Configuring Site to Site VPN on Cisco ASA 5510 v8.2

1.) Configure ISAKMP (IKE phase I)

enable ISAKMP on Interface:

```
ASA(config)# crypto isakmp enable [interface]
```

Configure Policy

```
ASA(config)# crypto isakmp policy [number]
ASA(config-isakmp-policy)# encryption [des, 3des, AES]
ASA(config-isakmp-policy)# authentication [psk, cert, crack]
ASA(config-isakmp-policy)# hash [md5, sha]
ASA(config-isakmp-policy)# group [DH group 1, 2, 5]
ASA(config-isakmp-policy)# lifetime [time in seconds]
```

(note: this is the lifetime of the KEY, not the tunnel)

2.) Configure IPsec (Phase II)

Define Transform Set

```
ASA(config)# crypto ipsec transform-set [name] [set 1] [set 2]
```

Multiple options with this command. Use esp-3des for set 1and esp-sha-hmac for set2. (Set 2 is the authentication)

```
ASA(config)# crypto ipsec security-association lifetime seconds
[lifetime in seconds]
ASA(config)# crypto ipsec security-association lifetime kilobytes
[lifetime in KB]
```

Note: the last 2 commands, configure the lifetime of the TUNNEL before it is re-built.

3.) configure ACL's

Create 1 Access List to identify the source/destination traffic that should be encrypted and put in the tunnel.

```
ASA(config)# access-list OUTSIDE_CRYPTO_1 extended permit ip [source
ip/mask] [destination ip/mask]
```

Create a second ACL for the NAT zero. The ACL should be exactly the same as the one above (or at least it normally will be), however they MUST be different names.

```
ASA(config)# access-list INSIDE_NAT0_OUT extended permit ip [source
ip/mask] [destination ip/mask]
```

4.) Configure NAT zero

NAT zero will exclude IP addresses from network address translation. This is for specific use when trying to get traffic into a VPN tunnel.

```
ASA(config)#  nat (inside) 0 access-list INSIDE_NAT0_OUT
```

5.) Create Crypto Map

```
ASA(config)#  crypto map [name] [number] match address [acl name]
```

In our case, the acl name is OUTSIDE_CRYPTO_1

```
ASA(config)#  crypto map [name] [number]  set pfs group1
ASA(config)#  crypto map [name] [number]  set peer [peer IP address]
ASA(config)#  crypto map [name] [number]  set transform-set [transform-
set name]
ASA(config)#  crypto map [name] interface outside
```

6.) Create tunnel group

```
ASA(config)#  tunnel-group [peer ip address/name] type ipsec-l2l
ASA(config)#  tunnel-group [peer ip address/name] ipsec-attributes
ASA(config-tunnel-ipsec)#  pre-shared-key [key]
```