Packet Tracer ASA Clientless VPN Lab

The purpose of this lab is to provide a more advanced understanding of Cisco’s ASA 5505 Adaptive Security Appliance; The Cisco ASA is a security device that combines firewall, antivirus, intrusion prevention, and virtual private network (VPN) capabilities. In this lab we will Packet Tracer 6.1 to learn how to configure the ASA as a basic Firewall with the addition of clientless vpn access. This knowledge is essential to passing the CCNA Security exam and will be used in daily in your position as a Cisco network engineer.

# Clientless VPN:

Clientless SSL VPN (WebVPN) allows for limited but valuable secure access to the corporate network from any location. Users can achieve secure browser-based access to corporate resources at anytime. This document provides a straightforward configuration for the Cisco Adaptive Security Appliance (ASA) 5500 series to allow Clientless SSL VPN access to internal network resources.

The SSL VPN technology can be utilized in three ways: Clientless SSL VPN, Thin-Client SSL VPN (Port Forwarding), and SSL VPN Client (SVC Tunnel Mode). Each has its own advantages and unique access to resources. In our lab we will be focusing on the clientless SSL VPN.

## 1. Clientless SSL VPN

A remote client needs only an SSL-enabled web browser to access http- or https-enabled web servers on the corporate LAN. Access is also available to browse for Windows files with the Common Internet File System (CIFS). A good example of http access is the Outlook Web Access (OWA) client.

## 2. Thin-Client SSL VPN (Port Forwarding)

A remote client must download a small, Java-based applet for secure access of TCP applications that use static port numbers. UDP is not supported. Examples include access to POP3, SMTP, IMAP, SSH, and Telnet. The user needs local administrative privileges because changes are made to files on the local machine. This method of SSL VPN does not work with applications that use dynamic port assignments, for example, several FTP applications.

Refer to Thin-Client SSL VPN (WebVPN) on ASA using ASDM Configuration Example in order to learn more about the Thin-Client SSL VPN.

## 3. SSL VPN Client (SVC-Tunnel Mode)

The SSL VPN Client downloads a small client to the remote workstation and allows full, secure access to the resources on the internal corporate network. The SVC can be downloaded permanently to the remote station, or it can be removed after the secure session ends.

Clientless SSL VPN can be configured on the Cisco VPN Concentrator 3000 and specific Cisco IOS® routers with Version 12.4(6)T and higher. Clientless SSL VPN access can also be configured on the Cisco ASA at the Command Line Interface (CLI) or with the Adaptive Security Device Manager (ASDM). The ASDM usage makes configurations more straightforward.

Clientless SSL VPN and ASDM must not be enabled on the same ASA interface. It is possible for the two technologies to coexist on the same interface if changes are made to the port numbers. It is highly recommended that ASDM is enabled on the inside interface, so WebVPN can be enabled on the outside interface.

# Learning Objectives:

* Configure group-policy.
* Configure local user database.
* Configure user attributes.
* Configure webvpn.
* Configure bookmarks.
* Configure tunnel-group.

**Lab Task:**

In this lab we will add our configuration to an existing Packet Tracer topology from a previous ASA lab. All basic configurations of routers and ASA have been completed.

## Configuring the Clientless VPN:

1. From the Config tab of the ASA select Bookmark Manager
2. Add a bookmark labeled Engineering with the url http://192.168.1.200.
3. In global configuration mode create a group-policy named remote\_users.

**group-policy remote\_users internal**

**group-policy remote\_users attributes**

**vpn-tunnel-protocol ssl-clientless**

**webvpn**

**url-list value Engineering**

1. In global configuration mode create a user client with the password cisco.
2. In global configuration mode assign the user client attributes.

**username client password 4IncP7vTjpaba2aF encrypted**

**username client attributes**

**vpn-group-policy remote\_users**

1. From the ASA Config tab select the User Manager.
2. Select Username client.
3. Select Bookmark Engineering.
4. Select Group Policy remote\_users.
5. Enter the Profile Name client-profile.
6. Press the set button.

## Verify configuration:

Using the following test insure the lab meets the above requirements.

### Inside:

1. From the Local PC-1 ping 209.165.200.11. (this may require doing it twice)
2. From the Local PC-1 ping 192.168.1.200. (this may require doing it twice)
3. From the Local PC-1 open the desktop and browse to freeccnalab.com
4. From the Local PC-1 open the desktop and browse to SharePoint.

### DMZ:

1. From the Local LT-1 ping 192.168.2.200. (this may require doing it twice)
2. From the Local LT-1 ping 209.165.200.11. (this may require doing it twice)
3. From the Local PC-1 open the desktop and browse to freeccnalab.com.
4. From the Local PC-1 open the desktop and browse to Local.

### Remote:

1. From the Remote PC ping 209.165.200.11. (this may require doing it twice)
2. From the Remote PC ping 192.168.1.200.
3. From the Remote PC ping 192.168.2.200.
4. From the Remote PC open the desktop and browse to freeccnalab.com.
5. From the Remote PC open the desktop and browse to SharePoint.
6. From the Remote PC open the desktop and browse to <https://209.165.200.226>.
7. Enter the username client and password cisco.
8. Navigate to Engineering in the list.
9. Insure you can access the Engineering server.