Clientless SSL VPN on the Cisco ASA 5505 Firewall

**Purpose;** To create a clientless SSL VPN connection on the Cisco ASA 5505 Firewall for remote access to web pages without the use of the client

**Background information:** Cisco`s ASA firewall is a security device that provides protection along with firewall and antivirus capabilities. The incorporated GUI (ASDM) that allows the firewall to be remotely managed. An important part of the ASDM is the wizards that installed into the GUI, such as the Clientless SSL VPN. By utilizing the clientless SSL VPN we can remotely access any webpage without a VPN client making the connection much easier.

**Lab Summary,** in this lab, we have access to the ASDM and will navigate to the wizards along the top tool bar. From the wizard’s section we will select VPN Wizards and followed by the option for a Clientless VPN.

Clientless SSL VPN walkthrough,

1. Firstly, you need to self-assign a trust point identity certificate. To do this you must open the Certification GUI located at the bottom, then exit out of the VPN wizard, go through the process for the simple certificate. This process is just clicking next a few times. Then reenter the VPN get to the certification step and click on the certificate you just created (look under date and find the one that matches your date and time)
2. After creating the certificate and selecting your certificate, the next step is to assign a primary DNS server. You can use any DNS server whether it be your Comcast or century link DNS server or a public one such as Google’s (4.4.4.4) or Microsoft`s (8.8.8.8)
3. Then under DNS lookup, DNS lookup must be enabled for one if not both interfaces. The outside or inside interface must be enabled.
4. We must create a new policy group or use the default policy group. I created a new one to give myself more flexibility over the settings, but the default policy group works as well. Make sure you know which connection profile goes with the policy group as we will use that later to sign into the SSL Clientless VPN
5. We must allow the outside interface access to the Clientless SSL VPN
6. Finally, until further notice we can skip the addition of book marks to our Clientless SSL VPN as they will not be useful until we get into the VPN and begin to visit sites.

After creating your Clientless SSL VPN in the ASDM Wizard we will venture to the webpage to make the connection. We will use the address of the outside address of the ASA and go to the admin page e.g. <https://xxxx.xxxx.xxxx.xxxx/admin>

When prompted enter the username and password of your client profile connected to your policy group that is associated with the Clientless SSL VPN. After gaining access to the Clientless SSL VPN you can enter the web address of any webpage and have a remote connection to the web page.

**Commands:**

ASA Version 9.2(4)14

!

hostname ciscoasa

enable password 8Ry2YjIyt7RRXU24 encrypted

names

ip local pool IPV4POOL1 192.168.11.1-192.168.11.10 mask 255.255.255.0

!

interface Ethernet0/0

 switchport access vlan 2

!

interface Ethernet0/1

!

interface Ethernet0/2

!

interface Ethernet0/3

!

interface Ethernet0/4

!

interface Ethernet0/5

!

interface Ethernet0/6

!

interface Ethernet0/7

!

interface Vlan1

 nameif inside

 security-level 100

 ip address 192.168.10.1 255.255.255.0

!

interface Vlan2

 nameif outside

 security-level 0

 ip address dhcp setroute

!

ftp mode passive

dns domain-lookup inside

dns domain-lookup outside

dns server-group DefaultDNS

 name-server 4.4.4.4

 name-server 8.8.8.8

object network obj\_any

 subnet 0.0.0.0 0.0.0.0

object network INSIDE\_SUBNET

 subnet 192.168.10.0 255.255.255.0

object network NETWORK\_OBJ\_192.168.11.0\_28

 subnet 192.168.11.0 255.255.255.240

object-group icmp-type ALLOW\_ICMP

 icmp-object echo-reply

 icmp-object time-exceeded

 icmp-object unreachable

 icmp-object traceroute

access-list INBOUND extended permit icmp any any object-group ALLOW\_ICMP

pager lines 24

logging enable

logging asdm informational

mtu inside 1500

mtu outside 1500

icmp unreachable rate-limit 1 burst-size 1

asdm image disk0:/asdm-751.bin

no asdm history enable

arp timeout 14400

no arp permit-nonconnected

!

object network obj\_any

 nat (inside,outside) dynamic interface

object network INSIDE\_SUBNET

 nat (inside,outside) dynamic interface

access-group INBOUND in interface outside

timeout xlate 3:00:00

timeout pat-xlate 0:00:30

timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02

timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00

timeout sip 0:30:00 sip\_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00

timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute

timeout tcp-proxy-reassembly 0:01:00

timeout floating-conn 0:00:00

dynamic-access-policy-record DfltAccessPolicy

user-identity default-domain LOCAL

http server enable

http 192.168.1.0 255.255.255.0 inside

http 0.0.0.0 0.0.0.0 inside

http 0.0.0.0 0.0.0.0 outside

no snmp-server location

no snmp-server contact

crypto ipsec ikev2 ipsec-proposal DES

 protocol esp encryption des

 protocol esp integrity sha-1 md5

crypto ipsec ikev2 ipsec-proposal 3DES

 protocol esp encryption 3des

 protocol esp integrity sha-1 md5

crypto ipsec ikev2 ipsec-proposal AES

 protocol esp encryption aes

 protocol esp integrity sha-1 md5

crypto ipsec ikev2 ipsec-proposal AES192

 protocol esp encryption aes-192

 protocol esp integrity sha-1 md5

crypto ipsec ikev2 ipsec-proposal AES256

 protocol esp encryption aes-256

 protocol esp integrity sha-1 md5

crypto ipsec security-association pmtu-aging infinite

crypto dynamic-map SYSTEM\_DEFAULT\_CRYPTO\_MAP 65535 set ikev2 ipsec-proposal AES256 AES192 AES 3DES DES

crypto map outside\_map 65535 ipsec-isakmp dynamic SYSTEM\_DEFAULT\_CRYPTO\_MAP

crypto map outside\_map interface outside

crypto ca trustpoint ASDM\_Launcher\_Access\_TrustPoint\_0

 enrollment self

 fqdn none

 subject-name CN=192.168.10.1,CN=ciscoasa

 keypair ASDM\_LAUNCHER

 crl configure

crypto ca trustpool policy

crypto ca certificate chain ASDM\_Launcher\_Access\_TrustPoint\_0

 certificate e0b61748

    308201cb 30820134 a0030201 020204e0 b6174830 0d06092a 864886f7 0d010105

    0500302a 3111300f 06035504 03130863 6973636f 61736131 15301306 03550403

    130c3139 322e3136 382e3130 2e31301e 170d3038 30343330 30303039 33355a17

    0d313830 34323830 30303933 355a302a 3111300f 06035504 03130863 6973636f

    61736131 15301306 03550403 130c3139 322e3136 382e3130 2e313081 9f300d06

    092a8648 86f70d01 01010500 03818d00 30818902 818100c3 3e672d94 48e385a8

    edae88a6 9713eb61 ab5c919b f212569c 77284baa fdaacec1 f350dbc9 2272c77d

    7d77c9e6 1d5d3d70 14590554 86852844 c40e7cf5 4eb22450 6d636ffa 38cac53d

    baa2f9a4 dc47b9e1 152b061e a29f6096 df181aab f02559eb 12f4ca95 6cf01873

    49db3136 7f3b2009 a3549296 c49c9c94 c16cdb72 5bb7f102 03010001 300d0609

    2a864886 f70d0101 05050003 81810046 a2a75850 cf737497 e4b83f64 f3e0e44e

    dbc4b8d4 4628e5b3 08acf34c 9b1021be 2a6c43a5 2247c26a 68f2397c 57bde812

    a284dd1e e67fd88c eb9a1408 3dbb24e0 766c6dcc 20d53024 a07cfa4e 26cf685b

    ed520b23 39d528fe f337cde6 57d104dd 276741f3 e1679262 e684e403 c7535631

    5aac1446 9447093f c42a36fe 4f184d

  quit

crypto ikev2 policy 1

 encryption aes-256

 integrity sha

 group 5 2

 prf sha

 lifetime seconds 86400

crypto ikev2 policy 10

 encryption aes-192

 integrity sha

 group 5 2

 prf sha

 lifetime seconds 86400

crypto ikev2 policy 20

 encryption aes

 integrity sha

 group 5 2

 prf sha

 lifetime seconds 86400

crypto ikev2 policy 30

 encryption 3des

 integrity sha

 group 5 2

 prf sha

 lifetime seconds 86400

crypto ikev2 policy 40

 encryption des

 integrity sha

 group 5 2

 prf sha

 lifetime seconds 86400

crypto ikev2 enable outside client-services port 443

crypto ikev2 remote-access trustpoint ASDM\_Launcher\_Access\_TrustPoint\_0

telnet 0.0.0.0 0.0.0.0 inside

telnet 0.0.0.0 0.0.0.0 outside

telnet timeout 5

no ssh stricthostkeycheck

ssh 0.0.0.0 0.0.0.0 inside

ssh 0.0.0.0 0.0.0.0 outside

ssh timeout 5

ssh key-exchange group dh-group1-sha1

console timeout 0

dhcpd auto\_config outside

!

dhcpd address 192.168.10.100-192.168.10.110 inside

dhcpd enable inside

!

threat-detection basic-threat

threat-detection statistics access-list

no threat-detection statistics tcp-intercept

ssl trust-point ASDM\_Launcher\_Access\_TrustPoint\_0 outside

ssl trust-point ASDM\_Launcher\_Access\_TrustPoint\_0 inside vpnlb-ip

ssl trust-point ASDM\_Launcher\_Access\_TrustPoint\_0 inside

webvpn

 enable outside

 anyconnect image disk0:/anyconnect-win-2.5.3055-k9.pkg 1

 anyconnect profiles live1\_client\_profile disk0:/live1\_client\_profile.xml

 anyconnect profiles test1\_client\_profile disk0:/test1\_client\_profile.xml

 anyconnect enable

 tunnel-group-list enable

group-policy SSLVPNGRPPOLICY internal

group-policy SSLVPNGRPPOLICY attributes

 vpn-tunnel-protocol ssl-clientless

 webvpn

  url-list none

group-policy GroupPolicy\_test1 internal

group-policy GroupPolicy\_test1 attributes

 wins-server none

 dns-server value 192.168.10.3

 vpn-tunnel-protocol ikev2 ssl-client

 default-domain none

 webvpn

  anyconnect profiles value test1\_client\_profile type user

group-policy GroupPolicy\_live1 internal

group-policy GroupPolicy\_live1 attributes

 wins-server none

 dns-server value 192.168.10.3

 vpn-tunnel-protocol ikev2 ssl-client ssl-clientless

 default-domain none

 webvpn

  anyconnect profiles value live1\_client\_profile type user

username live password mqoTSarIRLgKElOW encrypted

username cisco password 3USUcOPFUiMCO4Jk encrypted privilege 0

username cisco attributes

 vpn-group-policy SSLVPNGRPPOLICY

tunnel-group test1 type remote-access

tunnel-group test1 general-attributes

 address-pool IPV4POOL1

 default-group-policy GroupPolicy\_test1

tunnel-group test1 webvpn-attributes

 group-alias test1 enable

tunnel-group live1 type remote-access

tunnel-group live1 general-attributes

 address-pool IPV4POOL1

 default-group-policy GroupPolicy\_live1

tunnel-group live1 webvpn-attributes

 group-alias live1 enable

tunnel-group SSLVPN type remote-access

tunnel-group SSLVPN general-attributes

 default-group-policy SSLVPNGRPPOLICY

tunnel-group SSLVPN webvpn-attributes

 group-alias SSLVPN enable

!

class-map inspection\_default

 match default-inspection-traffic

!

!

policy-map type inspect dns preset\_dns\_map

 parameters

  message-length maximum client auto

  message-length maximum 512

policy-map global\_policy

 class inspection\_default

  inspect dns preset\_dns\_map

  inspect ftp

  inspect h323 h225

  inspect h323 ras

  inspect rsh

  inspect rtsp

  inspect esmtp

  inspect sqlnet

  inspect skinny

  inspect sunrpc

  inspect xdmcp

  inspect sip

  inspect netbios

  inspect tftp

  inspect ip-options

!

service-policy global\_policy global

prompt hostname context

no call-home reporting anonymous

Cryptochecksum:50bdcc9acc279a419f2e638608d4a8ef

: end

**Problems:**

I did have a few problems with getting the correct service policy group to show up (I had named mine SSLGRPPOLICY) and had to add an alias of the same name to get the group policy to show up when accessing the login page for the Clientless SSLVPN.

**Conclusion:** This lab is an excellent counterpart to the Remote Access VPN introduction I did previously as in conjunction both of these VPN`s can cover nearly all of your needs in regard to VPN`s. We have a clientless VPN for easy connections and a beefier VPN for established connections. The clientless VPN is incredibly useful as it was simple to set up, easy and intuitive to use, and worked remarkably quickly.