. Requires iOS 4.1 or later.

Customer Ratings

Description

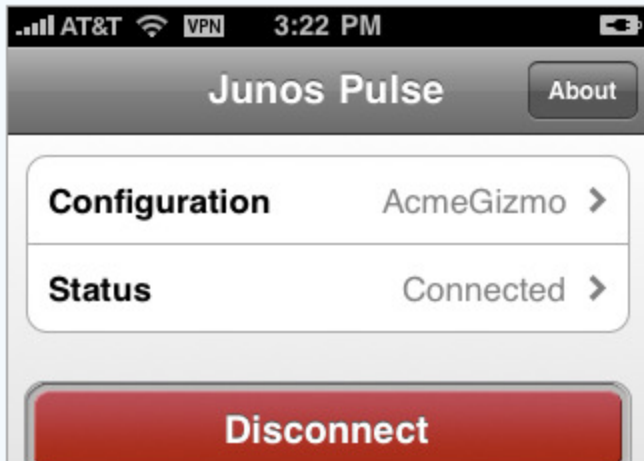
Junos Pulse for iOS enables secure connectivity over SSL VPN to corporate applications and data from anywhere, at any time. Using Junos Pulse, you can connect securely to your corporate Juniper Networks SA Series SSL VPN gateway and gain instant access to business applications and networked data from wherever you are.

[Juniper Networks Inc. Web Site](#) ▶ [Junos Pulse Support](#) ▶ [Application Licence Agreement](#) ▶ [...More](#)

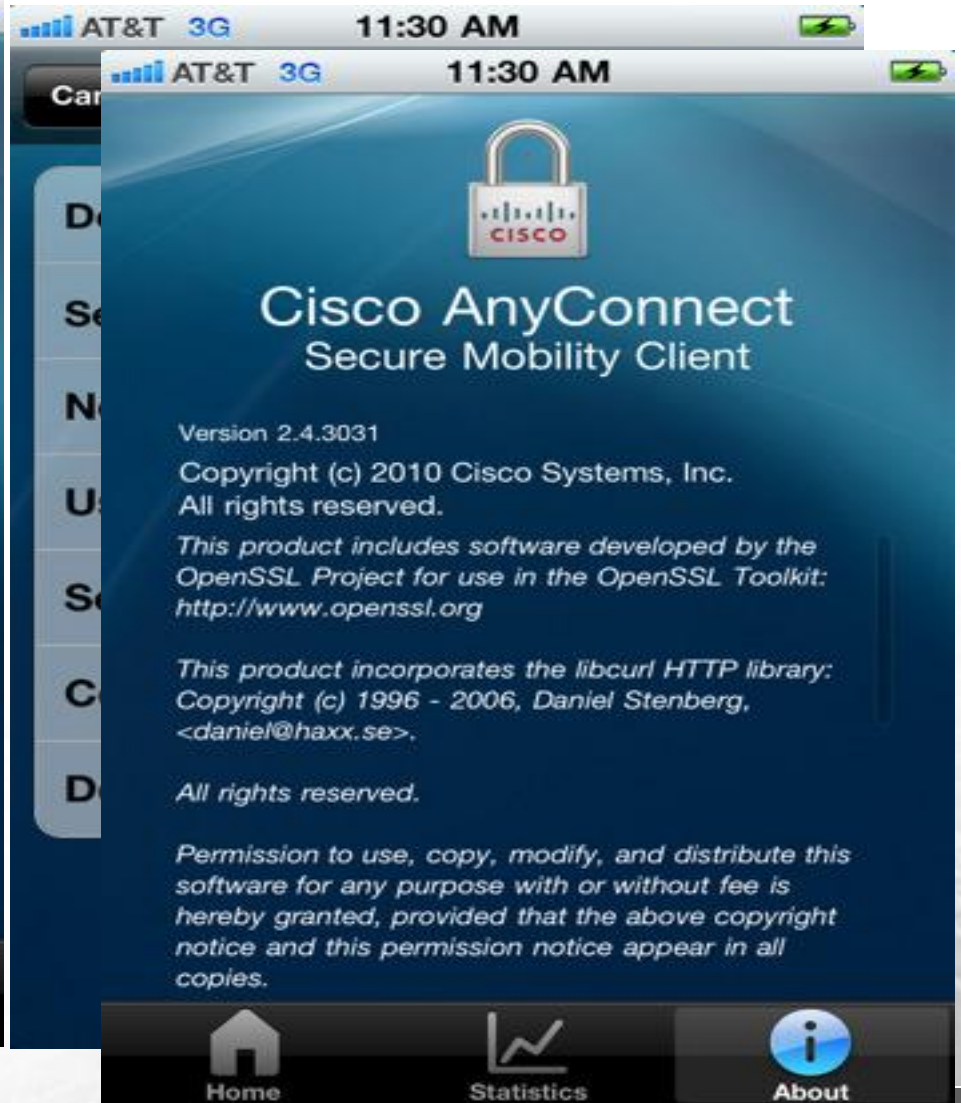
What's New In Version 1.0.0.7121

This is the first release of Junos Pulse for iOS.

iPhone Screenshots



SSL-VPN for iOS



Thanks

請參閱相關網頁

http://noc.twaren.net/noc_2008/Services/SSLVPN/