

Creación de una VPN Site2Site con Strongswan

–Seguridad y Alta Disponibilidad–

Por:

Gonzalo Rando Serna
MC Pareja Ferreira

2º ASIR

ÍNDICE

ÍNDICE	2
EXPLICACIÓN DE LA PRÁCTICA	3
SITUACIÓN INICIAL	3
PROBLEMAS ENCONTRADOS	4
FICHEROS RESULTANTES	5
PRUEBAS DE FUNCIONAMIENTO	7
CONCLUSIÓN	8

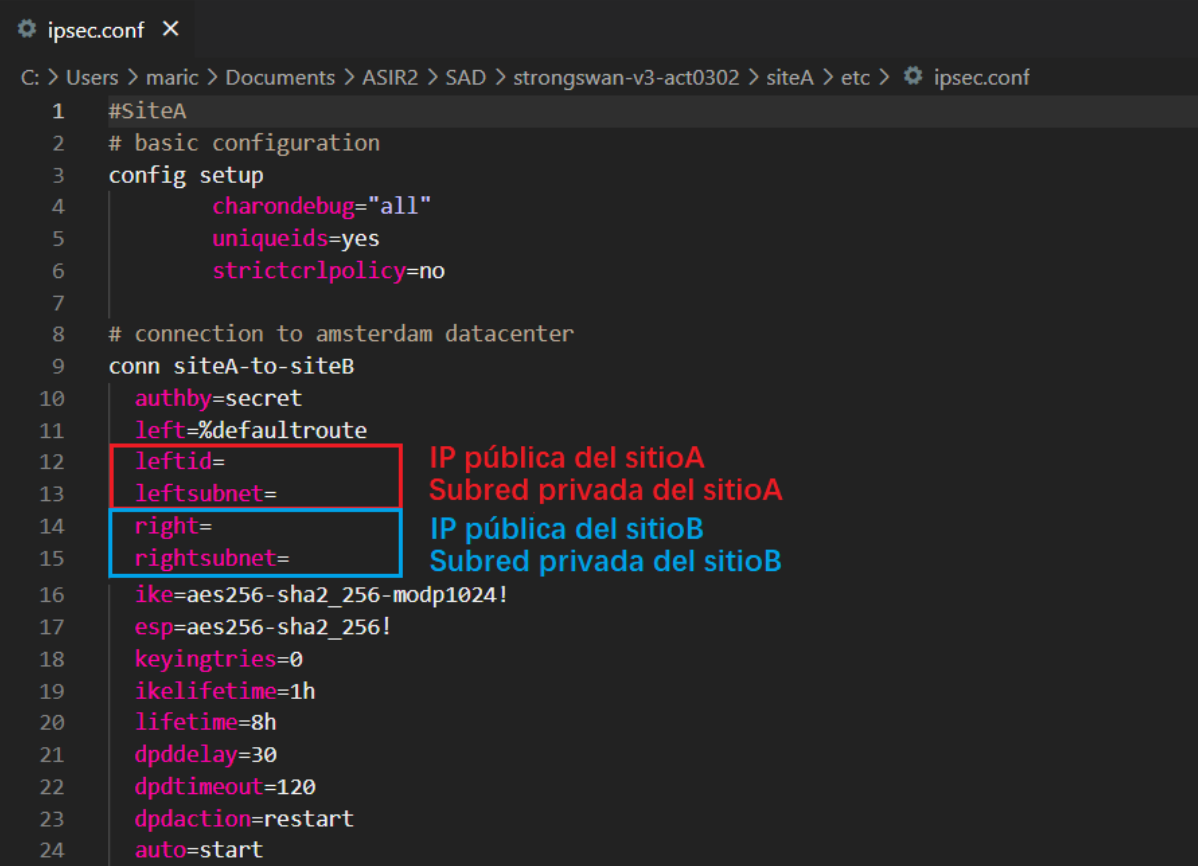
EXPLICACIÓN DE LA PRÁCTICA

El objetivo de esta práctica es crear una VPN Site2Site que permita a cada uno de los equipos de las dos redes existentes, acceder a los dos servidores web. Para la realización de la tarea contamos con la configuración de 4 contenedores Docker proporcionados por el profesor.

SITUACIÓN INICIAL

Al examinar la configuración, se observa que los ficheros de configuración VPN se encuentran incompletos.

En el caso del ipsec.conf de ambos contenedores, era necesario incluir la información pertinente a la configuración de red tanto del siteA como del siteB. La designación “left” hace referencia al site de trabajo; mientras que “right”, al site contrario.

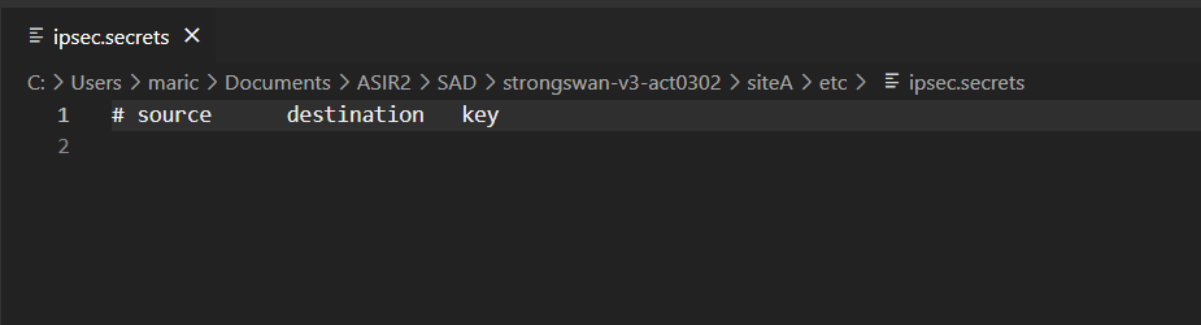


```
1  #SiteA
2  # basic configuration
3  config setup
4      charondebug="all"
5      uniqueids=yes
6      strictcrpolicyno
7
8  # connection to amsterdam datacenter
9  conn siteA-to-siteB
10     authby=secret
11     left=%defaulttroute
12     leftid=
13     leftsubnet=
14     right=
15     rightsubnet=
16     ike=aes256-sha2_256-modp1024!
17     esp=aes256-sha2_256!
18     keyingtries=0
19     ikelifetime=1h
20     lifetime=8h
21     dpddelay=30
22     dpdtimeout=120
23     dpdaction=restart
24     auto=start
```

IP pública del sitioA
Subred privada del sitioA

IP pública del sitioB
Subred privada del sitioB

Por su parte, el fichero de configuración `ipsec.secrets` estaba vacío y necesitaba rellenarse con las direcciones públicas tanto del site de origen como del site de destino y una contraseña precompartida (PSK).



```
ipsec.secrets X
C: > Users > maric > Documents > ASIR2 > SAD > strongswan-v3-act0302 > siteA > etc > ipsec.secrets
1 # source destination key
2
```

PROBLEMAS ENCONTRADOS

Uno de los principales problemas durante la realización de la práctica resultó ser la omisión de los espacios que rodean a los dos puntos en el fichero `ipsec.secrets`. Aunque ambos ficheros `ipsec.conf` eran correctos, este error hacía que Strongswan fallase y tardamos bastante tiempo hasta encontrar el fallo de sintaxis.

Una vez corregido el error, la VPN comenzó a funcionar correctamente.

FICHEROS RESULTANTES

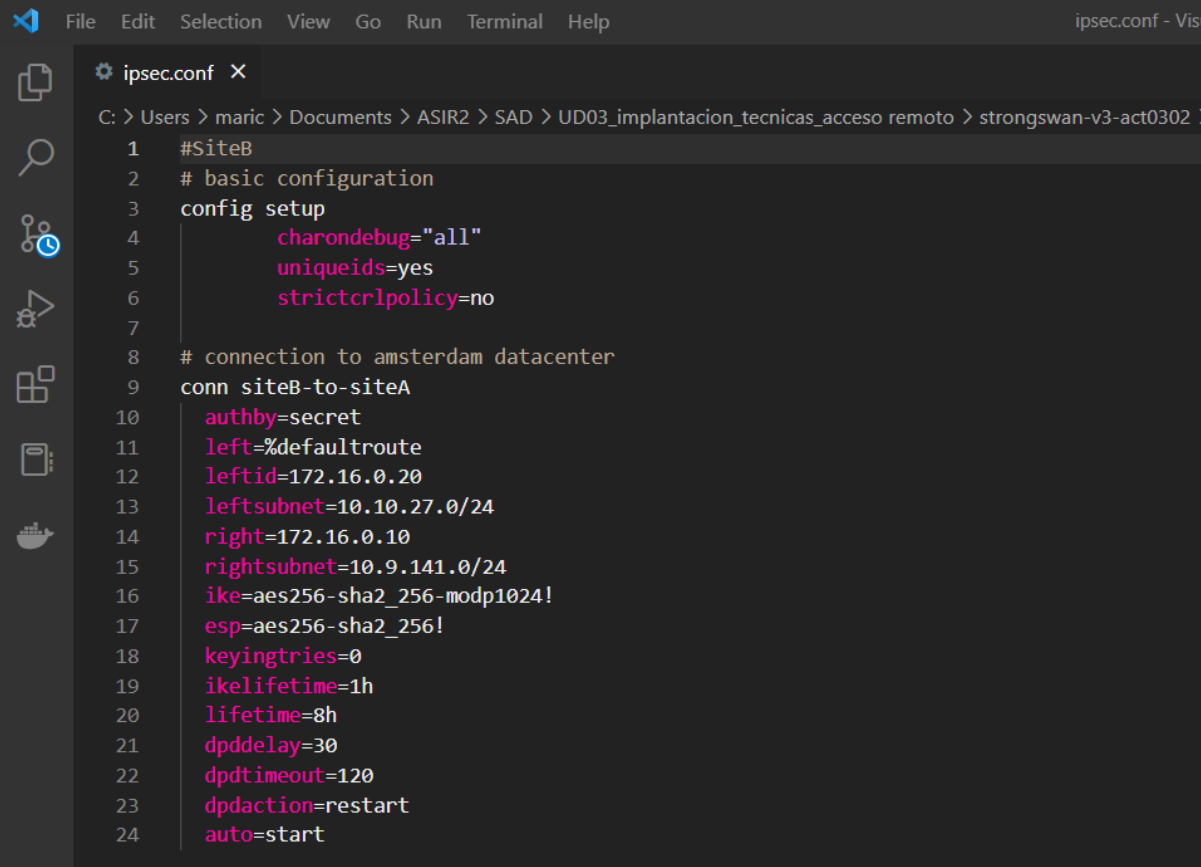
Fichero ipsec.conf (siteA)

```
ipsec.conf X
C: > Users > maric > Documents > ASIR2 > SAD > UD03_implantacion_tecnicas_acceso remoto > strongswan-v3-act0302
1  #SiteA
2  # basic configuration
3  config setup
4      charondebug="all"
5      uniqueids=yes
6      strictcrlpolicy=no
7
8  # connection to amsterdam datacenter
9  conn siteA-to-siteB
10     authby=secret
11     left=%defaultroute
12     leftid=172.16.0.10
13     leftsubnet=10.9.141.0/24
14     right=172.16.0.20
15     rightsubnet=10.10.27.0/24
16     ike=aes256-sha2_256-modp1024!
17     esp=aes256-sha2_256!
18     keyingtries=0
19     ikelifetime=1h
20     lifetime=8h
21     dpddelay=30
22     dpdtimeout=120
23     dpdaction=restart
24     auto=start
```

Fichero ipsec.secrets (siteA)

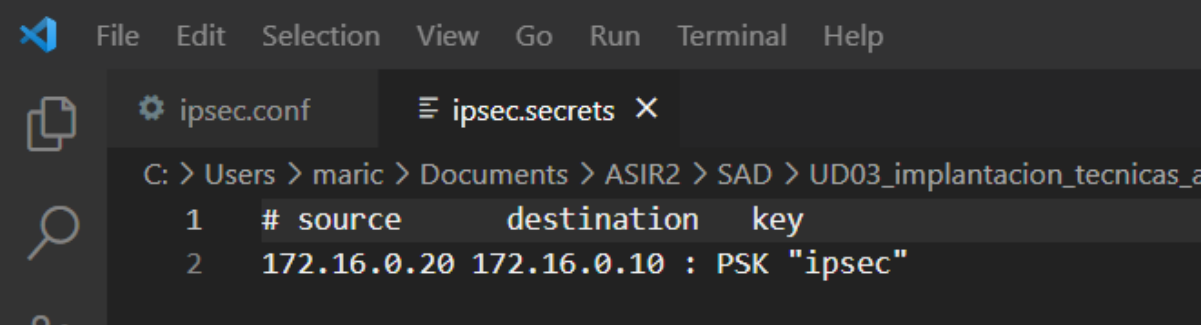
```
ipsec.secrets X
C: > Users > maric > Documents > ASIR2 > SAD > UD03_implantacion_tecnicas_acceso remoto > strongswan-v3-act0302 >
1  # source      destination  key
2  172.16.0.10 172.16.0.20 : PSK "ipsec"
```

Fichero ipsec.conf (siteB)



```
1 #SiteB
2 # basic configuration
3 config setup
4     charondebug="all"
5     uniqueids=yes
6     stricterpolicy=no
7
8 # connection to amsterdam datacenter
9 conn siteB-to-siteA
10     authby=secret
11     left=%defaulttroute
12     leftid=172.16.0.20
13     leftsubnet=10.10.27.0/24
14     right=172.16.0.10
15     rightsubnet=10.9.141.0/24
16     ike=aes256-sha2_256-modp1024!
17     esp=aes256-sha2_256!
18     keyingtries=0
19     ikelifetime=1h
20     lifetime=8h
21     dpddelay=30
22     dpdtimeout=120
23     dpdaction=restart
24     auto=start
```

Fichero ipsec.secrets (siteB)



```
1 # source      destination  key
2 172.16.0.20 172.16.0.10 : PSK "ipsec"
```

PRUEBAS DE FUNCIONAMIENTO

En primer lugar, realizamos un ipsec status en ambos contenedores para comprobar que el servicio funciona y la conexión VPN se ha establecido correctamente.

```
strongswan-v3-act0302-  
sitea-sw-1  
RUNNING  
Logs Inspect Stats  
Open in external terminal  
/ # ipsec status  
Shunted Connections:  
Bypass LAN 10.9.141.0/24: 10.9.141.0/24 === 10.9.141.0/24 PASS  
Bypass LAN 172.16.0.0/24: 172.16.0.0/24 === 172.16.0.0/24 PASS  
Security Associations (1 up, 0 connecting):  
siteA-to-siteB[1]: ESTABLISHED 3 minutes ago, 172.16.0.10[172.16.0.10]...172.16.0.20[172.16.0.20]  
siteA-to-siteB[2]: INSTALLED, TUNNEL, reqid 1, ESP SPIs: c3bae6b5_i c0ce15af_o  
siteA-to-siteB[2]: 10.9.141.0/24 === 10.10.27.0/24
```

```
strongswan-v3-act0302-  
siteb-sw-1  
RUNNING  
Logs Inspect Stats  
Open in external terminal  
/ # ipsec status  
Shunted Connections:  
Bypass LAN 10.10.27.0/24: 10.10.27.0/24 === 10.10.27.0/24 PASS  
Bypass LAN 172.16.0.0/24: 172.16.0.0/24 === 172.16.0.0/24 PASS  
Security Associations (1 up, 0 connecting):  
siteB-to-siteA[2]: ESTABLISHED 2 minutes ago, 172.16.0.20[172.16.0.20]...172.16.0.10[172.16.0.10]  
siteB-to-siteA[2]: INSTALLED, TUNNEL, reqid 1, ESP SPIs: c0ce15af_i c3bae6b5_o  
siteB-to-siteA[2]: 10.10.27.0/24 === 10.9.141.0/24
```

La captura muestra que se ha establecido la conexión VPN entre el siteA y el siteB.

Lo siguiente que debemos comprobar, es que una máquina de la red A pueda ver a una máquina de la red B. A continuación, lanzaremos un curl para comprobar que, efectivamente, podemos acceder al servidor web de la otra red.

```
strongswan-v3-act0302-sitea-sw-1 strongswan-v3-act0302-sitea-sw  
RUNNING  
Logs Inspect Stats  
Open in external terminal  
/ # curl 10.10.27.100  
Enhorabuena!
```

```
strongswan-v3-act0302-siteb-sw-1 strongswan-v3-act0302-siteb-sw  
RUNNING  
Logs Inspect Stats  
Open in external terminal  
/ # curl 10.9.141.100  
Enhorabuena!
```

La conexión VPN funciona correctamente.

CONCLUSIÓN

En esta práctica, hemos hecho uso de un túnel VPN Site2Site a través de la herramienta Strongswan, que nos ha permitido conectar dos redes internas y acceder desde un equipo situado en la red A a otro en la red B, y viceversa.

Si bien la configuración de IPsec es más compleja y tediosa, esta tecnología puede ser usada por las empresas para establecer conexiones seguras a través de Internet. Además, en contraste con las VPN SSL, que conectan a un usuario a una aplicación o servicio remoto específico, las VPN IPsec permiten conectar dos subredes locales, convirtiéndolas en una excelente opción para, por ejemplo, conectar redes de oficinas cada una en una localización diferente.