TRIỂN KHAI MẠNG ẢO (VITUAL PRIVATE NETWORK – VPN) CHO CƠ QUAN, DOANH NGHIỆP TRÊN NỀN ASA CISCO

KS.Nguyễn Trí Đức(*)

ThS. Phan Trần Điền(**)

Ngày nay, sự phát triển nhanh chóng của các công nghệ viễn thông tiên tiến như ISDN (Integrated Services Digital Network), ATM (Asynchronous Transfer Mode), ASDL (Asymmetric Digital Subscriber Line) và đặc biệt là Internet trong các năm qua kéo theo sự phát triển hàng loạt các dịch vụ mới đáp ứng các nhu cầu đa dạng của ứng dụng công nghệ thông tin. Một trong các loại dịch vụ đó là công nghệ mạng riêng ảo – VPN (Virtual Private Network). Trong xu hướng toàn cầu hóa hiện nay, sự phát triển của các cơ quan, doanh nghiệp, các văn phòng đại diện đòi hỏi việc hoạt động không phụ thuộc vào vị trí địa lý cố định, nhu cầu truy cập từ xa (ngoài văn phòng) vào mạng nội bộ để trao đổi dữ liệu hay sử dụng các ứng dụng ngày càng phổ biến. Đây là nhu cầu thiết thực, tuy nhiên do vấn đề bảo mật và an toàn thông tin nên các cơ quan ngại "mở" hệ thống mạng nội bộ của mình để cho phép nhân viên truy cập từ xa. Dưới đây chúng tôi sẽ giới thiệu một giải pháp truy cập từ xa qua mạng ảo VPN trên nền ASA CISCO có cơ chế mã hóa dựa trên giao thức IPSec nhằm đảm bảo an toàn thông tin.

Trước đây, để truy cập từ xa vào hệ thống mạng, người dùng phải sử dụng phương thức Remote Access quay số dựa trên mạng điện thoại. Việc sử dụng kỹ thuật quay số này vừa tốn kém vừa không an toàn. Trong khi đó, VPN (virtual private network) là công nghệ xây dựng hệ thống mạng riêng ảo nhằm đáp ứng nhu cầu chia sẻ thông tin, cho phép truy cập từ xa và tiết kiệm chi phí. VPN cho phép các máy tính truyền thông với nhau thông qua một môi trường chia sẻ như mạng Internet nhưng vẫn đảm bảo được tính riêng tư và bảo mật dữ liệu. Trong kỹ thuật VPN, để cung cấp kết nối giữa các máy tinh, các gói thông tin được bao bọc bằng một header có chứa những thông tin định tuyến, cho phép dữ liệu có thể gửi từ máy truyền qua môi trường mạng chia sẻ và đến máy nhận, như đường truyền riêng (tunnel). Để bảo đảm tính riêng tư và bảo mật trên môi trường chia sẻ này, các gói tin luôn được mã hóa và chỉ có thể được giải mã với những khóa thích hợp, ngăn ngừa trường hợp trộm gói tin trên đường truyền.

VPN có một số giải pháp triển khai thông dụng như Remote Access, Site To Site, Intranet/ Internal VPN. Trong đó, giải pháp Remote Access đáp ứng được nhu

(*)(**) Tổ bộ môn Tin học – Ngoại ngữ, Học viện Cán bộ Thành phố Hồ Chí Minh

cầu truy cập dữ liệu và ứng dụng cho người dùng ở xa, bên ngoài cơ quan, doanh nghiệp thông qua hệ thống mạng Internet. Qua giải pháp này, người dùng ở xa có thể khai thác dữ liệu, sử dụng email từ các máy chủ chứa dữ liệu, hệ thống máy chủ chứa mail nội bộ đặt ở cơ quan. Ngoài ra, VPN còn có thể triển khai giải pháp Site To Site thường được triển khai cho các cơ quan, doanh nghiệp có nhiều văn phòng chi nhánh nằm cách xa nhau, không thể sử dụng cáp mạng để trao đổi dữ liệu với nhau. Ví dụ một công ty đa quốc gia có nhu cầu chia sẻ thông tin giữa các chi nhánh đặt tại Singapore và Việt Nam, có thể xây dựng một hệ thống VPN Site-to-Site kết nối hai site Việt Nam và Singapore tạo một đường truyền riêng trên mạng Internet phục vụ quá trình truyền thông an toàn và hiệu quả. Ngoài ra, người ta còn có thể triển khai giải pháp Intranet/ Internal VPN trong một số tổ chức. Quá trình truyền dữ liệu giữa một số bộ phận được bảo đảm tính riêng tư, không cho phép những bộ phận khác truy cập. Hệ thống Intranet VPN có thể đáp ứng được yêu cầu này.

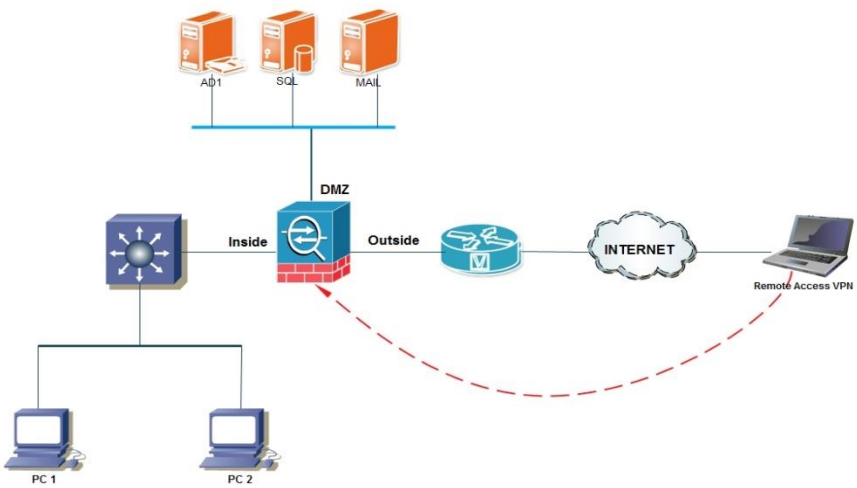
Việc triển khai một hệ thống ảo VPN cần có những thành phần cơ bản sau:

- ***User Authentication****:* Cung cấp cơ chế chứng thực người dùng, chỉ cho phép người dùng hợp lệ kết nối và truy cập hệ thống VPN.
- ***Address Management****:* Cung cấp địa chỉ IP hợp lệ cho người dùng sau khi gia nhập hệ thống VPN để có thể truy cập tài nguyên trên mạng nội bộ.
- ***Data Encryption****:* Cung cấp giải pháp mã hoá dữ liệu trong quá trình truyền nhằm bảo đảm tính riêng tư và toàn vẹn dữ liệu.
- ***Key Management****:* Cung cấp giải pháp quản lý các khoá dùng cho quá trình mã hoá và giải mã dữ liệu.
- **Giao thức bảo mật IPSEC (IP SECURITY PROTOCOL**): Khi truyền các gói tin, cần phải áp dụng các cơ chế mã hóa và chứng thực để bảo mật. Hiện nay có rất nhiều giải phải để thực hiện việc này, trong đó cơ chế mã hóa IPSEC hoạt động trên giao thức TCP/IP tỏ ra hiệu quả và tiết kiệm chi phí trong quá trình triển khai. Trong quá trình chứng thực hay mã hóa dữ liệu, IPSEC có thể sử dụng một hoặc cả hai giao thức bảo mật:
- ***AH (Authentication Header)***: Header của gói tin được mã hóa và bảo vệ phòng chống các trường hợp "ip spoofing" hay "man in the midle attack". Tuy nhiên trong trường hợp này phần nội dung thông tin chính không được bảo vệ.
- ***ESP (Encapsulating Security Payload)****:* Nội dung thông tin được mã hóa, ngăn chặn các trường hợp hacker đặt chương trình nghe lén và chặn bắt dữ

liệu trong quá trình truyền. Phương thức này rất hay được áp dụng, nhưng nếu muốn bảo vệ luôn cả phần header của gói tin thì phải kết hợp cả 2 giao thức AH và ESP.

Sau đây, chúng tôi trình bày các bước triển khai một giải pháp **Remote Access VPN** trên nền **Asa Cisco** như sau**:**

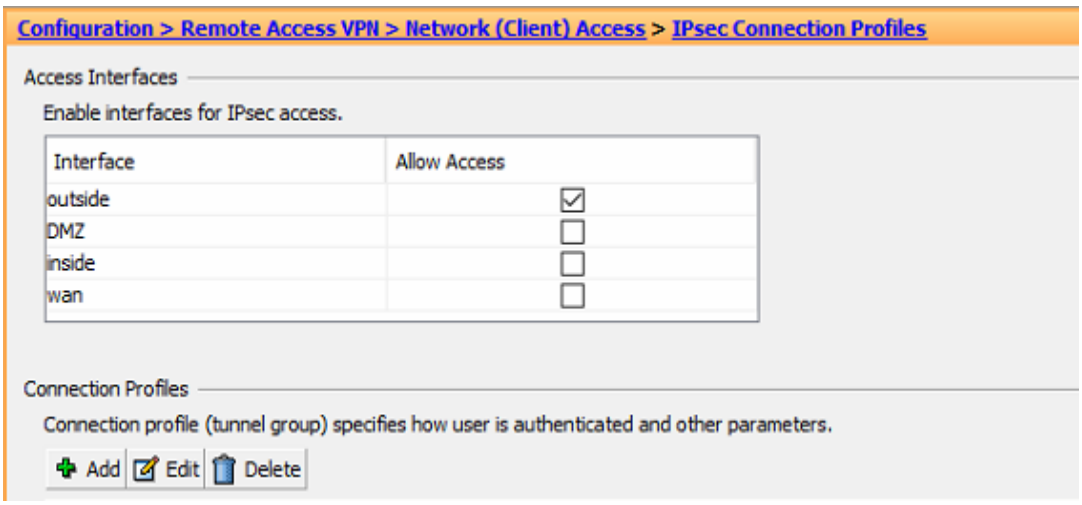
1. ***Mô hình thực hiện như sau:***



2. ***Các bước cấu hình:***

<u>Bước 1</u>: Bật IPsec VPN trên cổng sẽ tiếp nhận kết nối này. Ở đây chính là cổng outside.

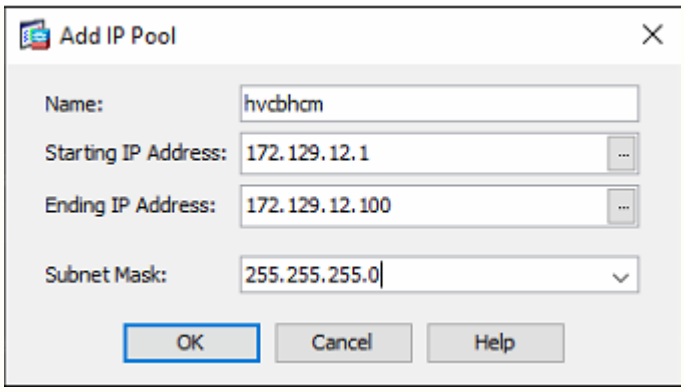
- Trên ASDM, vào **Configuration > Remote Access VPN > Network (Client) Access > IPsecConnection Profiles**, và check vào cổng mà ta muốn bật IPsec VPN.



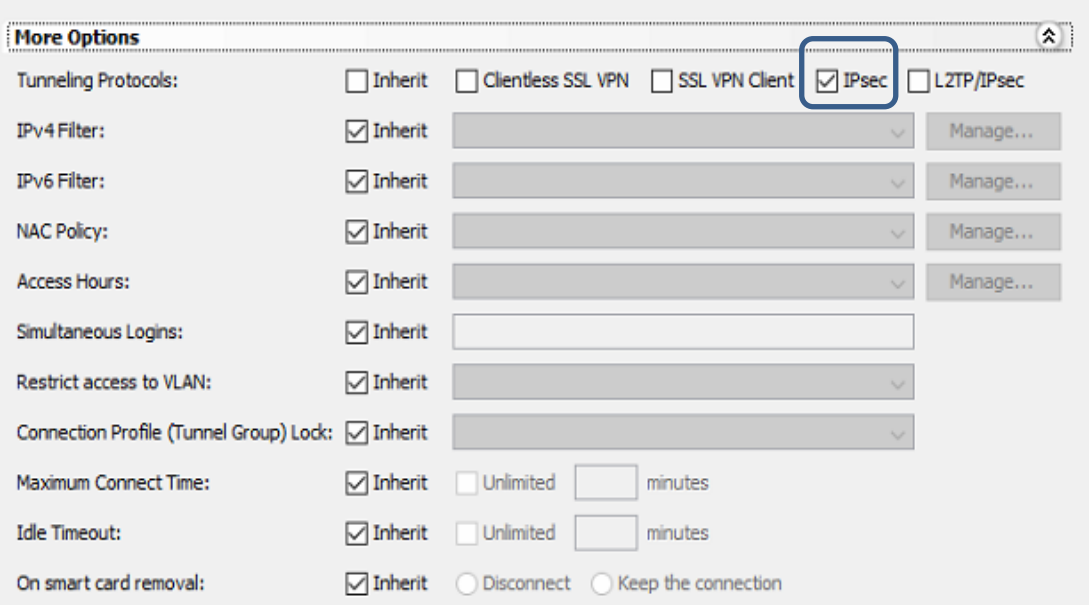
- Ngay sau khi bật IPsec VPN thì ASA sẽ tạo ra một loạt các IKE phase 1 policies và IKE phase 2 policies (transform sets) nhằm mục đích để thương lượng với những policies mà VPN client sẽ gửi ra khi khởi tạo kết nối đến ASA. Ngoài ra ASA cũng tạo ra một dynamic crypto map tên là SYSTEM_DEFAULT_CRYPTO_MAP và một static crypto map tên là outside_map. Dynamic crypto map được dùng để tham chiếu đến các transform sets sẽ dùng để thương lượng với VPN client, nhưng không được áp trực tiếp vào một interface nào. Thay vào đó, static crypto map được dùng để tham chiếu đến dynamic crypto map và sẽ được áp trực tiếp trên interface.

Bước 2: Cấu hình group policy cho kết nối của user

- Trên ASDM, vào **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**, chọn **Add**. Ở phần **General**, sau đó ta bỏ dấu check Inherit ở mục Address Pools và chọn **Select**. Ở cửa sổ mới ta chọn **Add** và nhập các thông tin về pool địa chỉ sẽ cấp cho user khi họ kết nối vào. Chọn **OK**.



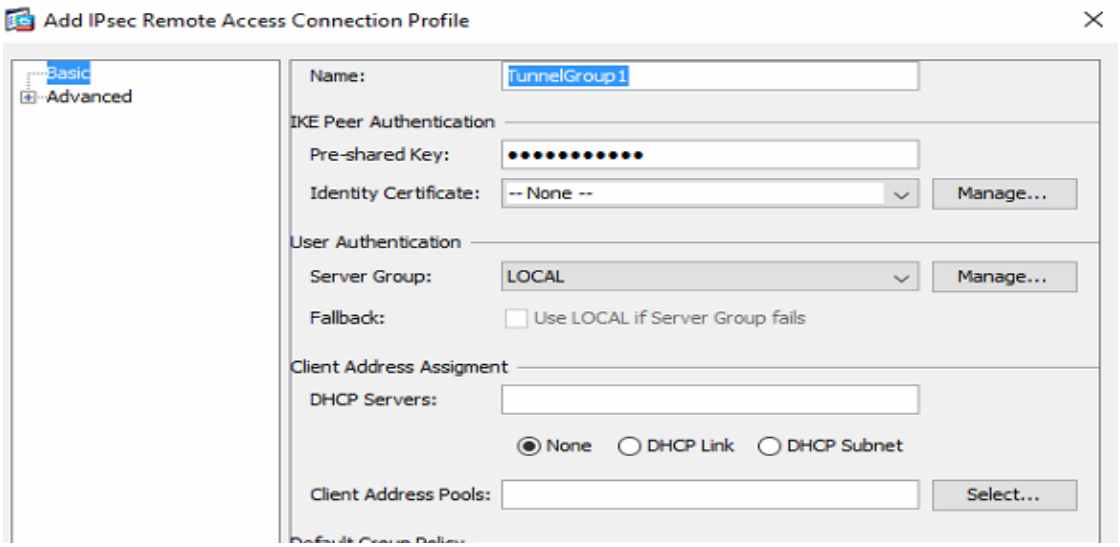
- Quay lại cửa sổ trước đó, ta chọn pool địa chỉ muốn cấp cho user và click vào **Assign** →, sau đó chọn **OK**
- Tiếp theo ta mở rộng phần **More Options**, bỏ dấu check Inherit ở mục Tunneling Protocols và chọn **IPsec**.



- Sang phần **Servers**, ta bỏ dấu check Inherit ở mục DNS Servers và nhập địa chỉ IP của DNS server mà ta sẽ cấp cho client. Chú ý rằng đây cần phải là các local DNS server để có thể phân giải được các tên miền nội bộ của công ty. Ta chỉ nên cấp một hoặc nhiều local DNS server (vd: 10.188.102.12, 10.188.102.13), không nên cấp lẫn lộn cả local và public DNS server (vd: 10.188.102.12, 8.8.8.8) để tránh các vấn đề có thể gặp phải khi phân giải các tên miền nội bộ.
- Tiếp theo ta mở rộng phần **More Options**, bỏ dấu check Inherit ở mục Default Domain và nhập vào tên miền của công ty (tên miền này sẽ được cấp cho client khi thực hiện kết nối VPN). Ở đây mình chọn (ví dụ:hcmca.edu.vn)

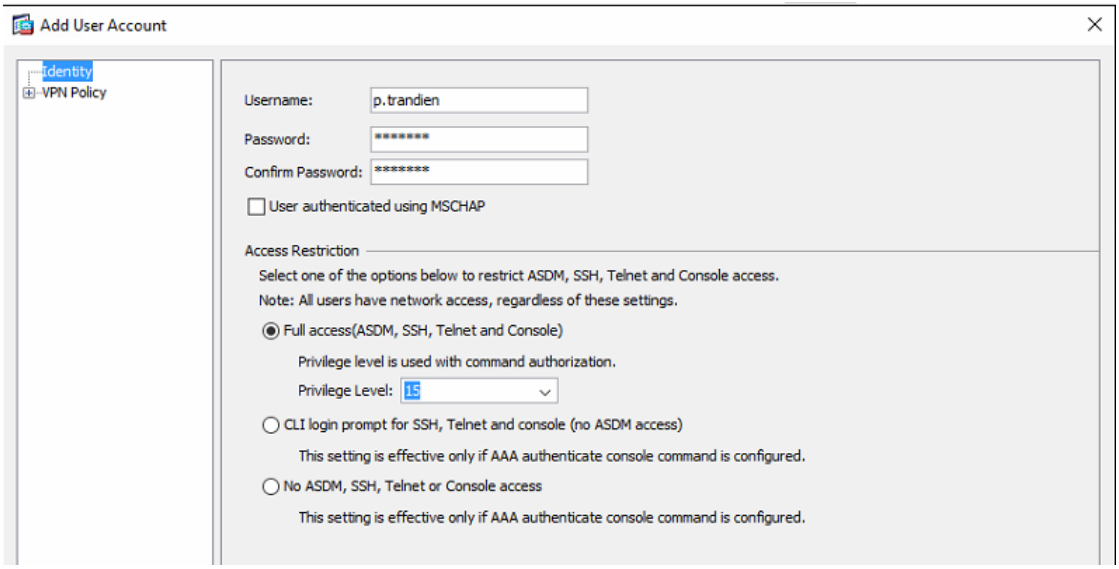
Bước 3: Cấu hình connection profile (tunnel group) cho kết nối của user.

- Trên ASDM, vào **Configuration > Remote Access VPN > Network (Client) Access > IPsec Connection Profiles**, chọn**Add**. Ở phần **Basic**, ta nhập các thông tin như hình dưới (có thể chọn pre-shared-key là một giá trị bất kỳ, miễn sao phải giống nhau giữa ASA và VPN client):



Bước 4: Tạo user account trên local database của ASA để chứng thực user.

- Trên ASDM, vào **Configuration > Remote Access VPN > AAA/Local Users > Local Users**, chọn **Add**, sau đó nhập thông tin username và password của user. Ta cũng có thể check vào ô **No ASDM, SSH, Telnet or Console access** nếu không muốn user được quyền ASDM, Telnet hoặc SSH vào thiết bị.



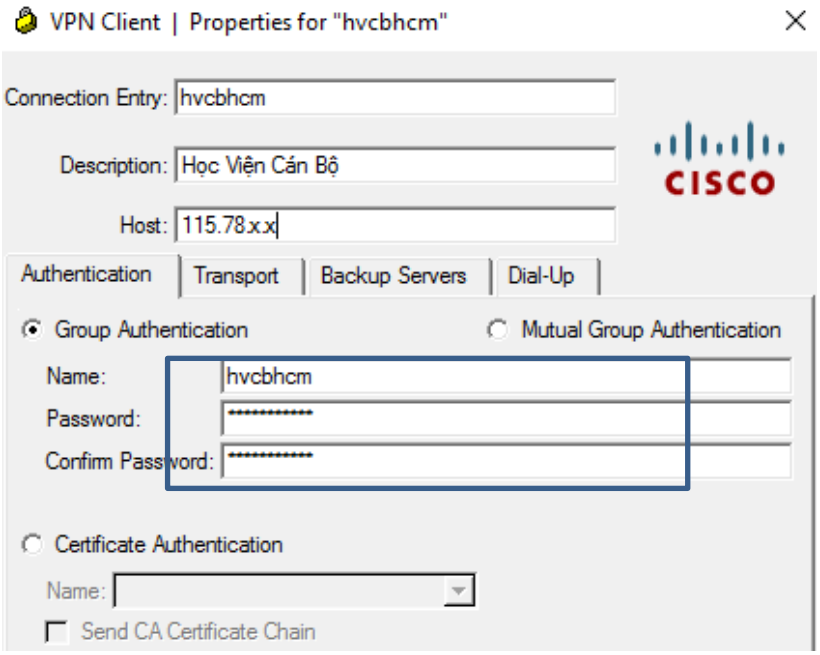
Sau khi cấu hình xong trên ASA. Tuy nhiên, tất cả các kết nối VPN từ VPN client đều phải đi qua thiết bị NAT, do đó ta cần đảm bảo NAT được bật trên ASA và các gói tin UDP Port 5000 và 4500 không bị chặn trên các thiết bị trung gian khi gửi đến ASA, cũng như không bị chặn trên ASA.

3. Để thiết lập cho Cisco VPN client, vào Connection Entries, chọn New:

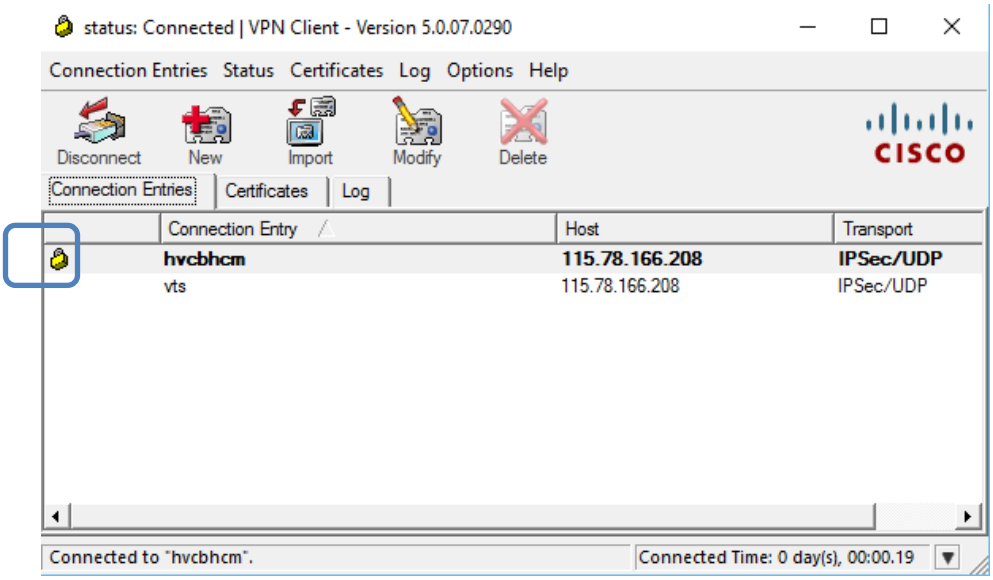
- Ở phần **Connection Entry**, ta có thể đặt một cái tên bất kỳ để dễ gợi nhớ. Ở đây, ta chọn là **hvcbhcm**. Tiếp theo ở phần **Description** ta có thể mô tả chi

tiết hơn về connection entry này, hoặc có thể để trống. Ở phần **Host** ta có thể nhập địa chỉ IP public hoặc domain name của VPN gateway mà ta sẽ kết nối tới. Ở đây mình nhập là 115.78.x.x. Sau đó ta sẽ chọn kiểu chứng thực là **Group Authentication**, đồng thời nhập vào tên của connection profile và pre-shared-key. Lưu ý rằng tên của connection profile này phải giống với tên của connection profile đã cấu hình trên ASA. Sau khi đã nhập đầy đủ các thông tin, ta chọn **Save**.

- Để tạo kết nối VPN thông qua connection entry đã cấu hình, ta double-click vào tên của connection entry. Nếu như IKE phase 1 policies được thương lượng thành công thì ASA sẽ yêu cầu user nhập tiếp **username** và **password**:



- Nếu như quá trình kết nối VPN thành công thì ASA sẽ xuất ra banner và VPN client có biểu tượng ổ khóa đóng lại như hình dưới đây:



Tóm lại, với giải pháp VPN sẽ giúp cho cơ quan, doanh nghiệp mở hệ thống mạng nội bộ của mình để nhân viên có thể truy cập từ xa như: Remote Access, Site to Site, Intranet/Internal VPN. Những giải pháp trên sẽ giúp cho nhân viên có thể khai thác thông tin như Email, hệ thống máy chủ chứa dữ liệu của đơn vị mà không phụ thuộc vào vị trí địa lý cố định, có thể truy cập từ xa (ngoài văn phòng) vào mạng nội bộ để trao đổi dữ liệu. Tất cả những dữ liệu trao đổi sẽ được mã hóa dựa trên giao thức IPSec nhằm đảm bảo an toàn thông tin, ngăn ngừa trường hợp trộm gói tin trên đường truyền.

Tài liệu tham khảo

[1]. Giải pháp mạng cho doanh nghiệp trên nền thiết bị draytek, địa chỉ: http://www.draytek.com.vn/marketnewsdetail.aspx?id=264

[2]. Cấu hình IPsec VPN client trên Cisco ASA, địa chỉ: http://hocmang.net/2014/12/14/cau-hinh-ipsec-vpn-client-tren-cisco-asa/

[3]. VPN là gì?, địa chỉ: https://sites.google.com/site/rocbin/vpn-la-gi

[4].Võ Viết Minh Nhật, Nguyễn Ngọc Thủy, Mạng riêng ảo VPN, Khoa CNTT-D9HKH Huế.

[5]. Configuring Easy VPN on the ASA 5505, địa chỉ: http://www.cisco.com/c/en/us/td/docs/security/asa/asa72/configuration/guide/conf_gd/ezvpn505.html

[6]. Cisco ASA Series VPN ASDM Configuration Guide, địa chỉ: http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/asdm71/vpn/asdm_71_vpn_config.pdf

[7]. Hướng dẫn cấu hình VPN host –to – Lan, địa chỉ: http://www.draytek.com.vn/documentdetails.aspx?id=145