Using a VPN with Niagara Systems

July 2013

What is a VPN?

"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?

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

How can I setup a VPN?

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

IMPORTANT:
This information in this document is based on the assumption that the only IP devices on the network are Niagara devices. If Niagara 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 Niagara and corporate systems while providing required access to the Niagara 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.
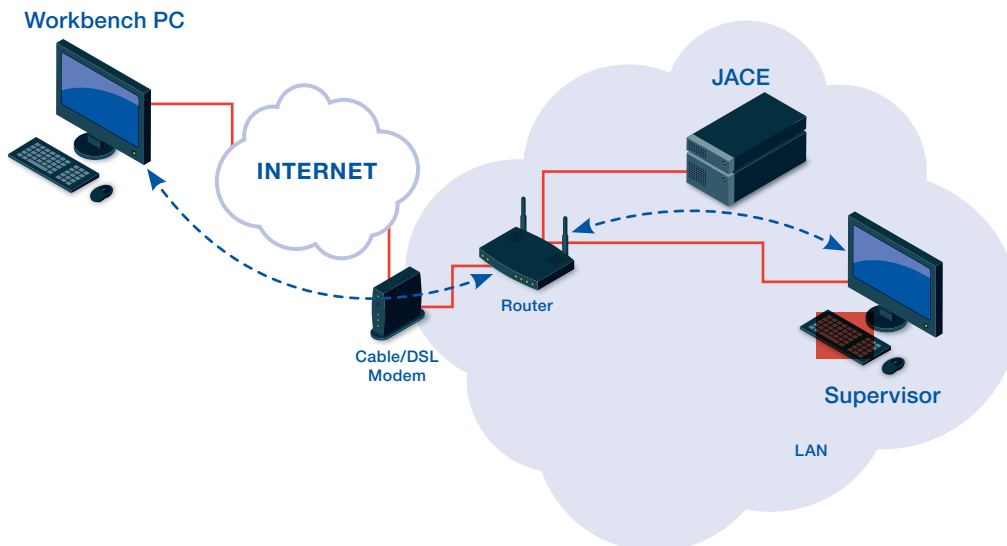
Network Diagrams

Consider the following typical Niagara setup. One or more JACEs and/or a Supervisor are connected via a router to form a LAN. The Supervisor and possibly the JACEs 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 Niagara system to be accessed. Alternatively, one could expose the Supervisor only and use Niagara Fox/HTTP/Platform Tunneling to reach other systems.
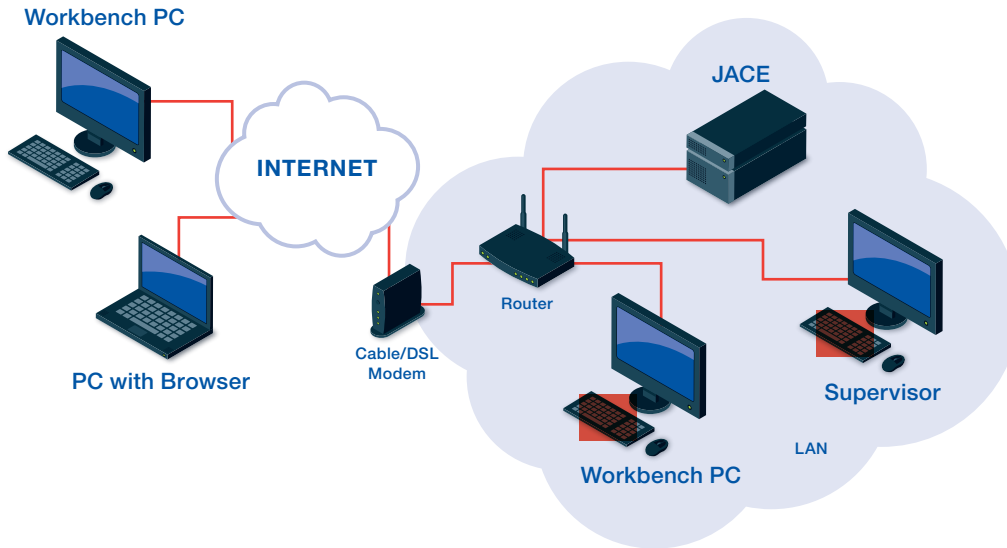
If all ports are forwarded, this configuration gives full access (Web/Fox/Daemon) to all 3 Niagara systems via the Internet. **The diagram below shows Workbench opening a Fox connection.**

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

There at least two significant security flaws with this approach:

1 *An automated port scan from the Internet is able to identify all 9 ports as Niagara systems.*

- *Systems can be identified even without Niagara 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 Setup with a VPN

The diagram below shows the same system with the addition of a security gateway capable of acting as a VPN Server.
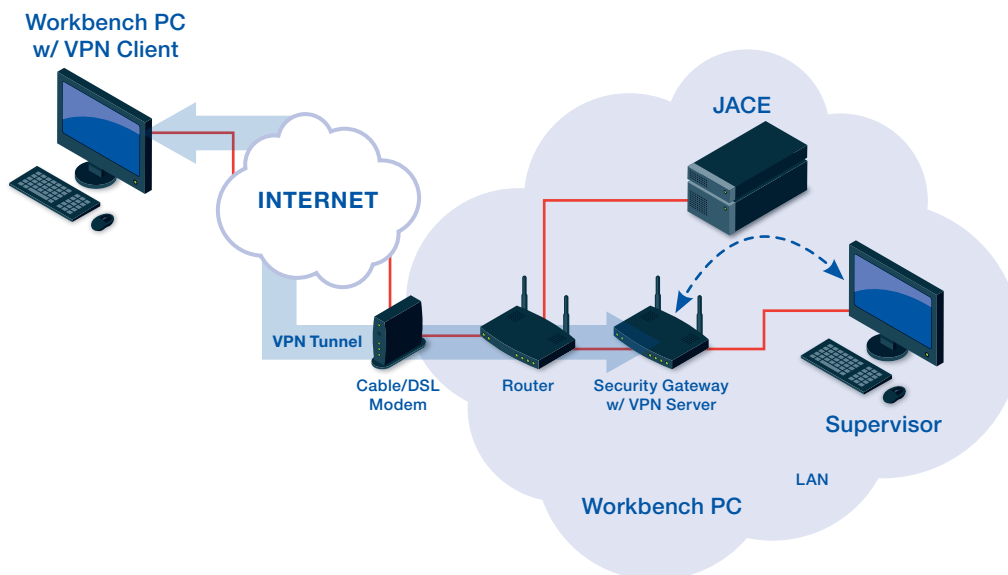
In this case, a VPN tunnel is created between the Workbench PC and the VPN server running on the Security Gateway. All traffic running through this tunnel is encrypted. The only port that must be exposed to the Internet is the VPN port on the Security Gateway.

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 Niagara 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-Niagara devices on the LAN, but the VPN should be configured to only allow access to the Niagara systems. Additionally, you should only allow access to required Niagara services.

Will a VPN affect LAN access to JACEs?

No. LAN access to the Niagara devices remains the same as always. VPN only affects ability to reach Niagara devices from external networks such as the Internet.

If I use a VPN, will Niagara 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 Niagara Networking?

Niagara 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 Niagara. This document refers to and comments on the ZyWALL documentation:

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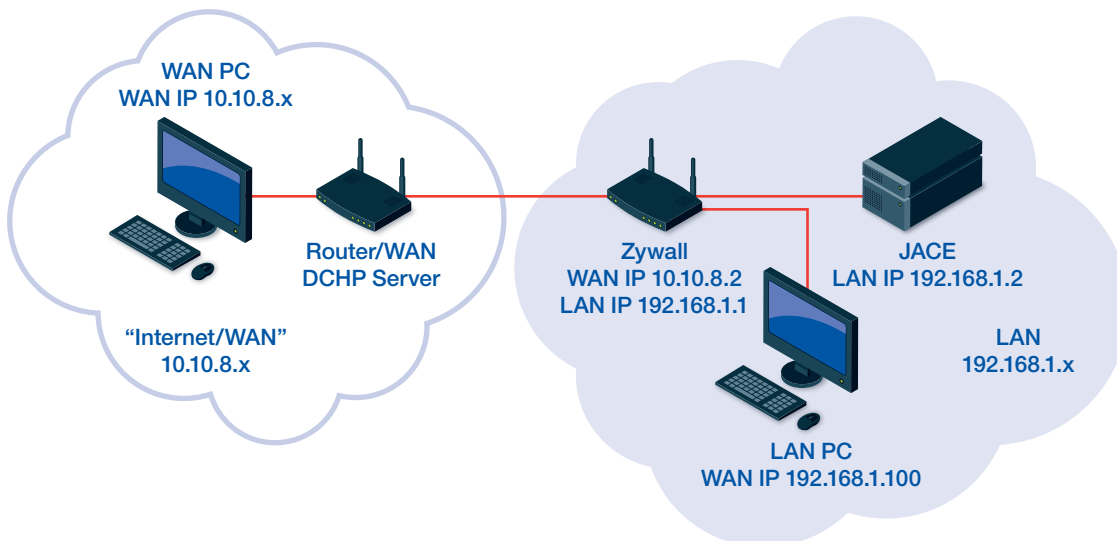ftp://ftp2.zyxel.com/ZyWALL_USG_20/user_guide/ZyWALL%20USG%2020_v3-00_Ed1.pdf

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 Niagara JACE 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 JACEs 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.*

WAN PC
WAN IP 10.10.8.x

Router/WAN
DCHP Server

"Internet/WAN"
10.10.8.x

Zywall
WAN IP 10.10.8.2
LAN IP 192.168.1.1

JACE
LAN IP 192.168.1.2

LAN
192.168.1.x

LAN PC
WAN IP 192.168.1.100

ZyWALL – Initial Setup

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).*
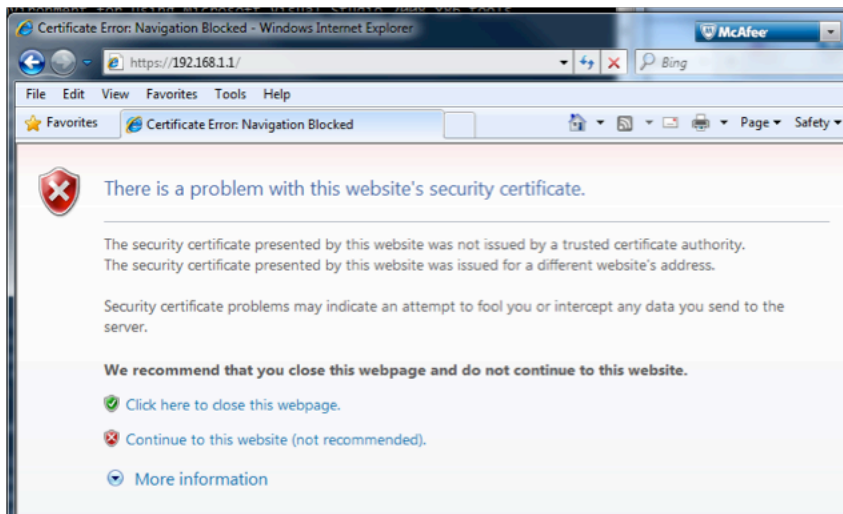
4 *After acknowledging the security warning, enter the default user name **(admin)** and password **(1234)** and click "Login."*
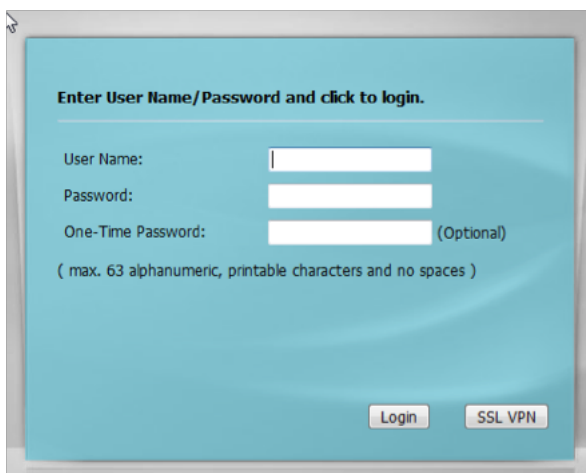
5 *You are prompted to enter a new "Admin" password. Enter the password, then log back into the system.*
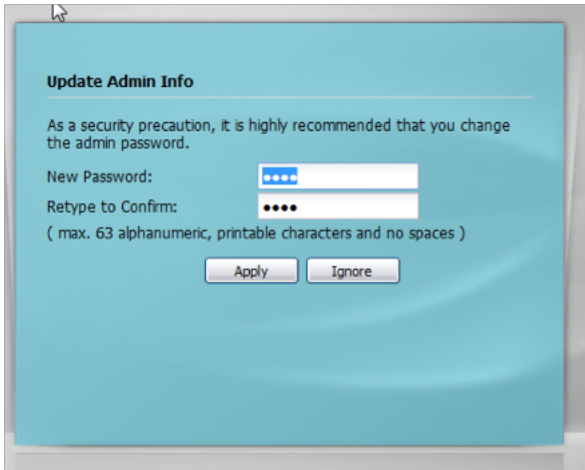
The Installation Setup Wizard start screen displays.

6 *Do not use the Wizard. Instead, select "Go To Dashboard" to open the Dashboard Screen.*
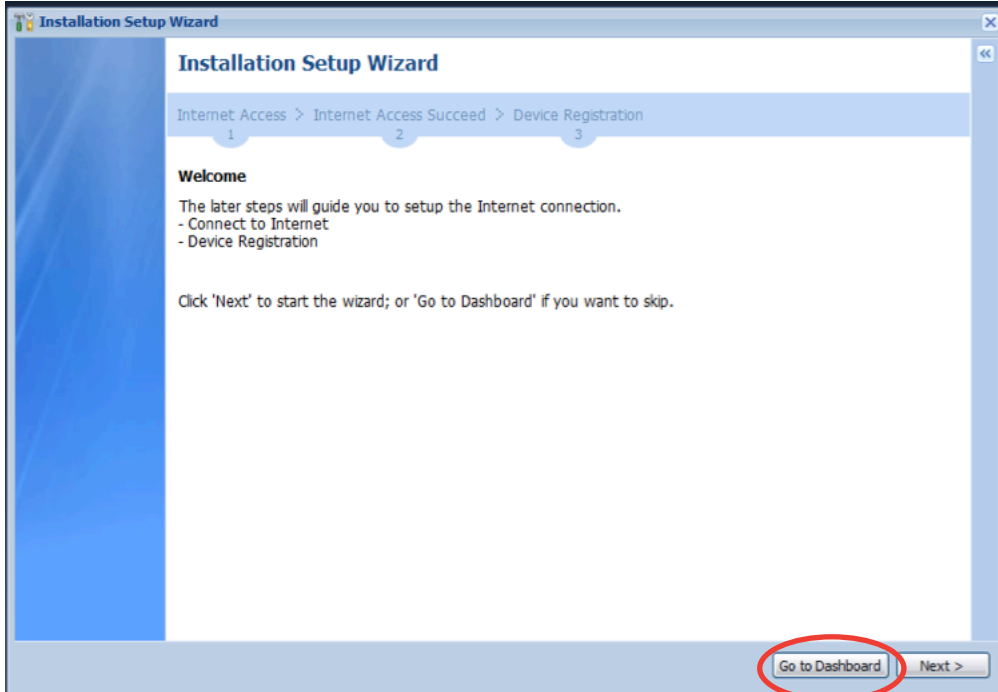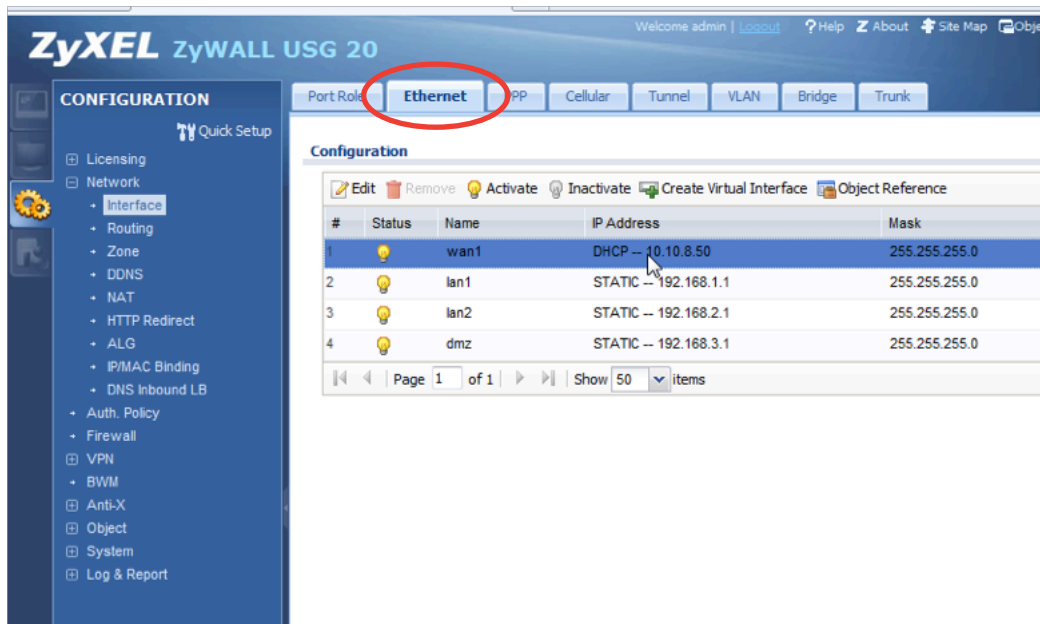
The Dashboard screen opens, as shown below:

7 *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 below).*
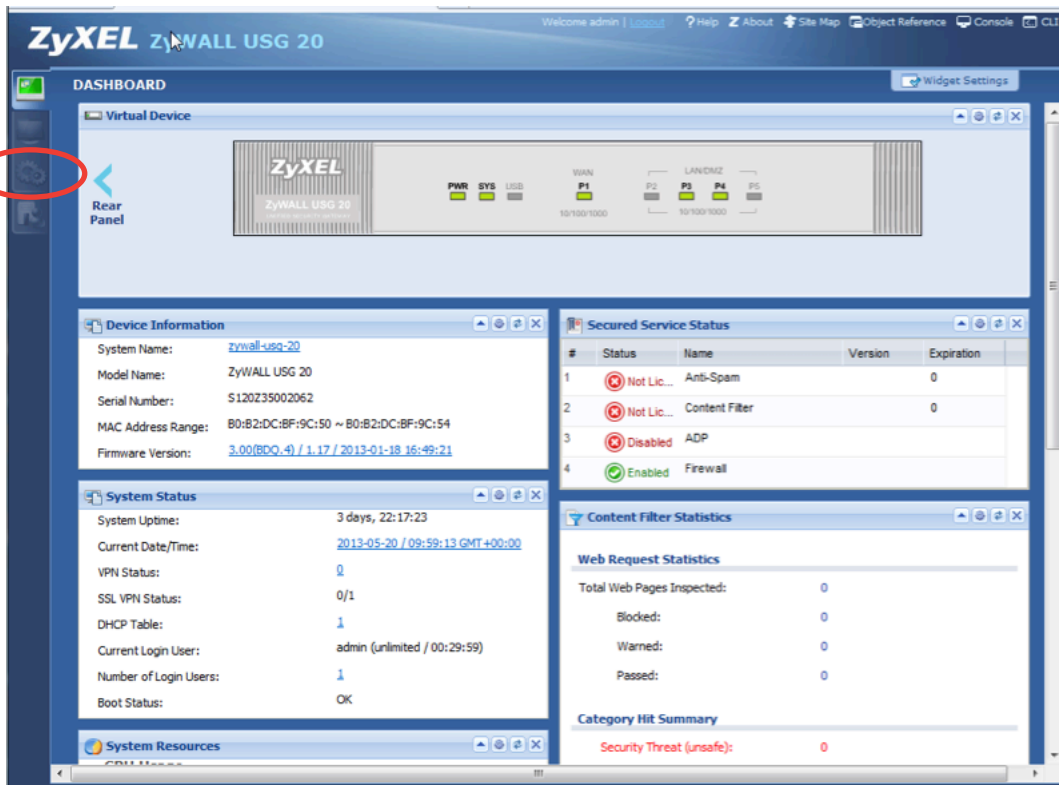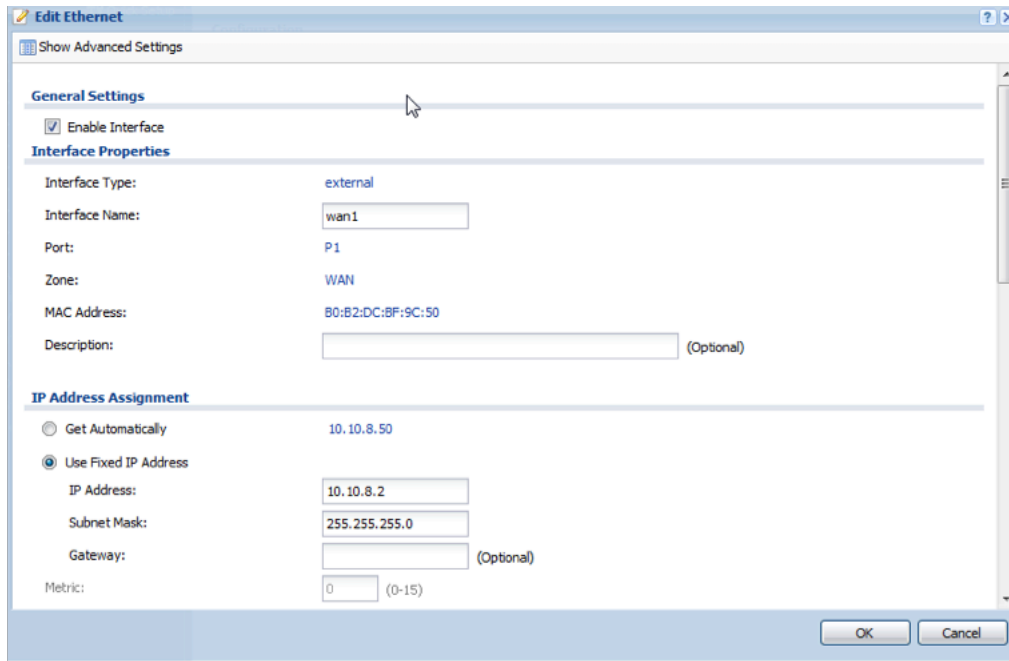
8 *On the Configuration Tab, select* **Configuration > Network > Interface**, *then the Ethernet tab.*

9 *Double click on the* **wan1** *interface and configure it with the static IP, then select* **OK** *and verify your WAN address, as described in the next step.*

10 *Verify 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.***

VPN Server Setup

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.*
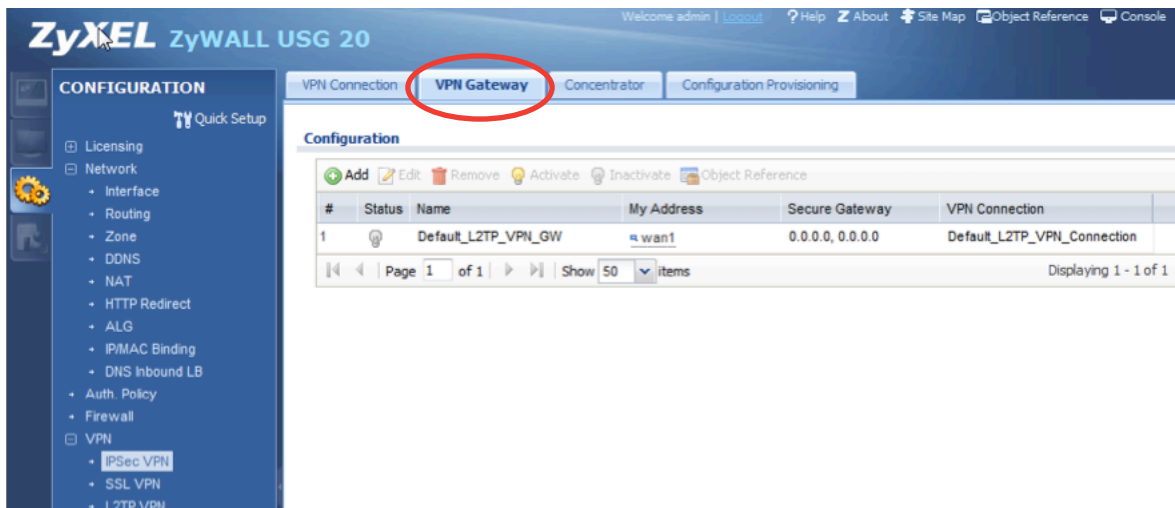
- *Check the Enable box in the "Edit VPN Gateway Default_L2TP_VPN _GW" dialog box.*

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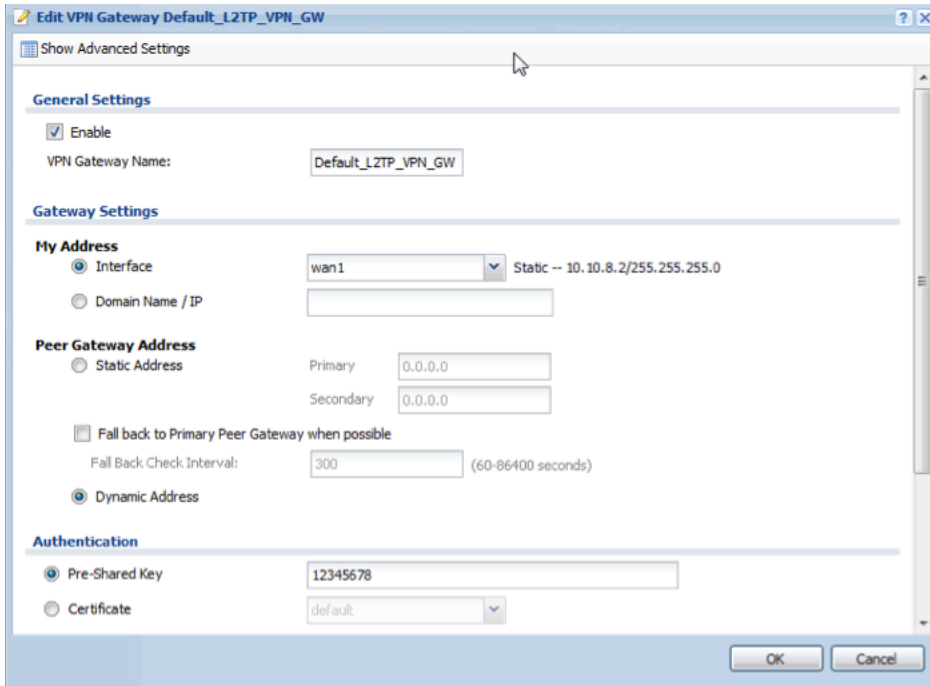
Alternatively the ZyWALL device allows use of certificates to identify valid clients. This requires more setup, but provides an additional layer of security. Certificate generation and management are beyond the scope of this document.

4.6.1 Step 2
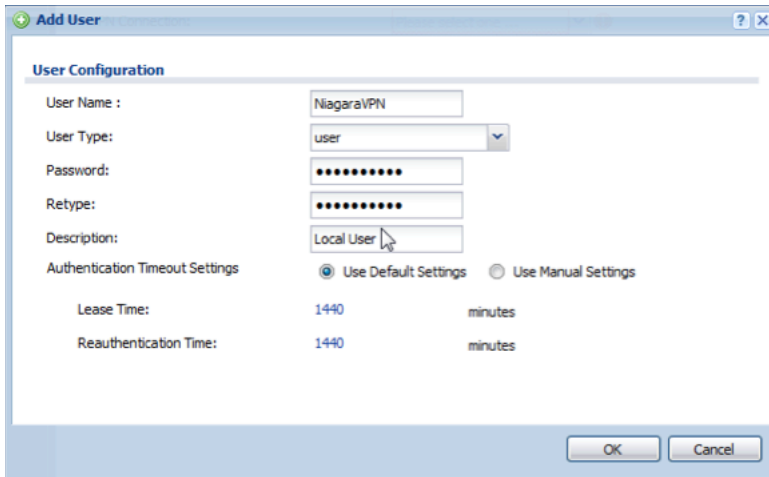- *Follow ZyWall directions, with the exception of the IP address – use 10.10.8.2.*
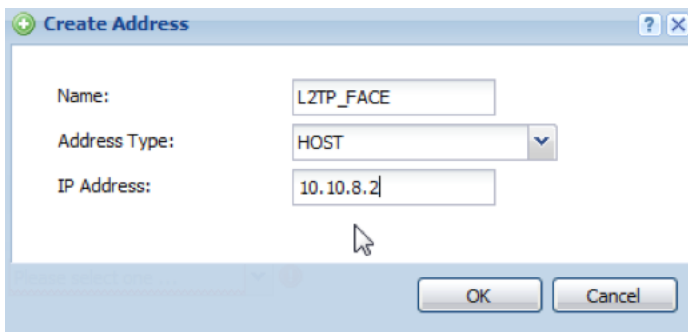
4.6.1 Step 3

Follow Step 3 as in the document with the exception of user name. We are naming our user "NiagaraVPN" instead of "L2TP-Test." Remember the username 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.

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 Tunneling

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 JACE 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 Niagara 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. Next, is adding exceptions to permit web, fox and (if required) Platform traffic.*
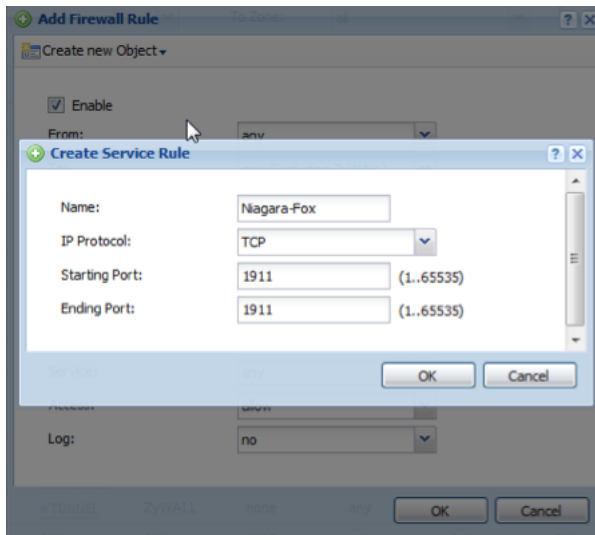
To enable HTTP traffic only, add a new rule allowing the HTTP service.
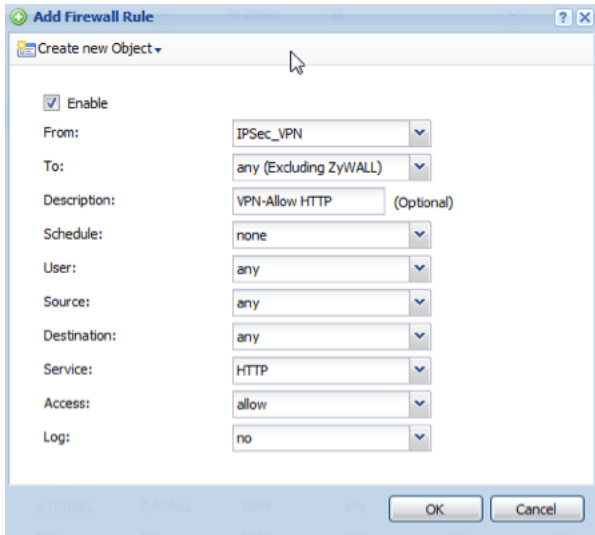
To enable Fox connections, a new type of service must be created. Select **Add***, then* **Create New Object** *of type* **Service***. Name the Service Niagara-Fox and give it the appropriate port number (1911 by default).*

Add a new rule permitting Fox traffic:

Similarly, a rule can be setup to allow access to Niagara 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.***

This document is provided to assist you in optimizing the security benefits that can be gained by accessing the Niagara^AX Framework through a VPN, and to provide some practical advice that may be useful to you in setting up a VPN. Nothing contained in it constitutes either a representation or a warranty, nor is it intended to provide assurance against security breaches, as that is not possible to do. Tridium is not affiliated in any way with ZyXEL, has no responsibility for any ZyXEL, product and this guide is not intended as an endorsement of the ZyWall USG-20 or of any other product. This document is not a substitute for advice of an information technology professional who is knowledgeable about your specific computing environment and any VPN product you may choose to employ. Nothing in this guide shall be deemed to expand or modify in any way any of the provisions of the End User License Agreement applicable to the Niagara^AX Framework.