Cisco ASA Site to Site

Verification: NAT or transparent mode

> Value should return (Firewall mode: Router)

```
show firewall
```

> **Always do a backup!!!**

```
copy running-config disk0:/running-config-backup-DDMMYYYY
```

ACL / No NAT Rules

Change net-local and and remote for local and remote IP

> You do not need to create a object for the LAN if you already have one for another tunnel // You also **can not** have 2 tunnels with the same remote IP's

```
object-group network net-local
network-object 10.1.2.0 255.255.255.0
object-group network net-remote
network-object 192.168.1.0 255.255.255.0
```

Create a cryptomap ACL

```
access-list outside_1_cryptomap extended permit ip object-group net-local object-group net-remote
```

Allow traffic between the two sites to bypass NAT

> Always check the name of interface on the port channel, the tunnel will not work if your interface is named inside3

```
nat (inside,outside) source static net-local net-local destination static net-remote net-remote
```

IKEV1 - Route based

```
tunnel-group 199.168.1.100 type ipsec-l2l
tunnel-group 199.168.1.100 ipsec-attributes
 ikev1 pre-shared-key *****

crypto ikev1 policy 10
 authentication pre-share
 encryption aes-256
 hash sha
 lifetime 3600
 group 5

crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac

crypto ipsec profile vpn1
 set ikev1 transform-set ESP-AES-256-SHA
 set security-association lifetime seconds 3600

interface Tunnel1
 nameif int-vpn1
 ip address 192.168.0.1 255.255.255.252
 tunnel source interface outside
 tunnel destination 199.168.1.100
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile vpn1

access-list vpn1-inbound extended permit ip any any
access-list vpn1-outbound extended permit ip any any
access-group vpn1-inbound in interface int-vpn1
access-group vpn1-outbound out interface int-vpn1

route int-vpn1 10.10.10.0 255.255.255.0 192.168.0.2 1
```

IKEV1 - Policy based

Create the tunnel group, and configure the pre-shared key. (In ex; 199.168.1.100 = Remote WAN)

```
tunnel-group 199.168.1.100 type ipsec-l2l
tunnel-group 199.168.1.100 ipsec-attributes
pre-shared-key INSERT_SECURE_PRE_SHARED_KEY_HERE
```

Declare the most common transform sets (only do once).

```
crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
```

Phase 1 parameters

```
crypto ikev1 policy 10
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
### Enable ikev1 on the outside interface - THIS JUST NEED TO BE CONFIGURED ONCE YOU SETUP THE
FIRST VPN
crypto ikev1 enable outside
crypto ikev1 am-disable #(// Main mode remove this line for aggressive mode)
```

Enable ikev1 on the outside interface -**THIS JUST NEED TO BE DONE ON THE FIRST IKEV1 VPN**

```
crypto ikev1 enable outside
```

Set main mode // Do not include this line for aggressive mode

> This is a global setting, if you add the line bellow in a ASA that contains a tunnel that uses aggressive mode, it will break the other tunnel

```
crypto ikev1 am-disable
```

Phase 2 parameters

> If you remove the ACL used by a tunnel, it will **remove** the line crypto map outside_map 1 match address ACL_NAME // Only set **PFS** if configured on the remote side, else skip the line

```
crypto map outside_map 1 match address outside_1_cryptomap
crypto map outside_map 1 set peer 199.168.1.100
crypto map outside_map 1 set transform-set ESP-3DES-SHA
crypto map outside_map 1 set pfs group2
crypto map outside_map 1 set security-association lifetime seconds 3600
```

Enable the crypto map in the outside interface - **THIS JUST NEED TO BE DONE ON THE FIRST IKEV1 VPN**

```
crypto map outside_map interface outside
```

IKEV2

Create the tunnel group, and configure the pre-shared key. (In ex; 199.168.1.100 = Remote WAN)

```
group-policy GroupPolicy_IKEv2 internal
group-policy GroupPolicy_IKEv2 attributes
vpn-idle-timeout none
vpn-tunnel-protocol ikev2

tunnel-group 199.168.1.100 type ipsec-l2l
tunnel-group 199.168.1.100 general-attributes
default-group-policy GroupPolicy_IKEv2
tunnel-group 199.168.1.100 ipsec-attributes
ikev2 remote-authentication pre-shared-key ***
ikev2 local-authentication pre-shared-key ***
```

Declare the transform sets

```
crypto ipsec ikev2 ipsec-proposal ESP-AES-256-SHA
 protocol esp encryption aes-256
 protocol esp integrity sha-1
```

Phase 1 parameters

```
crypto ikev2 policy 20
encryption aes-256
integrity sha
group 2
prf sha
lifetime seconds 86400
```

Phase 2 parameters

```
crypto map outside_map 1 match address outside_1_cryptomap
crypto map outside_map 1 set pfs
crypto map outside_map 1 set peer 199.168.1.100
crypto map outside_map 1 set ikev2 ipsec-proposal ESP-AES-256-SHA
crypto map outside_map 1 set security-association lifetime seconds 3600
crypto ikev2 enable outside
```

NAT

If the request needs to go over the nated IP, do no use the ACL / Nat rules above, configure something like this:

```
nat (INSIDE,OUTSIDE) source static PRENAT_IP POSTNAT_IP destination static DESTINATION_IP
DESTINATION_IP
```

```
access-list outside_1_cryptomap extended permit ip host NATTED_SOURCE_IP host
NATTED_DESTINATION_IP
```

Troubleshooting/Debug

Useful links:

- http://www.cisco.com/en/US/products/ps6120/products_tech_note09186a00807e0aca.shtml#solunf
- http://www.cisco.com/c/en/us/td/docs/security/asa/asa72/configuration/guide/conf_gd/ike.html
- http://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/vpn_ike.html#pgfId-1042302

Test connection (Run command 2x)

```
packet-tracer input inside icmp 10.1.2.100 8 0 192.168.1.100
```

Check IKEV1 Logs

```
debug crypto ikev1 127
```

Check IKEV2 Logs

```
debug crypto ikev2 protocal
```

Clear tunnel session

```
clear isakmp sa
```

Find pre-shared key

```
more system:running-config | grep pre-shared
```

Check basic VPN session information

```
sh isakmp sa
```

Check details on VPN session (Detailed)

```
show vpn-sessiondb detail ra-ikev1-ipsec
```

Capture traffic for the ACL related to the VPN

```
capture test access-list outside_1_cryptomap interface inside real-time
```

> Once you are done, always remember to save your config

Revision #13
Created 2017-08-21 19:45:45 UTC by Dave
Updated 2020-02-19 05:37:25 UTC