Manual No: **577014-129** • Revision: **A**

Network Router for ATG Applications

Installation Manual

VEEDER-ROOT

Notice

Veeder-Root makes no warranty of any kind with regard to this publication, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

Veeder-Root shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this publication.

The information contained in this publication may be subject to change without notice.

Contents

Purpose:

This manual provides instructions for configuring a Cisco™ RV042 10/100 4-Port Virtual Private Network (VPN) Firewall Router for use with Veeder-Root's TLS family of ATG's.

Intended Users:

This manual is intended for Authorized Service Contractors (ASCs) and Customer Specified Contractors (CSCs) who are certified to install a Veeder-Root ATG.

Required Tools

The following tools and equipment are required to configure the firewall router:

- Laptop with a terminal emulator
- Category 5 (Cat-5) Crossover cable (for connection between Laptop and TLS-350 only)
- Category 5 (Cat-5) Straight cable (for connection between Laptop and TLS-450/450PLUS/TLS4 and router)
- Two available LAN IP addresses – to be provided by IT authority.

Related Manuals

577013-776 TCP/IP Interface Module Installation Guide

Contractor Certification Requirements

Veeder-Root requires the following minimum training certifications for contractors who will install and setup the equipment discussed in this manual:

Installer Certification (Level 1): Contractors holding valid Installer Certification are approved to perform wiring and conduit routing; equipment mounting; probe, sensor and carbon canister vapor polisher installation; wireless equipment installation; tank and line preparation; and line leak detector installation.

Technician Certification (Level 2/3): Contractors holding valid Technician Certifications are approved to perform installation checkout, startup, programming and operations training, system tests, troubleshooting and servicing for all Veeder-Root Series Tank Monitoring Systems, including Line Leak Detection. In addition, Contractors with the following sub-certification designations are approved to perform installation checkout, startup, programming, system tests, troubleshooting, service techniques and operations training on the designated system.

Wireless 2
Tall Tank

Warranty Registrations may only be submitted by selected Distributors.

Introduction

The following walks through a typical configuration for the router. Router configurations will vary depending on your site network architecture and requirements. Please work with your IT advisor for what is best for your site.

Instructions

Laptop Configuration

Part 1) Determining the temporary laptop IP address

The following procedure must be used to program the laptop to use a static Internet Protocol (IP) address to communicate on the firewall router's Local Area Network (LAN). This does require knowledge of the previously assigned LAN addresses. If a network map is not available for an established site, the simplest approach is to look at the ATG's IP address through the front panel interface, then configure a laptop static address on the same subnet.

For a TLS-450 or TLS450PLUS, the ATG's IP address is located at Menu-> Setup-> Communications-> Ethernet Port[1]. In this example, the IP address is 192.168.11.104, with a subnet Mask of 255.255.255.0. Also note the IP gateway address of 192.168.11.254 for this example.

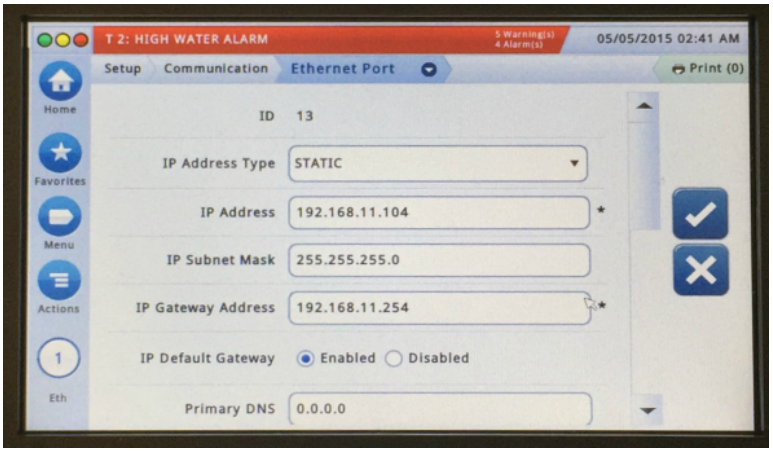


Figure 1: TLS-450/450PLUS/4 console location of IP address

From this information, we can construct the network mapping. For our example, the following IP addressing was used:

[1] Instructions also apply to a TLS4c/i console. For a TLS-350, see the "TCP/IP Module IP Address/Configuration Using Telnet" of the TCP/IP Interface Module Installation Guide (Veeder-Root p/n 577013-776) for instructions on accessing the module IP address.

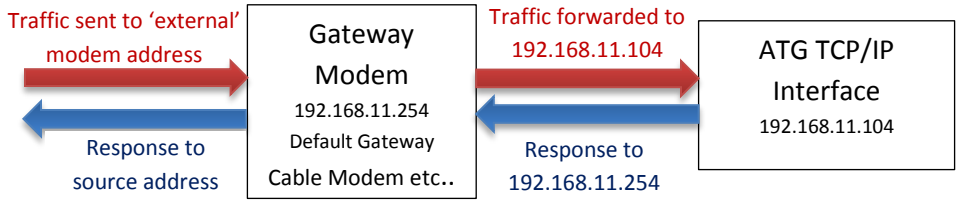


Figure 2: Network element mapping example before Cisco RV04 Router added

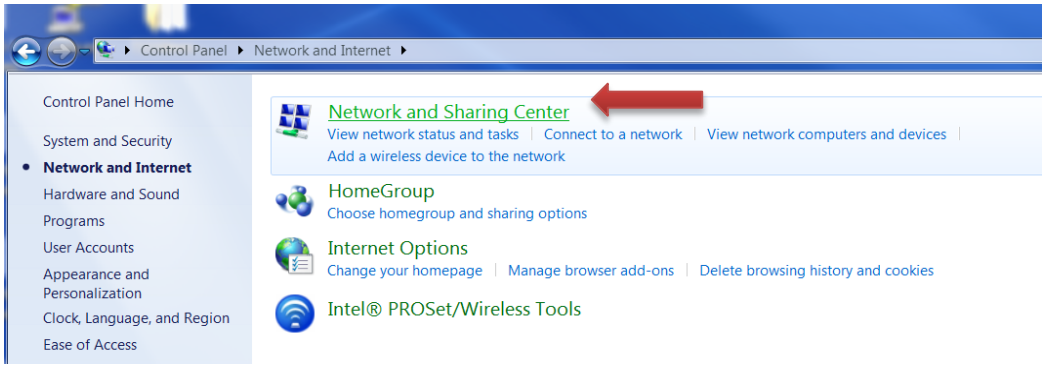
All devices were found to be 192.168.11.x. The laptop should be renamed to an unused address between 192.168.11.1 and 192.168.11.255. For this example, we will use **192.168.11.98**.

Part 2) Accessing the Laptop's Internet Protocol version4 (TCP/IPv4) Connection Properties

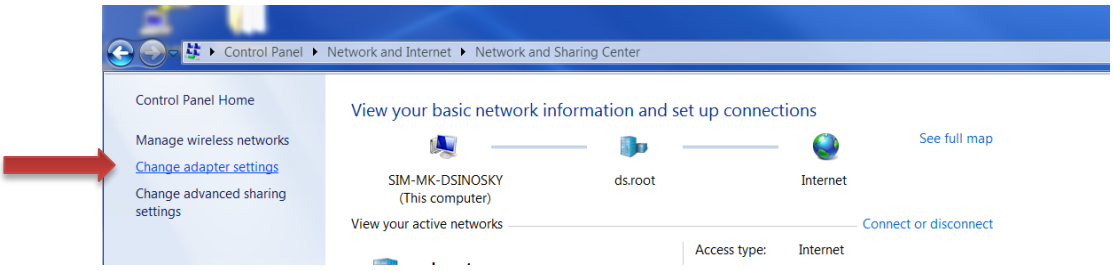
Note: the references and screenshots provided in this manual may vary based on the hardware and version of Windows that is used.

For Windows 7, TCP/IPv4 properties can be found as follows:

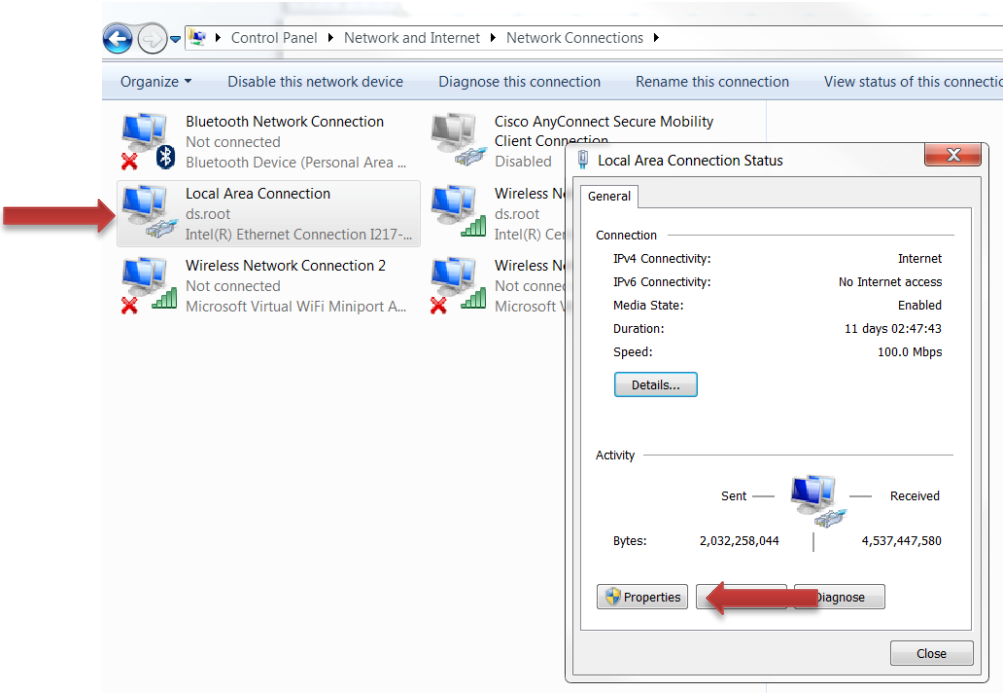
Go To Control Panel → Network and Internet→ Network Sharing Center



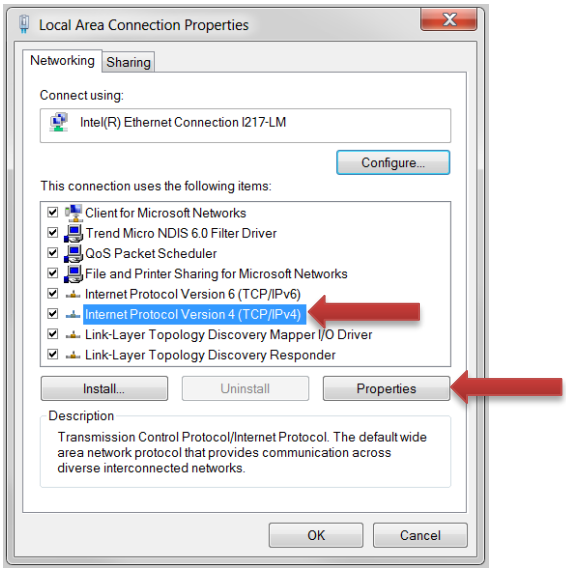
Click on Change Adapter settings:



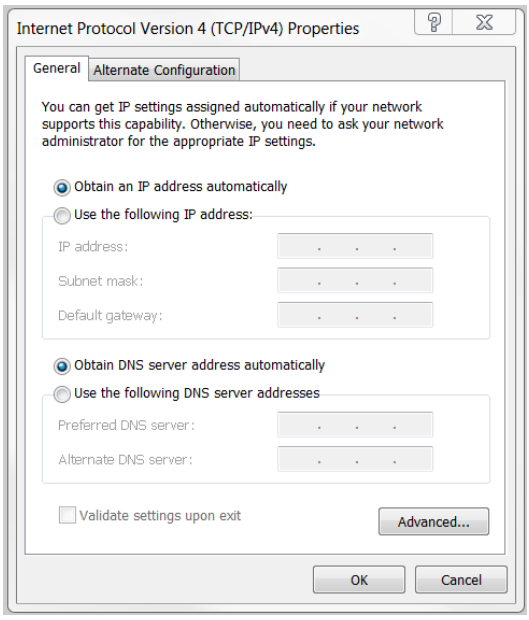
Double-Click on Local Area Connection, followed by Properties:



Highlight Internet Protocol Version 4 (TCP/IPv4) then click properties:



The Internet Protocol Version 4 (TCP/IPv4) Properties window will appear. ***Important Information: Note the current IP address programming, as you will want to reset to these parameters later.***



Select the **Use the following IP** address radio button and enter:

IP Address:	192.168.11.98 [from Part 1]
Subnet mask:	255.255.255.0
Default Gateway:	192.168.11.254 [from Part 1]

Re-addressing the elements

Part 1) Mapping the new configuration

The next step is to reserve one additional IP address. For this example, we will use **192.168.11.99**. To avoid reconfiguration of the gateway modem, we will reallocate the current ATG TCP/IP address to the Cisco RV04 router. The ATG TCP/IP address will be renamed to the reserved IP address, **192.168.11.99**. See revised mapping below.

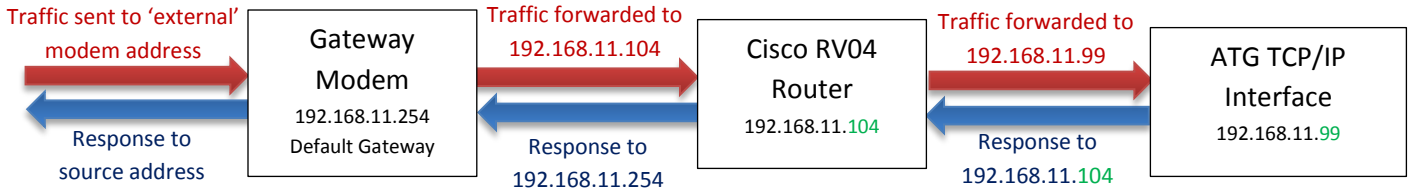


Figure 3: Network element mapping example after Cisco RV04 Router added

Part 2) Reprogramming the ATG

The next step is to reprogram our ATG according to the network mapping established in Part 1.

For a TLS-450 or TLS450PLUS, under **Menu-> Setup-> Communications-> Ethernet Port, the IP address will be changed to 192.168.11.99** for this example.

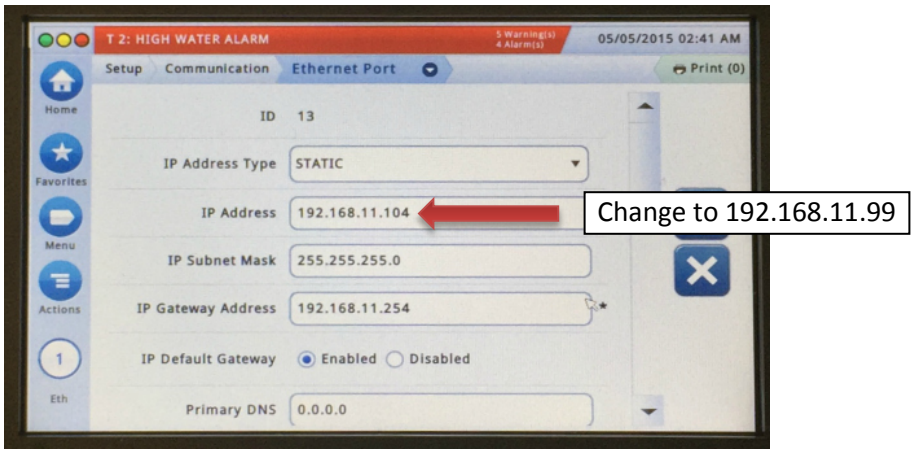


Figure 4: TLS-450/450PLUS/4 changing the IP address

Part 3) Connecting the Cisco Router

Insert your Cisco RV04 between the modem and the ATG:

1. Disconnect the Ethernet cable from the gateway modem into the ATG on the ATG side.
2. Connect this Ethernet cable from the gateway modem into the WAN port of the RV04.

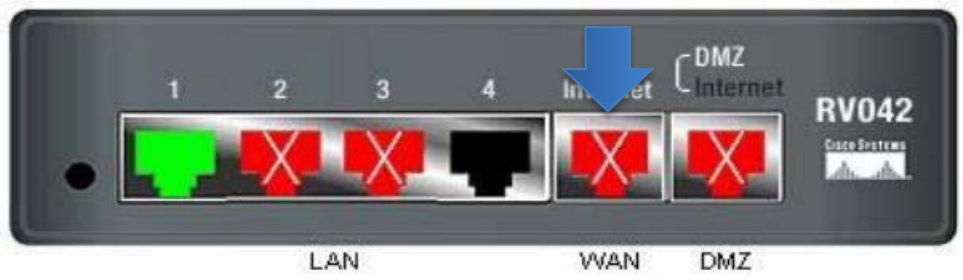


Figure 5: WAN port connector on the Cisco RV04

3. Connect a straight Ethernet cat 5 cable from LAN port 1 back to the original TCP/IP connector on the ATG

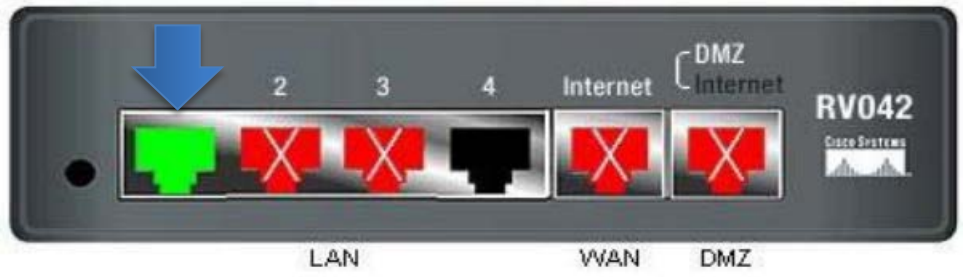


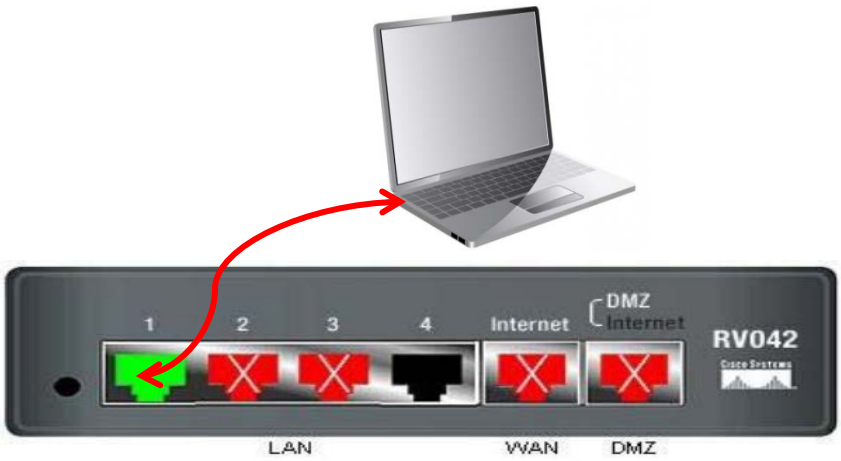
Figure 6: LAN port connector on the Cisco RV04

Programming the Cisco Router

Part 1) Communicating with the router

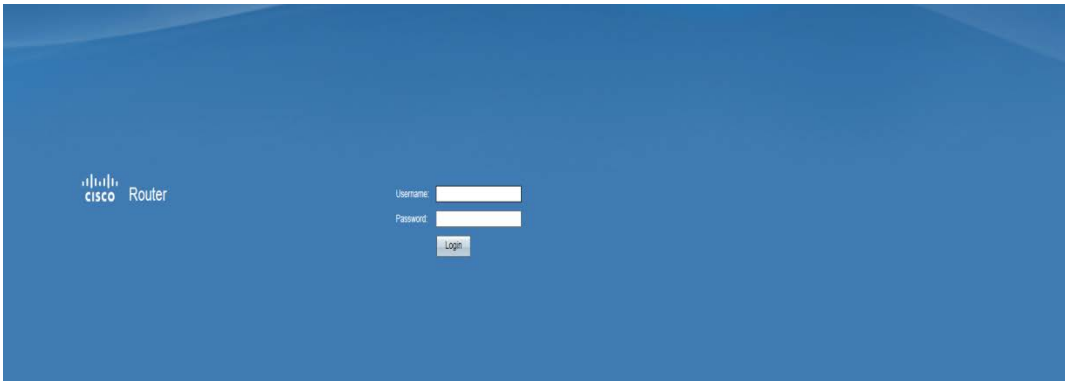
To utilize the router for security purposes with your Veeder-Root Automatic Tank Gauge you will need to configure the router to meet your unique security standards and LAN configuration.

1. Disconnect the CAT5 cable you connected in part 2 from port 1.
2. Connect your laptop using a Cat 5 cable that is in use, to configure the router to port 1 of the firewall router



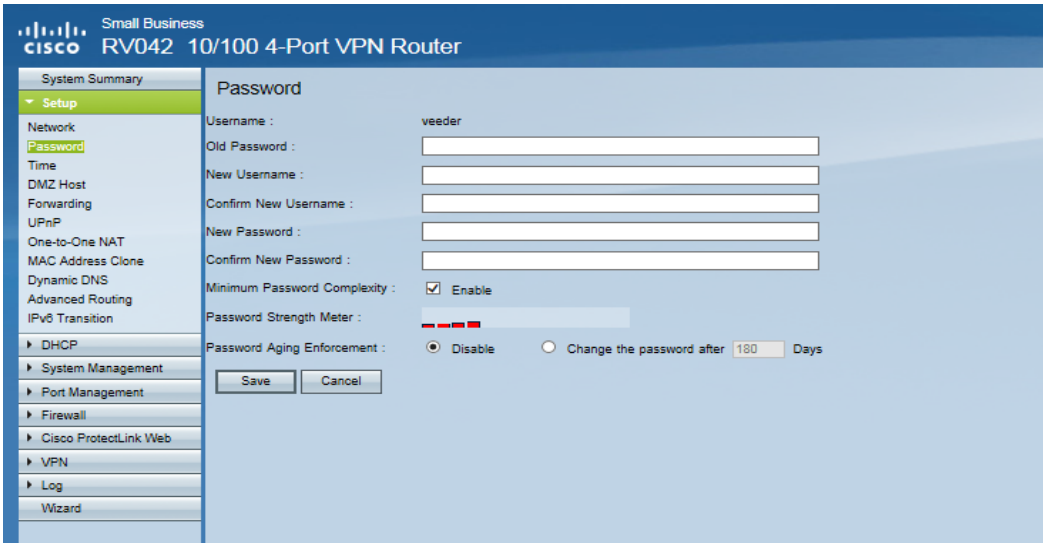
3. Open a browser window (i.e. Internet Explorer) on the laptop.
4. Enter IP Address for Cisco Router assigned to 192.168.11.104 in the address bar and select Enter.

5. The Network Password dialog box should appear.



Enter default login: **User Name = Admin | Password = Admin**

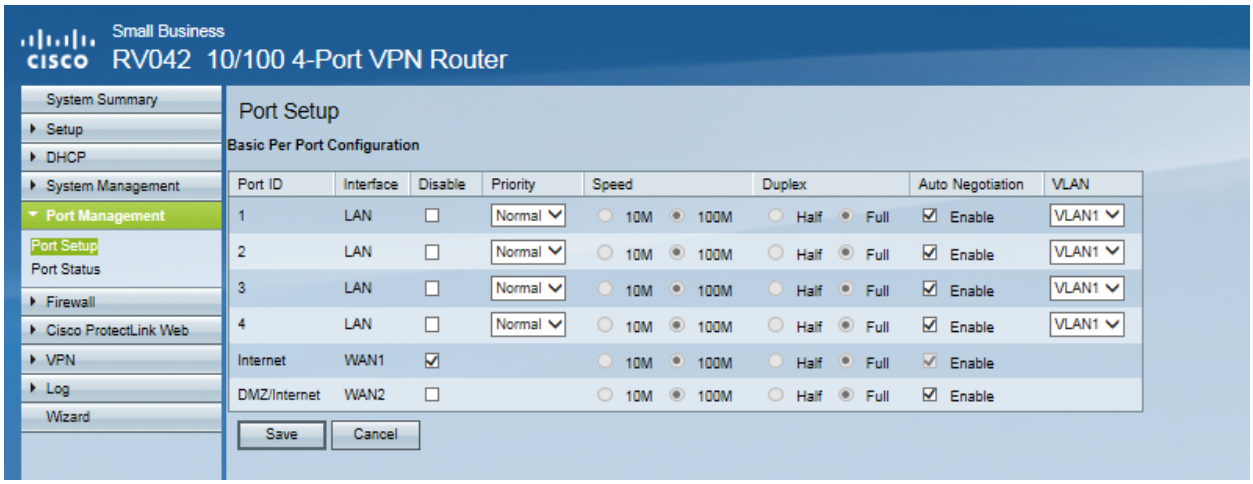
6. The first time you log into router, the device will require you to change the password. You may also change the Username if desired.



a. Enter **Admin** as the old password.
b. Enter **New Username** if desired.
c. Confirm **New Username.**
d. Enter new password. **Note**: The password can have a maximum of seven characters, including a digit and a special character such as '$'.
e. Confirm new password.
f. Minimum Password Complexity: **(Enable)**
g. Password Aging Enforcement: **(Disable)** unless your organization requires password changes periodically.
h. Click **Save**.

Part 2) Configuring router traffic management: Port Management

All unused ports on the router should be disabled. At a minimum, port ID 1 (LAN) and Internet (WAN1) should be enabled.

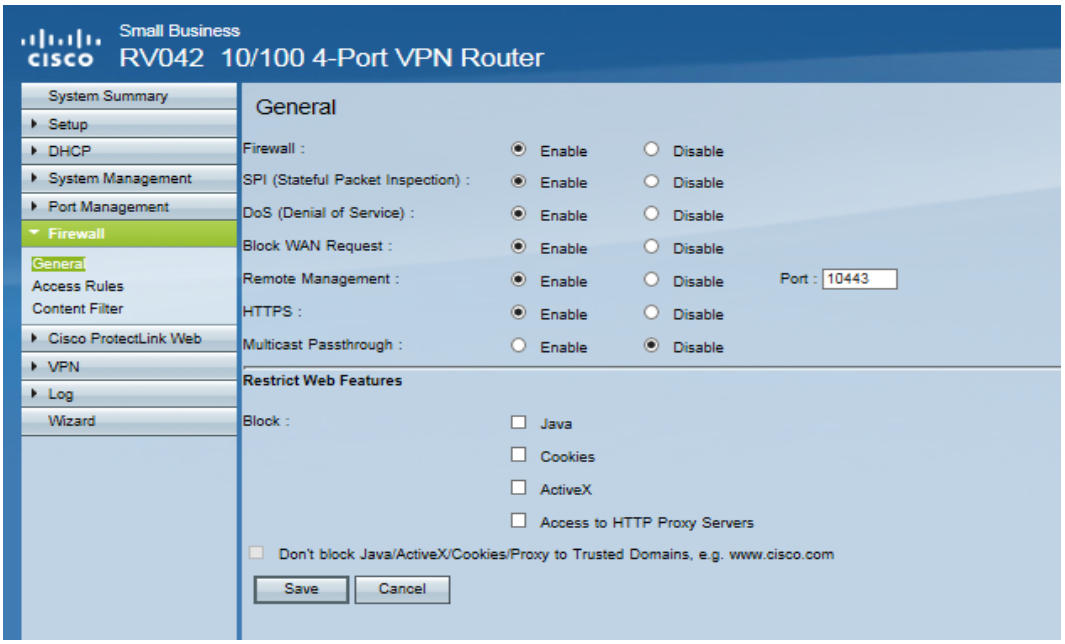


1. Select the **Port Management-> Port Setup** menu. The router default will have only LAN port 1 enabled at startup.
    a. Ensure all unused ports are disabled by checking the **Disable** column checkboxes.
    b. Ensure **Internet** (Interface **WAN1**) is enabled by unchecking **Disable.**
    c. Click **Save**.

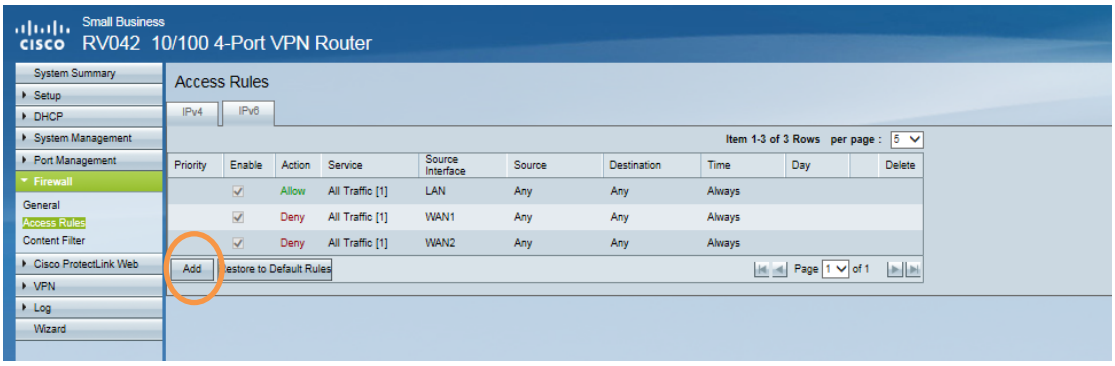
Part 3) Configuring router traffic management: Service Management

Service Management is required to set up a 'service' to classify traffic by (type/port). Rules can then be applied to each service in the next step. This section creates the two service classes that are required to communicate to a Veeder-Root Automatic Tank Gauge: 'HTTPS' and 'TLS4'. *Note: HTTPS may already be included as a default service class; if so skip step 2.*

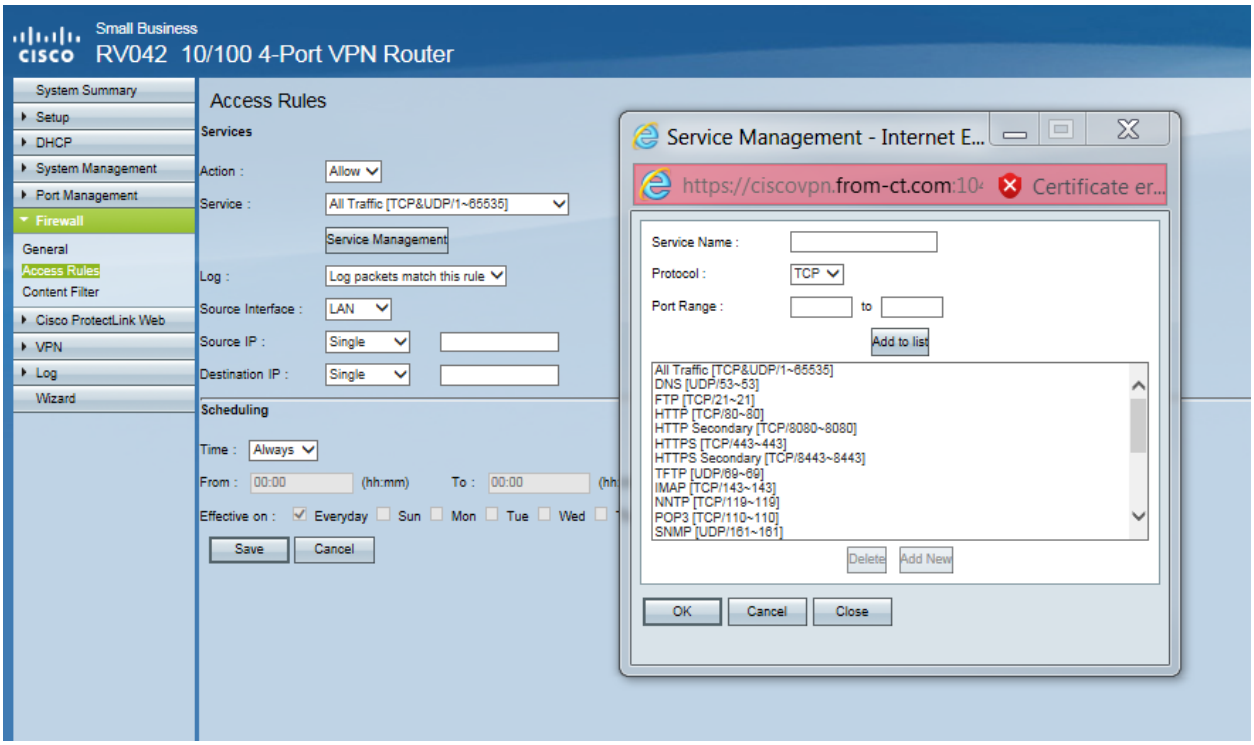
1. Select the **Firewall** menu. Select **General.** Leave settings as default.
    *Note: if accessing router remotely, program **Remote Management Port** to assigned port #.*



2. Setting Service types
    a. Click on **Firewall**, Select **Access Rules**.
    b. Click **Add.**

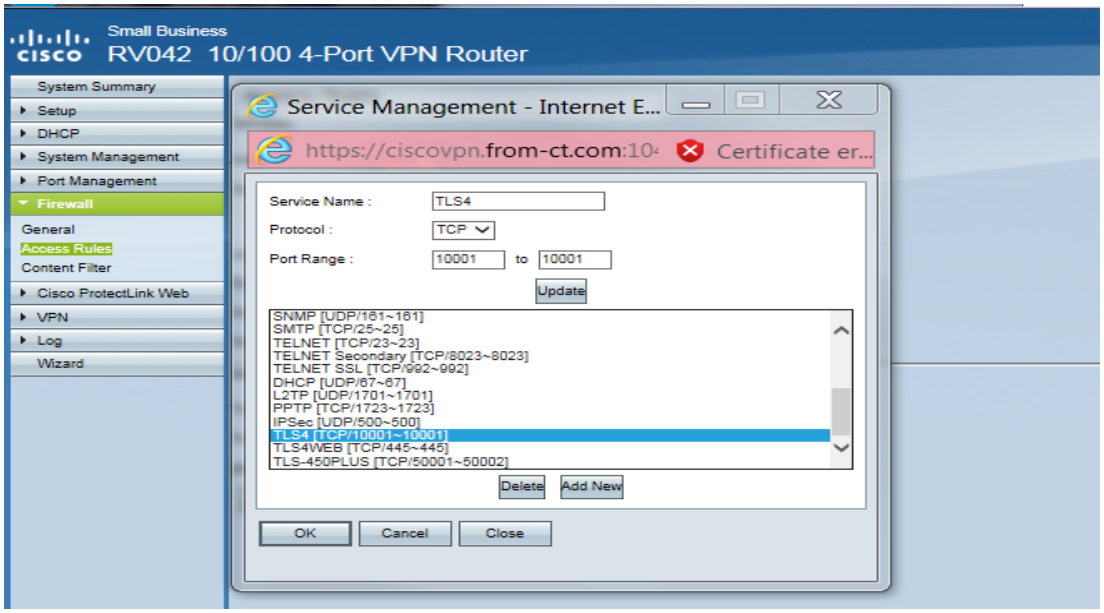


    c. Action: Select **Allow**.
    d. Click **Service Management**. A pop-up screen will appear so Service types may be added.



i. Enter Service Name: **HTTPS**
ii. Select Protocol : **TCP**
iii. Set Port Range: **443** to **443**
iv. Click **Add to List**.

To ensure you have access to the ATG Telnet ports you will need to add an additional service **TLS4** such as the example below.

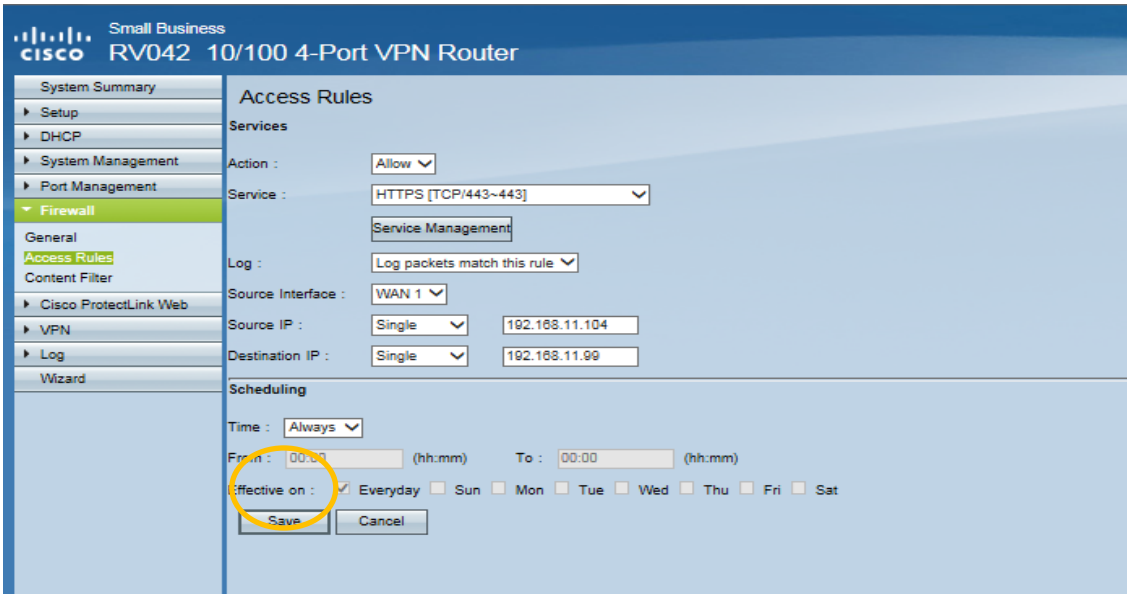


Part 4) Configuring router traffic management: Rules Management

After Completing the Service Management section you will need to continue to configure the **Access Rules** portion of the Router Setup. This will allow the service types created in the previous step to pass to the Veeder-Root Automatic Tank Gauge, while denying all other service types.

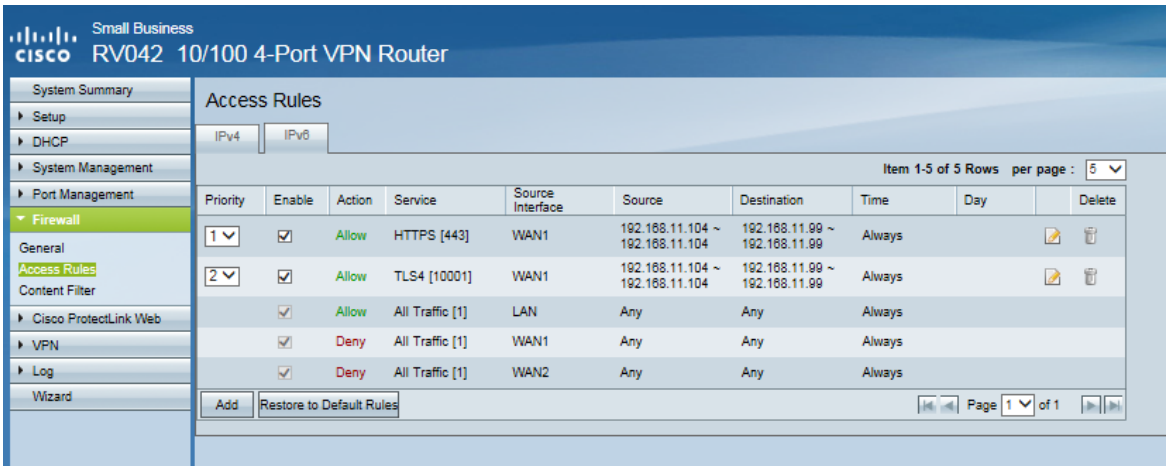
e. Action: **Allow**
f. Service: Select per Service Management list in *Part 3*, ex. **TLS4[TCP/10001]**
g. Log: **Log packets match this rule**
h. Source Interface: **WAN 1**
i. Source IP Example: Router (192.168.11.104)
j. Destination IP Example: ATG (192.168.11.99)
k. Click **Save**.

Note: Scheduling may also be used if desired for access rules.



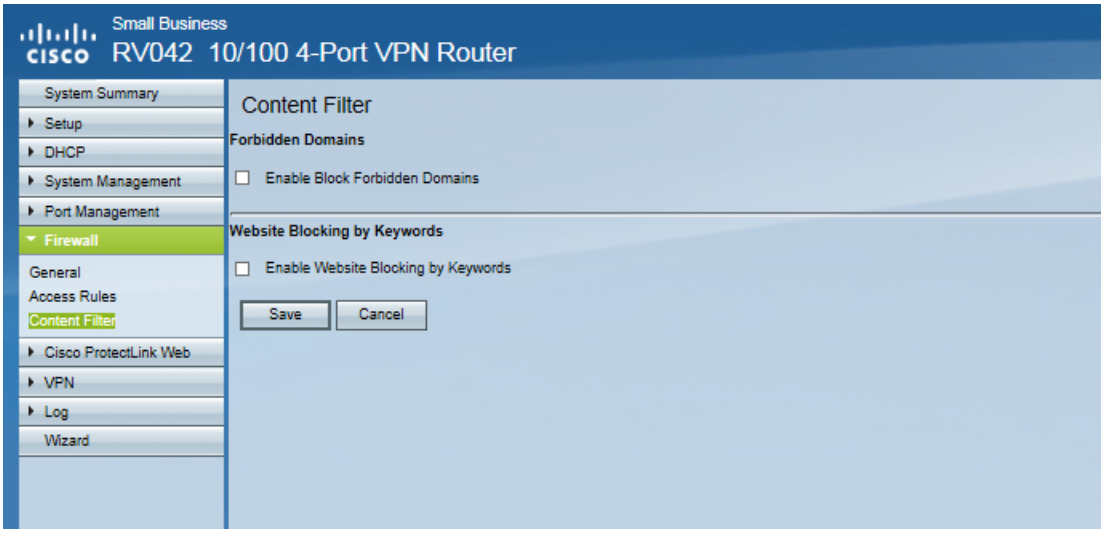
To add additional Access rules- Click on Add and configure based on your network settings. Example below:

a. Click **Add**
b. Action: **Allow**
c. Service: **HTTPS [TCP/443-443]**
d. Log: **Log packets match this rule**
e. Source Interface: **WAN 1**
f. Source IP Example: Router (192.168.11.104)
g. Destination IP Example: ATG (192.168.11.99)



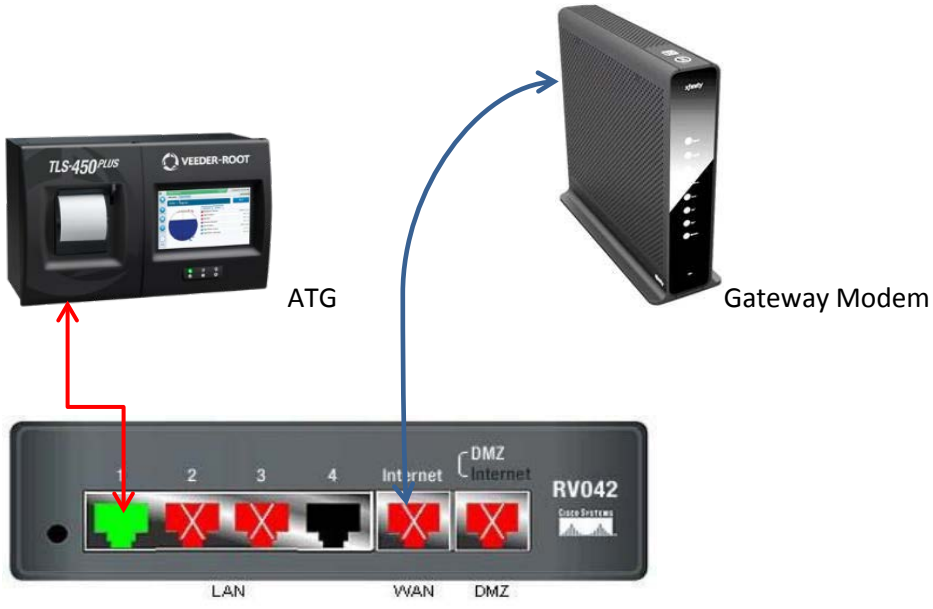
Select **Content Filter** - Leave as Default.

a. Click **Save.**



9. Click on **Logout** in the Upper Right Hand Corner.

10. Disconnect Laptop from Router.
11. Reconnect ATG to Router.



12. Test all devices that have permissions.
13. Test non-authorized devices to verify router is setup properly.

VEEDER-ROOT

For technical support, sales or other assistance, please visit:
www.veeder.com