1/28/19

Remote access VPN-AnyConnect-Shared Secret

Cisco CCNAS Period 5

Purpose:

This lab is a very practical lab, as where it can be used anywhere at any time. It’s a very important security implement for businesses for protection against data hack and loss. Remote access VPN is slightly different from Site-to-Site VPN. Were Site to Site is a secure connection between two company’s routers for security between two established locations. On the other hand, you have Remote access VPN, where you can be anywhere with internet connection and be able to browse the web securely with your own VPN.

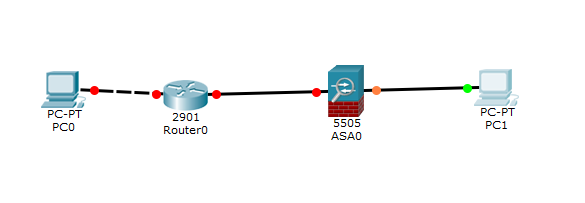
Background:

Remote access VPN had a few drops here and there, where we needed to research things about Split Tunneling and referring to applications and software such as Cisco AnyConnect. AnyConnect is a software that allows us to VPN through a set ASA with Remote access VPN setup on it to allow our traffic to be encrypted when accessing the public web. Split Tunneling allowed us to be able to connect to a public domain such as the internet and a local WAN or LAN simultaneously. The Wizard on the ASA allowed us to set up a Remote access VPN quite efficiently with only a few bumps. When the Remote access VPN is setup, it works like a secret message writer. First, the information you are trying to send out to the public network is sent to the VPN server you have connected to, then it will encrypt and send your information out from the VPN server, so the information looks like it’s coming from another place, successfully blocking anyone who wants to steal or track your information. This lab is slightly different from remote access where in the wizard, there is only one choice for what type of authentication you want to use. But if you want to do Shared secret VPN, you just list certifications as none and continue the wizard and it will configure the VPN as a shared secret. Older versions then the Cisco ASA 5505(9.2(4)) might have the option in the wizard to choose shared secrets. The Shared secret uses a tunnel to transfer traffic and you can verify this in the cog button of your Cisco AnyConnect client, though it might take a while to show up.

Lab Setup:

Simple setup: Cisco AnyConnect mobility client, 1 Cisco 2901 router, 1 Cisco 5505 ASA, and 2 Computers (one connected to the router and one on the inside interface of the ASA)

Topology:



ASA configurations:

hostname JASA

enable password 2KFQnbNIdI.2KYOU encrypted

names

ip local pool VPN\_Pool 10.14.0.5-10.14.0.20 mask 255.255.255.0

ip local pool Net\_Range 15.0.0.1-15.0.0.10 mask 255.255.255.0

interface Vlan1

nameif inside

security-level 50

ip address 10.14.0.1 255.255.255.0

interface Vlan2

nameif outside

security-level 50

ip address 172.16.10.1 255.255.255.0

ftp mode passive

same-security-traffic permit inter-interface

same-security-traffic permit intra-interface

object network obj\_any

subnet 0.0.0.0 0.0.0.0

object network NETWORK\_OBJ\_10.14.0.0\_27

subnet 10.14.0.0 255.255.255.224

access-list outside\_access\_out extended permit icmp any any

access-list VPNACL standard permit 10.14.0.0 255.255.255.0

pager lines 24

logging enable

logging asdm informational

mtu inside 1500

mtu outside 1500

icmp unreachable rate-limit 1 burst-size 1

icmp permit any inside

icmp permit any outside

no asdm history enable

arp timeout 14400

no arp permit-nonconnected

nat (inside,outside) source static any any destination static NETWORK\_OBJ\_10.14.0.0\_27 NETWORK\_OBJ\_10.14.0.0\_27 no-proxy-arp route-lookup

object network obj\_any

nat (inside,outside) dynamic interface

access-group outside\_access\_out out interface outside

route outside 192.168.1.2 255.255.255.255 172.16.10.2 1

user-identity default-domain LOCAL

http server enable

http 192.168.1.0 255.255.255.0 inside

http 10.14.0.0 255.255.255.0 inside

http 172.16.10.0 255.255.255.0 outside

http 10.14.0.0 255.255.255.0 outside

no snmp-server location

no snmp-server contact

crypto ipsec security-association pmtu-aging infinite

crypto ca trustpoint \_SmartCallHome\_ServerCA

no validation-usage

crl configure

crypto ca trustpoint Jeffs-vpn-Cert

enrollment self

subject-name CN=ciscoasa

keypair CCNP\_VPN\_KEY

crl configure

telnet timeout 5

no ssh stricthostkeycheck

ssh timeout 5

ssh key-exchange group dh-group1-sha1

console timeout 0

dhcpd auto\_config outside

!

threat-detection basic-threat

threat-detection statistics access-list

no threat-detection statistics tcp-intercept

webvpn

enable inside

enable outside

anyconnect image disk0:/anyconnect-win-2.0.0343-k9.pkg 1

anyconnect enable

tunnel-group-list enable

group-policy GroupPolicy\_SSL\_VPN internal

group-policy GroupPolicy\_SSL\_VPN attributes

wins-server value 8.8.8.8

dns-server value 8.8.8.8

vpn-tunnel-protocol ssl-client

split-tunnel-network-list value VPNACL

default-domain value cisco.com

group-policy GroupPolicy\_Jeffrey-VPN internal

group-policy GroupPolicy\_Jeffrey-VPN attributes

wins-server value 8.8.8.8

dns-server value 8.8.8.8

vpn-tunnel-protocol ssl-client

default-domain value Cisco.com

username jeffrey password F.se0xFQ7j.paL/Y encrypted

tunnel-group SSL\_VPN type remote-access

tunnel-group SSL\_VPN general-attributes

address-pool VPN\_Pool

address-pool Net\_Range

default-group-policy GroupPolicy\_SSL\_VPN

tunnel-group SSL\_VPN webvpn-attributes

group-alias SSL\_VPN enable

tunnel-group Jeffrey-VPN type remote-access

tunnel-group Jeffrey-VPN general-attributes

address-pool VPN\_Pool

default-group-policy GroupPolicy\_Jeffrey-VPN

tunnel-group Jeffrey-VPN webvpn-attributes

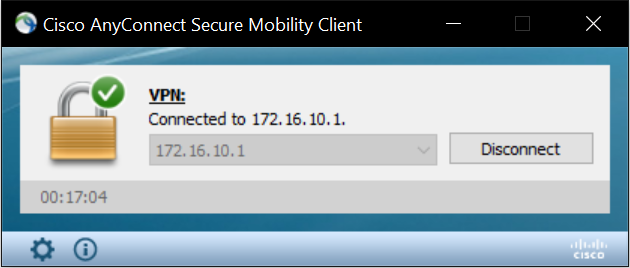
group-alias Jeffrey-VPN enable

Router Configurations:

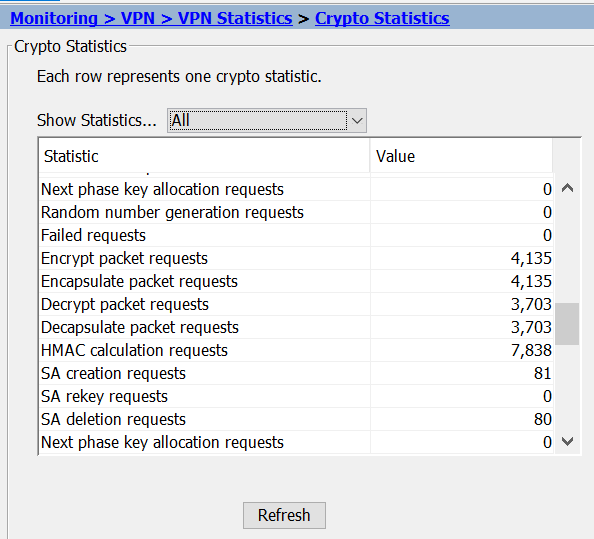
Basic router Configurations such as ip address:

<Omitted for it is redundant>

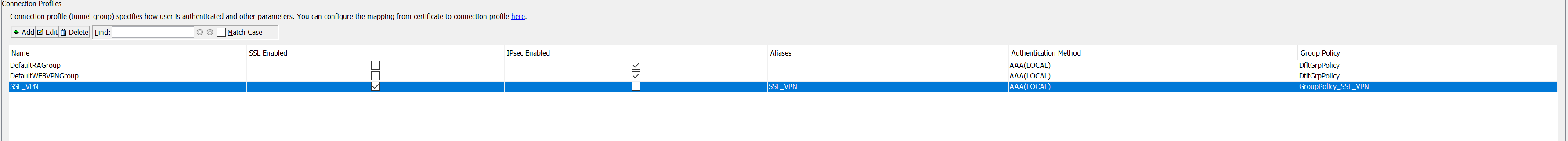
Screen Shots:



This is the AnyConnect Client working and connected to my ASA’s external IP Address



This is the Monitoring on the Cisco ASA where it tells us how many packets have been encapsulated or encrypted and decrypted.



This is the SSL client that I made on the ASA with the Wizard.

Problems:

No problems this time around except for the fact that we couldn’t find the button for shared secret and found out that it is just leaving the certificates blank. There were no up to date guides online for use to use but everything was the same with setting it up. Also, for some reason, Jaxon’s computer couldn’t RDP out, but I could RDP in. And everything was checked to allow it.

Conclusion:

Not feeling that it was any different from Certificate VPN. Only the set-up wizard was a bit different.