

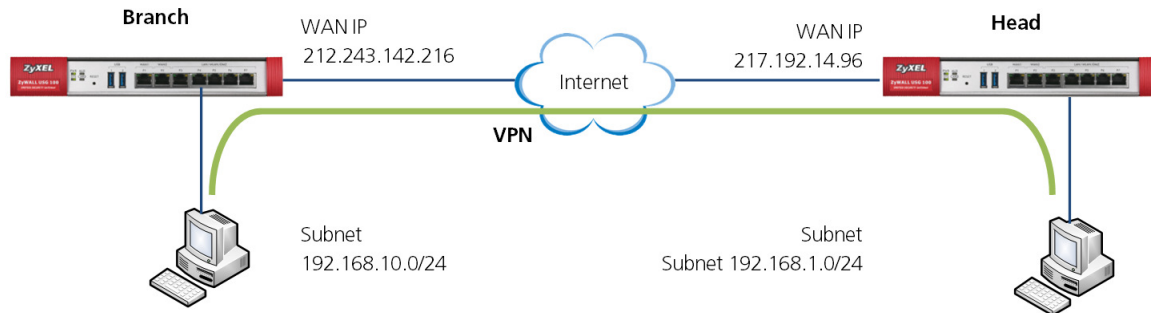


VPN IPSec

**Exemple de configuration
ZyXEL Série ZyWALL USG**

Mars 2010 / HAL

MISE EN PLACE



VPN PEER TO PEER CLASSIQUE

[Configuration](#) > [Object](#) > [Address](#) > [Add](#)

Sur le ZyWALL Head, effectuer les paramétrages suivants :

The screenshot shows the 'Add Address Rule' dialog box on the ZyWALL Head. The fields are filled as follows:

Name:	Branch_SUBNET
Address Type:	SUBNET
Network:	192.168.10.0
Netmask:	255.255.255.0

Buttons: OK, Cancel

Sur le ZyWALL Branch, effectuer les paramétrages suivants :

The screenshot shows the 'Add Address Rule' dialog box on the ZyWALL Branch. The fields are filled as follows:

Name:	Head_SUBNET
Address Type:	SUBNET
Network:	192.168.1.0
Netmask:	255.255.255.0

Buttons: OK, Cancel

PARAMETRAGES PHASE 1

Configuration > VPN > IPSec VPN > VPN Gateway > Add
ZyWALL Head

Add VPN Gateway

Show Advanced Settings

General Settings

Enable

VPN Gateway Name: gtw_Branch

Gateway Settings

My Address

Interface: wan1

Domain Name / IP

Peer Gateway Address

Static Address

Primary: 212.243.142.216

Secondary: 0.0.0.0

Fall back to Primary Peer Gateway when possible

Fall Back Check Interval: 300 (60-86400 seconds)

Dynamic Address

Authentication

Pre-Shared Key: mysecretkey

Certificate: default (See My Certificates)

OK Cancel

ZyWALL Branch

Add VPN Gateway

Show Advanced Settings

General Settings

Enable

VPN Gateway Name: gtw_Head

Gateway Settings

My Address

Interface: wan1

Domain Name / IP

Peer Gateway Address

Static Address

Primary: 217.192.14.96

Secondary: 0.0.0.0

Fall back to Primary Peer Gateway when possible

Fall Back Check Interval: 300 (60-86400 seconds)

Dynamic Address

Authentication

Pre-Shared Key: mysecretkey

Certificate: default (See My Certificates)

OK Cancel

PARAMETRAGES PHASE 2

Configuration > VPN > IPSec VPN > VPN Connection > Add
ZyWALL Head

The screenshot shows the 'Add VPN Connection' dialog box with the following settings:

- General Settings:** Enable; Connection Name: Branch
- VPN Gateway:** Application Scenario: Site-to-site (selected); VPN Gateway: gtw_Branch; IP: wan1 212.243.142.216 0.0.0.0
- Policy:** Local policy: Head_SUBNET; Remote policy: Branch_SUBNET
- Phase 2 Settings:** SA Life Time: 86400 (180 - 3000000 Seconds)
- Related Settings:** Add this VPN connection to IPsec_VPN zone.

ZyWALL Branch, cet objet a été créé sur la page 4

The screenshot shows the 'Add VPN Connection' dialog box with the following settings:

- General Settings:** Enable; Connection Name: Head
- VPN Gateway:** Application Scenario: Site-to-site (selected); VPN Gateway: gtw_Head; IP: wan1 217.192.14.96 0.0.0.0
- Policy:** Local policy: Branch_SUBNET; Remote policy: Head_SUBNET
- Phase 2 Settings:** SA Life Time: 86400 (180 - 3000000 Seconds)
- Related Settings:** Add this VPN connection to IPsec_VPN zone.

SA MONITOR

Monitor > VPN Monitor > IPSec

ZyWALL Head, un rafraîchissement (Refreshg) de la page montre si les valeurs augmentent en permanence. On en conclut lors de la recherche d'erreurs qu'il y a des paquets Inbound et Outbound qui passent.

Current IPSec Security Associations

Name:

Policy:

#	Name ^	Encapsulation	Policy	Algorithm	Up Time	Timeout	Inbound(Bytes)	Outbound(Bytes)
1	Branch	Tunnel	192.168.1.0/24 <-> 192.168.10.0/24	DES/SHA1	30845	55585	882(119952 bytes)	1764(148176 bytes)

Page 1 of 1 | Show 50 items | Displaying 1 - 1 of 1

ZyWALL Branch

Current IPSec Security Associations

Name:

Policy:

#	Name ^	Encapsulation	Policy	Algorithm	Up Time	Timeout	Inbound(Bytes)	Outbound(Bytes)
1	Head	Tunnel	192.168.10.0/24 <-> 192.168.1.0/24	DES/SHA1	30810	55620	881(119816 bytes)	1762(148008 bytes)

Page 1 of 1 | Show 50 items | Displaying 1 - 1 of 1

TROUBLE SHOOTING AVEC LOGS (IKE)

Monitor > Log

Dans le champ d'affichage, les entrées Log peuvent être triées selon le type.

Logs

Display:

Email Log Now Refresh Clear Log

#	Time	Priority	Category	Message	Source	Destination	Note
1	2010-03-24 16:16:22	info	IKE	Tunnel [WIZ_VPN_USG300.Branch:0x6553920f9] built successfully	212.243.142.197:500	212.243.142.214:500	IKE_LOG
2	2010-03-24 16:16:22	info	IKE	[SA]: [Responder:212.243.142.214][Initiator:212.243.142.197][Policy:192.168.100.0/24-192.168...	212.243.142.197:500	212.243.142.214:500	IKE_LOG
3	2010-03-24 16:16:22	info	IKE	Recv:[HASH]	212.243.142.197:500	212.243.142.214:500	IKE_LOG
4	2010-03-24 16:16:22	info	IKE	Send:[HASH][SA][NONCE][ID][ID]	212.243.142.214:500	212.243.142.197:500	IKE_LOG
5	2010-03-24 16:16:22	info	IKE	Recv:[HASH][SA][NONCE][ID][ID]	212.243.142.197:500	212.243.142.214:500	IKE_LOG
6	2010-03-24 16:16:22	info	IKE	Send:[D][HASH]	212.243.142.214:500	212.243.142.197:500	IKE_LOG
7	2010-03-24 16:16:22	info	IKE	Phase 1 IKE SA process done	212.243.142.214:500	212.243.142.197:500	IKE_LOG
8	2010-03-24 16:16:22	info	IKE	Recv:[D][HASH][NOTIFY:INITIAL_CONTACT]	212.243.142.197:500	212.243.142.214:500	IKE_LOG
9	2010-03-24 16:16:22	info	IKE	Send:[KE][NONCE]	212.243.142.214:500	212.243.142.197:500	IKE_LOG
10	2010-03-24 16:16:22	info	IKE	Recv:[KE][NONCE]	212.243.142.197:500	212.243.142.214:500	IKE_LOG
11	2010-03-24 16:16:22	info	IKE	Send:[SA][VD][VD]	212.243.142.214:500	212.243.142.197:500	IKE_LOG
12	2010-03-24 16:16:22	info	IKE	The cookie pair is : 0xfa2cb5dbc4971707 / 0xf30afb02f5cc0fcc [count=6]	212.243.142.214:500	212.243.142.197:500	IKE_LOG
13	2010-03-24 16:16:22	info	IKE	Tunnel [WIZ_VPN_USG300.Branch] Recvng IKE request	212.243.142.197:500	212.243.142.214:500	IKE_LOG
14	2010-03-24 16:16:22	info	IKE	Recv:[SA][VD][VD]	212.243.142.197:500	212.243.142.214:500	IKE_LOG
15	2010-03-24 16:16:22	info	IKE	The cookie pair is : 0xfa2cb5dbc4971707 / 0xf30afb02f5cc0fcc [count=7]	212.243.142.197:500	212.243.142.214:500	IKE_LOG
16	2010-03-24 16:16:22	info	IKE	Recv Main Mode request from [212.243.142.197]	212.243.142.197:500	212.243.142.214:500	IKE_LOG

L'établissement du tunnel IKE a fonctionné sans problème.

Logs

Display:

Email Log Now Refresh Clear Log

#	Time	Priority	Category	Message	Source	Destination	Note
1	2010-03-24 16:16:22	info	IKE	Tunnel [WIZ_VPN_USG300.Branch:0x6553920f9] built successfully	212.243.142.197:500	212.243.142.214:500	IKE_LOG
2	2010-03-24 16:16:22	info	IKE	[SA]: [Responder:212.243.142.214][Initiator:212.243.142.197][Policy:192.168.100.0/24-192.168...	212.243.142.197:500	212.243.142.214:500	IKE_LOG
3	2010-03-24 16:16:22	info	IKE	Recv:[HASH]	212.243.142.197:500	212.243.142.214:500	IKE_LOG
4	2010-03-24 16:16:22	info	IKE	Send:[HASH][SA][NONCE][ID][ID]	212.243.142.214:500	212.243.142.197:500	IKE_LOG
5	2010-03-24 16:16:22	info	IKE	Recv:[HASH][SA][NONCE][ID][ID]	212.243.142.197:500	212.243.142.214:500	IKE_LOG
6	2010-03-24 16:16:22	info	IKE	Send:[D][HASH]	212.243.142.214:500	212.243.142.197:500	IKE_LOG
7	2010-03-24 16:16:22	info	IKE	Phase 1 IKE SA process done	212.243.142.214:500	212.243.142.197:500	IKE_LOG
8	2010-03-24 16:16:22	info	IKE	Recv:[D][HASH][NOTIFY:INITIAL_CONTACT]	212.243.142.197:500	212.243.142.214:500	IKE_LOG
9	2010-03-24 16:16:22	info	IKE	Send:[KE][NONCE]	212.243.142.214:500	212.243.142.197:500	IKE_LOG
10	2010-03-24 16:16:22	info	IKE	Recv:[KE][NONCE]	212.243.142.197:500	212.243.142.214:500	IKE_LOG
11	2010-03-24 16:16:22	info	IKE	Send:[SA][VD][VD]	212.243.142.214:500	212.243.142.197:500	IKE_LOG
12	2010-03-24 16:16:22	info	IKE	The cookie pair is : 0xfa2cb5dbc4971707 / 0xf30afb02f5cc0fcc [count=6]	212.243.142.214:500	212.243.142.197:500	IKE_LOG
13	2010-03-24 16:16:22	info	IKE	Tunnel [WIZ_VPN_USG300.Branch] Recvng IKE request	212.243.142.197:500	212.243.142.214:500	IKE_LOG
14	2010-03-24 16:16:22	info	IKE	Recv:[SA][VD][VD]	212.243.142.197:500	212.243.142.214:500	IKE_LOG
15	2010-03-24 16:16:22	info	IKE	The cookie pair is : 0xfa2cb5dbc4971707 / 0xf30afb02f5cc0fcc [count=7]	212.243.142.197:500	212.243.142.214:500	IKE_LOG
16	2010-03-24 16:16:22	info	IKE	Recv Main Mode request from [212.243.142.197]	212.243.142.197:500	212.243.142.214:500	IKE_LOG

Exemple d'un problème en Phase 1

#	Time	Priority	Category	Message	Source	Destination	Note
2	2010-03-24 16:19:03	info	IKE	The cookie pair is : 0x5c9b04c34475cae7 / 0x9c4ccbab7678bfe1	212.243.142.215:500	212.243.142.197:500	IKE_LOG
3	2010-03-24 16:19:03	info	IKE	The cookie pair is : 0x5c9b04c34475cae7 / 0x9c4ccbab7678bfe1 [count=2]	212.243.142.197:500	212.243.142.215:500	IKE_LOG
4	2010-03-24 16:19:03	info	IKE	The cookie pair is : 0x5c9b04c34475cae7 / 0x0000000000000000	212.243.142.197:500	212.243.142.215:500	IKE_LOG
5	2010-03-24 16:19:03	info	IKE	Send:[NOTFY:NO_PROPOSAL_CHOSEN] [count=2]	212.243.142.215:500	212.243.142.197:500	IKE_LOG
6	2010-03-24 16:19:03	info	IKE	The cookie pair is : 0x5fbb1270d7af684d / 0xc51be07c75d25876	212.243.142.215:500	212.243.142.197:500	IKE_LOG
7	2010-03-24 16:19:03	info	IKE	[SA] : No proposal chosen [count=2]	212.243.142.197:500	212.243.142.215:500	IKE_LOG
8	2010-03-24 16:19:03	info	IKE	[D] : Tunnel [Studerus_Test] Remote IP mismatch [count=2]	212.243.142.197:500	212.243.142.215:500	IKE_LOG
9	2010-03-24 16:19:03	info	IKE	Recv:[SA][V][VD] [count=2]	212.243.142.197:500	212.243.142.215:500	IKE_LOG
10	2010-03-24 16:19:03	info	IKE	The cookie pair is : 0x5fbb1270d7af684d / 0xc51be07c75d25876 [count=2]	212.243.142.197:500	212.243.142.215:500	IKE_LOG
11	2010-03-24 16:19:03	info	IKE	Recv Main Mode request from [212.243.142.197] [count=2]	212.243.142.197:500	212.243.142.215:500	IKE_LOG
12	2010-03-24 16:19:03	info	IKE	The cookie pair is : 0x5fbb1270d7af684d / 0x0000000000000000	212.243.142.197:500	212.243.142.215:500	IKE_LOG
13	2010-03-24 16:19:03	info	IKE	The cookie pair is : 0x8b989773d4add77d / 0xa94de414fbb76096	212.243.142.214:500	212.243.142.197:500	IKE_LOG
14	2010-03-24 16:19:03	info	IKE	The cookie pair is : 0x8b989773d4add77d / 0xa94de414fbb76096 [count=2]	212.243.142.197:500	212.243.142.214:500	IKE_LOG
15	2010-03-24 16:19:03	info	IKE	The cookie pair is : 0x8b989773d4add77d / 0x0000000000000000	212.243.142.197:500	212.243.142.214:500	IKE_LOG
16	2010-03-24 16:19:03	info	IKE	Send:[NOTFY:NO_PROPOSAL_CHOSEN] [count=2]	212.243.142.214:500	212.243.142.197:500	IKE_LOG

Exemple de l'établissement d'un tunnel IKE avec mauvaise PSK

#	Time	Priority	Category	Message	Source	Destination	Note
1	2010-03-24 16:20:35	info	IKE	Recv:[NOTFY:INVALID_ID_INFORMATION]	212.243.142.197:500	212.243.142.215:500	IKE_LOG
2	2010-03-24 16:20:35	info	IKE	The cookie pair is : 0xd35789b2a90b1f6b / 0x43d59f4ed47063bc [count=2]	212.243.142.215:500	212.243.142.197:500	IKE_LOG
3	2010-03-24 16:20:35	info	IKE	The cookie pair is : 0xd35789b2a90b1f6b / 0x43d59f4ed47063bc [count=4]	212.243.142.197:500	212.243.142.215:500	IKE_LOG
4	2010-03-24 16:20:35	info	IKE	The cookie pair is : 0xd35789b2a90b1f6b / 0x0000000000000000	212.243.142.197:500	212.243.142.215:500	IKE_LOG
5	2010-03-24 16:20:35	info	IKE	Send:[NOTFY:INVALID_PALOAD_TYPE]	212.243.142.215:500	212.243.142.197:500	IKE_LOG
6	2010-03-24 16:20:35	info	IKE	Tunnel [Branch] Phase 1 pre-shared key mismatch	212.243.142.197:500	212.243.142.215:500	IKE_LOG
7	2010-03-24 16:20:35	info	IKE	Send:[KE][NONCE] [count=2]	212.243.142.215:500	212.243.142.197:500	IKE_LOG
8	2010-03-24 16:20:34	info	IKE	Recv:[KE][NONCE] [count=2]	212.243.142.197:500	212.243.142.215:500	IKE_LOG
9	2010-03-24 16:20:34	info	IKE	Send:[SA][V][VD] [count=2]	212.243.142.215:500	212.243.142.197:500	IKE_LOG
10	2010-03-24 16:20:34	info	IKE	The cookie pair is : 0xe4d45ad147110608 / 0x35d79e4e1a501ee4 [count=3]	212.243.142.215:500	212.243.142.197:500	IKE_LOG
11	2010-03-24 16:20:34	info	IKE	Tunnel [WZ_VPN_USG300.Branch] Recvng IKE request [count=2]	212.243.142.197:500	212.243.142.215:500	IKE_LOG
12	2010-03-24 16:20:34	info	IKE	Recv:[SA][V][VD] [count=2]	212.243.142.197:500	212.243.142.215:500	IKE_LOG

Exemple de l'établissement d'un tunnel IKE avec erreur en Phase 2 (Active Protocol, Encryption Algorithm, Authentication Algorithm ou Perfect Forwarding Secrecy (PFS))

#	Time	Priority	Category	Message	Source	Destination	Note
1	2010-03-24 16:23:19	info	IKE	Send:[HASH][NOTFY:NO_PROPOSAL_CHOSEN]	212.243.142.214:500	212.243.142.197:500	IKE_LOG
2	2010-03-24 16:23:19	info	IKE	The cookie pair is : 0x87854094a38b4772 / 0x1a7b94d99889c256	212.243.142.214:500	212.243.142.197:500	IKE_LOG
3	2010-03-24 16:23:19	info	IKE	[SA] : No proposal chosen	212.243.142.197:500	212.243.142.214:500	IKE_LOG
4	2010-03-24 16:23:19	info	IKE	Recv:[HASH][SA][NONCE][ID][ID]	212.243.142.197:500	212.243.142.214:500	IKE_LOG
5	2010-03-24 16:23:19	info	IKE	The cookie pair is : 0x87854094a38b4772 / 0x1a7b94d99889c256 [count=2]	212.243.142.197:500	212.243.142.214:500	IKE_LOG
6	2010-03-24 16:22:59	info	IKE	Send:[HASH][NOTFY:NO_PROPOSAL_CHOSEN]	212.243.142.214:500	212.243.142.197:500	IKE_LOG
7	2010-03-24 16:22:59	info	IKE	The cookie pair is : 0x87854094a38b4772 / 0x1a7b94d99889c256	212.243.142.214:500	212.243.142.197:500	IKE_LOG
8	2010-03-24 16:22:59	info	IKE	[SA] : No proposal chosen	212.243.142.197:500	212.243.142.214:500	IKE_LOG
9	2010-03-24 16:22:58	info	IKE	Recv:[HASH][SA][NONCE][ID][ID]	212.243.142.197:500	212.243.142.214:500	IKE_LOG
10	2010-03-24 16:22:58	info	IKE	The cookie pair is : 0x87854094a38b4772 / 0x1a7b94d99889c256 [count=2]	212.243.142.197:500	212.243.142.214:500	IKE_LOG
11	2010-03-24 16:22:44	info	IKE	Send:[HASH][NOTFY:NO_PROPOSAL_CHOSEN]	212.243.142.214:500	212.243.142.197:500	IKE_LOG
12	2010-03-24 16:22:43	info	IKE	[SA] : No proposal chosen	212.243.142.197:500	212.243.142.214:500	IKE_LOG