

ZyXEL

ZyWALL > VPN > L2TP VPN > Session Monitor

Status

L2TP VPN Session Monitor

Current L2TP Session

#	User Name	Hostname	Assigned IP	Public IP	Action
1	kkoenig	Unknown	192.168.201.2	80.187.96.1	↔

Refresh

ZyWALL

- Licensing
- Network
  - Interface
  - Routing
  - Zone
  - DDNS
  - Virtual Server
  - HTTP Redirect
  - ALG
  - IP/MAC Binding
- Firewall
- VPN
  - IPSec VPN
  - SSL VPN
  - L2TP VPN
- AppPatrol
- Anti-X
- Device HA
- Object
- System
- Maintenance

Message Ready.

Lokales Intranet

ZyXEL

ZyWALL > VPN > L2TP VPN > L2TP VPN

Status

L2TP VPN Session Monitor

General Settings

Enable L2TP Over IPSec

VPN Connection: L2TP\_VPN\_Connection

IP Address Pool: L2TP\_Pool

Authentication Method: default

Allowed User: L2TP\_User

Keep Alive Timer: 60 (1-180 seconds)

First DNS Server (Optional): 192.101.111.20

Second DNS Server (Optional): 192.101.111.10

First WINS Server (Optional):

Second WINS Server (Optional):

Apply Reset

VPN-Account-Info bearbeiten

Abbrechen USG-200 Sichern

L2TP PPTP IPSec

Beschreibung USG-200

Server hostname.dyn dns.org

Account L2TP\_User

RSA-SecurID

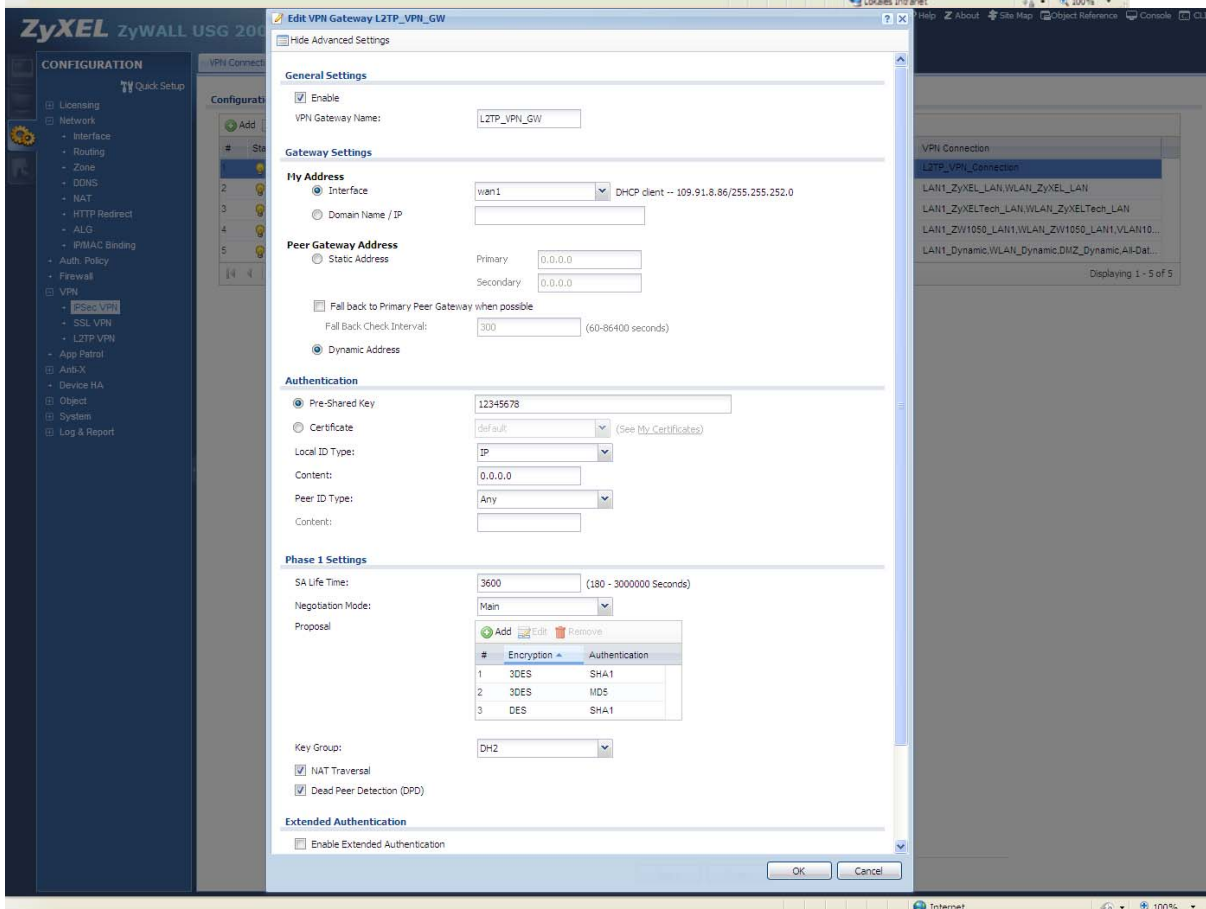
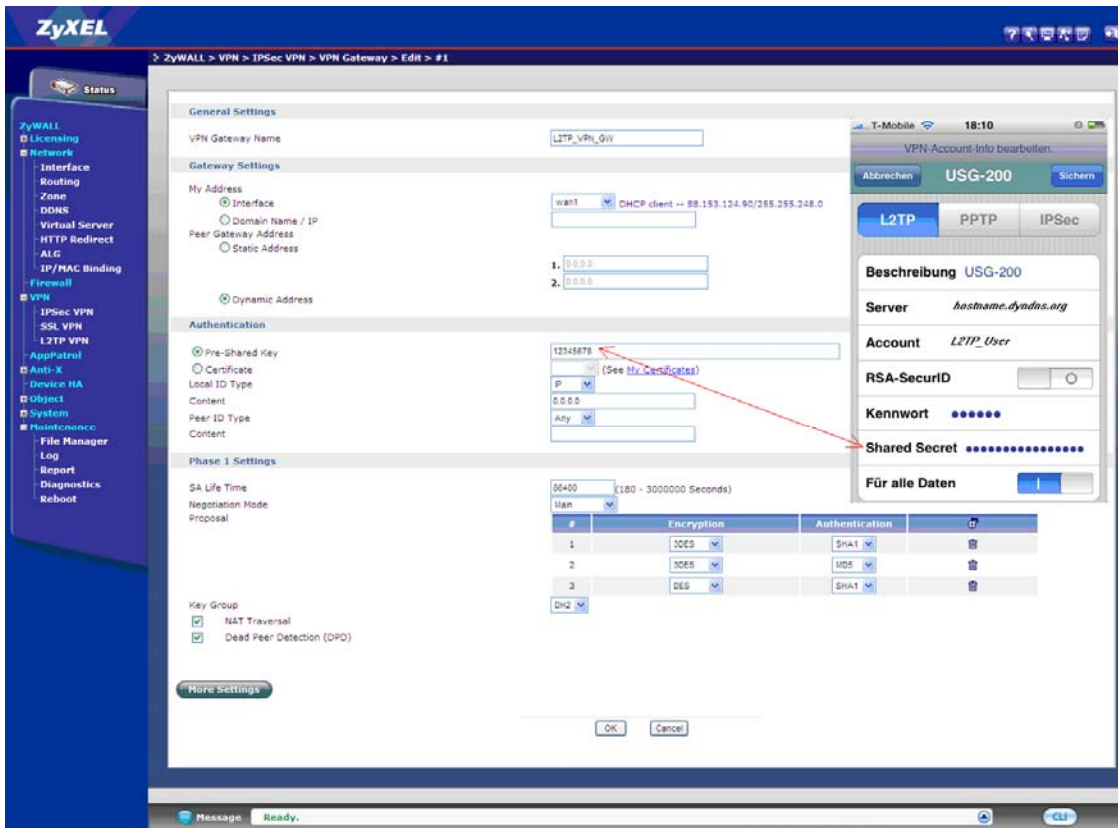
Kennwort .....

Shared Secret .....

Für alle Daten

Message Ready.

Lokales Intranet



**ZyXEL** ZyWALL > VPN > IPSec VPN > VPN Connection > Edit > #1

**Status**

**ZyWALL**

- Licensing
- Network
  - Interface
  - Routing
  - Zone
  - DDNS
- Virtual Server
  - HTTP Redirect
  - ALG
  - IP/MAC Binding
- Firewall
- VPN
  - IPSec VPN
  - SSL VPN
  - L2TP VPN
- AppPatrol
- Anti-X
  - Device HA
- Object
- System
  - File Manager
  - Log
  - Report
  - Diagnostics
  - Reboot

**General Settings** Basic

Connection Name: L2TP\_VPN\_Connection

Nailed-Up  
 Enable Replay Detection  
 Enable NetBIOS broadcast over IPSec

**VPN Gateway** Basic

Application Scenario  
 Site-to-site  
 Site-to-site with Dynamic Peer  
 Remote Access (Server Role)  
 Remote Access (Client Role)

VPN Gateway: L2TP\_VPN\_GW wan1: 0.0.0.0, 0.0.0.0

Manual Key  
 Manual Key

My Address:   
 Secure Gateway Address:   
 SPI:  (256 - 4095)  
 Encapsulation Mode: Tunnel  
 Active Protocol: ESP  
 Encryption Algorithm: DES  
 Authentication Algorithm: SHA1  
 Encryption Key:   
 Authentication Key:

**Policy** Basic

Local policy: WAN1\_IP INTERFACE IP, 88.153.124.90  
 Remote policy: DynamicHOST HOST, 0.0.0.0  
 Policy Enforcement

**Phase 2 Settings** Basic

SA Life Time: 1800 (180 - 3000000 Seconds)  
 Active Protocol: ESP  
 Encapsulation: Transport

#	Encryption	Authentication	
1	3DES	SHA1	<input type="checkbox"/>
2	3DES	MD5	<input type="checkbox"/>
3	DES	SHA1	<input type="checkbox"/>

Perfect Forward Secrecy (PFS): none

Message: Ready.

**ZyXEL ZyWALL USG** Edit VPN Connection L2TP\_VPN\_Connection

Hide Advanced Settings Create new Object

**General Settings**

Enable  
 Connection Name: L2TP\_VPN\_Connection  
 Nailed-Up  
 Enable Replay Detection  
 Enable NetBIOS broadcast over IPSec

**VPN Gateway**

Application Scenario  
 Site-to-site  
 Site-to-site with Dynamic Peer  
 Remote Access (Server Role)  
 Remote Access (Client Role)

VPN Gateway: L2TP\_VPN\_GW wan1: 0.0.0.0, 0.0.0.0

Manual Key  
 Manual Key

My Address:   
 Secure Gateway Address:   
 SPI:  (256 - 4095)  
 Encapsulation Mode: Tunnel  
 Active Protocol: ESP  
 Encryption Algorithm: DES  
 Authentication Algorithm: SHA1  
 Encryption Key:   
 Authentication Key:

**Policy**

Local policy: WAN1\_IP INTERFACE IP, 109.91.8.86  
 Remote policy: DynamicHOST HOST, 0.0.0.0  
 Policy Enforcement

**Phase 2 Settings**

SA Life Time: 1800 (180 - 3000000 Seconds)  
 Active Protocol: ESP  
 Encapsulation: Transport

Proposal

#	Encryption	Authentication
+		

OK Cancel

**ZyXEL** ZyWALL > VPN > IPSec VPN > VPN Connection > Edit > #1

Encapsulation Mode: Tunnel  
 Active Protocol: ESP  
 Encryption Algorithm: DES  
 Authentication Algorithm: SHA1  
 Encryption Key:   
 Authentication Key:

**Policy** Basic

Local policy: WAN1\_IP INTERFACE IP: 88.153.124.90  
 Remote policy: DynamicHOST HOST: 0.0.0.0  
 Policy Enforcement

**Phase 2 Settings** Basic

SA Life Time: 3600 (180 - 3000000 Seconds)  
 Active Protocol: ESP  
 Encapsulation: Transport  
 Proposal:

#	Encryption	Authentication	
1	3DES	SHA1	<input type="checkbox"/>
2	3DES	MD5	<input type="checkbox"/>
3	DES	SHA1	<input type="checkbox"/>

Perfect Forward Secrecy (PFS): none

**Related Settings**

Add this VPN connection to IPsec\_VPN zone.

**Connectivity Check**

Enable Connectivity Check  
 Check Method:   
 Check Period:  (5-30 Seconds)  
 Check Timeout:  (1-10 Seconds)  
 Check Fail Tolerance:  (1-10)  
 Check This Address  (Domain Name or IP Address)  
 Check the First and Last IP Address in the Remote Policy  
 Log

More Settings

OK Cancel

**ZyXEL ZyWALL USG** Edit VPN Connection L2TP\_VPN\_Connection

Encapsulation: Transport  
 Proposal:

#	Encryption	Authentication
1	3DES	SHA1
2	3DES	MD5
3	DES	SHA1

Perfect Forward Secrecy (PFS): none

**Related Settings**

Add this VPN connection to IPsec\_VPN zone.

**Connectivity Check**

Enable Connectivity Check  
 Check Method: icmp  
 Check Period:  (5-30 Seconds)  
 Check Timeout:  (1-10 Seconds)  
 Check Fail Tolerance:  (1-10)  
 Check This Address  Domain Name or IP Address  
 Check the First and Last IP Address in the Remote Policy  
 Log

**Inbound/Outbound traffic NAT**

Outbound Traffic

Source NAT  
 Source: Please select one ...  
 Destination: Please select one ...  
 SNAT: Please select one ...

Inbound Traffic

Source NAT  
 Source: Please select one ...  
 Destination: Please select one ...  
 SNAT: Please select one ...

Destination NAT

#	Original IP	Mapped IP	Protocol	Original Port Start	Original Port End	Mapped Port Start	Mapped Port End
No data to display							

Page 1 of 1 | Show 50 items

OK Cancel

**ZyXEL** > ZyWALL > Maintenance > Log > View Log

View Log Log Settings

Log File: All Log

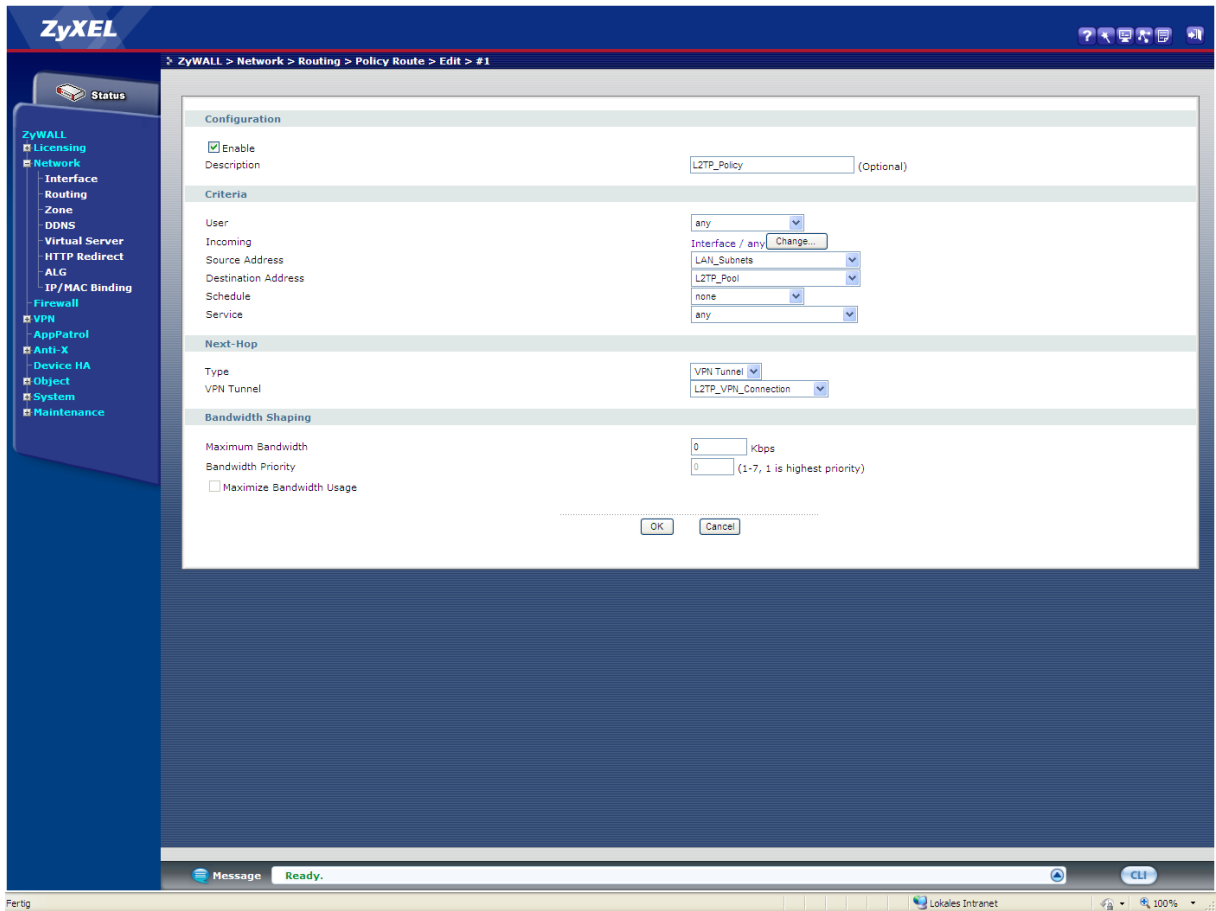
Total logging entries: 38

32 26 entries per page Page: 1 of 1 (38/38)

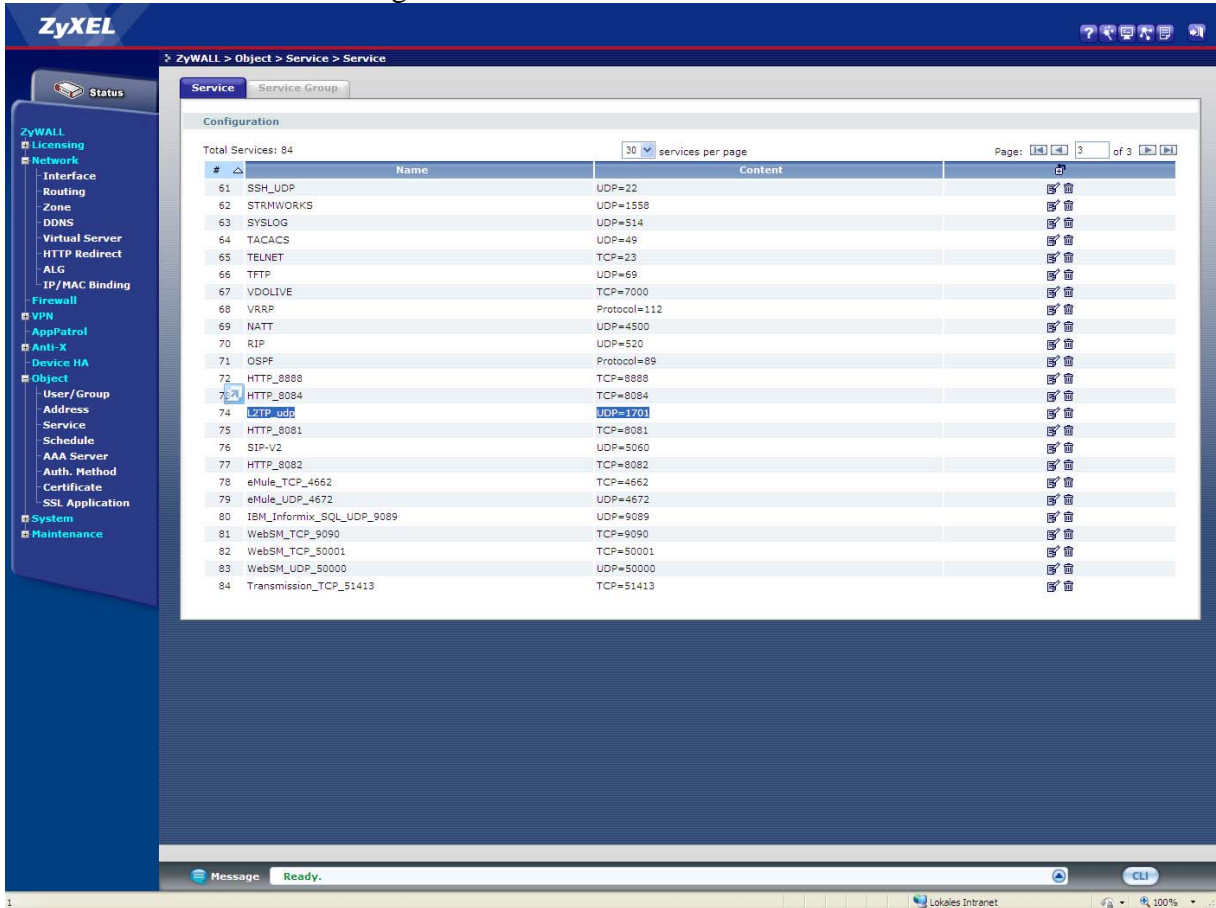
#	Time	Priority	Category	Message	Source	Destination	Note
1	2009-06-03 18:19:22	Info	FW rule	srcPort: 48, from: 192.168.1.1 to: 192.168.1.1, service: LTPF, rule: LTPF, action: ACCEPT	192.168.1.1	192.168.1.1	ACCESS FORWARD
2	2009-06-03 18:19:22	Info	LTPF rule: LTPF	User logging has been started on LTPF rule: LTPF action	80.187.86.1	88.153.124.80	LTPF Server
3	2009-06-03 18:19:27	Info	FW rule	srcPort: 80, from: 192.168.1.1 to: 192.168.1.1, service: LTPF, rule: LTPF, action: ACCEPT	80.187.86.1	88.153.124.80	ACCESS FORWARD
4	2009-06-03 18:19:27	Info	SSL	Dynamic Tunnel [LTPF_PHL_0] LTPF_PHL_Connector: 0x70000000 built success fully	80.187.86.1	88.153.124.80	SSL LOG
5	2009-06-03 18:19:27	Info	SSL	The ssls peer is: 0x0000000000000000 / 0x0000000000000000	80.187.86.1	88.153.124.80	SSL LOG
6	2009-06-03 18:19:27	Info	SSL	[SSL] [Session: 88.153.124.80] [Peer: 80.187.86.1] [Key: 88.153.124.80-10.102.102.70] [ESP: 0x0000000000000000]	80.187.86.1	88.153.124.80	SSL LOG
7	2009-06-03 18:19:27	Info	SSL	Key: [48] [0x00000000]	80.187.86.1	88.153.124.80	SSL LOG
8	2009-06-03 18:19:27	Info	SSL	Send [48] [0x00000000]	88.153.124.80	80.187.86.1	SSL LOG
9	2009-06-03 18:19:27	Info	SSL	Key: [48] [0x00000000]	80.187.86.1	88.153.124.80	SSL LOG
10	2009-06-03 18:19:28	Info	SSL	Key: [48] [0x00000000]	80.187.86.1	88.153.124.80	SSL LOG
11	2009-06-03 18:19:28	Info	SSL	Send [0x00000000]	88.153.124.80	80.187.86.1	SSL LOG
12	2009-06-03 18:19:28	Info	SSL	Phase 1 IKE SA process done	88.153.124.80	80.187.86.1	SSL LOG
13	2009-06-03 18:19:28	Info	SSL	The ssls peer is: 0x0000000000000000 / 0x0000000000000000	88.153.124.80	80.187.86.1	SSL LOG
14	2009-06-03 18:19:28	Info	SSL	Key: [48] [0x00000000]	80.187.86.1	88.153.124.80	SSL LOG
15	2009-06-03 18:19:28	Info	SSL	Send [48] [0x00000000]	88.153.124.80	80.187.86.1	SSL LOG
16	2009-06-03 18:19:28	Info	SSL	Key: [48] [0x00000000]	80.187.86.1	88.153.124.80	SSL LOG
17	2009-06-03 18:19:28	Info	SSL	Key: [48] [0x00000000]	88.153.124.80	80.187.86.1	SSL LOG
18	2009-06-03 18:19:28	Info	SSL	Send [48] [0x00000000]	88.153.124.80	80.187.86.1	SSL LOG
19	2009-06-03 18:19:28	Info	SSL	The ssls peer is: 0x0000000000000000 / 0x0000000000000000	88.153.124.80	80.187.86.1	SSL LOG
20	2009-06-03 18:19:28	Info	SSL	Tunnel [LTPF_PHL_0] LTPF_PHL_Connector: Keying IKE request	80.187.86.1	88.153.124.80	SSL LOG
21	2009-06-03 18:19:28	Info	SSL	Key: [48] [0x00000000]	80.187.86.1	88.153.124.80	SSL LOG
22	2009-06-03 18:19:28	Info	SSL	The ssls peer is: 0x0000000000000000 / 0x0000000000000000	80.187.86.1	88.153.124.80	SSL LOG
23	2009-06-03 18:19:28	Info	SSL	Key: Main Mode request from [80.187.86.1]	80.187.86.1	88.153.124.80	SSL LOG
24	2009-06-03 18:19:28	Info	SSL	The ssls peer is: 0x0000000000000000 / 0x0000000000000000	80.187.86.1	88.153.124.80	SSL LOG
25	2009-06-03 18:19:28	Info	SSL	Send [48] [0x00000000]	88.153.124.80	212.117.87.1	SSL LOG
26	2009-06-03 18:19:28	Info	SSL	The ssls peer is: 0x7877335054w0 / 0x187182070520d8	212.117.87.1	88.153.124.80	SSL LOG
27	2009-06-03 18:19:28	Info	SSL	Key: [48] [0x00000000]	212.117.87.1	88.153.124.80	SSL LOG
28	2009-06-03 18:19:28	Info	SSL	The ssls peer is: 0x7877335054w0 / 0x187182070520d8	212.117.87.1	88.153.124.80	SSL LOG
29	2009-06-03 18:19:28	Info	SSL	Tunnel [LTPF_PHL_Connector: 0x00000000] is disconnected	88.153.124.80	80.187.86.1	SSL LOG
30	2009-06-03 18:19:28	Info	SSL	Tunnel [LTPF_PHL_Connector: 0x00000000] is disconnected	88.153.124.80	80.187.86.1	SSL LOG
31	2009-06-03 18:19:28	Info	SSL	Key: [48] [0x00000000]	212.117.87.1	88.153.124.80	SSL LOG
32	2009-06-03 18:19:28	Info	SSL	The ssls peer is: 0x0000000000000000 / 0x187182070520d8	212.117.87.1	88.153.124.80	SSL LOG
33	2009-06-03 18:19:28	Info	SSL	Key: [48] [0x00000000]	212.117.87.1	88.153.124.80	SSL LOG
34	2009-06-03 18:19:28	Info	SSL	The ssls peer is: 0x7877335054w0 / 0x187182070520d8	212.117.87.1	88.153.124.80	SSL LOG
35	2009-06-03 18:19:28	Info	SSL	Send [48] [0x00000000]	88.153.124.80	212.117.87.1	SSL LOG
36	2009-06-03 18:19:28	Info	SSL	The ssls peer is: 0x0000000000000000 / 0x187182070520d8	88.153.124.80	212.117.87.1	SSL LOG
37	2009-06-03 18:19:28	Info	SSL	Send [48] [0x00000000]	88.153.124.80	212.117.87.1	SSL LOG
38	2009-06-03 18:19:28	Info	SSL	The ssls peer is: 0x7877335054w0 / 0x187182070520d8	88.153.124.80	212.117.87.1	SSL LOG

Message Ready

Lokales Intranet 82%



Service L2TP/UDP-1701 anlegen.



Den erstellten Service L2TP/UDP-1701 noch in die Gruppe „Default\_Allow\_WAN\_To\_ZyWALL“ legen - fertig.

The screenshot shows the ZyXEL web management interface. The breadcrumb navigation at the top reads: ZyWALL > Object > Service > Service Group > Edit > #10. The left sidebar contains a navigation menu with categories: ZyWALL, Licensing, Network, Interface, Routing, Zone, DDNS, Virtual Server, HTTP Redirect, ALG, IP/MAC Binding, Firewall, VPN, AppPatrol, Anti-X, Device HA, Object, User/Group, Address, Service, Schedule, AAA Server, Auth. Method, Certificate, SSL Application, System, and Maintenance. The main content area is titled "Configuration" and shows the following details:

- Name: Default\_Allow\_WAN\_To\_ZyWALL
- Description: AH ESP HTTPS IKE L2TP NATT PING S...

Below the configuration fields is a "Member List" section with two columns:

- Available:** A list of protocols including AH, AUTH, Any\_TCP, Any\_UDP, BGP, BOOTP\_CLIENT, BOOTP\_SERVER, CU\_SEEIME\_TCP1, and CU\_SEEIME\_TCP2.
- Member:** A list of protocols including AH, ESP, HTTPS, IKE, L2TP\_udp, NATT, PING, SIP-V2, and VRRP.

Between the two columns are arrows for adding (>) and removing (<) members. At the bottom of the Member List section are "OK" and "Cancel" buttons. The interface also shows a "Message Ready." status bar and a "CLI" button at the bottom right.