Using a VPN with CentraLine^{AX} Systems

User Guide

by Honeywell

TABLE OF CONTENTS

INTRODUCTION

What Is a VPN?

A "Virtual Private Network" or VPN is a mechanism to extend a private network across a public network such as the Internet. A VPN creates a point-to-point connection or "tunnel" across the Internet between two computers. The tunnel encrypts the data between VPN endpoints, preventing data from being deciphered without the required encryption keys:

Why Use a VPN?

Using a VPN provides an additional layer of security to your CentraLine^{AX} system without compromising your ability to access CentraLine^{AX}. A VPN can help protect your Niagara system from Internet based attacks by requiring an additional layer of authentication to access CentraLine^{AX} resources. It can prevent automated Internet port scans tools from detecting the CentraLine^{AX} system

How Can I Set Up a VPN?

This document describes how to use an Internet Security Gateway to provide VPN access to your HAWK.

Important

This information in this document is based on the assumption that the only IP devices on the network are CentraLine^{AX} devices. If CentraLine^{AX} devices share a network with other devices (such as a corporate LAN), DO NOT follow the approach described in the following pages. Instead, work with the customer's IT department to determine the best method to protect both the CentraLine^{AX} and corporate systems while providing required access to the CentraLine^{AX} systems.

In any scenario, if the VPN is installed or configured improperly, you can expose devices to the public Internet. If you are unsure about how to best configure and test your configuration, please consult an IT expert

NETWORK DIAGRAMS

Consider the following typical CentraLine^{AX} set-up. One or more HAWKs and/or a Supervisor are connected via a router to form a LAN. The Supervisor and possibly the HAWKs are exposed to the Internet via DSL or Cable Modem connection. Port forwarding in the Router allows the Daemon, Fox and/or Web ports for each CentraLine^{AX} system to be accessed. Alternatively, one could expose the Supervisor only and use CentraLine^{AX} Fox/HTTP/Platform Tunneling to reach other systems

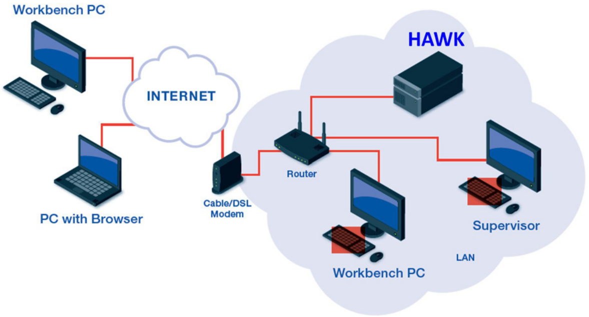


Fig. 1. Typical CentraLine^{AX} set-up

If all ports are forwarded, this configuration gives full access (Web/Fox/Daemon) to all 3 CentraLine^{AX} systems via the Internet. Fig. 2 shows Workbench opening a Fox connection.

- The Workbench PC opens a connection to the public IP address of the router.
- The router then forwards the connection to the Supervisor.

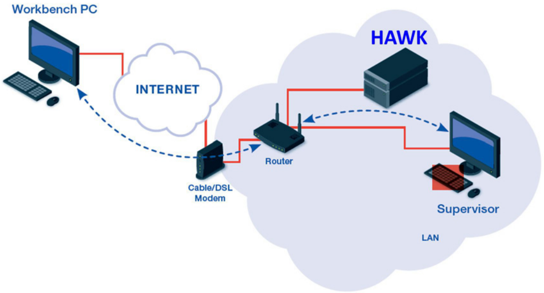


Fig. 2. Typical CentraLine^{AX} set-up with Workbench opening a Fox connection

There at least two significant security flaws with this approach:

1. **An automated port scan from the Internet is able to identify all nine ports as CentraLine^{AX} systems.**
   - Systems can be identified even without CentraLine^{AX} Station or platform credentials.
   - If weak or default passwords are used for Station or Platform accounts, an attacker can quickly gain access to the systems.
   - Attackers use automated tools to identify systems and then look for known or new vulnerabilities in those systems to exploit.
2. **Communication between Workbench and Browsers to the system is not encrypted.**

Network Set-Up with a VPN

Fig. 3 shows the same system with the addition of a security gateway capable of acting as a VPN Server.

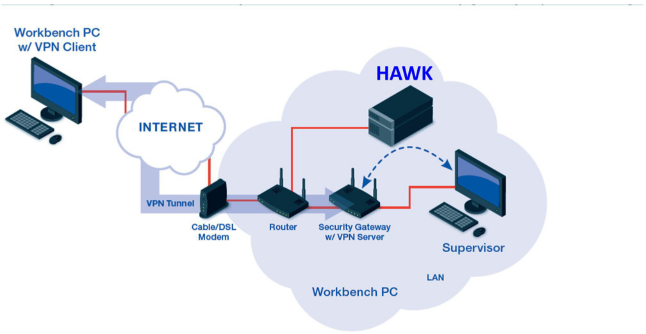


Fig. 3. Typical CentraLine^{AX} set-up with security gateway acting as VPN

In this case, a VPN tunnel is created between the Workbench PC and the VPN server running on the Security Gateway. All traffic running through this tunnel is encrypted. The only port that must be exposed to the Internet is the VPN port on the Security Gateway.

Once the VPN tunnel is created, the Workbench PC is effectively part of the local LAN network. A Fox, Web, or Platform connection can be opened to the Supervisor using the Supervisor's LAN IP address.

It is important to note that traffic between the Security Gateway and Supervisor is NOT encrypted unless you use SSL.

FAQ

I already use SSL – do I still need to use a VPN?

Use of a VPN is still recommended as an additional layer of security. Attacks can come from both inside and outside of your network.

Once I setup a VPN, do I still need to use SSL?

Yes. The VPN only provides encryption between the VPN endpoints – the VPN client and server. Traffic from the VPN endpoint to and from the CentraLine^{AX} Station is not encrypted unless SSL is used.

I'm running AX 3.6 or earlier without SSL support – should I still install a VPN?

Yes. The VPN still helps protect against Internet based attacks on your system.

Do I still need a firewall?

Yes. You should set up firewall rules to restrict Internet access to the VPN server port only. You should also consider setting up rules with the VPN server to restrict VPN access to only the required IP addresses and ports. For example, there may be non-CentraLine^{AX} devices on the LAN, but the VPN should be configured to only allow access to the CentraLine^{AX} systems. Additionally, you should only allow access to required CentraLine^{AX} services.

Will a VPN affect LAN access to HAWKs?

No. LAN access to the CentraLine^{AX} devices remains the same as always. VPN only affects ability to reach CentraLine^{AX} devices from external networks such as the Internet.

If I use a VPN, will CentraLine^{AX} HTTP, Fox and Platform tunneling work?

Tunneling works normally over VPN. You will need to update IP address assignments.

What is the impact of VPN on CentraLine^{AX} Networking?

CentraLine^{AX} Networking between systems on the LAN still functions the same whether or not there is a VPN installed.

When I connect to a VPN, do I lose all other network connectivity?

While your VPN client is connected to the remote VPN network, your Workbench (client) PC will have a new "Default Gateway" to allow you to make connections to stations on the VPN network. Typically, this happens without your knowledge, and is mostly transparent. The change is undone after disconnecting from the VPN, and re-done when you reconnect.

However (while you are connected to the VPN network) if your Workbench (client) PC tries to connect to sites on the [public] Internet or any other network through any router, you will find that you cannot reach those sites.

If you must be able to reach those sites while connected to the VPN network, you will need to add static routes (temporary or permanent) to your Workbench PC's TCP/IP configuration. The setting of those routes is beyond the scope of this document, because they are specific to your PC's network, your VPN network, and any other networks you try to reach.

It is possible (but unlikely) that you cannot resolve these routing issues. This may happen if one or more of these networks have overlapping addresses. Consult with a TCP/IP expert if necessary.

Likewise, if you use L2TP, PPOE, PPTP, or PPP for any part of your underlying network connection, the VPN client will probably conflict with it. Specifically, Windows only allows one connection of these four protocol types to be active at any given time.

What is the impact on Single Sign On?

You will need to define the SSO Domain and the hosts of the SSO Domain in your Workbench PC's "hosts" file or default DNS server. The DNS server of the VPN will not be able to provide name services without changing your Workbench PC's TCP/IP configuration.

I use Dynamic DNS – can I still use a dynamic DNS provider with VPN?

Yes. You will need to register the IP address of the VPN gateway and firewall with the DDNS provider.

What is the impact of VPN on my system performance?

Impact to performance should be minimal. It does take a little longer to setup the connection.

References

Microsoft TechNet VPN Overview

http://technet.microsoft.com/en-us/library/bb742566.aspx

SETTING UP A VPN USING A ZYWALL GATEWAY

The ZyWALL USG-20 unified security gateway (from ZyXEL) is a cost effective device that you can add to an existing installation to provide VPN server capability. The rest of this document describes how to setup a ZyWALL device for use with CentraLine^{AX}. This document refers to and comments on the ZyWALL documentation:

Zywall USG Series Unified Security Gateway User's Guide at: ftp://ftp2.zyxel.com/ZyWALL_USG_20/user_guide/ZyWALL%20USG%2020_v3-00_Ed1.pdf

Network Diagram

These instructions use the following network configuration:

- The 10.10.8.X subnet represents the Internet.
- The 192.168.1.X subnet represents the internal LAN.
- The goal is to provide access to the CentraLine^{AX} HAWK via WAN and LAN connections.

NOTE: There are four (4) TCP/IP networks employed in this example. Each of these four networks must have unique (non-colliding, non-overlapping) addresses.

- Network (A) is the private network on which the HAWKs and Supervisors ("stations") reside.
- Network (B) is the Internet connection or any un-trusted network.
- Network (C) is the private network on which the Workbench PC resides.
- Network (D) is the VPN channel itself.

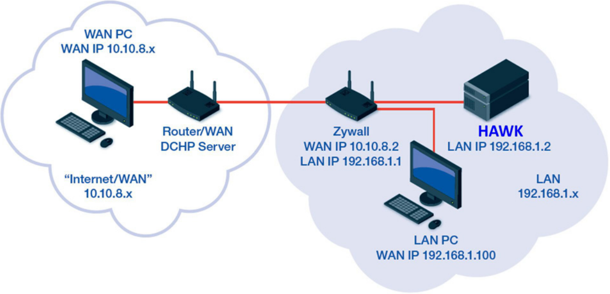
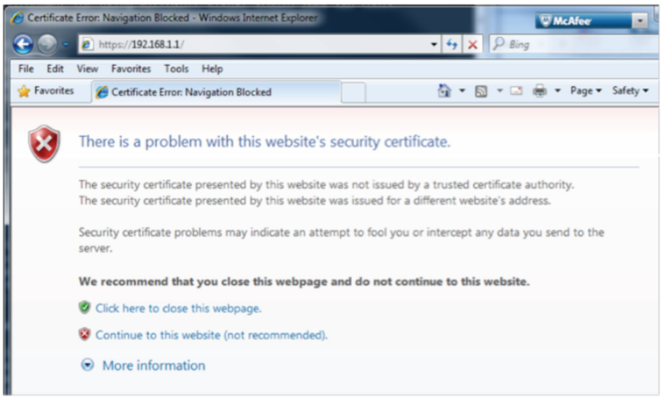


Fig. 4. Example CentraLine^{AX} set-up with four TCP/IP networks

ZyWALL – Initial Set-Up

Document references in the following procedure refer to sections in the Zywall USG Series Unified Security Gateway User's Guide (ftp://ftp2.zyxel.com/ZyWALL_USG_20/user_guide/ZyWALL%20USG%2020_v3-00_Ed1.pdf)

1. **Connect a cable from ZyWALL P2 or P3 to your PC or laptop.**
2. **Turn on power to the ZyWALL device. ZyWALL has a DHCP server and assigns your computer an IP address on the 192.168.1.x subnet. The ZyWall defaults to IP address 192.168.1.1. See section 1.4.1 Web Configurator Access.**
3. **Open a browser and enter https://192.168.1.1. You may be presented with a security warning. The ZyWALL uses a self-signed certificate to identify itself and the certificate isn't signed by a trusted entity. Since you are directly connected to the ZyWALL, you can trust this certificate (and optionally add it to your trust store to avoid getting warning in the future).**


Certificate Error: Navigation Blocked - Windows Internet Explorer
McAfee
https://192.168.1.1/
Bing
File Edit View Favorites Tools Help
Favorites
Certificate Error: Navigation Blocked
Page
Safety

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

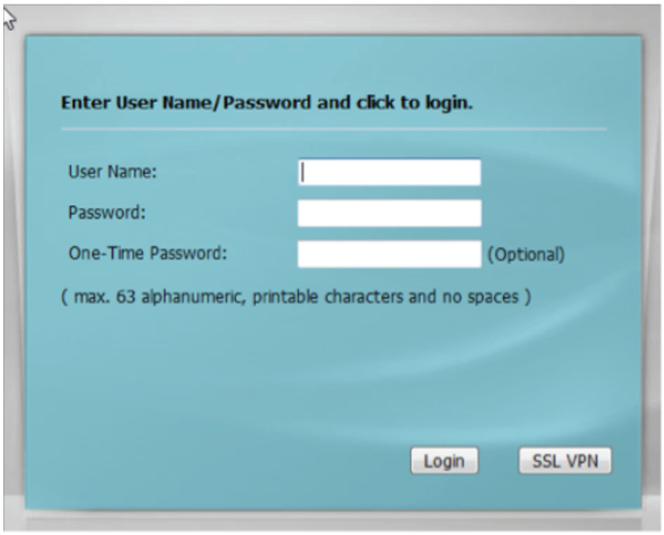
Click here to close this webpage.

Continue to this website (not recommended).

More information

Fig. 5. ZyWALL certificate

4. **After acknowledging the security warning, enter the default user name (admin) and password (1234) and click "Login."**



Enter User Name/Password and click to login.

User Name:

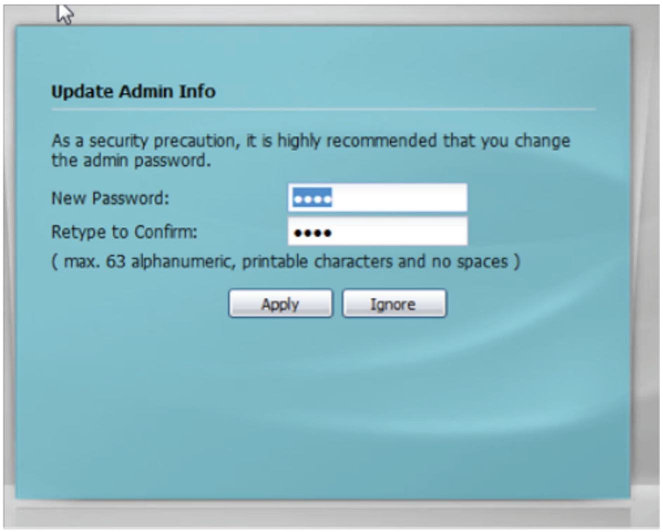
Password:

One-Time Password: (Optional)

(max. 63 alphanumeric, printable characters and no spaces)

Fig. 6. Entering default user name and password

5. **You will then be prompted to enter a new "Admin" password. Enter the password, then log back into the system.**



Update Admin Info

As a security precaution, it is highly recommended that you change the admin password.

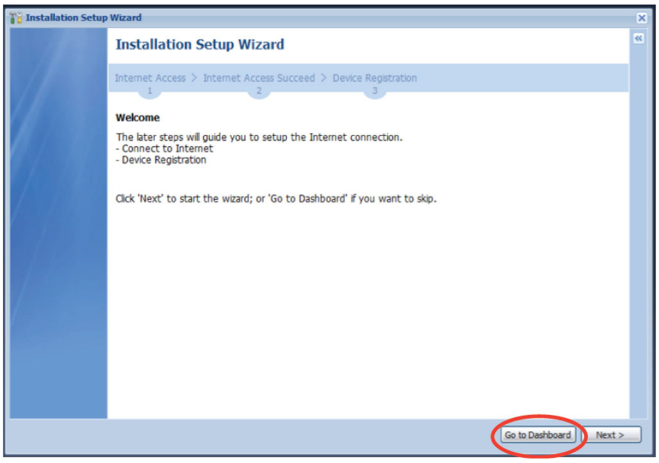
New Password: ••••

Retype to Confirm: ••••

(max. 63 alphanumeric, printable characters and no spaces)

Fig. 7. Entering new admin password

6. **The Installation Set-Up Wizard start screen will then display. Do not use the Wizard. Instead, select "Go To Dashboard" to open the Dashboard screen.**



Installation Setup Wizard

Internet Access > Internet Access Succeed > Device Registration

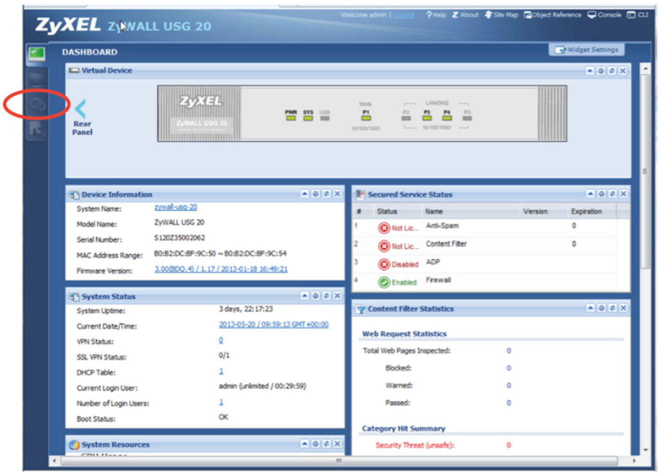
Welcome

The later steps will guide you to setup the Internet connection.
- Connect to Internet
- Device Registration

Click 'Next' to start the wizard; or 'Go to Dashboard' if you want to skip.

Fig. 8. Dashboard screen

7. **The Dashboard screen will then open (see Fig. 9). The first task is to configure the WAN (Internet) IP address. For this example, use a static IP address of 10.10.8.2. Select the Configuration Tab (circled in Fig. 9).**



Device Information

System Name: zywall-usg-20

Model Name: ZyWALL USG 20

Serial Number: S120Z35002062

MAC Address Range: B0:B2:DC:BF:9C:50 ~ B0:B2:DC:BF:9C:54

Firmware Version: 3.00(BDQ.4) / 1.17 / 2013-01-18 16:49:21

System Status

System Uptime: 3 days, 22:17:23

Current Date/Time: 2013-05-20 / 09:59:13 GMT+00:00

VPN Status: 0

SSL VPN Status: 0/1

DHCP Table: 1

Current Login User: admin (unlimited / 00:29:59)

Number of Login Users: 1

Boot Status: OK

Secured Service Status

#	Status	Name	Version	Expiration
1	Not Lic...	Anti-Spam		0
2	Not Lic...	Content Filter		0
3	Disabled	ADP		
4	Enabled	Firewall		

Content Filter Statistics

Web Request Statistics

Total Web Pages Inspected: 0

Blocked: 0

Warned: 0

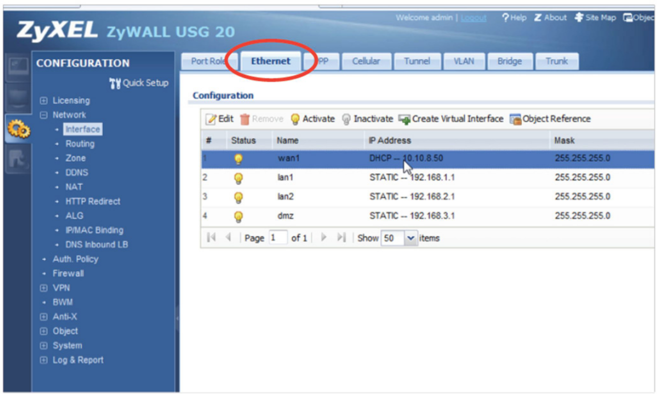
Passed: 0

Category Hit Summary

Security Threat (unsafe): 0

Fig. 9. Configuring the WAN IP address

8. **On the Configuration tab, select Configuration > Network > Interface, then the Ethernet tab.**



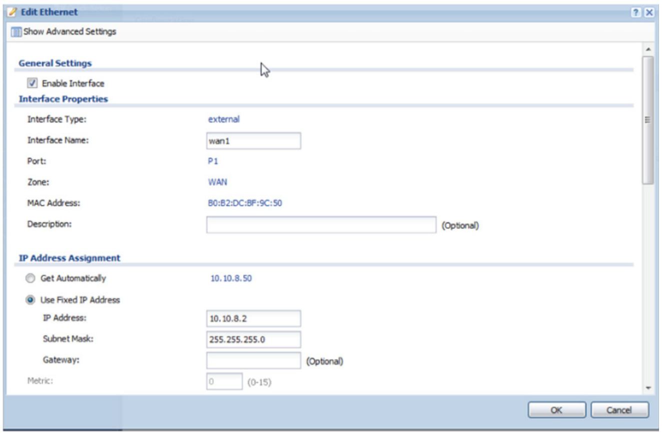
#	Status	Name	IP Address	Mask
1		wan1	DHCP -- 10.10.8.50	255.255.255.0
2		lan1	STATIC -- 192.168.1.1	255.255.255.0
3		lan2	STATIC -- 192.168.2.1	255.255.255.0
4		dmz	STATIC -- 192.168.3.1	255.255.255.0

Page 1 of 1 | Show 50 items

Fig. 10. Selecting the Ethernet tab

9. **Double click on the wan1 interface and configure it with the static IP address.**

10. **Select OK and verify your WAN address as follows.**
    - Disconnect your cable from P2 on the ZyWall device.
    - Plug into the router so you can access the 10.10.8.x network.
    - Verify that you can access the ZyWALL configuration via https://10.10.8.2.



Edit Ethernet

Show Advanced Settings

General Settings

☑ Enable Interface

Interface Properties

Interface Type: external

Interface Name: wan1

Port: P1

Zone: WAN

MAC Address: B0:B2:DC:BF:9C:50

Description: (Optional)

IP Address Assignment

○ Get Automatically 10.10.8.50

● Use Fixed IP Address

IP Address: 10.10.8.2

Subnet Mask: 255.255.255.0

Gateway: (Optional)

Metric: 0 (0-15)

Fig. 11. Verifying your WAN address

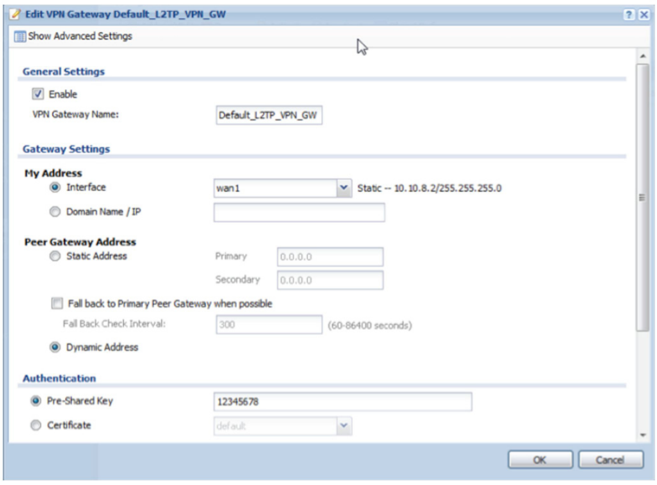
VPN Server Set-Up

This section follows the steps described in Section 4.6.1 L2TP VPN Example of the Zywall USG Series Unified Security Gateway User's Guide. Additional notes are provided here are necessary for clarity.

NOTE: L2TP is used because Windows, Android and iOS devices have built in support for creating VPN client connections.

4.6.1 Step 1:
Select Configuration > VPN > IPSecVPN, then click on the VPN Gateway tab, shown below.

- Check the Enable box in the "Edit VPN Gateway Default_L2TP_VPN _GW" dialog box.
- We are using a static WAN address of 10.10.8.2.
- The "My Address" field should already be properly populated.
- Select a pre-shared key for Authentication and Keep this key secure – if others discover the key, then they will be able to login to your VPN.



Edit VPN Gateway Default_L2TP_VPN_GW

Show Advanced Settings

General Settings

☑ Enable

VPN Gateway Name: Default_L2TP_VPN_GW

Gateway Settings

My Address

● Interface wan1 Static -- 10.10.8.2/255.255.255.0

○ Domain Name / IP

Peer Gateway Address

○ Static Address Primary 0.0.0.0

Secondary 0.0.0.0

□ Fall back to Primary Peer Gateway when possible

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

● Dynamic Address

Authentication

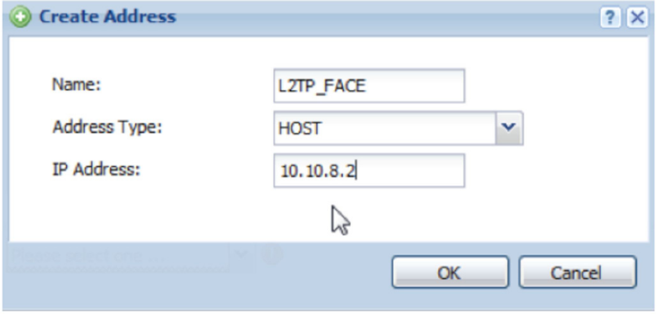
● Pre-Shared Key 12345678

○ Certificate default

Fig. 12. Using certificates to identify valid clients

Alternatively the ZyWALL device allows use of certificates to identify valid clients. This requires more setup, but provides an additional layer of security. Certificate generation and management are beyond the scope of this document.

4.6.1 Step 2:
Follow ZyWALL directions, with the exception of the IP address – use 10.10.8.2.



Create Address

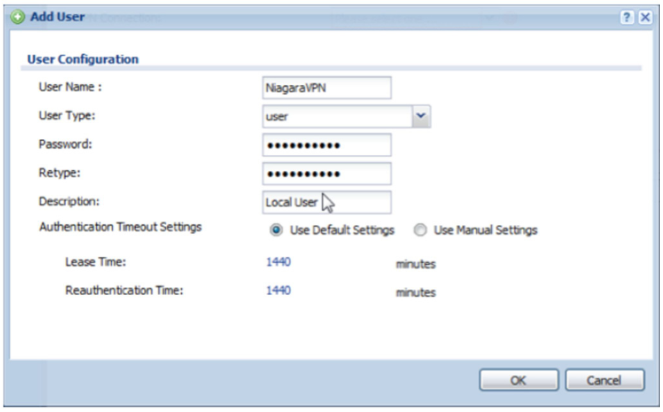
Name: L2TP_FACE

Address Type: HOST

IP Address: 10.10.8.2

Fig. 13. Entering name, address type, and IP address

4.6.1 Step 3:
Follow Step 3 as in the document, with the exception of the user name. We are naming our user "NiagaraVPN" instead of "L2TP-Test." Remember the user name and password you choose in this step. These will be used when setting up the VPN client to validate the client to ZyWALL VPN server.



Add User

User Configuration

User Name : NiagaraVPN

User Type: user

Password: ••••••••••

Retype: ••••••••••

Description: Local User

Authentication Timeout Settings ● Use Default Settings ○ Use Manual Settings

Lease Time: 1440 minutes

Reauthentication Time: 1440 minutes

Fig. 14. User configuration

4.6.2 Configuring Policy Routing:
To configure Policy Routing as described in 4.6.2, select Configuration > Network > Routing > Policy Route > Add (in IPv4 Configuration). Follow steps as described in 4.6.2. Additional configuration under this part is optional (setting up ZyWall management through Tunnel).

At this point, the ZyWALL is setup to accept incoming VPN connections. Next step is to configure a client to connect to the VPN.

VPN Client Configuration

VPN Client setup is detailed in 4.6.6 Configuring L2TP VPN in Windows. Follow the steps outlined there. Remember to specify the proper user name and password.

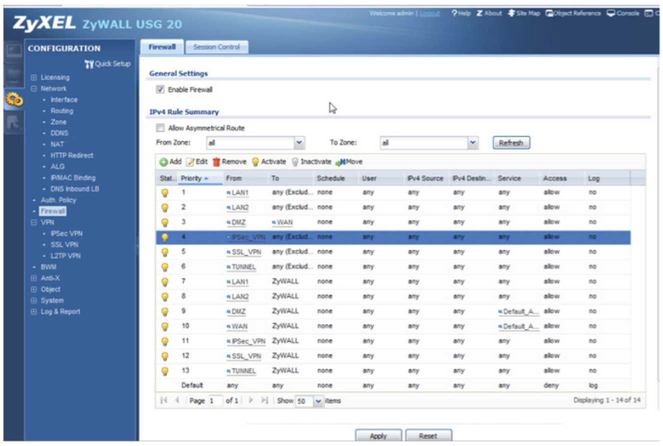
Test VPN Tunnelling

Using a PC on the 10.10.8.x network, open VPN connection as described in 4.6.6 under "Connect Using L2TP VPN." Enter user name and password when prompted. Once a connection is made, open Workbench or a browser and verify that you can access the HAWK at 192.168.1.2.

Setting Up Firewall Rules

There are still a few more steps to take to harden the configuration. As currently configured, ZyWall will pass all traffic once the VPN connection is established. Our goal is to only allow access to required CentraLine^{AX} services, so this default policy is too permissive.

Select the Configuration > Firewall, IPSec_VPN rule. Double click to edit and change policy to deny. This prevents a VPN user from accessing anything beyond ZyWALL. The next step is to add exceptions to permit web, fox, and (if required) Platform traffic.



General Settings

☑ Enable Firewall

IPv4 Rule Summary

□ Allow Asymmetrical Route

From Zone: all To Zone: all Refresh

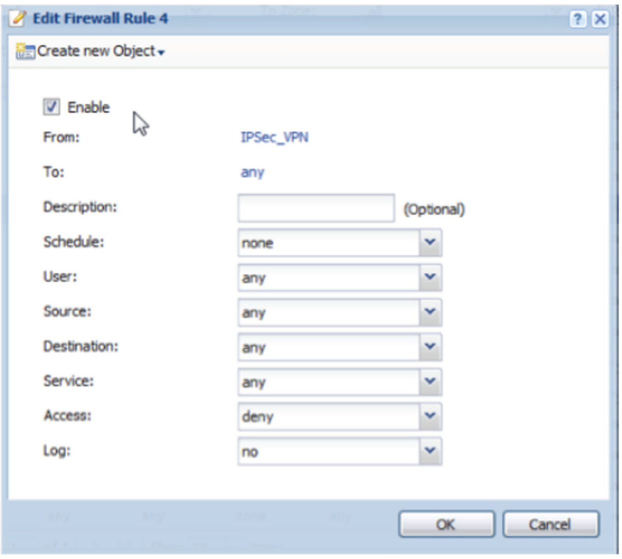
Add Edit Remove Activate Inactivate Move

Stat...	Priority	From	To	Schedule	User	IPv4 Source	IPv4 Destin...	Service	Access	Log
💡	1	LAN1	any (Exclud...	none	any	any	any	any	allow	no
💡	2	LAN2	any (Exclud...	none	any	any	any	any	allow	no
💡	3	DMZ	WAN	none	any	any	any	any	allow	no
💡	4	IPSec_VPN	any (Exclud...	none	any	any	any	any	allow	no
💡	5	SSL_VPN	any (Exclud...	none	any	any	any	any	allow	no
💡	6	TUNNEL	any (Exclud...	none	any	any	any	any	allow	no
💡	7	LAN1	ZyWALL	none	any	any	any	any	allow	no
💡	8	LAN2	ZyWALL	none	any	any	any	any	allow	no
💡	9	DMZ	ZyWALL	none	any	any	any	Default_A...	allow	no
💡	10	WAN	ZyWALL	none	any	any	any	Default_A...	allow	no
💡	11	IPSec_VPN	ZyWALL	none	any	any	any	any	allow	no
💡	12	SSL_VPN	ZyWALL	none	any	any	any	any	allow	no
💡	13	TUNNEL	ZyWALL	none	any	any	any	any	allow	no
	Default	any	any	none	any	any	any	any	deny	log

Page 1 of 1 Show 50 items Displaying 1 - 14 of 14

Apply Reset

Fig. 15. Adding exceptions



☑ Enable

From: IPSec_VPN

To: any

Description: (Optional)

Schedule: none

User: any

Source: any

Destination: any

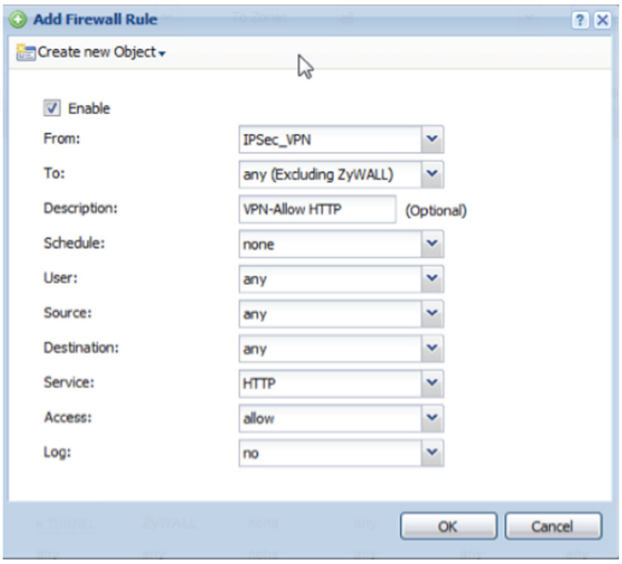
Service: any

Access: deny

Log: no

Fig. 16. Editing Firewall rules

To enable HTTP traffic, only, add a new rule allowing the HTTP service.



☑ Enable

From: IPSec_VPN

To: any (Excluding ZyWALL)

Description: VPN-Allow HTTP (Optional)

Schedule: none

User: any

Source: any

Destination: any

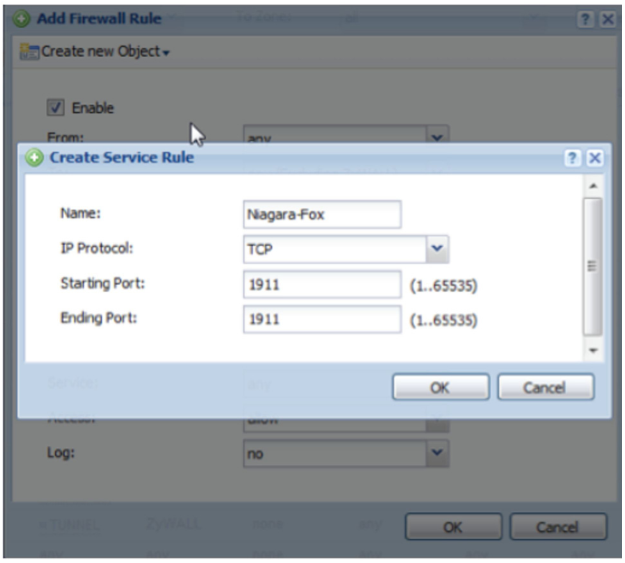
Service: HTTP

Access: allow

Log: no

Fig. 17. Enabling HTTP traffic, only

To enable Fox connections, a new type of service must be created. Select Add, then Create New Object of type Service. Name the Service CentraLine^{AX}-Fox and give it the appropriate port number (1911 by default).



☑ Enable

From: any

Name: Niagara-Fox

IP Protocol: TCP

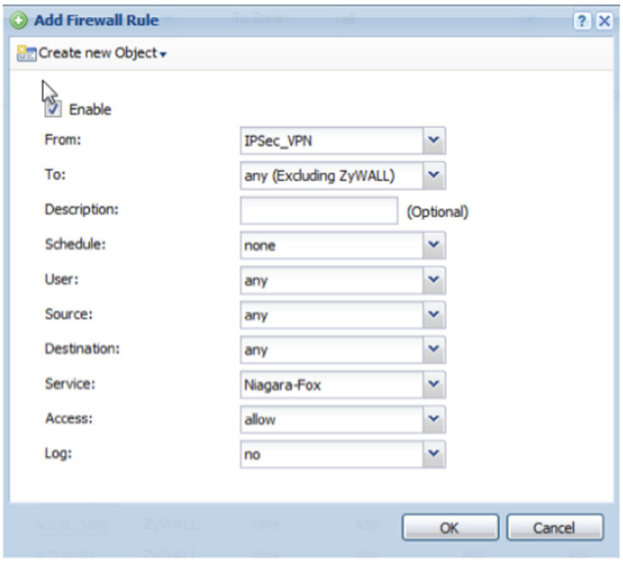
Starting Port: 1911 (1..65535)

Ending Port: 1911 (1..65535)

Log: no

Fig. 18. Enabling Fox connections

Add a new rule permitting Fox traffic.



Add Firewall Rule

☑ Enable

From: IPSec_VPN

To: any (Excluding ZyWALL)

Description: (Optional)

Schedule: none

User: any

Source: any

Destination: any

Service: Niagara-Fox

Access: allow

Log: no

Fig. 19. Adding a new rule permitting Fox traffic

Similarly, a rule can be established to allow access to CentraLine^AX Daemon (default port 3011).

Creating Additional Users

- By assigning each user a unique name and password, you can enable and disable users as required.
- You can add new users via Configuration > Object > User/Group, User tab.
- You can create a group containing all of your VPN users via Configuration > Object > User/Group, Group tab. Once the group is configured, you can switch the VPN configuration to allow users in this group via Configuration > VPN > L2TP VPN, Allowed User field.

Additional Hardening Steps

- Prevent access to ZyWALL configuration via Internet by changing WAN to ZyWALL firewall rule.
- Restrict VPN access to only certain IPs, not just certain ports.
- Always do configuration in a secure location using direct connections whenever possible.
- Keep firmware up to date.
- Back up configuration – See Section 6.4 – How to Manage ZyWALL Configuration.

Manufactured for and on behalf of the Environmental and Combustion Controls Division of Honeywell Technologies Sàrl, Rolle, Z.A. La Pièce 16, Switzerland by its Authorized Representative:

CentraLine
Honeywell GmbH
Böblinger Strasse 17
71101 Schönaich, Germany
Phone +49 7031 637 845
Fax +49 7031 637 846
info@centraline.com
www.centraline.com

Printed in Germany.
Subject to change
without notice.
EN2Z-0986GE51 R1213

CENTRALINE®
by Honeywell