REDIRECCIONAMIENTO DE TÚNELES VPN EN ASA

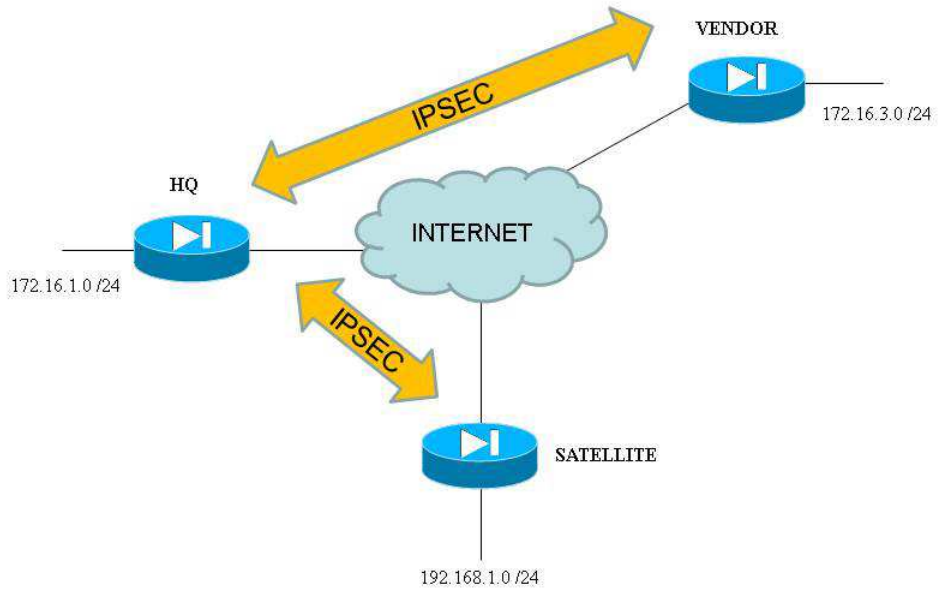
Introducción. En los equipos PIX, por arquitectura, existía una restricción que no permitía redirigir el tráfico entrante en un interfaz para ser re-transmitido por esta misma interfaz. A partir de la versión 7.0 para PIX y ASA, se permite esta redirección de tráfico con lo cual podemos tener redes Hub & Spoke entre equipos ASA en VPN/IPSEC. Antes de esta versión en los firewalls de Cisco este tipo de escenarios solo era posible con routers. Para poder habilitar esta opción solo se necesita configurar el siguiente comando global:

same-security-traffic permit intra-interface

http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_configuration_example09186a00804675ac.shtml

Cabe mencionar, que a pesar de esta modificación los equipos PIX y ASA deben ser considerados como equipos de seguridad y no como equipos de ruteo.

Topología.



Objetivo.

En la topología mostrada previamente, tenemos 3 sitios con un firewall ASA corriendo una versión 7.X o superior. Existe un túnel de IPSEC entre el ASA HQ y el ASA SATELLITE, así como un túnel entre el ASA HQ y el ASA VENDOR. La intención para este ejemplo es que el tráfico de la red SATELLITE (192.168.1.0/24) utilice el mismo túnel que se tiene hacia HQ y una vez en este equipo sea mandado hacia VENDOR, sin tener que crear un túnel nuevo entre SATELLITE y VENDOR. El resultado final es que la red 192.168.1.0/24 debe tener comunicación con la red 172.16.3.0/24. A través de los túneles previamente establecidos.

Configuración del PIX/ASA.

- Como mejor práctica siempre es recomendable que cada vez que se modifique la configuración de un túnel de IPSEC se remueva el mapa (crypto map) del túnel de la interfaz donde está aplicado. Esto es con el fin de borrar por completo la base de datos de IPSEC y evitar problemas por corrupción de la misma al modificar la configuración.
- El primer paso consiste en agregar las nuevas redes que deben tener comunicación a través de los túneles. Es decir, el túnel entre HQ y SATELLITE debe ahora incluir el tráfico entre las redes 192.168.1.1/24 y 172.16.3.0/24. De igual manera, en el túnel entre HQ y VENDOR esta misma regla debe agregarse en los dos equipos:

```
SATELLITE(config)# access-list SAT permit ip 192.168.1.0
255.255.255.0 172.16.1.0 255.255.255.0
SATELLITE(config)# access-list SAT permit ip 192.168.1.0
255.255.255.0 172.16.3.0 255.255.255.0
```

```
VENDOR(config)# access-list VEND permit ip 172.16.3.0 255.255.255.0
172.16.1.0 255.255.255.0
VENDOR(config)# access-list VEND permit ip 172.16.3.0 255.255.255.0
192.168.1.0 255.255.255.0
```

```
HQ(config)# access-list SAT permit ip 172.16.1.0 255.255.255.0
192.168.1.0 255.255.255.0
HQ(config)# access-list SAT permit ip 172.16.3.0 255.255.255.0
192.168.1.0 255.255.255.0

HQ(config)# access-list VEND permit ip 172.16.1.0 255.255.255.0
172.16.3.0 255.255.255.0
HQ(config)# access-list VEND permit ip 192.168.1.0 255.255.255.0
172.16.3.0 255.255.255.0
```

- Las líneas de configuración delineadas arriba son las nuevas líneas en la configuración de las listas de acceso que definen el tráfico interesante de los túneles. Las líneas que no aparecen marcadas ya existían previamente en la configuración de los túneles.
- Cabe resaltar que de acuerdo a la configuración para los equipos remotos VENDOR y SATELLITE, el equipo HQ parece ser el origen de las redes 192.168.1.0 y 172.16.3.0 respectivamente.
- Si se tienen reglas de NAT 0 o bien NO-NAT, estas también deben ser modificadas para agregar los nuevos flujos de tráfico.
- El siguiente paso consiste en permitir el redireccionamiento del tráfico en la interfaz que recibe los paquetes encriptados en HQ. Esto se hace con la ayuda de un solo comando:

```
HQ(config)# same-security-traffic permit inter-interface
```

- Una vez aplicado el mapa en las interfaces correspondientes de los tres equipos bastará mandar un PING para iniciar la negociación y confirmar que los equipos VENDOR y SATELLITE ya están comunicándose a través de HQ:

```
SATELLITE(config)# ping inside 172.16.3.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.2, timeout is 2 seconds:
??!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 1/1/1 ms

SATELLITE(config)# ping inside 172.16.1.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.3, timeout is 2 seconds:
?!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
SATELLITE(config)#
```

- Como siempre, las primeras fallas en la prueba de PING se dan mientras el túnel es negociado.
- Como última confirmación, podemos revisar que en la base de datos de IPSEC en SATELLITE, todo el tráfico se manda directo al túnel que se tiene con HQ.

```
SATELLITE# show crypto ipsec sa
interface: outside
    Crypto map tag: MYMAP, seq num: 1, local addr: 10.88.171.47

      access-list SAT permit ip 192.168.1.0 255.255.255.0 172.16.1.0
255.255.255.0
      local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
      current_peer: 10.88.171.50

      #pkts encaps: 804, #pkts encrypt: 804, #pkts digest: 804
      #pkts decaps: 804, #pkts decrypt: 804, #pkts verify: 804
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 804, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

    Crypto map tag: MYMAP, seq num: 1, local addr: 10.88.171.47

      access-list SAT permit ip 192.168.1.0 255.255.255.0 172.16.3.0
255.255.255.0
      local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (172.16.3.0/255.255.255.0/0/0)
      current_peer: 10.88.171.50

      #pkts encaps: 1004, #pkts encrypt: 1004, #pkts digest: 1004
      #pkts decaps: 1003, #pkts decrypt: 1003, #pkts verify: 1003
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 1004, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0
```

Variación usando NAT en HQ.

- En este tipo de escenarios generalmente hay algún equipo al cual no se tiene acceso por ser controlado por otra administración. Para este ejemplo, consideremos que no es posible modificar nada en la configuración de VENDOR. Esta restricción nos lleva a utilizar NAT en HQ para que el tráfico de la red 192.168.1.0/24 aparezca como tráfico originado en 172.16.1.0/24 que sí está permitido en la configuración de VENDOR.
- Como en el ejemplo ya citado, lo primero que debemos hacer es configurar las listas de acceso en HQ y SATELLITE:

```
SATELLITE(config)# access-list SAT permit ip 192.168.1.0
255.255.255.0 172.16.1.0 255.255.255.0
SATELLITE(config)# access-list SAT permit ip 192.168.1.0
255.255.255.0 172.16.3.0 255.255.255.0
```

```
HQ(config)# access-list SAT permit ip 172.16.1.0 255.255.255.0
192.168.1.0 255.255.255.0
HQ(config)# access-list SAT permit ip 172.16.3.0 255.255.255.0
192.168.1.0 255.255.255.0

HQ(config)# access-list VEND permit ip 172.16.1.0 255.255.255.0
172.16.3.0 255.255.255.0
```

- Como se puede observar solo se modifica el túnel entre HQ y SATELLITE.
- El siguiente paso es configurar una regla de NAT para el tráfico de SATELLITE que trate de alcanzar a VENDOR. Dicho flujo de tráfico va a ser modificado con el fin de que el origen parezca provenir de la red 172.16.1.0/24 en HQ. La regla de NAT que mejor se acomoda a este escenario es una regla de NAT dinámico (no tenemos control sobre cuándo se manda tráfico desde SATELLITE). También es conveniente re-utilizar una misma dirección en la regla de NAT, por lo que para este ejemplo usaremos PAT:

```
HQ(config)# access-list NATSAT permit ip 192.168.1.0 255.255.255.0
172.16.3.0 255.255.255.0

HQ(config)# nat (outside) 1 access-list NATSAT
HQ(config)# global (outside) 1 172.16.1.254
```

- Hay que observar que tanto el comando NAT como el comando GLOBAL se aplican para la misma interfaz en donde el mapa (crypto map) está aplicado. La razón es que el tráfico protegido llega a esta interfaz, se desencripta, se le aplica NAT y después se vuelve a subir sobre un segundo túnel de IPSEC.
- El hecho de que la regla GLOBAL incluye una IP que pertenece a la interfaz inside no genera conflictos en el equipo ya que es una IP que asignamos para la regla de NAT y no directamente a la interfaz. Aun así hay que evitar que la IP que estemos usando para el NAT (en este caso 172.16.1.254) no está asignada a ningún equipo, ya que cualquier tráfico que cruce al firewall buscando a este equipo se vería afectado por las entradas existentes en las tablas de conexiones y NAT del mismo firewall.
- Como en el caso anterior, hay que permitir el redireccionamiento del tráfico en el firewall HQ:

```
HQ(config)# same-security-traffic permit inter-interface
```

- Finalmente, para confirmar que los túneles funcionan como se espera, mandamos una prueba de PING desde SATELLITE hacia VENDOR una vez que volvemos a colocar los mapas después de los cambios en la configuración:

SATELLITE(config)# ping inside 172.16.3.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

- En HQ podemos comprobar que la regla de NAT se está llevando a cabo:

HQ(config)# sh xlate
1 in use, 1 most used
PAT Global 172.16.1.254(18100) Local 192.168.1.1 ICMP id 4388