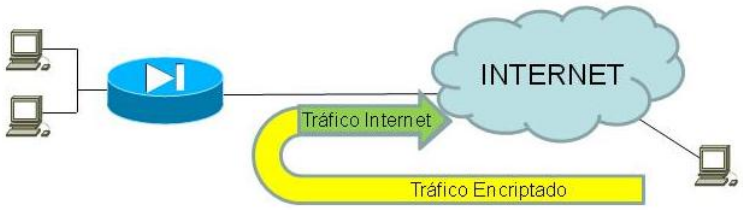
INTERNET CENTRAL PARA CLIENTES DE VPN EN ASA

Introducción. La opción "Split-tunneling" nos permite indicarle a un cliente de VPN qué tráfico debe ser mandado a través de un túnel de IPSEC y qué tráfico debe ser mandado sin encriptar por la conexión local. Sin embargo, en ocasiones por políticas internas es necesario que todo el tráfico sea encriptado y mantener el acceso a Internet pero a través de un sitio central. Esta segunda opción también es conocida como "Internet on a stick".

http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00805734ae.shtml

Topología.



Objetivo.
En los equipos PIX, por arquitectura existía una restricción que no permitía redirigir el tráfico entrante en un interfaz para ser transmitido por esta misma interfaz. A partir de la versión 7.0 para PIX y ASA, se permite esta redirección de tráfico. Cabe mencionar, que a pesar de esta modificación los equipos PIX y ASA deben ser considerados como equipos de seguridad y no equipos de ruteo. Por esta razón si el diseño de la red requiere que el ASA ó el PIX hagan redireccionamiento de tráfico en una misma interfaz de manera cotidiana, la red debe ser rediseñada para evitar esta situación o bien utilizar un equipo de ruteo que haga esta función.

Configuración del PIX/ASA.

- El PIX/ASA va a recibir el tráfico encriptado por su interfaz de salida y después redirigir el tráfico que va hacia Internet por la misma interfaz ("U-Turn"). Por lo general, la IP con la que el tráfico encriptado está llegando será una dirección privada asignada a través de un servidor DHCP o bien por medio de una pool de direcciones. Por esta razón, se requiere una regla de NAT para permitir que la conexión a Internet sea exitosa.
- El primer paso consiste en asegurarse que la sesión de VPN para los clientes remotos está configurada para encriptar todo el tráfico:

```
group-policy VPNCLIENTS internal
group-policy VPNCLIENTS attributes
 wins-server value 192.168.1.50
 dns-server value 192.168.1.50
 split-tunnel-policy tunnelall
 default-domain value cisco.com
```

- El siguiente paso consiste en permitir el redireccionamiento del tráfico en la interfaz que recibe los paquetes encriptados. Esto se hace con la ayuda de un solo comando:

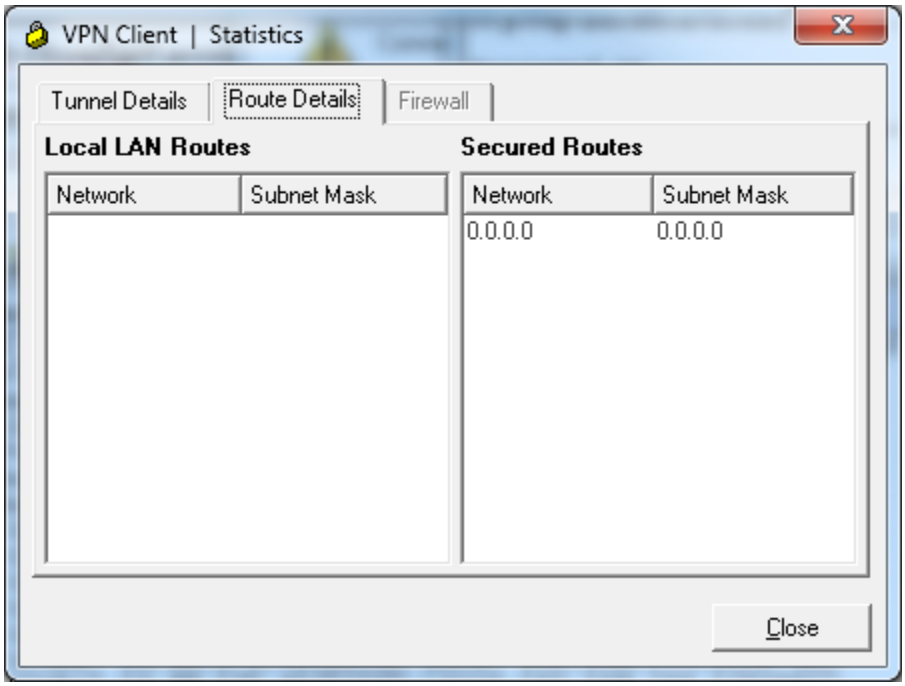
```
ASA-1(config)# same-security-traffic permit inter-interface
```

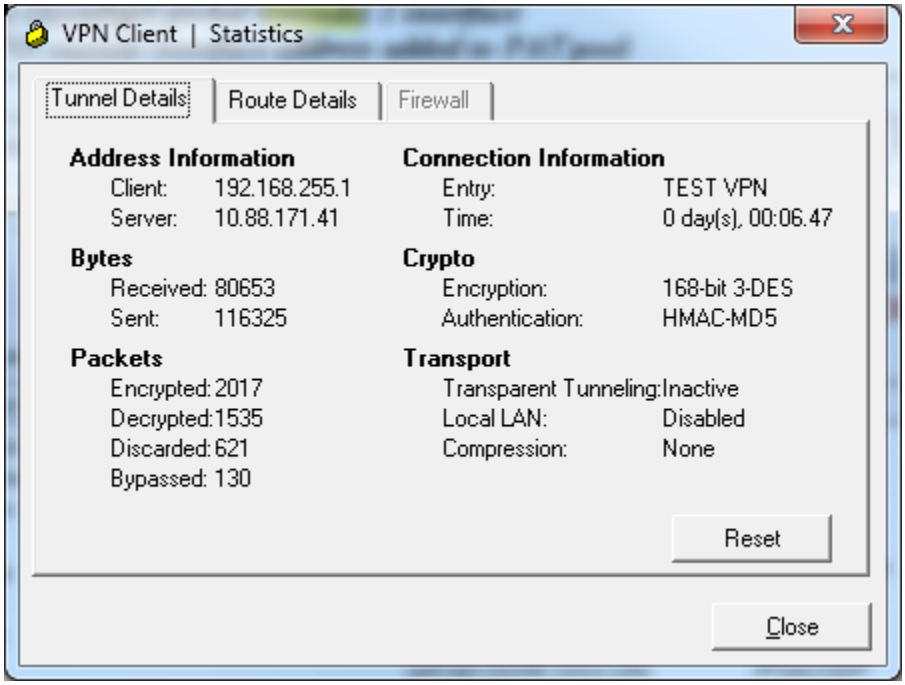
- Finalmente, se crea una regla de NAT dinámica para el tráfico proveniente del cliente de VPN. Cabe resaltar que se utiliza la misma interfaz tanto para el comando "nat" como para el comando "global" (la interfaz que tiene asignada el mapa de encripción). También es posible crear traducciones estáticas, pero no es lo más común. En este ejemplo, los clientes de VPN reciben una IP dentro de la red 192.168.255.0/24 y la interfaz de salida es la interfaz "outside":

```
ASA-1(config)# access-list remotelan permit ip 192.168.255.0 255.255.255.0 any

ASA-1(config)# nat (outside) 1 access-list remotelan
ASA-1(config)# global (outside) 1 interface
INFO: outside interface address added to PAT pool
```

- En las siguientes figuras, se observa cómo el cliente de VPN encripta todo el tráfico, las estadísticas del software y la tabla de traducciones del ASA para el cliente remoto con IP 192.168.255.1 (en una configuración estándar de clientes de VPN no deberíamos ver traducciones de NAT.






```
ASA-1# sh xlate
18 in use, 40 most used
PAT Global 10.88.171.41(1139) Local 192.168.255.1(60479)
PAT Global 10.88.171.41(1138) Local 192.168.255.1(62222)
PAT Global 10.88.171.41(1135) Local 192.168.255.1(62233)
PAT Global 10.88.171.41(4) Local 192.168.255.1(137)
PAT Global 10.88.171.41(1134) Local 192.168.255.1(55550)
PAT Global 10.88.171.41(1041) Local 192.168.255.1(59083)
PAT Global 10.88.171.41(1133) Local 192.168.255.1(49417)
PAT Global 10.88.171.41(3) Local 192.168.255.1 ICMP id 1
```