

En este documento se detallan los diversos logs que pueden aparecernos en la creación de túneles VPN IPsec en los dispositivos ZyWALL USG:

- 1- Túnel Abierto sin Problemas
- 2- Pre-Shared Key Diferente
- 3- Identificador FQDN Diferente
- 4- Desajuste en Fase 1
- 5- Desajuste en Fase 2 (Autenticación o Encriptación)
- 6- Desajuste en Fase 2 (Direccionamiento IP)

### 1. Túnel Abierto sin problemas:

#	Time	Priority	Category	Message	Source	Destination	Note
1	2008-06-24 10:39:14	info	IKE	Tunnel [VPN_Zy70:vpn_zy70:0xe027380e] built successfully	81.32.147.6:500	88.2.180.178:500	IKE_LOG
2	2008-06-24 10:39:14	info	IKE	Send:[HASH]	81.32.147.6:500	88.2.180.178:500	IKE_LOG
3	2008-06-24 10:39:14	info	IKE	[SA]: [Initiator:81.32.147.6][Responder:88.2.180.178][Policy:192.168.1.0/24-192.168.28.0/24][ESP des-cbc-hmac	88.2.180.178:500	81.32.147.6:500	IKE_LOG
4	2008-06-24 10:39:14	info	IKE	Recv:[HASH][SA][NONCE][ID][ID][NOTFY:RESPONDER_LIFETIME]	88.2.180.178:500	81.32.147.6:500	IKE_LOG
5	2008-06-24 10:39:14	info	IKE	Send:[HASH][SA][NONCE][ID][ID]	81.32.147.6:500	88.2.180.178:500	IKE_LOG
6	2008-06-24 10:39:14	info	IKE	Start Phase 2: Quick Mode	81.32.147.6:500	88.2.180.178:500	IKE_LOG
7	2008-06-24 10:39:14	info	IKE	Phase 1 IKE SA process done	81.32.147.6:500	88.2.180.178:500	IKE_LOG
8	2008-06-24 10:39:14	info	IKE	Recv:[ID][HASH][NOTFY:INITIAL_CONTACT]	88.2.180.178:500	81.32.147.6:500	IKE_LOG
9	2008-06-24 10:39:14	info	IKE	Send:[ID][HASH][NOTFY:INITIAL_CONTACT]	81.32.147.6:500	88.2.180.178:500	IKE_LOG
10	2008-06-24 10:39:13	info	IKE	Recv:[KE][NONCE]	88.2.180.178:500	81.32.147.6:500	IKE_LOG
11	2008-06-24 10:39:13	info	IKE	Send:[KE][NONCE]	81.32.147.6:500	88.2.180.178:500	IKE_LOG
12	2008-06-24 10:39:13	info	IKE	The cookie pair is : 0xed594f2b82b1bd22 / 0xbb44021ba663f887 [count=8]	81.32.147.6:500	88.2.180.178:500	IKE_LOG
13	2008-06-24 10:39:13	info	IKE	Recv:[SA][VID][VID]	88.2.180.178:500	81.32.147.6:500	IKE_LOG
14	2008-06-24 10:39:13	info	IKE	The cookie pair is : 0xed594f2b82b1bd22 / 0xbb44021ba663f887 [count=4]	88.2.180.178:500	81.32.147.6:500	IKE_LOG
15	2008-06-24 10:39:13	info	IKE	Send:[SA][VID][VID]	81.32.147.6:500	88.2.180.178:500	IKE_LOG
16	2008-06-24 10:39:13	info	IKE	Send Main Mode request to [88.2.180.178]	81.32.147.6:500	88.2.180.178:500	IKE_LOG
17	2008-06-24 10:39:13	info	IKE	Tunnel [vpn_zy70] Sending IKE request	81.32.147.6:500	88.2.180.178:500	IKE_LOG
18	2008-06-24 10:39:13	info	IKE	The cookie pair is : 0xed594f2b82b1bd22 / 0x0000000000000000 [count=2]	81.32.147.6:500	88.2.180.178:500	IKE_LOG

Este es un log de una VPN que se ha creado satisfactoriamente. Podemos ver 6 paquetes que han sido transmitidos y 4 recibidos en negociación "Main Mode"

Index 15 y 13: Negociación de parámetros de seguridad

Index 11 y 10: Realizando el intercambio de claves Diffie Hellman

Index 9 y 8: Uso de Pre-shared Key para autenticación

Después de finalizar la negociación de la fase 1 satisfactoriamente, empieza la negociación de la fase 2.

Index 5 y 4: Solo cuando apliquemos PFS se realizarán más intercambios de clave, <KE> .

Los dos gateways VPN negocian su política VPN (campos <ID><ID>)

Index 1: El túnel se ha establecido con éxito

## 2. Pre-Shared Key Diferente:

#	Time	Priority	Category	Message	Source	Destination	Note
1	2008-06-24 07:41:04	info	IKE	[COOKIE] Invalid cookie, no sa found	88.2.180.178:500	83.56.224.107:500	IKE_LOG
2	2008-06-24 07:41:04	info	IKE	The cookie pair is : 0xa17ae8135c6c6624 / 0x6c311fab63401800	88.2.180.178:500	83.56.224.107:500	IKE_LOG
3	2008-06-24 07:40:07	info	IKE	Send:[NOTIFY:INVALID_ID_INFORMATION]	83.56.224.107:500	88.2.180.178:500	IKE_LOG
4	2008-06-24 07:40:07	info	IKE	Recv:[KE][NONCE]	88.2.180.178:500	83.56.224.107:500	IKE_LOG
5	2008-06-24 07:40:07	info	IKE	Send:[KE][NONCE]	83.56.224.107:500	88.2.180.178:500	IKE_LOG
6	2008-06-24 07:40:07	info	IKE	The cookie pair is : 0xc5cba99fe1d22484 / 0x62fc542365070f34 [count=3]	83.56.224.107:500	88.2.180.178:500	IKE_LOG
7	2008-06-24 07:40:07	info	IKE	Recv:[SA][VID][VID]	88.2.180.178:500	83.56.224.107:500	IKE_LOG
8	2008-06-24 07:40:07	info	IKE	The cookie pair is : 0xc5cba99fe1d22484 / 0x62fc542365070f34 [count=2]	88.2.180.178:500	83.56.224.107:500	IKE_LOG
9	2008-06-24 07:40:07	info	IKE	Send:[SA][VID][VID]	83.56.224.107:500	88.2.180.178:500	IKE_LOG
10	2008-06-24 07:40:07	info	IKE	Send Main Mode request to [88.2.180.178]	83.56.224.107:500	88.2.180.178:500	IKE_LOG
11	2008-06-24 07:40:07	info	IKE	Tunnel [vpn_zy70] Sending IKE request	83.56.224.107:500	88.2.180.178:500	IKE_LOG
12	2008-06-24 07:40:07	info	IKE	The cookie pair is : 0xc5cba99fe1d22484 / 0x0000000000000000 [count=2]	83.56.224.107:500	88.2.180.178:500	IKE_LOG
13	2008-06-24 07:40:07	info	IKE	ISAKMP SA [VPN_Zy70] is disconnected [count=2]	83.56.224.107:500	88.2.180.178:500	IKE_LOG
14	2008-06-24 07:40:07	info	IKE	The cookie pair is : 0xa17ae8135c6c6624 / 0x6c311fab63401800	83.56.224.107:500	88.2.180.178:500	IKE_LOG
15	2008-06-24 07:39:39	info	IKE	IKE Packet Retransmit	83.56.224.107:500	88.2.180.178:500	IKE_LOG
16	2008-06-24 07:39:39	info	IKE	The cookie pair is : 0xa17ae8135c6c6624 / 0x6c311fab63401800	83.56.224.107:500	88.2.180.178:500	IKE_LOG
17	2008-06-24 07:39:23	info	IKE	IKE Packet Retransmit	83.56.224.107:500	88.2.180.178:500	IKE_LOG
18	2008-06-24 07:39:23	info	IKE	The cookie pair is : 0xa17ae8135c6c6624 / 0x6c311fab63401800	83.56.224.107:500	88.2.180.178:500	IKE_LOG
19	2008-06-24 07:39:14	info	IKE	[COOKIE] Invalid cookie, no sa found	88.2.180.178:500	83.56.224.107:500	IKE_LOG
20	2008-06-24 07:39:14	info	IKE	The cookie pair is : 0xbf7a4d9f0dd95336 / 0x8ed864b4626a55eb	88.2.180.178:500	83.56.224.107:500	IKE_LOG
21	2008-06-24 07:39:08	info	IKE	IKE Packet Retransmit [count=4]	83.56.224.107:500	88.2.180.178:500	IKE_LOG
22	2008-06-24 07:39:07	info	IKE	Send:[ID][HASH][NOTIFY:INITIAL_CONTACT]	83.56.224.107:500	88.2.180.178:500	IKE_LOG
23	2008-06-24 07:39:07	info	IKE	Recv:[KE][NONCE]	88.2.180.178:500	83.56.224.107:500	IKE_LOG
24	2008-06-24 07:39:07	info	IKE	Send:[KE][NONCE]	83.56.224.107:500	88.2.180.178:500	IKE_LOG
25	2008-06-24 07:39:07	info	IKE	The cookie pair is : 0xa17ae8135c6c6624 / 0x6c311fab63401800 [count=6]	83.56.224.107:500	88.2.180.178:500	IKE_LOG
26	2008-06-24 07:39:07	info	IKE	Recv:[SA][VID][VID]	88.2.180.178:500	83.56.224.107:500	IKE_LOG
27	2008-06-24 07:39:07	info	IKE	The cookie pair is : 0xa17ae8135c6c6624 / 0x6c311fab63401800 [count=3]	88.2.180.178:500	83.56.224.107:500	IKE_LOG
28	2008-06-24 07:39:07	info	IKE	Send:[SA][VID][VID]	83.56.224.107:500	88.2.180.178:500	IKE_LOG
29	2008-06-24 07:39:07	info	IKE	Send Main Mode request to [88.2.180.178]	83.56.224.107:500	88.2.180.178:500	IKE_LOG
30	2008-06-24 07:39:07	info	IKE	Tunnel [vpn_zy70] Sending IKE request	83.56.224.107:500	88.2.180.178:500	IKE_LOG

Si la Pre-shared Key no coincide en ambos extremos, se mostrará el siguiente mensaje de notificación **INVALID\_ID\_INFORMATION**. Si nos encontramos con este problema deberemos verificar que los dos extremos usen la misma Pre-shared key.

## 3. Identificador FQDN Diferente:

#	Time	Priority	Category	Message	Source	Destination	Note
1	2008-06-24 07:43:14	info	IKE	ISAKMP SA [VPN_Zy70] is disconnected	83.56.224.107:500	88.2.180.178:500	IKE_LOG
2	2008-06-24 07:43:14	info	IKE	The cookie pair is : 0x4fd6f7b8d69386a0 / 0x2f4a8523622214f8 [count=3]	83.56.224.107:500	88.2.180.178:500	IKE_LOG
3	2008-06-24 07:43:14	info	IKE	The cookie pair is : 0x4fd6f7b8d69386a0 / 0x2f4a8523622214f8 [count=2]	88.2.180.178:500	83.56.224.107:500	IKE_LOG
4	2008-06-24 07:43:14	info	IKE	The cookie pair is : 0x4fd6f7b8d69386a0 / 0x0000000000000000 [count=2]	83.56.224.107:500	88.2.180.178:500	IKE_LOG
5	2008-06-24 07:43:14	info	IKE	Send:[NOTIFY:INVALID_ID_INFORMATION] [count=2]	83.56.224.107:500	88.2.180.178:500	IKE_LOG
6	2008-06-24 07:43:14	info	IKE	(ID) : Tunnel [vpn_zy70] Phase 1 ID mismatch	88.2.180.178:500	83.56.224.107:500	IKE_LOG
7	2008-06-24 07:43:14	info	IKE	Recv:[ID][HASH][NOTIFY:INITIAL_CONTACT]	88.2.180.178:500	83.56.224.107:500	IKE_LOG
8	2008-06-24 07:43:14	info	IKE	Send:[ID][HASH][NOTIFY:INITIAL_CONTACT]	83.56.224.107:500	88.2.180.178:500	IKE_LOG
9	2008-06-24 07:43:14	info	IKE	Recv:[KE][NONCE] [count=2]	88.2.180.178:500	83.56.224.107:500	IKE_LOG
10	2008-06-24 07:43:14	info	IKE	Send:[KE][NONCE] [count=2]	83.56.224.107:500	88.2.180.178:500	IKE_LOG
11	2008-06-24 07:43:14	info	IKE	The cookie pair is : 0xe74a29fe4c33dbcl / 0x5bd941f4b7b09816 [count=3]	83.56.224.107:500	88.2.180.178:500	IKE_LOG
12	2008-06-24 07:43:13	info	IKE	Recv:[SA][VID][VID] [count=2]	88.2.180.178:500	83.56.224.107:500	IKE_LOG
13	2008-06-24 07:43:13	info	IKE	The cookie pair is : 0xe74a29fe4c33dbcl / 0x5bd941f4b7b09816 [count=4]	88.2.180.178:500	83.56.224.107:500	IKE_LOG
14	2008-06-24 07:43:13	info	IKE	Send:[SA][VID][VID] [count=2]	83.56.224.107:500	88.2.180.178:500	IKE_LOG
15	2008-06-24 07:43:13	info	IKE	Send Main Mode request to [88.2.180.178] [count=2]	83.56.224.107:500	88.2.180.178:500	IKE_LOG
16	2008-06-24 07:43:13	info	IKE	Tunnel [vpn_zy70] Sending IKE request [count=2]	83.56.224.107:500	88.2.180.178:500	IKE_LOG
17	2008-06-24 07:43:13	info	IKE	The cookie pair is : 0xe74a29fe4c33dbcl / 0x0000000000000000 [count=2]	83.56.224.107:500	88.2.180.178:500	IKE_LOG

Si los valores de los Identificadores FQDN no coinciden en ambos extremos, se mostrará el siguiente mensaje de notificación **Phase 1 ID mismatch**, además del mensaje **INVALID\_ID\_INFORMATION**. Si nos encontramos con este problema deberemos verificar que los dos extremos usen los mismos valores de Identificadores FQDN.

#### 4. Desajuste en Fase 1:

#	Time	Priority	Category	Message	Source	Destination	Note
1	2008-06-24 07:17:52	info	IKE	The cookie pair is : 0x53030b77f999a353 / 0x18b0c9e5bc8cea74	83.56.224.107:500	88.2.180.178:500	IKE_LOG
2	2008-06-24 07:17:52	info	IKE	The cookie pair is : 0x53030b77f999a353 / 0x18b0c9e5bc8cea74	88.2.180.178:500	83.56.224.107:500	IKE_LOG
3	2008-06-24 07:17:51	info	IKE	The cookie pair is : 0x53030b77f999a353 / 0x0000000000000000 [count=2]	83.56.224.107:500	88.2.180.178:500	IKE_LOG
4	2008-06-24 07:17:51	info	IKE	ISAKMP SA [VPN_Zy70] is disconnected [count=2]	83.56.224.107:500	88.2.180.178:500	IKE_LOG
5	2008-06-24 07:17:51	info	IKE	The cookie pair is : 0xb3d01b6c4fa6b55a / 0xc3581b5183be628d	83.56.224.107:500	88.2.180.178:500	IKE_LOG
6	2008-06-24 07:17:51	info	IKE	Recv:[NOTFY:NO_PROPOSAL_CHOSEN] [count=2]	88.2.180.178:500	83.56.224.107:500	IKE_LOG
7	2008-06-24 07:17:51	info	IKE	The cookie pair is : 0xb3d01b6c4fa6b55a / 0xc3581b5183be628d	88.2.180.178:500	83.56.224.107:500	IKE_LOG
8	2008-06-24 07:17:51	info	IKE	Send:[SA][VID][VID] [count=2]	83.56.224.107:500	88.2.180.178:500	IKE_LOG
9	2008-06-24 07:17:51	info	IKE	Send Main Mode request to [88.2.180.178] [count=2]	83.56.224.107:500	88.2.180.178:500	IKE_LOG
10	2008-06-24 07:17:51	info	IKE	Tunnel [vpn_zy70] Sending IKE request [count=2]	83.56.224.107:500	88.2.180.178:500	IKE_LOG
11	2008-06-24 07:17:51	info	IKE	The cookie pair is : 0xb3d01b6c4fa6b55a / 0x0000000000000000 [count=2]	83.56.224.107:500	88.2.180.178:500	IKE_LOG

Si parámetros de la Fase 1, como los de autenticación o encriptación no coinciden en ambos extremos, el mensaje de error mostrado será **NO\_PROPOSAL\_CHOSEN**. Si nos encontramos con este problema, deberemos verificar que los dos extremos usen los mismos parámetros de autenticación y encriptación.

#### 5. Desajuste en Fase 2 (Autenticación o Encriptación):

#	Time	Priority	Category	Message	Source	Destination	Note
1	2008-06-24 07:25:53	info	IKE	[COOKIE] Invalid cookie, no sa found	88.2.180.178:500	83.56.224.107:500	IKE_LOG
2	2008-06-24 07:25:53	info	IKE	ISAKMP SA [VPN_Zy70] is disconnected	83.56.224.107:500	88.2.180.178:500	IKE_LOG
3	2008-06-24 07:25:53	info	IKE	Recv:[HASH][NOTFY:NO_PROPOSAL_CHOSEN]	88.2.180.178:500	83.56.224.107:500	IKE_LOG
4	2008-06-24 07:25:53	info	IKE	Send:[HASH][SA][NONCE][ID][ID]	83.56.224.107:500	88.2.180.178:500	IKE_LOG
5	2008-06-24 07:25:53	info	IKE	Start Phase 2: Quick Mode	83.56.224.107:500	88.2.180.178:500	IKE_LOG
6	2008-06-24 07:25:53	info	IKE	Phase 1 IKE SA process done	83.56.224.107:500	88.2.180.178:500	IKE_LOG
7	2008-06-24 07:25:53	info	IKE	Recv:[ID][HASH][NOTFY:INITIAL_CONTACT]	88.2.180.178:500	83.56.224.107:500	IKE_LOG
8	2008-06-24 07:25:52	info	IKE	Send:[ID][HASH][NOTFY:INITIAL_CONTACT]	83.56.224.107:500	88.2.180.178:500	IKE_LOG
9	2008-06-24 07:25:52	info	IKE	Recv:[KE][NONCE]	88.2.180.178:500	83.56.224.107:500	IKE_LOG
10	2008-06-24 07:25:52	info	IKE	Send:[KE][NONCE]	83.56.224.107:500	88.2.180.178:500	IKE_LOG
11	2008-06-24 07:25:52	info	IKE	The cookie pair is : 0x740be9a586d71386 / 0x6a111c99b8ad036a [count=6]	83.56.224.107:500	88.2.180.178:500	IKE_LOG
12	2008-06-24 07:25:52	info	IKE	Recv:[SA][VID][VID]	88.2.180.178:500	83.56.224.107:500	IKE_LOG
13	2008-06-24 07:25:52	info	IKE	The cookie pair is : 0x740be9a586d71386 / 0x6a111c99b8ad036a [count=5]	88.2.180.178:500	83.56.224.107:500	IKE_LOG
14	2008-06-24 07:25:52	info	IKE	Send:[SA][VID][VID]	83.56.224.107:500	88.2.180.178:500	IKE_LOG
15	2008-06-24 07:25:52	info	IKE	Send Main Mode request to [88.2.180.178]	83.56.224.107:500	88.2.180.178:500	IKE_LOG
16	2008-06-24 07:25:52	info	IKE	Tunnel [vpn_zy70] Sending IKE request	83.56.224.107:500	88.2.180.178:500	IKE_LOG
17	2008-06-24 07:25:52	info	IKE	The cookie pair is : 0x740be9a586d71386 / 0x0000000000000000 [count=2]	83.56.224.107:500	88.2.180.178:500	IKE_LOG

Si parámetros de la Fase 2, como los de autenticación o encriptación no coinciden en ambos extremos, tras la creación de la Fase 1 el mensaje de error mostrado será **NO\_PROPOSAL\_CHOSEN**. Si nos encontramos con este problema, deberemos verificar que los dos extremos usen los mismos parámetros de autenticación y encriptación.

## 6. Desajuste en Fase 2 (Direccionamiento IP):

#	Time	Priority	Category	Message	Source	Destination	Note
1	2008-06-24 10:22:34	info	IKE	[COOKIE] Invalid cookie, no sa found [count=2]	88.2.180.178:500	81.32.147.6:500	IKE_LOG
2	2008-06-24 10:22:34	info	IKE	ISAKMP SA [VPN_Zy70] is disconnected	81.32.147.6:500	88.2.180.178:500	IKE_LOG
3	2008-06-24 10:22:34	info	IKE	Recv:[HASH][NOTFY:INVALID_ID_INFORMATION]	88.2.180.178:500	81.32.147.6:500	IKE_LOG
4	2008-06-24 10:22:33	info	IKE	Send:[HASH][SA][NONCE][ID][ID]	81.32.147.6:500	88.2.180.178:500	IKE_LOG
5	2008-06-24 10:22:33	info	IKE	Start Phase 2: Quick Mode	81.32.147.6:500	88.2.180.178:500	IKE_LOG
6	2008-06-24 10:22:33	info	IKE	Phase 1 IKE SA process done	81.32.147.6:500	88.2.180.178:500	IKE_LOG
7	2008-06-24 10:22:33	info	IKE	Recv:[ID][HASH][NOTFY:INITIAL_CONTACT]	88.2.180.178:500	81.32.147.6:500	IKE_LOG
8	2008-06-24 10:22:33	info	IKE	Send:[ID][HASH][NOTFY:INITIAL_CONTACT]	81.32.147.6:500	88.2.180.178:500	IKE_LOG
9	2008-06-24 10:22:33	info	IKE	Recv:[KE][NONCE]	88.2.180.178:500	81.32.147.6:500	IKE_LOG
10	2008-06-24 10:22:33	info	IKE	Send:[KE][NONCE]	81.32.147.6:500	88.2.180.178:500	IKE_LOG
11	2008-06-24 10:22:33	info	IKE	The cookie pair is : 0x228b0fb1c2cb0461 / 0xf755a14906b330bd [count=6]	81.32.147.6:500	88.2.180.178:500	IKE_LOG
12	2008-06-24 10:22:33	info	IKE	Recv:[SA][VID][VID]	88.2.180.178:500	81.32.147.6:500	IKE_LOG
13	2008-06-24 10:22:33	info	IKE	The cookie pair is : 0x228b0fb1c2cb0461 / 0xf755a14906b330bd [count=6]	88.2.180.178:500	81.32.147.6:500	IKE_LOG
14	2008-06-24 10:22:33	info	IKE	Send:[SA][VID][VID]	81.32.147.6:500	88.2.180.178:500	IKE_LOG
15	2008-06-24 10:22:33	info	IKE	Send Main Mode request to [88.2.180.178]	81.32.147.6:500	88.2.180.178:500	IKE_LOG
16	2008-06-24 10:22:33	info	IKE	Tunnel [vpn_zy70] Sending IKE request	81.32.147.6:500	88.2.180.178:500	IKE_LOG
17	2008-06-24 10:22:33	info	IKE	The cookie pair is : 0x228b0fb1c2cb0461 / 0x0000000000000000 [count=2]	81.32.147.6:500	88.2.180.178:500	IKE_LOG

Si los parámetros de direcciones IP no coinciden en ambos extremos, las conexiones IKE fallarán en la Fase 2, y el mensaje de error mostrado será la notificación **INVALID\_ID\_INFORMATION**. Si nos encontramos con este problema, deberemos verificar que los dos extremos usen los mismos parámetros de direccionamiento IP.