# Probe System Firewall

## Quick Reference Guide

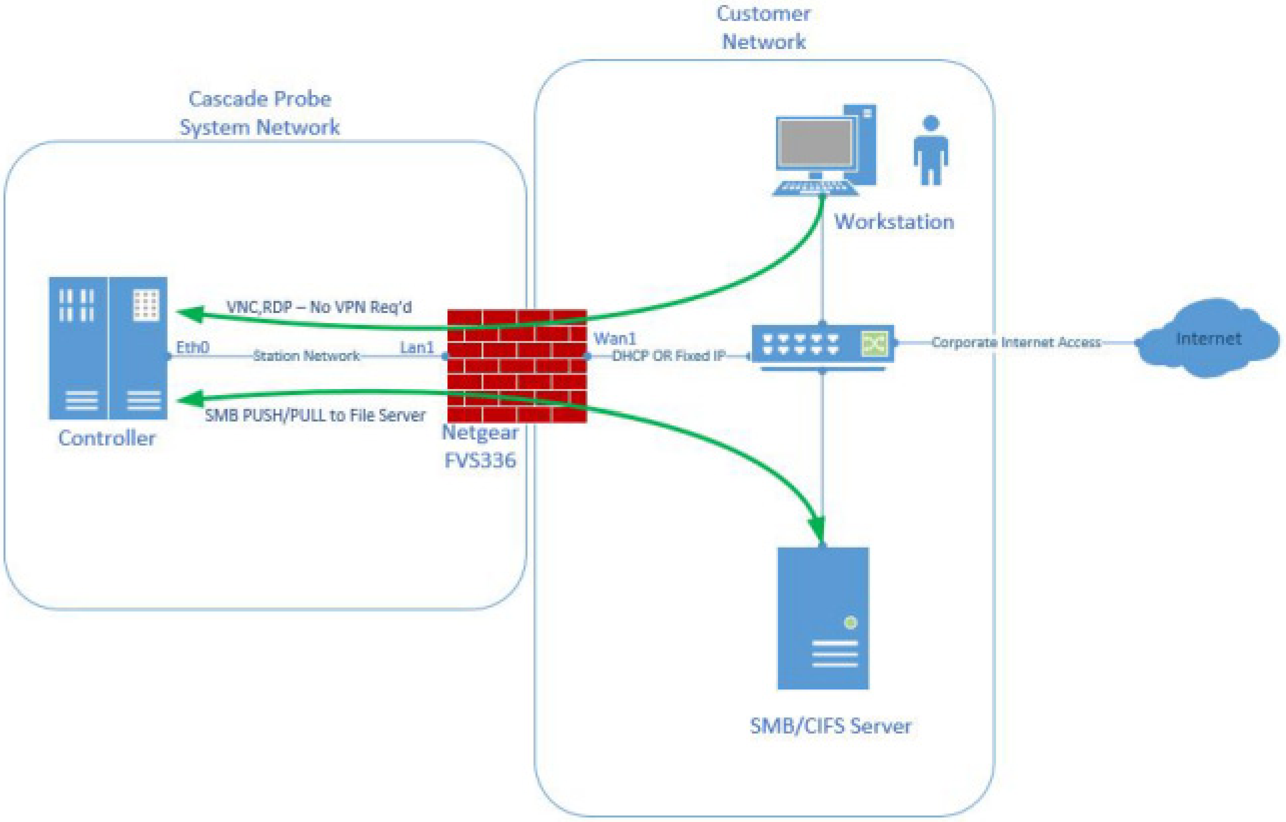
## Overview

This information in this document describes a solution using the NETGEAR ProSafe FVS336GV2 Firewall to enable secure operation of Windows XP-based probe system controllers beyond the expiration of Microsoft security updates (April 8th, 2014). Check with your corporate IT department to determine if this method is approved for Windows XP-based controller operation within your corporate network. An alternative VLAN configuration with Access Control Lists is also described here.

The assumptions made in this document are as follows:

- The existing firewall obtains WAN addressing from a DHCP server, unless otherwise specified.
- Probe system controllers are isolated from the corporate network. General users can gain access only through permitted means such as VNC or RDP.
- Probe system controllers are allowed access to the corporate network using firewall access rules, in order to access devices such as file servers.
- Outbound access to all services is allowed.
- The controller is protected by corporate antivirus and filtering, configured by the organization. If this is not the case, see Adding Alternate Antivirus and Filtering Capability on page 6.

## Connecting the Probe System Controller to the Firewall



# Probe System Firewall

Before connecting the probe system to the firewall:

- Upgrade the NetGear ProSafe device to the recommended firmware version.
- Confirm WAN configuration is using DHCP, unless corporate requirements dictate otherwise. If static IP addressing is required, see step 4 on page 4.

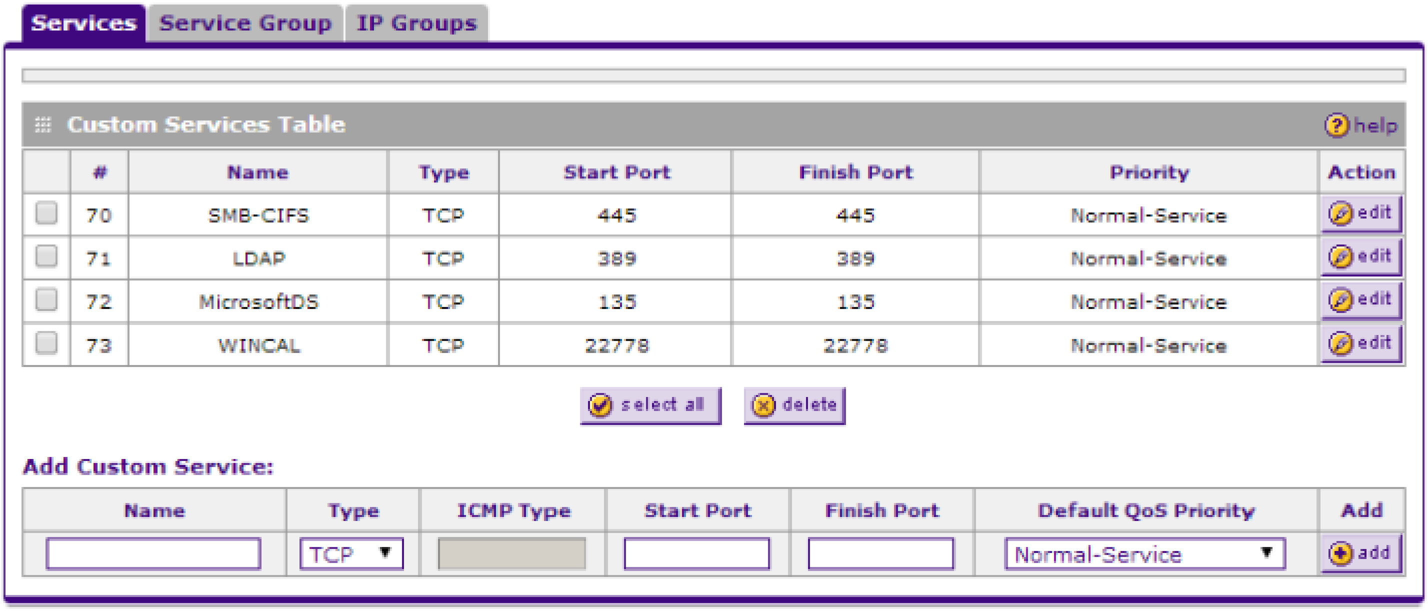
To connect the probe system to the firewall:

1. Connect firewall WAN 1 to your corporate network.
2. Connect the controller to LAN 1.
3. Power on the firewall and wait 60 seconds.
4. Configure the controller IP and LAN settings:
   – IP address: 192.168.1.2
   – Subnet Mask: 255.255.255.0
   – Gateway: 192.168.1.1
   – DNS: assign corporate DNS servers appropriate for your site
5. From the probe system controller web browser, go to: https://192.168.1.1.
6. Log in using the default testing credentials:
   – User name: admin
   – Password: password

## Configuring the NETGEAR Firewall

1. Change the factory default Admin and Guest passwords. *(Path: Root > Users)*
2. Configure Custom Services as shown.

*Path: Root > Security > Services > Services*



Custom Services Table

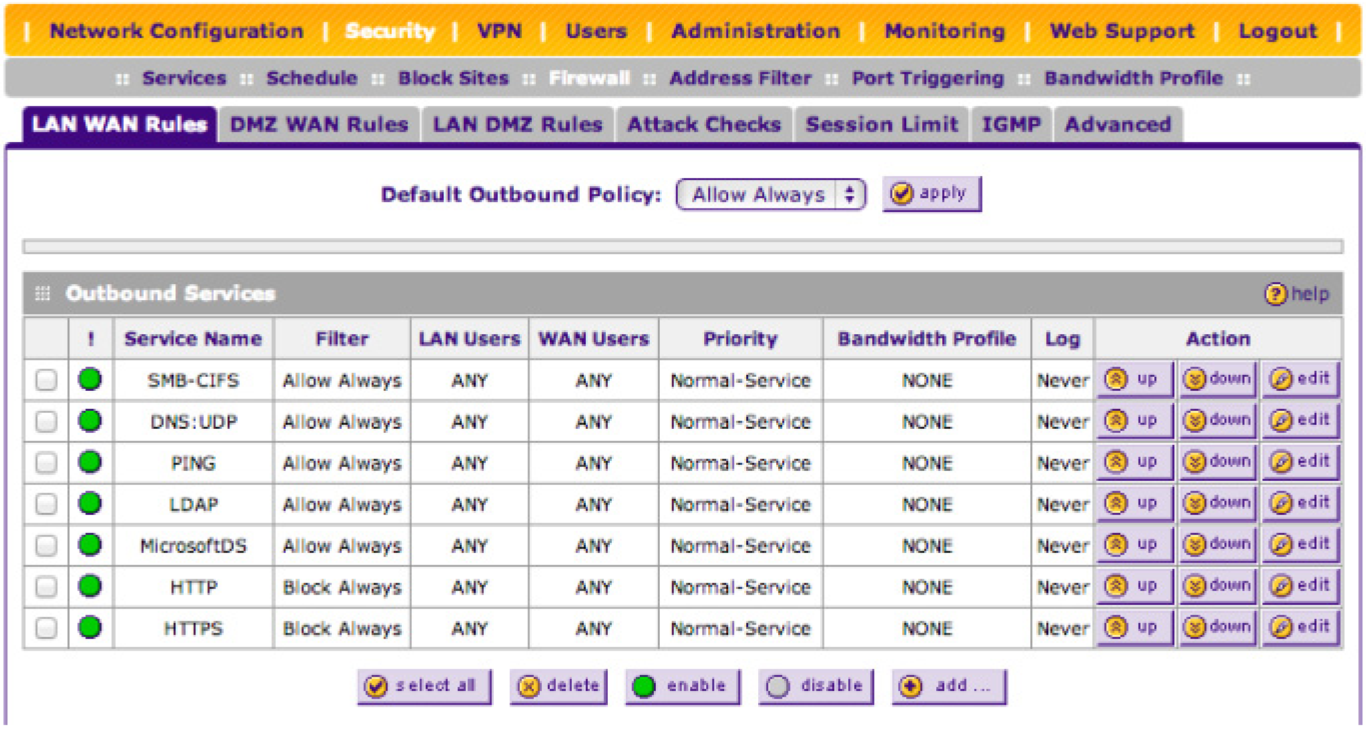
| | # | Name | Type | Start Port | Finish Port | Priority | Action |
|---|---|---|---|---|---|---|---|
| □ | 70 | SMB-CIFS | TCP | 445 | 445 | Normal-Service | edit |
| □ | 71 | LDAP | TCP | 389 | 389 | Normal-Service | edit |
| □ | 72 | MicrosoftDS | TCP | 135 | 135 | Normal-Service | edit |
| □ | 73 | WINCAL | TCP | 22778 | 22778 | Normal-Service | edit |

Add Custom Service:

| Name | Type | ICMP Type | Start Port | Finish Port | Default QoS Priority | Add |
|---|---|---|---|---|---|---|
| | TCP ▼ | | | | Normal-Service ▼ | add |

3. Configure the Outbound and Inbound LAN WAN rules as shown.

*Path: Root > Security > Firewall > LAN WAN Rules > Outbound Services*
*Default Outbound Policy: Allow Always.*

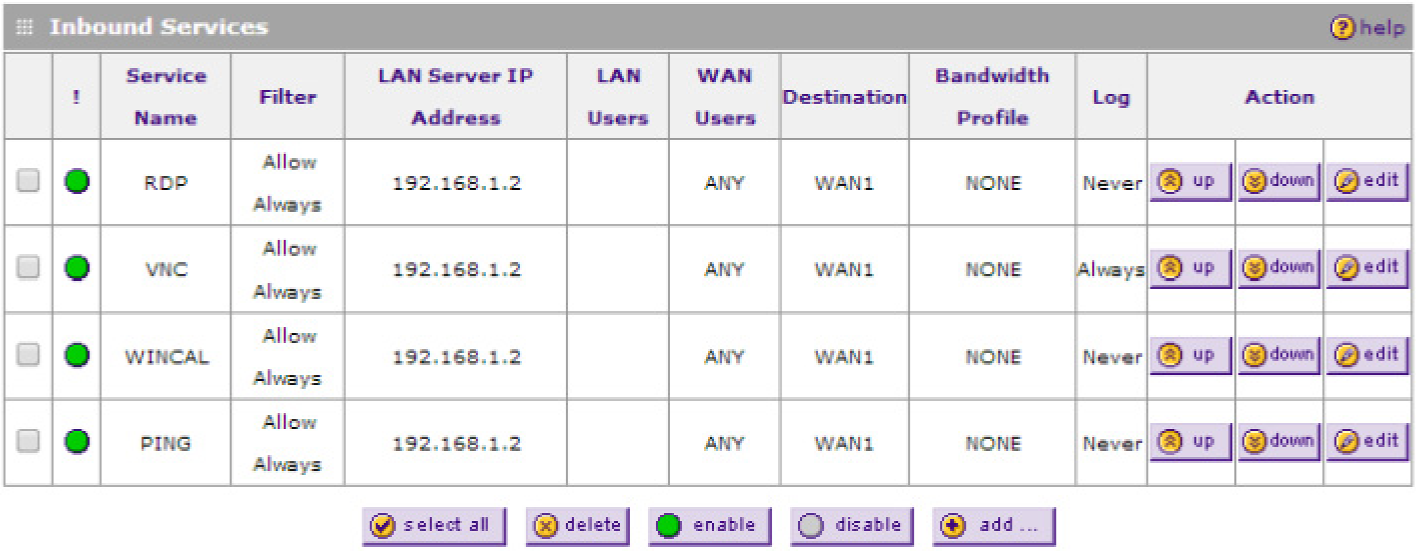

| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Block Sites :: Firewall :: Address Filter :: Port Triggering :: Bandwidth Profile ::
LAN WAN Rules
DMZ WAN Rules
LAN DMZ Rules
Attack Checks
Session Limit
IGMP
Advanced
apply
help
select all
delete
enable
disable
add ...

Default Outbound Policy: Allow Always

Outbound Services

| | ! | Service Name | Filter | LAN Users | WAN Users | Priority | Bandwidth Profile | Log | Action |
|---|---|---|---|---|---|---|---|---|---|
| □ | ● | SMB-CIFS | Allow Always | ANY | ANY | Normal-Service | NONE | Never | up down edit |
| □ | ● | DNS:UDP | Allow Always | ANY | ANY | Normal-Service | NONE | Never | up down edit |
| □ | ● | PING | Allow Always | ANY | ANY | Normal-Service | NONE | Never | up down edit |
| □ | ● | LDAP | Allow Always | ANY | ANY | Normal-Service | NONE | Never | up down edit |
| □ | ● | MicrosoftDS | Allow Always | ANY | ANY | Normal-Service | NONE | Never | up down edit |
| □ | ● | HTTP | Block Always | ANY | ANY | Normal-Service | NONE | Never | up down edit |
| □ | ● | HTTPS | Block Always | ANY | ANY | Normal-Service | NONE | Never | up down edit |

*Path: Root > Security > Firewall > LAN WAN Rules > Inbound Services*

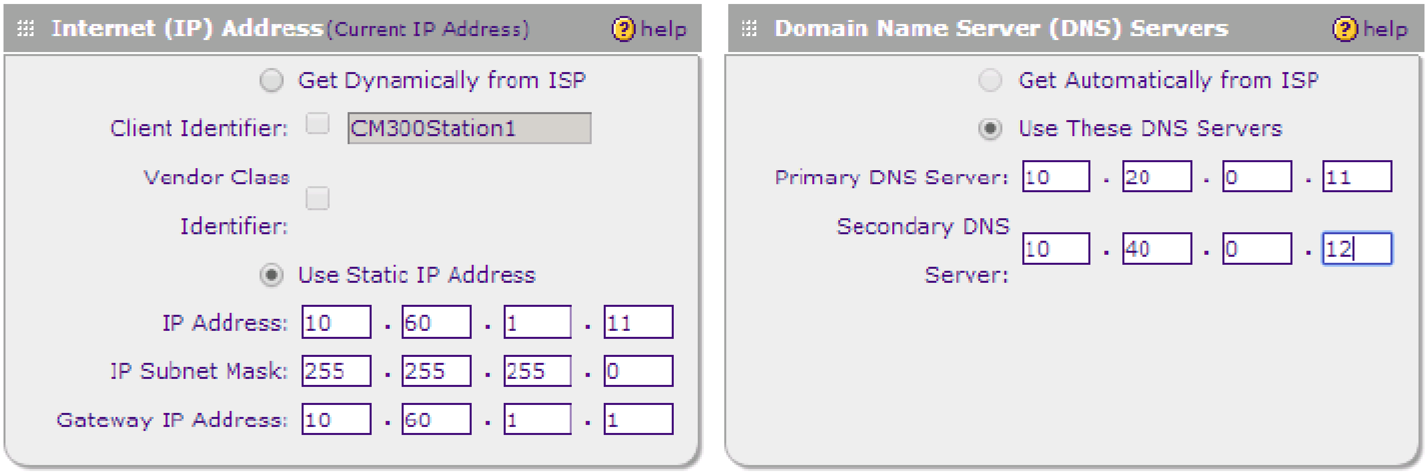


Inbound Services

| | ! | Service Name | Filter | LAN Server IP Address | LAN Users | WAN Users | Destination | Bandwidth Profile | Log | Action |
|---|---|---|---|---|---|---|---|---|---|---|
| □ | ● | RDP | Allow Always | 192.168.1.2 | | ANY | WAN1 | NONE | Never | up down edit |
| □ | ● | VNC | Allow Always | 192.168.1.2 | | ANY | WAN1 | NONE | Always | up down edit |
| □ | ● | WINCAL | Allow Always | 192.168.1.2 | | ANY | WAN1 | NONE | Never | up down edit |
| □ | ● | PING | Allow Always | 192.168.1.2 | | ANY | WAN1 | NONE | Never | up down edit |

4. Configure static IP addressing for WAN connections:
   a. Gather the following firewall connection and login information from the corporate IT department:
      – IP Address (example: 10.60.1.11)
      – Subnet Mask (example: 255.255.255.0)
      – Gateway IP Address (example: 10.60.1.1)
      – Internal DNS Servers (2 preferred), used for access to file servers (examples: 10.20.0.11, 10.40.0.12)
   b. From the probe system controller web browser, go to: https://192.168.1.1 to connect to the firewall.
   c. Enter the IP addressing information in the corresponding fields, as shown:

*Path: Root > Network Configuration > WAN1 ISP Settings*



**Internet (IP) Address** (Current IP Address) ? help

○ Get Dynamically from ISP

Client Identifier: □ CM300Station1

Vendor Class Identifier: □

● Use Static IP Address

IP Address: 10 . 60 . 1 . 11

IP Subnet Mask: 255 . 255 . 255 . 0

Gateway IP Address: 10 . 60 . 1 . 1

**Domain Name Server (DNS) Servers** ? help

○ Get Automatically from ISP

● Use These DNS Servers

Primary DNS Server: 10 . 20 . 0 . 11

Secondary DNS Server: 10 . 40 . 0 . 12

   d. Click Apply.
   e. Verify your connection to the firewall from the corporate network by pinging the IP address.

# Optional Configuration Settings

## Adding VPN Access

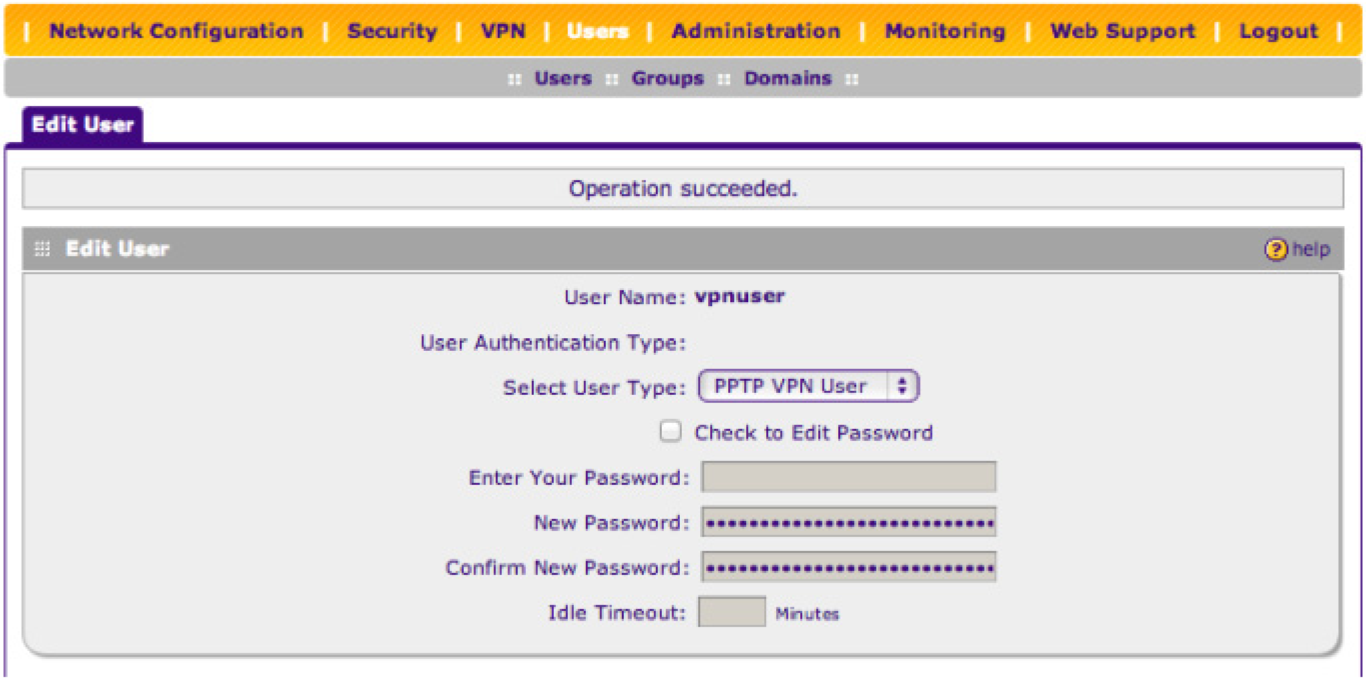
**NOTE**

*This step is required only if files need to be copied directly to probe system controller from corporate network.*

# Probe System Firewall

1. Create the following accounts:

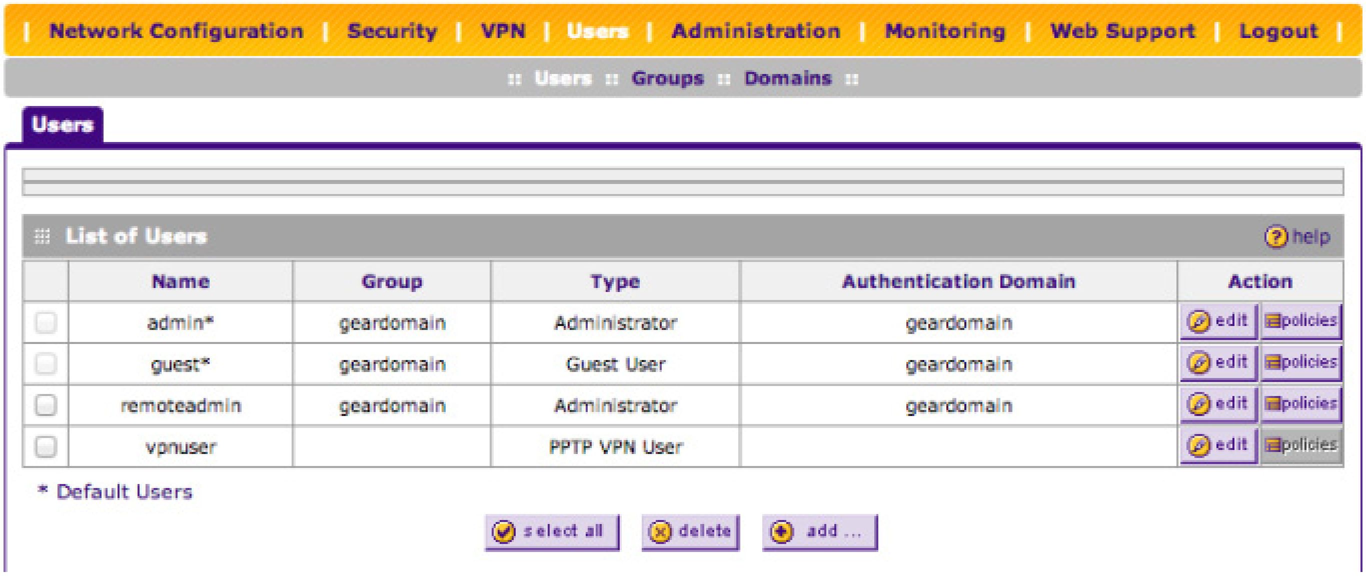
*Path: Root > Users > Users*


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Users :: Groups :: Domains ::
Edit User
help

Operation succeeded.

**Edit User**

| | |
|---|---|
| User Name: | vpnuser |
| User Authentication Type: | |
| Select User Type: | PPTP VPN User |
| | □ Check to Edit Password |
| Enter Your Password: | |
| New Password: | •••••••••••••••••••••••••••• |
| Confirm New Password: | •••••••••••••••••••••••••••• |
| Idle Timeout: | Minutes |


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Users :: Groups :: Domains ::
Users
help
select all
delete
add ...

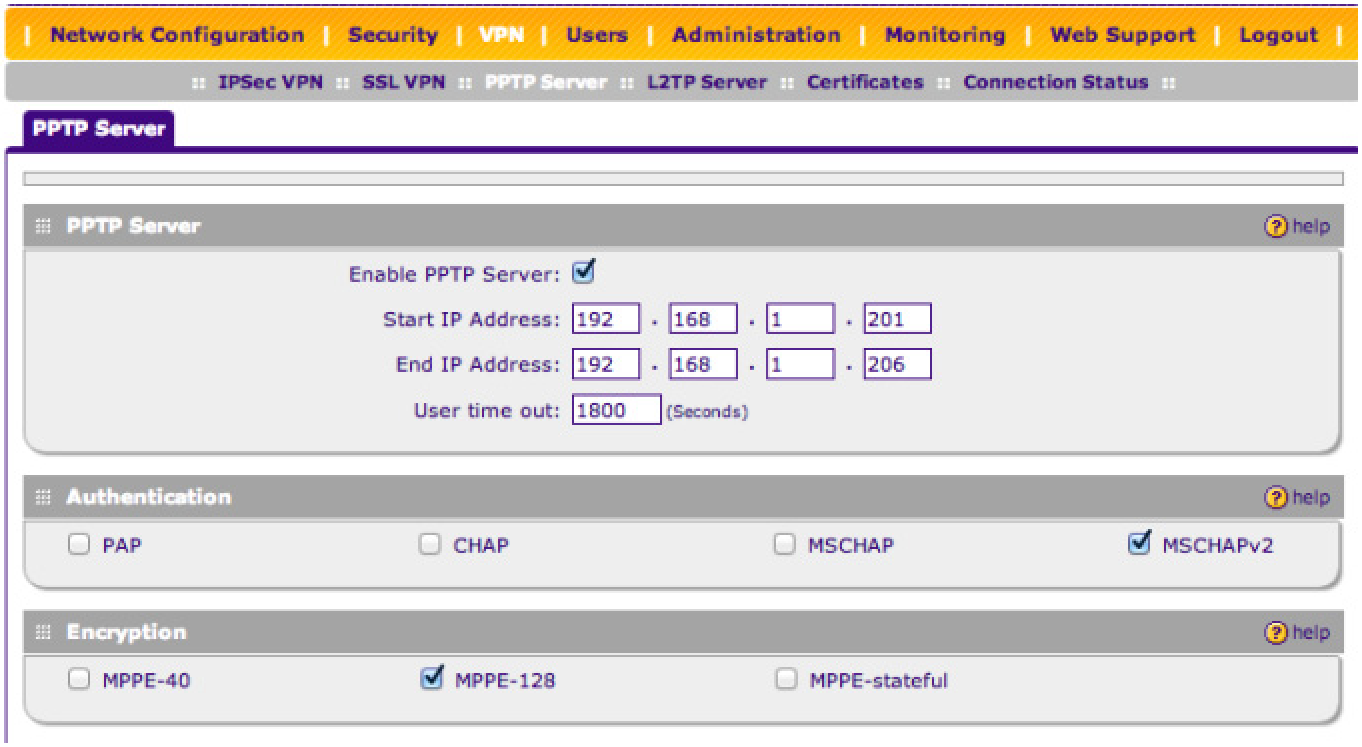
**List of Users**

| | Name | Group | Type | Authentication Domain | Action |
|---|---|---|---|---|---|
| □ | admin* | geardomain | Administrator | geardomain | edit policies |
| □ | guest* | geardomain | Guest User | geardomain | edit policies |
| □ | remoteadmin | geardomain | Administrator | geardomain | edit policies |
| □ | vpnuser | | PPTP VPN User | | edit policies |

* Default Users

2. Configure the VPN Server as shown:

*Path: Root > VPN > PPTP Server*


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: PPTP Server :: L2TP Server :: Certificates :: Connection Status ::
PPTP Server
help

**PPTP Server**

Enable PPTP Server: ☑

Start IP Address: 192 . 168 . 1 . 201

End IP Address: 192 . 168 . 1 . 206

User time out: 1800 (Seconds)

**Authentication**

☐ PAP ☐ CHAP ☐ MSCHAP ☑ MSCHAPv2

**Encryption**

☐ MPPE-40 ☑ MPPE-128 ☐ MPPE-stateful

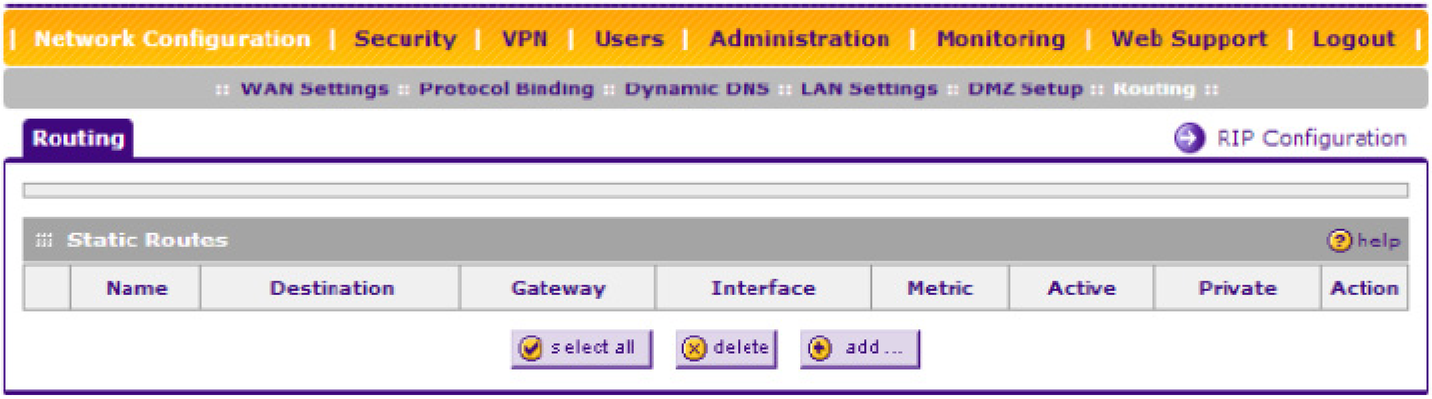
## Securing Access to Specified Network Segments

This option enables you to configure routing to control access to systems outside of the probe system network. This configuration offers a greater granularity of control by allowing or denying where the probe system is allowed to route, and further restricts access to services (see step 3 on page 3) by allowing access only to certain network segments. Involvement of a network engineer in the process of adding route information is recommended.

Two configuration options are available:

- Static routing - requires knowledge of all network segments necessary for the operation of probe system to critical systems such as DNS servers, probe operators management workstation, file services and other services.
- Dynamic RIPv2 routing - dynamically updates the routes, making configuration easier for long term operation. This option does require network engineer involvement in configuring network routing on the WAN interface.

*Path: root > Network Configuration > Routing*


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing ::
Routing
RIP Configuration
help
select all
delete
add ...

**Static Routes**

| | Name | Destination | Gateway | Interface | Metric | Active | Private | Action |
|---|---|---|---|---|---|---|---|---|

# Probe System Firewall

## Adding Alternate Antivirus and Filtering Capability

Ideally, system antivirus and filtering software should be implemented by the customer. However, in the absence of corporate managed antivirus and filtering software, or if the standard corporate antivirus software is incompatible with the probe system software, a locally managed client is recommended.

Go to www.forticlient.com for a good example of antivirus and filtering software which is free for unmanaged clients. For more information on provided services, go to www.fortiguard.com.

## Firewall Purchase Alternatives

If placement of a firewall between the probe system and the corporate network is not permitted, a routed VLAN with Access Control Lists can be configured according to corporate policies. Note that this configuration does enable the use of multiple systems.

### Example (inbound and outbound ACL, using Cisco nomenclature):

- Corporate network:  10.1.0.0/16
- Station Network:  10.10.10.0/24
- Station 1 IP: 10.10.10.1
- Station 2 IP: 10.10.10.2

(Allows only RDP, VNC and ICMP inbound from the corporate network)

```
ip access-list extended stations-in
 permit tcp 10.1.0.0 0.0.255.255 host 10.10.10.1 eq 3389
 permit tcp 10.1.0.0 0.0.255.255 host 10.10.10.2 eq 3389
 permit tcp 10.1.0.0 0.0.255.255 host 10.10.10.1 eq 5900
 permit tcp 10.1.0.0 0.0.255.255 host 10.10.10.2 eq 5900
 permit icmp 10.1.0.0 0.0.255.255 host 10.10.10.1
 permit icmp 10.1.0.0 0.0.255.255 host 10.10.10.2
```

(Allows traffic only to the corporate network, can be further restricted by services if necessary, denies Internet traffic. Do not deny Internet traffic if using Forticlient software, as it is required for updates.)

```
ip access-list extended stations-out
 permit icmp host 10.10.10.1 10.1.0.0 0.0.255.255
 permit icmp host 10.10.10.2 10.1.0.0 0.0.255.255
 permit ip host 10.10.10.1  10.1.0.0 0.0.255.255
 permit ip host 10.10.10.2  10.1.0.0 0.0.255.255
 permit ip host 10.10.10.1 0.0.0.0 0.0.0.0  (only add if Internet access is necessary)
 permit ip host 10.10.10.2 0.0.0.0 0.0.0.0  (only add if Internet access is necessary)
```

## Notice of Normal Use

The statements, technical information and recommendations contained herein are believed to be accurate as of the date hereof. Information in this document is subject to change without notice. The user has the responsibility to read and follow carefully all safety and use instructions. Since the conditions and methods of use of the product and of the information referred to herein are beyond our control, Cascade Microtech, Inc. expressly disclaims any and all liability as to any results obtained or arising from any use of the product or reliance on such information; NO WARRANTY OF FITNESS FOR ANY PARTICULAR PURPOSE, WARRANTY OF MERCHANTABILITY OR ANY OTHER WARRANTY, EXPRESS OR IMPLIED, IS MADE CONCERNING THE GOODS DESCRIBED OR THE INFORMATION PROVIDED HEREIN.

The information provided herein relates only to the specific product designated and may not be applicable when such product is used in combination with other materials or in any process. The user assumes all liability for misuse or alteration of the product, or for use in any manner not described in the Cascade Microtech, Inc. documentation.

Nothing contained herein constitutes a license to practice under any patent and it should not be construed as an inducement to infringe any patent and the user is advised to take appropriate steps to be sure that any proposed use of the product will not result in patent infringement.

Data subject to change without notice.

**Cascade Microtech, Inc.**
**Corporate Headquarters**
toll free: +1-800-550-3279
phone: +1-503-601-1000
email: cmi_sales@cmicro.com

**Germany**
phone: +49-89-9090195-0
email: cmg_sales@cmicro.com

**Japan**
phone: +81-3-5615-5150
email: cmj_sales@cmicro.com

**China**
phone: +86-21-3330-3188
email: cmc_sales@cmicro.com

**Singapore**
phone: +65-6873-7482
email: cms_sales@cmicro.com

**Taiwan**
phone: +886-3-5722810
email: cmt_sales@cmicro.com