10/25/18

CCNAS Site to Site VPN

Jeffrey Xu period 5

10/25/18

**Purpose:**

This lab was a very important one. Site to Site VPN is one of the most fundamental configurations in security. Site to Site VPN allows packets and information between two networks to be encrypted so hackers with Wireshark can’t sniff the packets and steal information. Most other configurations go hand in hand with site to site VPN.

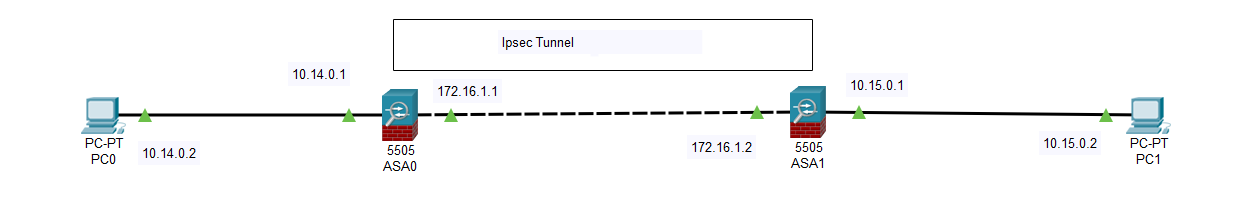
**BACKGROUND:**

Site to Site VPN is a way to encrypt traffic between to networks over the internet. The way Site to Site VPN works is like this: imagine you have a VIP(Information) who wants to get from one city(router/firewall) to another. But in between the two cities(internet), there are lots of enemies. So, they disguise the VIP with a special box(protocol) called ISAKMP. So, when the VIP is traveling between the two cities, the enemies don’t know what’s under the box. This allows us to keep our traffic secure. The first time you set up this lab, it’s hard. But after multiple trial and error, I was able to gain a deeper understanding on what I needed to add to my configurations. There are many aspects of this lab such as Crypto map, including IPSEC tunneling, interesting traffic with access-lists and Nat. All of these had to be configured with caution because ASA’s are really picky on what you write. The ASA’s wording and setup with commands also needed to be counted for.

**LAB SETUP:**

For this lab, we included 2 ASA’s and a Switch for Monitoring the information coming through the interfaces. I didn’t use ASDM much and preferred using CLI to configure my ASA instead, only using it to check statuses. You could add a router in between the two ASA and it wouldn’t change that much.

Topology:



Configurations for ASA1:

hostname Site-A

enable password 2KFQnbNIdI.2KYOU encrypted

names

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 0

ip address 10.14.0.1 255.255.255.0

interface Vlan2

nameif outside

security-level 0

ip address 172.16.1.1 255.255.255.0

ftp mode passive

same-security-traffic permit inter-interface

object network obj\_any

subnet 0.0.0.0 0.0.0.0

object network Local-Network

subnet 10.14.0.0 255.255.255.0

object network External-Network

subnet 10.15.0.0 255.255.255.0

access-list 111 extended permit ip object Local-Network object External-Network

pager lines 24

logging asdm informational

mtu outside 1500

mtu inside 1500

icmp unreachable rate-limit 1 burst-size 1

icmp permit any outside

icmp permit any inside

no asdm history enable

arp timeout 14400

no arp permit-nonconnected

nat (inside,outside) source static Local-Network Local-Network destination static External-Network External-Network no-proxy-arp route-lookup

object network obj\_any

nat (inside,outside) dynamic interface

route outside 0.0.0.0 0.0.0.0 172.16.1.2 1

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 10.14.0.0 255.255.255.0 inside

no snmp-server location

no snmp-server contact

crypto ipsec ikev1 transform-set ESP-AES-SHA esp-aes esp-sha-hmac

crypto ipsec security-association pmtu-aging infinite

crypto map outside\_map 1 match address 111

crypto map outside\_map 1 set pfs group1

crypto map outside\_map 1 set peer 172.16.1.2

crypto map outside\_map 1 set ikev1 transform-set ESP-AES-SHA

crypto map outside\_map interface outside

crypto ca trustpoint \_SmartCallHome\_ServerCA

no validation-usage

crl configure

crypto ca trustpool policy

crypto ca certificate chain \_SmartCallHome\_ServerCA

crypto ikev1 enable outside

crypto ikev1 enable inside

crypto ikev1 policy 10

authentication pre-share

encryption aes

hash sha

group 2

lifetime 86400

telnet timeout 5

no ssh stricthostkeycheck

ssh timeout 5

ssh key-exchange group dh-group1-sha1

console timeout 0

no threat-detection statistics tcp-intercept

tunnel-group 172.16.1.2 type ipsec-l2l

tunnel-group 172.16.1.2 ipsec-attributes

ikev1 pre-shared-key \*\*\*\*\*

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

inspect icmp

inspect icmp error

service-policy global\_policy global

prompt hostname context

call-home reporting anonymous

Cryptochecksum:0b6ae6dbcec2d6f0900f1e199823ee23

: end

Configurations for ASA2:

hostname Site-B

enable password 2KFQnbNIdI.2KYOU encrypted

names

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 0

ip address 10.15.0.1 255.255.255.0

interface Vlan2

nameif outside

security-level 0

ip address 172.16.1.2 255.255.255.0

ftp mode passive

same-security-traffic permit inter-interface

object network obj\_any

subnet 0.0.0.0 0.0.0.0

object network Local-Network

subnet 10.15.0.0 255.255.255.0

object network External-Network

subnet 10.14.0.0 255.255.255.0

access-list 111 extended permit ip object Local-Network object External-Network

pager lines 24

logging asdm informational

mtu outside 1500

mtu inside 1500

no failover

icmp unreachable rate-limit 1 burst-size 1

icmp permit any outside

icmp permit any inside

no asdm history enable

arp timeout 14400

no arp permit-nonconnected

nat (inside,outside) source static Local-Network Local-Network destination static External-Network External-Network no-proxy-arp route-lookup

object network obj\_any

nat (inside,outside) dynamic interface

route outside 0.0.0.0 0.0.0.0 172.16.1.1 1

route outside 10.14.0.0 255.255.255.0 10.14.0.2 1

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 10.15.0.0 255.255.255.0 inside

no snmp-server location

no snmp-server contact

crypto ipsec ikev1 transform-set ESP-AES-SHA esp-aes esp-sha-hmac

crypto ipsec security-association pmtu-aging infinite

crypto map outside-map 1 match address 111

crypto map outside-map 1 set pfs group1

crypto map outside-map 1 set peer 172.16.1.1

crypto map outside-map 1 set ikev1 transform-set ESP-AES-SHA

crypto map outside-map interface outside

crypto ca trustpoint \_SmartCallHome\_ServerCA

no validation-usage

crl configure

crypto ca trustpool policy

crypto ikev1 enable outside

crypto ikev1 enable inside

crypto ikev1 policy 1

authentication pre-share

encryption aes

hash sha

group 2

lifetime 86400

tunnel-group 172.16.1.1 type ipsec-l2l

tunnel-group 172.16.1.1 ipsec-attributes

ikev1 pre-shared-key \*\*\*\*\*

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

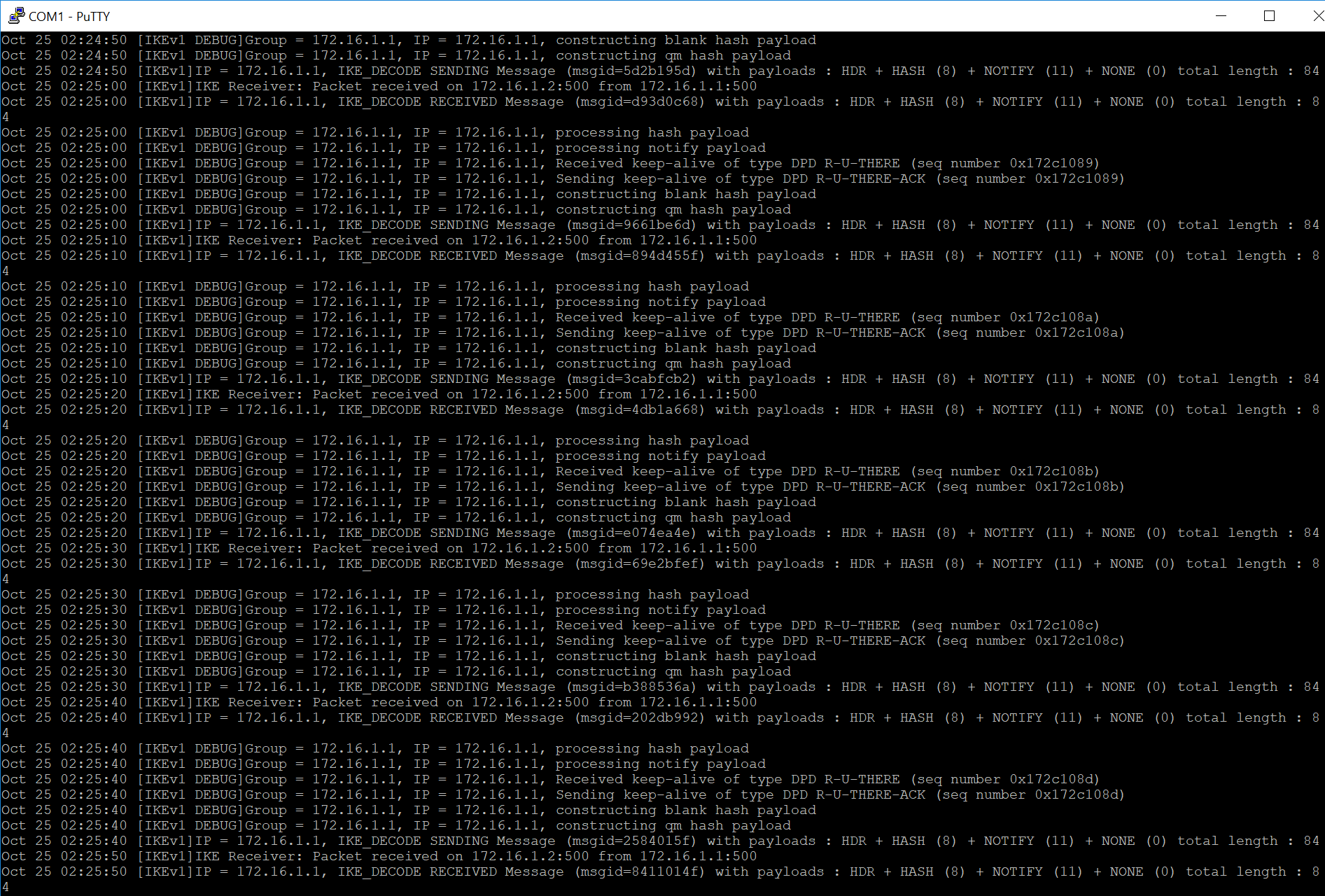
inspect ip-options

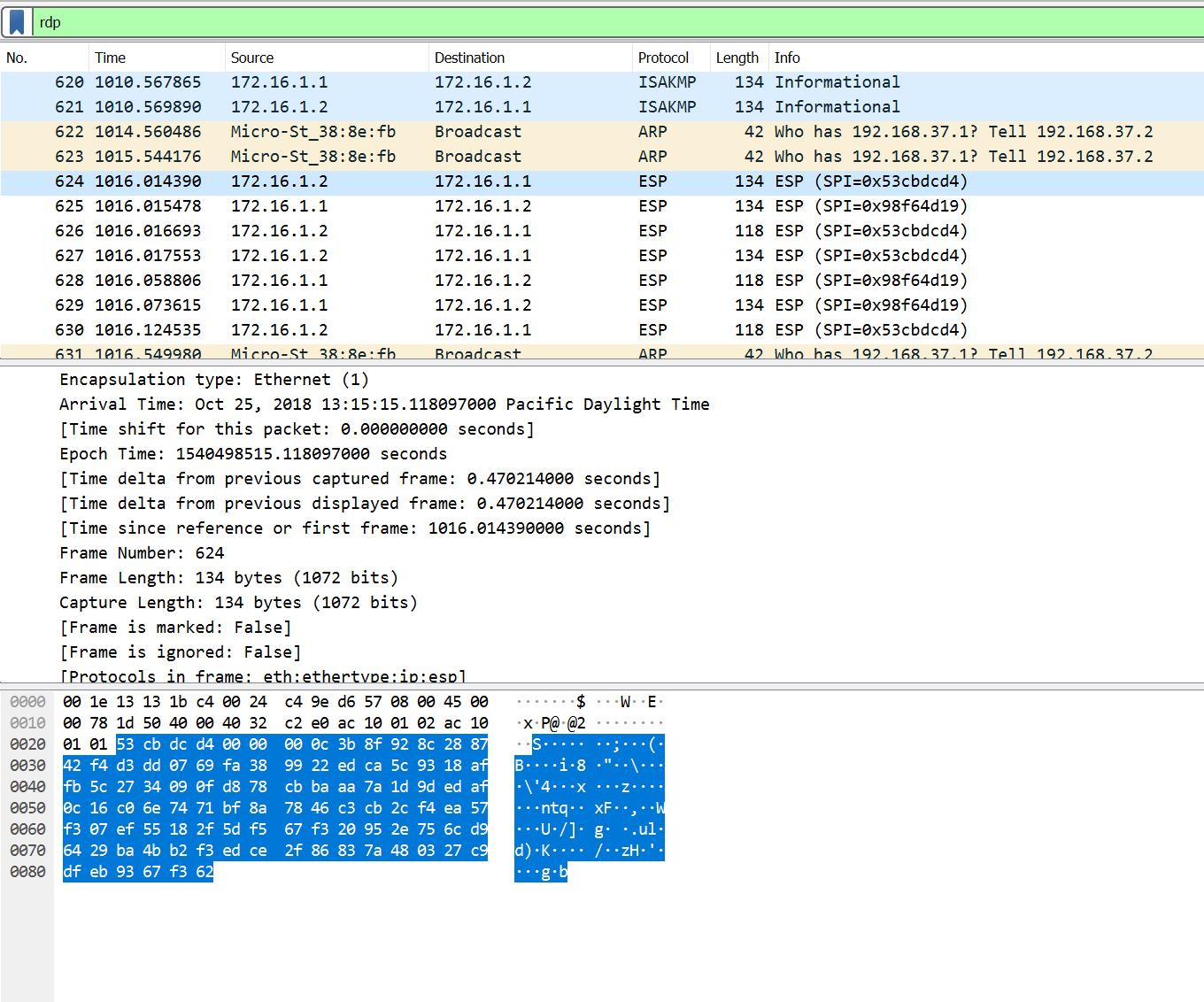
service-policy global\_policy global

Cryptochecksum:c73c05bfb879c0193e6600302f91fa9a

: end

Debug and Wireshark





**Problems:**

I had many problems with the wording of different commands in the ASA. Some of the guides online were outdates with only a few to research. I used too much time trying to get ICMP working but in the end, didn’t even need to configure it and made my way through. I had problems with the new access-list system with egress and ingress. Crypto map and IKSAPM stuff was easy at first, but I understood nothing until I configured it 3-4 times. Most of my time was worrying about Pinging and ICMP packets. Interesting traffic was a bit wearied until I started understanding Crypto map. To deal with the ISAKMP problems and IPSEC problems, I used the Debug crypto ISAKMP/IPSEC 127 to find out what was wrong with the transferring of data.

**Conclusion:**

Overall, I feel like this lab was very beneficial to learn. I believe that we are going to be doing more and more labs with Site to Site VPN or other types of VPN included. I used too much time working on ICMP packets and not focusing on VPN itself. I learned a lot more about how to use ASA and their behavior and how they act with another ASA.