CONFIGUACIÓN VPN IPSEC ENTRE DOS ZONAS DMZ UTILIZANDO ASA5505 DE CISCO
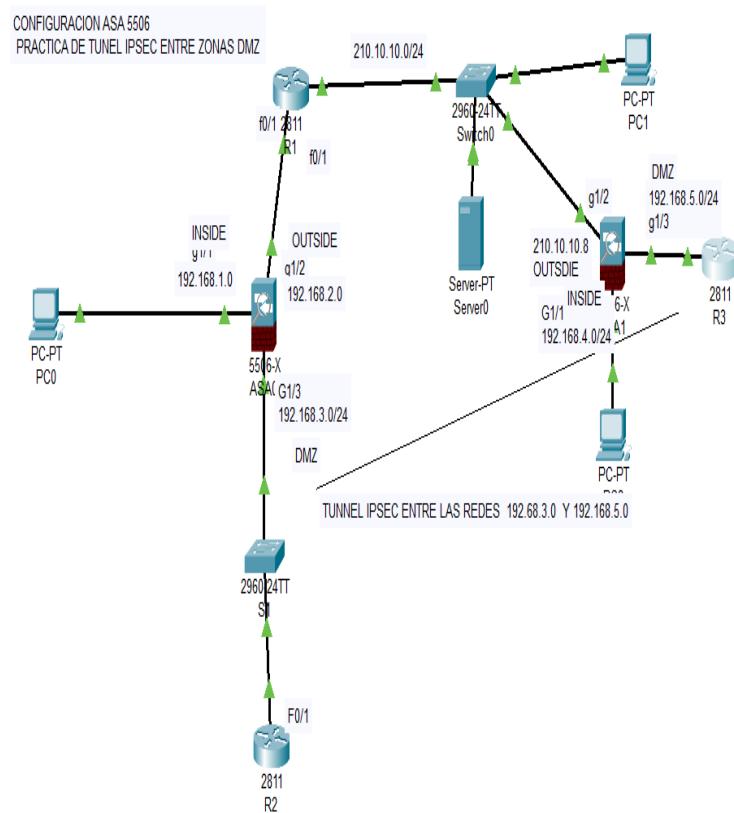

ASA1#sh run

: Saved

:

ASA Version 9.6(1)

```
!
hostname ASA1
names
!
interface GigabitEthernet1/1
nameif INSIDE
security-level 100
ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet1/2
nameif OUTSIDE
security-level 0
ip address 192.168.2.1 255.255.255.0
!
interface GigabitEthernet1/3
nameif DMZ
security-level 50
ip address 192.168.3.1 255.255.255.0
!
interface GigabitEthernet1/4
no nameif
no security-level
no ip address
shutdown
!
interface GigabitEthernet1/5
no nameif
no security-level
no ip address
shutdown
!
interface GigabitEthernet1/6
no nameif
no security-level
no ip address
shutdown
!
interface GigabitEthernet1/7
no nameif
no security-level
no ip address
shutdown
!
interface GigabitEthernet1/8
no nameif
no security-level
no ip address
```

```
shutdown
!
interface Management1/1
management-only
no nameif
no security-level
no ip address
shutdown
!
object network DMZ-NET
subnet 192.168.3.0 255.255.255.0
nat (DMZ,OUTSIDE) dynamic interface
object network INSIDE-NET
subnet 192.168.1.0 255.255.255.0
nat (INSIDE,OUTSIDE) dynamic interface
object network NET_LOCAL
subnet 192.168.3.0 255.255.255.0
object network NET_REMOTA
subnet 192.168.5.0 255.255.255.0
object network OUTSIDE-DMZ
subnet 192.168.2.0 255.255.255.0
nat (OUTSIDE,DMZ) dynamic interface
!
route OUTSIDE 0.0.0.0 0.0.0.0 192.168.2.2 1
!
access-list acl1 extended permit icmp any
access-list VPN_ACL extended permit ip object NET_LOCAL object NET_REMOTA
!
!
access-group acl1 in interface OUTSIDE
access-group acl1 out interface OUTSIDE
!
!
class-map inspection_default
match default-inspection-traffic
class-map revision
match default-inspection-traffic
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect tftp
policy-map politaglobal
```

```
class revision
inspect http
inspect icmp
!
service-policy global_policy global
!
telnet timeout 5
ssh timeout 5
!
!
crypto ipsec ikev1 transform-set VPN_SET esp-aes esp-sha-hmac
!
crypto map VPN_MAP 10 match address VPN_ACL
crypto map VPN_MAP 10 set peer 210.10.10.8
crypto map VPN_MAP 10 set ikev1 transform-set VPN_SET
crypto map VPN_MAP interface OUTSIDE
crypto ikev1 enable OUTSIDE
crypto ikev1 policy 10
encr aes
authentication pre-share
group 2
!
tunnel-group 210.10.10.8 type ipsec-l2l
tunnel-group 210.10.10.8 ipsec-attributes
ikev1 pre-shared-key cisco
!
ASA1#


R2>
R2>enable
R2#sh run
Building configuration...

Current configuration : 793 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R2
!
!
!
!
```

```
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO2811/K9 sn FTX10176789-
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface FastEthernet0/1
ip address 192.168.3.2 255.255.255.0
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.3.1
ip route 192.168.2.0 255.255.255.0 192.168.3.1
```

```
ip route 210.10.10.0 255.255.255.0 192.168.3.1
ip route 192.168.5.0 255.255.255.0 192.168.3.1
!
ip flow-export version 9
!
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
end


R2#

1#sh run
Building configuration...

Current configuration : 816 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1
!
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
```

!
!
!
license udi pid CISCO2811/K9 sn FTX101787HG-
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
ip address 210.10.10.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 192.168.2.2 255.255.255.0
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
ip classless
ip route 192.168.3.0 255.255.255.0 192.168.2.1
ip route 192.168.5.0 255.255.255.0 210.10.10.8
ip route 192.168.4.0 255.255.255.0 210.10.10.8
ip route 192.168.1.0 255.255.255.0 192.168.2.1
!
ip flow-export version 9
!
!
!
!

```
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
end


R1#

ASA-UFV#SH RUN
: Saved
:
ASA Version 9.6(1)
!
hostname ASA-UFV
names
!
interface GigabitEthernet1/1
nameif INSIDE
security-level 100
ip address 192.168.4.1 255.255.255.0
!
interface GigabitEthernet1/2
nameif OUTSIDE
security-level 0
ip address 210.10.10.8 255.255.255.0
!
interface GigabitEthernet1/3
nameif DMZ
security-level 50
ip address 192.168.5.1 255.255.255.0
!
interface GigabitEthernet1/4
no nameif
no security-level
no ip address
shutdown
!
interface GigabitEthernet1/5
```

```
no nameif
no security-level
no ip address
shutdown
!
interface GigabitEthernet1/6
no nameif
no security-level
no ip address
shutdown
!
interface GigabitEthernet1/7
no nameif
no security-level
no ip address
shutdown
!
interface GigabitEthernet1/8
no nameif
no security-level
no ip address
shutdown
!
interface Management1/1
management-only
no nameif
no security-level
no ip address
shutdown
!
object network DMZ-NET
subnet 192.168.5.0 255.255.255.0
nat (DMZ,OUTSIDE) dynamic interface
object network INSIDE-NET
subnet 192.168.4.0 255.255.255.0
nat (INSIDE,OUTSIDE) dynamic interface
object network NET_LOCAL
subnet 192.168.5.0 255.255.255.0
object network NET_REMOTA
subnet 192.168.3.0 255.255.255.0
object network OUTSIDE-DMZ
subnet 210.10.10.0 255.255.255.0
nat (OUTSIDE,DMZ) dynamic interface
!
route OUTSIDE 0.0.0.0 0.0.0.0 210.10.10.1 1
!
access-list acl1 extended permit icmp any
```

```
access-list VPN_ACL extended permit ip object NET_LOCAL object NET_REMOTA
!
!
access-group acl1 in interface OUTSIDE
access-group acl1 out interface OUTSIDE
!
!
class-map inspection_default
match default-inspection-traffic
class-map revision
match default-inspection-traffic
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect tftp
policy-map politicarevisa
class revision
inspect dns
inspect ftp
inspect http
inspect icmp
inspect tftp
!
service-policy global_policy global
!
telnet timeout 5
ssh timeout 5
!
!
crypto ipsec ikev1 transform-set VPN_SET esp-aes esp-sha-hmac
!
crypto map VPN_MAP 10 match address VPN_ACL
crypto map VPN_MAP 10 set peer 192.168.2.1
crypto map VPN_MAP 10 set ikev1 transform-set VPN_SET
crypto map VPN_MAP interface OUTSIDE
crypto ikev1 enable OUTSIDE
crypto ikev1 policy 10
encr aes
authentication pre-share
group 2
!
tunnel-group 192.168.2.1 type ipsec-l2l
```

```
tunnel-group 192.168.2.1 ipsec-attributes
ikev1 pre-shared-key cisco
!
ASA-UFV#

R_DMZ2>
R_DMZ2>ENABLE
R_DMZ2#
R_DMZ2#SH RUN
Building configuration...

Current configuration : 845 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R_DMZ2
!
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO2811/K9 sn FTX10175P9C-
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
```

```
!
!
!
!
!
interface FastEthernet0/0
ip address 192.168.5.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Vlan1
no ip address
shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.5.1
ip route 210.10.10.0 255.255.255.0 192.168.5.1
ip route 192.168.1.0 255.255.255.0 192.168.5.1
ip route 192.168.2.0 255.255.255.0 192.168.5.1
ip route 192.168.3.0 255.255.255.0 192.168.5.1
!
ip flow-export version 9
!
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
end
```

R_DMZ2#