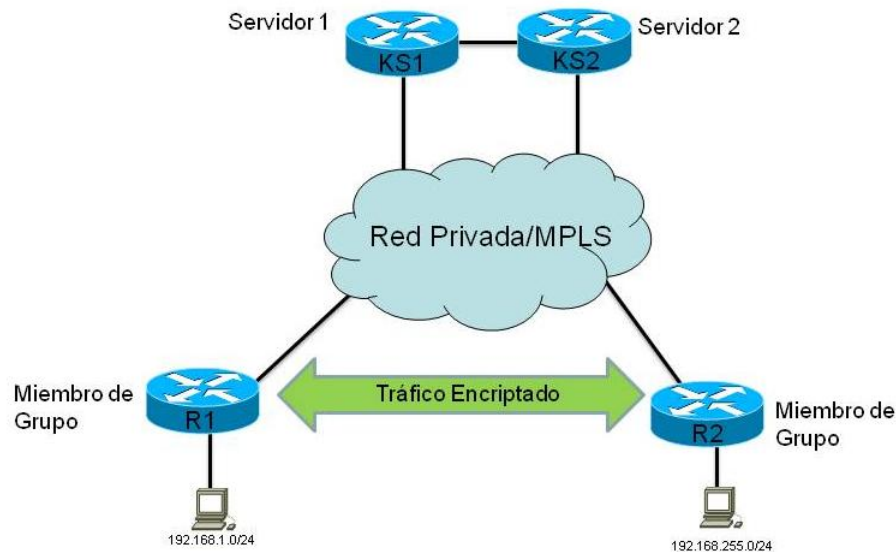


GETVPN – SERVIDORES EN MODO COOPERATIVO

Introducción. GETVPN es una tecnología que no requiere la negociación de túneles punto a punto. Esta tecnología mantiene la información original del encabezado de capa 3 y encripta el resto de los datos lo que permite utilizar la mejor ruta posible dentro de una red y gracias a esto también permite encriptar tráfico multicast. Es por estas características que GETVPN es implementado principalmente en redes privadas IP ó MPLS.

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6635/ps7180/deployment_guide_c07_554713.html

Topología.



Modo de Operación.

Una implementación de GETVPN requiere de tres componentes: un servidor, miembros de grupo y un grupo GDOI. Los miembros de grupo se encargan de encriptar y desencriptar todo el tráfico, mientras que el servidor se encarga de distribuir las llaves de encriptación a todos los miembros de un mismo grupo. El servidor selecciona una sola llave de encriptación para un mismo grupo durante un cierto tiempo. Como los miembros del grupo usan la misma llave cualquier equipo es capaz de encriptar y desencriptar la información que viene de otro miembro.

Cada miembro de grupo levanta una sesión GDOI (Group Domain of Interpretation) con el servidor con el fin de recibir la llave de encriptación y la información del tráfico a encriptar (política de encriptación). Como ya no es necesario negociar una sesión única de encriptación entre los miembros del mismo grupo se reduce la carga sobre los equipos en cada punta.

Se requiere por lo menos un servidor para una implementación de GETVPN, si se requiere mantener un esquema de redundancia los servidores deben configurarse en modo cooperativo y es preferible que existan trayectorias redundantes para la comunicación entre servidores como se muestra en la figura anterior.

Configuración de los servidores primario y secundario.

- Configure la política de ISAKMP con la que los servidores se comunicarán con los miembros de cada grupo:

```
crypto isakmp policy 10
authentication <pre-share/rsa-sig>
encr aes 256
group 2
lifetime 86400
```

- Configure la política de IPSEC:

```
crypto ipsec transform-set MYSET esp-aes 256 esp-sha-hmac
!
crypto ipsec profile GETVPN
set security-association lifetime seconds 28800
set transform-set MYSET
```

- Configure el grupo GDOI (GETLIST es la lista de acceso que define el tráfico interesante que requiere ser encriptado por los miembros del grupo):

```
crypto gdoi group GETVPN
identity number 1
server local
rekey retransmit 10 number 3
rekey authentication mypubkey rsa GETKEY
sa ipsec 10
profile GETVPN
match address ipv4 GETLIST
replay time window-size 5
address ipv4 <IP DEL SERVIDOR>
```

- Configure la redundancia de los servidores (dentro de la configuración del grupo GDOI):

SERVIDOR PRIMARIO

```
crypto gdoi group GETVPN  
server local  
local priority 100  
peer address ipv4 <IP SERVIDOR SECUNDARIO>
```

SERVIDOR SECUNDARIO

```
crypto gdoi group GETVPN  
server local  
local priority 90  
peer address ipv4 <IP SERVIDOR PRIMARIO>
```

- El servidor firma todos los mensajes a los miembros de grupo con la llave RSA que se configura en el grupo GDOI. Operando en modo cooperativo, los dos o más servidores en redundancia deben manejar las mismas llaves RSA para mantener la continuidad de las actualizaciones periódicas de GETVPN.
- Para esto se tiene que generar una llave exportable en el servidor primario:

```
KEYSERVER1(config)#crypto key generate rsa exportable label GETKEY modulus 1024  
% You already have RSA keys defined named GETKEY.  
% They will be replaced.  
  
% The key modulus size is 1024 bits  
% Generating 1024 bit RSA keys, keys will be exportable...[OK]  
  
KEYSERVER1(config)#
```

- Después de esto se exportan las llaves en el servidor primario:

```
KEYSERVER1(config)#crypto key export rsa GETKEY pem terminal 3des cisco123
% Key name: GETKEY
Usage: General Purpose Key
Key data:
-----BEGIN PUBLIC KEY-----
MIGfMA0GCsqGSIb3DQEBAQUAA4GNADCBiQKBgQCxsu04UdmAd51phDnQ5/HITW
vF
LMAuf9mzq+tErqww4CBKVE7oB1MHR5exYoFCoXxxW1u95zLC6eplW64X4Ce9Ji78
/MiR6pSk7UazC2eMGhw+oUa67eN/g7eohmh1ST8h2yb4vu12d4amjOjh0KGXoB7
89H2Eo2OzOmi8+Sd7QIDAQAB
-----END PUBLIC KEY-----
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,894FDC21ABF65DBA

i7ZA63nPnQkEKUa3hWtemywLjTtt2FSS740gkZIH+WmkWt9kRNe6tjzKiUB+UD+8
v0XxM182Ht2KPTXGcqdmLEYuKq7WsTB+sW2fDJpcVwbwUMTv5XMTMth8P58IsMmO
2r7q4SsILpEBppI31VyC731y1WkQUEU8369Y+sHm0jJqs1tau3H2zMOD/zASAIJd
jXZedEtH+Z7XnzdRJoYcuVffg+UOTGiKoz1clx6esYenm2nw2STPkOYykm2IkWIX
N2NdhOFQFBIG/iS47YbVI86WyeBnzCLrx4NMYbrIbNywrC6clOaOhv0UlydUw6Bb
urVtOAmfqD/v6BddBG00IfbBLJjrLIDxb/2EF669UHuf6Zff7iinhfPci6Q/oC38
aDotgMo8SuTtUbtJy8/nkXqwbcoPR+zmkIK9INn3fAS8WLWzvn/I97JhBTcnVmAp6
qOVhI/Ty18sOMFGO91aDYFeFzH7mE1UavB2iYRg2X1Ccp/qIzGS4M6mw6EDW3Od9
ZL1wrzE6UwNw9dNU4X2ojn9/qYEI6TbXKAfnTZ4W0PER19c6VD3MMATAvRQkYQ0h
G3CWqWXn8HQi8aaiGg0TErnAyHXLUrjjwWVR8GJd8bJI1mljMdUrI+iMm1j/a2rW
O1VMycQwfkHY2pMn3LIPWKzYa8f7y7kOfGY68TxMNFQrmavcSg3hVIB9/WP9YHKN
NS0/wofHwjfCanFQN3qMAqgMo7cu5De2xR9Gfm1ZKeQkjCLC1+9mJBp0agKpsIQU
gTKmNBHFihy5bLmZLZF1HIbM2VBAHJ/RiY40a2o2y0TxpgXStg3VVg==
-----END RSA PRIVATE KEY-----
```

- Finalmente, se copian las llaves privada y pública en el servidor secundario:

```

KEYSERVER2(config)#crypto key import rsa GETKEY pem exportable terminal cisco123
% Enter PEM-formatted public General Purpose key or certificate.
% End with a blank line or "quit" on a line by itself.
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCxsu04UdmAd51phDnQ5/HITW
vF
LMauf9mzq+tErqww4CBKVE7oB1MHR5exYoFCoXxxW1u95zLC6eplW64X4Ce9Ji78
/MIIR6pSk7UazC2eMGhw+oUa67eN/g7eohmh1ST8h2yb4vu12d4amjOjh0KGXoB7
89H2Eo2OzOmi8+Sd7QIDAQAB
-----END PUBLIC KEY-----

% Enter PEM-formatted encrypted private General Purpose key.
% End with "quit" on a line by itself.
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,894FDC2IABF65DBA

i7ZA63nPnQkEKUa3hWtemywLjTt2FSS740gkZIH+WmkWt9kRNe6tjzKiUB+UD+8
v0XxM182Ht2KPTXGcqdmIEYuKq7WsTB+sW2fdJpcVwbwUMTv5XMTMth8P58IsMmO
2r7q4SsILpEBppI31VyC731y1WkQUEU8369Y+sHm0jJqs1tau3H2zMOD/zASAIJd
jXZedEtH+Z7XnzdRJoYcuVffg+UOTGiKoz1clx6esYenm2nw2STPkOYykm2IkWIX
N2NdhOFQFBIG/iS47YbVI86WyeBnzCLrx4NMYbrIbNywrC6clOaOhv0UlydUw6Bb
urVtOAmfQD/v6BddBG00IfbBLJjrLIDxb/2EF669UHuf6Zff7iinhfPci6Q/oC38
aDOtgMo8SuTtUbtJy8/nkXqwbcoPR+zmIK9INn3fAS8WLWzvn/197JhBTcnVmAp6
qOVhI/Ty18sOMFGO91aDYFeFzH7mE1UavB2iYRg2X1Cep/qIzgS4M6mw6EDW3Od9
ZL1wrzE6UwNw9dNU4X2ojn9/qYEI6TbXKAfnTZ4W0PER19c6VD3MMATAvRQkYQ0h
G3CWqWXn8HQi8aaiGg0TErnAyHXLurjwWVR8GJd8bJI1mljMdUrI+iMm1j/a2rW
O1VMYcqwfkHY2pMn3LIPWkzYa8f7y7kOfGY68TxMNFQrmavcSg3hVIB9/WP9YHKN
NS0/wofHwjfCanFQN3qMAqgMo7cu5De2xR9Gfm1ZKeQkjCLC1+9m.JBp0agKpsIQU
gTKmNBHFThy5bLmZLZF1HibM2VBAHJ/RiY40a2o2y0TxpgXStg3VVg==
-----END RSA PRIVATE KEY-----

quit
% Key pair import succeeded.

KEYSERVER2(config)#

```