FREEDOM IQ

THE INTELLIGENT PHONE SOLUTION

AdTran Internet Configuration Guide v1.15

# ADTRAN 3120 / 3130

# Internet Configuration Guide

FREEDOMVOICE®

169 Saxony Road, Suite 212
Encinitas, CA 92024
Phone & Fax: (800) 477-1477

## Table of Contents

# Introduction

Thank you for choosing FreedomIQ from FreedomVoice for an industry-leading hosted VoIP phone system. We are glad to have you on board as part of our team and this document should help answer any questions you may have on setting up the AdTran router.

We are providing two (2) documents which fully address setting up the AdTran router. This is the first document: **Internet Configuration Guide** that covers setting up basic Internet access. The second document: **AdTran QoS Configuration Guide** provides the procedure for configuring QoS (Quality of Service) on the device.

This document; the **Internet Configuration Guide** will step you through the procedure for configuring Internet access on the AdTran 3120/3130 router in its new or reset state. Setting up the router is a four step process:

1) Configuration of the Public Interface
2) Disabling the SIP ALG (application level gateway)
3) Configuring SNTP (simple network team protocol)
4) Enabling Remote Access

# ADTRAN 3120 / 3130

## Product Information: ADTRAN 3120

The ADTRAN 3120 series is a Fixed-port Access Router that is ideal for enterprise-level Internet access and/or IP Telephony using broadband access such as DSL or cable. The 3120 includes one Ethernet WAN port, an integrated four-port Ethernet Switch, a built-in firewall for network security, QoS to priority delay sensitive traffic like VoIP, and a host of other features such as DHCP, Network Address Translation (NAT), and IPSec VPN.

**Features:**

- Fixed-port Access Router for broadband access such as DSL or cable
- Ethernet WAN Interface and Integral four-port, non-blocking, Ethernet switch
- Stateful inspection firewall for network security
- Quality of Service (QoS) for delay-sensitive traffic like Voice over IP (VoIP)
- Inherent URL filtering for easy content filtering
- IPSec Virtual Private Network (VPN) for secure corporate connectivity across the Internet

## Product Information: ADTRAN 3130

The ADTRAN 3130 series is a Fixed-port Access Router that is ideal for enterprise-level Internet access and/or IP Telephony ADSL, ADSL2, or ADSL2+ broadband access. The 3130 includes one ADSL WAN port, integrated four port switch, built in firewall, QoS, DHCP, NAT, and an IPSec VPN.

**Features:**

- Fixed-port Access Router for ADSL, ADSL2, or ADSL2+
- ADSL WAN Interface and Integral four-port, non-blocking, Ethernet switch
- Stateful inspection firewall for network security
- Quality of Service (QoS) for delay-sensitive traffic like Voice over IP (VoIP)
- Inherent URL filtering for easy content filtering
- IPSec Virtual Private Network (VPN) for secure corporate connectivity across the Internet

## Change Default Username/Password

It is important that you change the default username and password to something secure. This new login information ensures that no one within the LAN can make unauthorized changes, but can also be used as the default remote login information for remote access to the router in the event changes need to be made remotely by a dealer or a FreedomIQ representative.

Default login information:

- Gateway: “10.10.10.1”
- Username: “admin”
- Password: “password”

Follow these steps to udpate the admin login information:

1. From the “System” section in the left column, select “Passwords”.
2. Scroll to the bottom of the page and select the “Enable” tab.
3. Check “Use password” and enter your new password twice.
4. Click the “Apply” button toward the bottom of the page.
5. Click the “Save” button at the top of the page.

## Configuring Internet Access

The AdTran 3120/3130 is easy to set up via the GUI with minimal configuration. **Your ISP should have provided you with general instructions** related to your internet connection. If you are unsure what these settings are, contact your ISP with regard to the settings you will need for your router. In 99% of all cases your service provider will either have you to set your router to DHCP mode or they will provide you with IP address, Gateway address, Subnet Mask and DNS server settings. **You will need this information to continue the set up.**

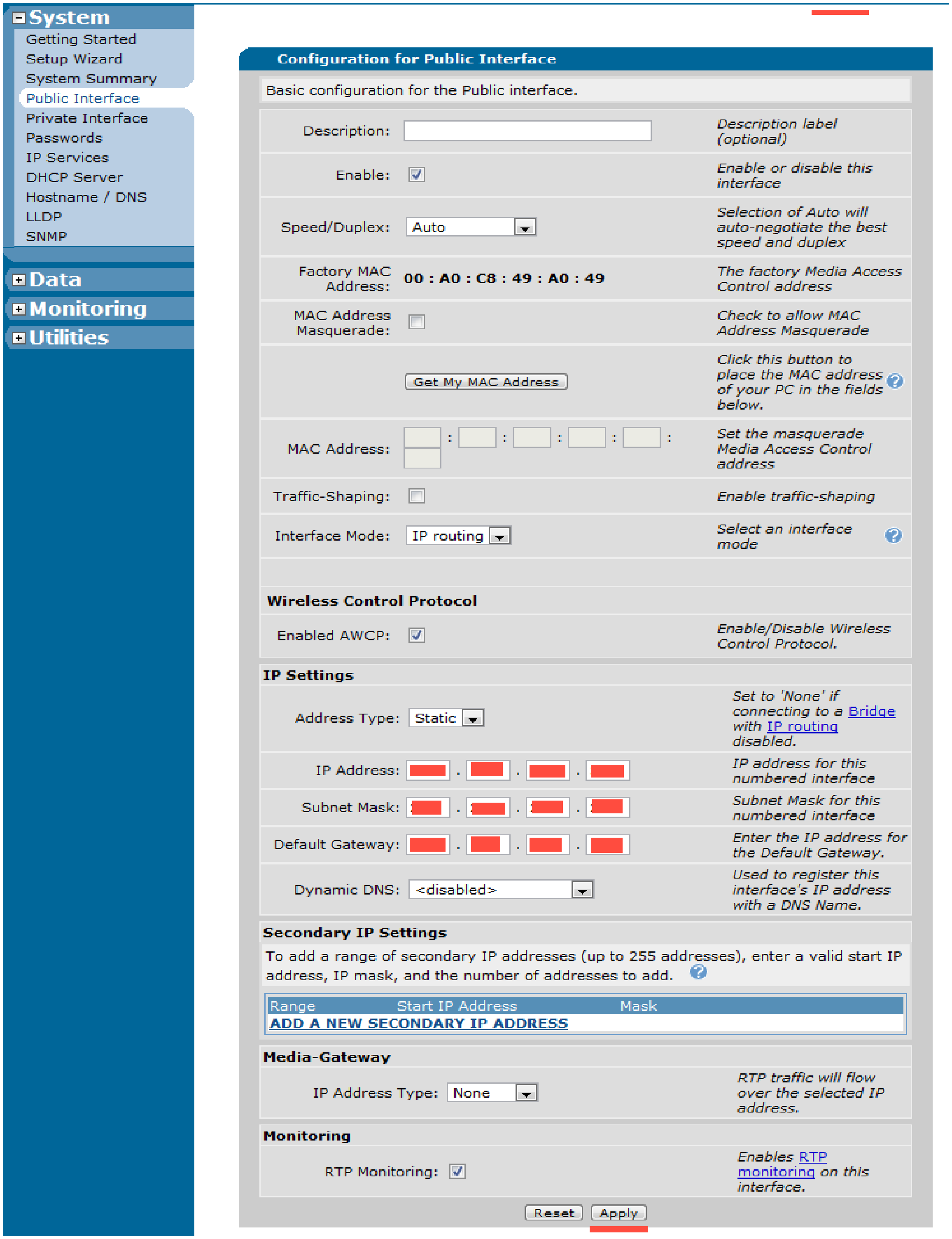
Follow these steps to configure internet access:

1. From the “System” section in the left column, select “Public Interface”.
2. Go to “IP Settings” halfway down the page. Your ISP settings will determine whether you need to choose “Static” or “DHCP” from the drop down. If your ISP has provided you with a specific IP, select “Static”. If you select “DHCP” skip to step 10. (Screenshot Internet)
3. Enter your IP address in the related field.
4. Enter your subnet mask in the related field.
5. Enter your default gateway in the related field.
6. Click the “Apply” button toward the bottom of the page.
7. Click the “Save” button at the top of the page.
8. From the “System” section in the left column, select “Hostname/DNS”.
9. Enter the primary and secondary DNS addresses provided by ISP. (Screenshot DNS)
10. Click the “Apply” button toward the bottom of the page.
11. Click the “Save” button at the top of the page.
12. Cycle power on the router and give the device 3-5 minutes to boot.
13. Cycle power on any connected devices such as computers, phones etc.

**NOTE: See next page for configuration screenshot.**

# Configuration Screen 1 of 2

**System → Public Interface** (Back to instructions)



**Configuration for Public Interface**

Basic configuration for the Public interface.

| | | |
|---|---|---|
| Description: | | *Description label (optional)* |
| Enable: | ☑ | *Enable or disable this interface* |
| Speed/Duplex: | Auto ▾ | *Selection of Auto will auto-negotiate the best speed and duplex* |
| Factory MAC Address: | **00 : A0 : C8 : 49 : A0 : 49** | *The factory Media Access Control address* |
| MAC Address Masquerade: | □ | *Check to allow MAC Address Masquerade* |
| | Get My MAC Address | *Click this button to place the MAC address of your PC in the fields below.* |
| MAC Address: | : : : : : | *Set the masquerade Media Access Control address* |
| Traffic-Shaping: | □ | *Enable traffic-shaping* |
| Interface Mode: | IP routing ▾ | *Select an interface mode* |

**Wireless Control Protocol**

| | | |
|---|---|---|
| Enabled AWCP: | ☑ | *Enable/Disable Wireless Control Protocol.* |

**IP Settings**

| | | |
|---|---|---|
| Address Type: | Static ▾ | *Set to 'None' if connecting to a Bridge with IP routing disabled.* |
| IP Address: | [redacted] . [redacted] . [redacted] . [redacted] | *IP address for this numbered interface* |
| Subnet Mask: | [redacted] . [redacted] . [redacted] . [redacted] | *Subnet Mask for this numbered interface* |
| Default Gateway: | [redacted] . [redacted] . [redacted] . [redacted] | *Enter the IP address for the Default Gateway.* |
| Dynamic DNS: | <disabled> ▾ | *Used to register this interface's IP address with a DNS Name.* |

**Secondary IP Settings**

To add a range of secondary IP addresses (up to 255 addresses), enter a valid start IP address, IP mask, and the number of addresses to add.

| Range | Start IP Address | Mask |
|---|---|---|
| ADD A NEW SECONDARY IP ADDRESS | | |

**Media-Gateway**

| | | |
|---|---|---|
| IP Address Type: | None ▾ | *RTP traffic will flow over the selected IP address.* |

**Monitoring**

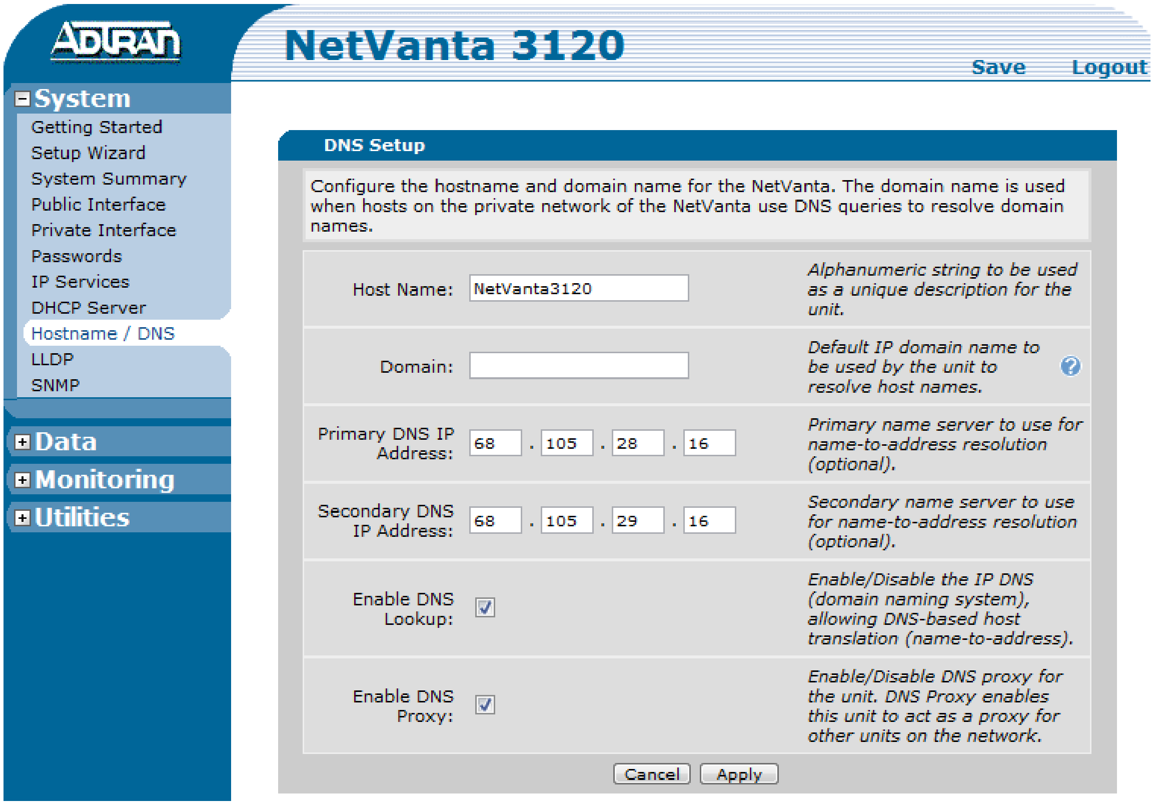
| | | |
|---|---|---|
| RTP Monitoring: | ☑ | *Enables RTP monitoring on this interface.* |

Reset Apply

***NOTE: On Adtran 3130 DSL routers, the default gateway option is listed under "Data"→"Router/Bridge"→"Default Gateway".***

## Configuration Screen 2 of 2

**System → Hostname / DNS** (Back to instructions)



**DNS Setup**

Configure the hostname and domain name for the NetVanta. The domain name is used when hosts on the private network of the NetVanta use DNS queries to resolve domain names.

| | | |
|---|---|---|
| Host Name: | NetVanta3120 | *Alphanumeric string to be used as a unique description for the unit.* |
| Domain: | | *Default IP domain name to be used by the unit to resolve host names.* |
| Primary DNS IP Address: | 68 . 105 . 28 . 16 | *Primary name server to use for name-to-address resolution (optional).* |
| Secondary DNS IP Address: | 68 . 105 . 29 . 16 | *Secondary name server to use for name-to-address resolution (optional).* |
| Enable DNS Lookup: | ☑ | *Enable/Disable the IP DNS (domain naming system), allowing DNS-based host translation (name-to-address).* |
| Enable DNS Proxy: | ☑ | *Enable/Disable DNS proxy for the unit. DNS Proxy enables this unit to act as a proxy for other units on the network.* |

## Disable SIP ALG

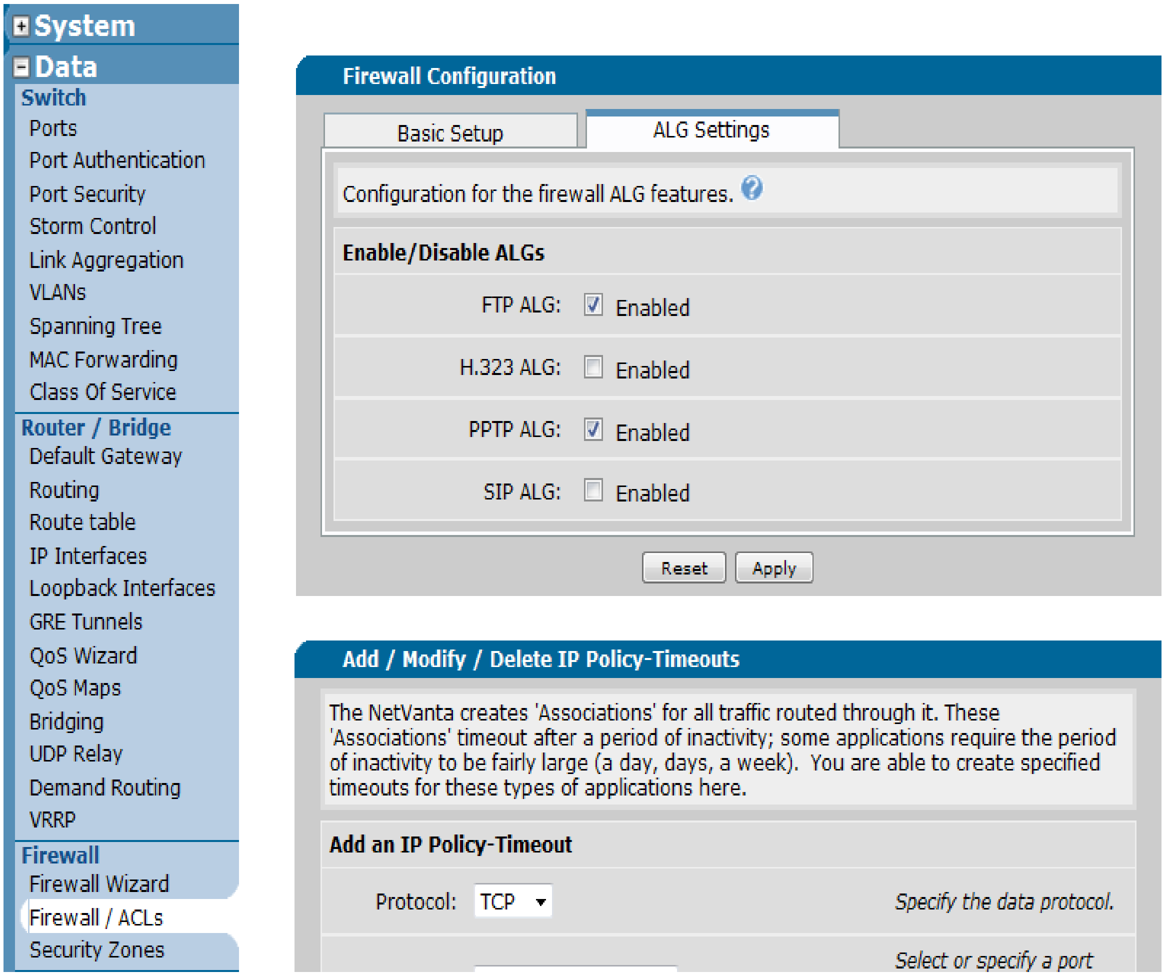
The AdTran 3120/3130 needs to have SIP ALG disabled to function properly with the FreedomIQ service. The AdTran router will not work with FreedomIQ if SIP ALG is enabled. This is an option typically used for premise based VoIP systems. Disabling this option is a simple check box within the router configuration. If you purchased this router from FreedomVoice the SIP ALG setting will already be disabled by default and you can skip this step.

To access the SIP ALG option follow these steps:

1. In left column select Firewall.
2. In left column under firewall select “Firewall / ACLs”.
3. In the main screen click on the “ALG Settings” tab.
4. In the main screen uncheck the “SIP ALG” option.
5. In the main screen click the “Apply” button.
6. At the top of the screen click the “Save” button.

## SIP ALG Settings

**Data → Firewall / ACLs → ALG Settings**



Configuration for the firewall ALG features.

**Enable/Disable ALGs**

FTP ALG: ☑ Enabled

H.323 ALG: □ Enabled

PPTP ALG: ☑ Enabled

SIP ALG: □ Enabled

The NetVanta creates 'Associations' for all traffic routed through it. These 'Associations' timeout after a period of inactivity; some applications require the period of inactivity to be fairly large (a day, days, a week). You are able to create specified timeouts for these types of applications here.

**Add an IP Policy-Timeout**

Protocol: TCP — *Specify the data protocol.*

*Select or specify a port*

## Configuring SNTP (Simple Network Time Protocol)

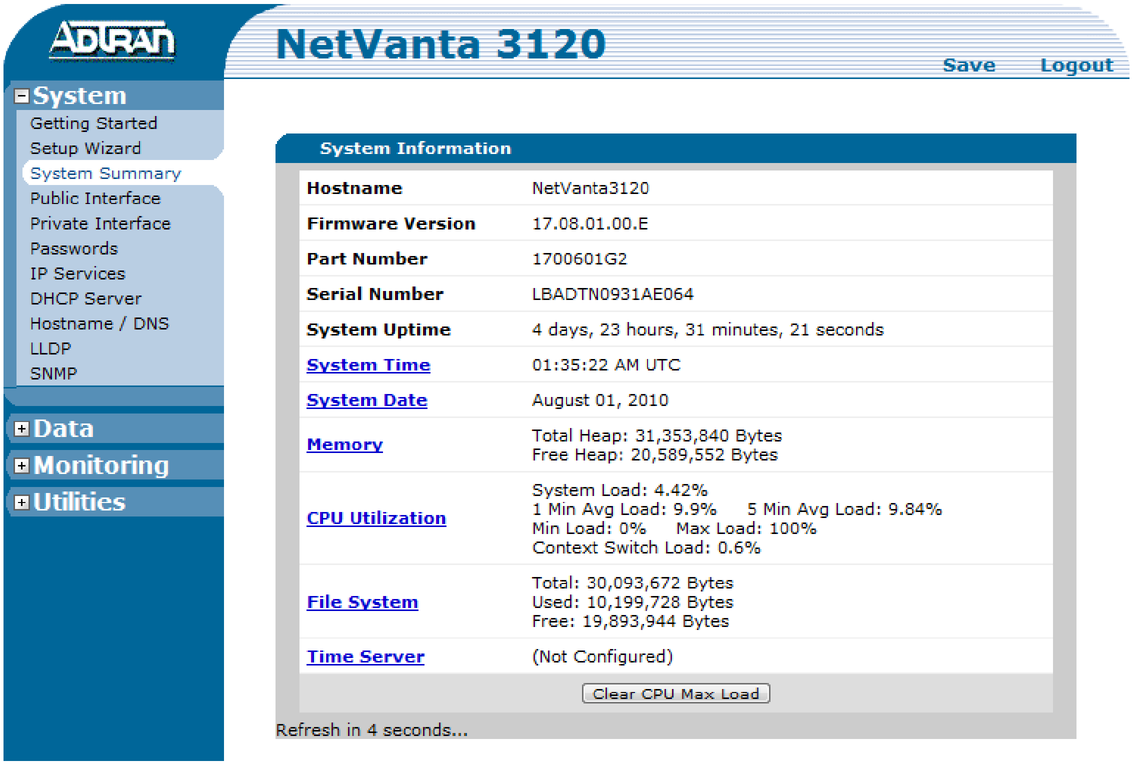
The ADTRAN 3120/3130 should have the SNTP configured so that logs and voice quality monitoring reflect the proper time in the event that traffic logs need to be viewed for a specific time. If you purchased this router from FreedomVoice, the SNTP server will already be set up for Pacific Time. In this case you will just need to choose the correct time zone for your area.

To set up SNTP follow these steps:

1. In left column select “System”.
2. In left column under system select “System Summary”.
3. In the main screen click on the “Time Server” link.
4. In the main screen at the time server drop down, select “SNTP”. (Screenshot SNTP)
5. In the field SNTP Server Hostname type in your SNTP server (time.apple.com).
6. At the bottom of the screen click the “Apply” button.
7. At the top of the screen click the “Save” button.

## SNTP Settings 1 of 2

**System → System Summary**



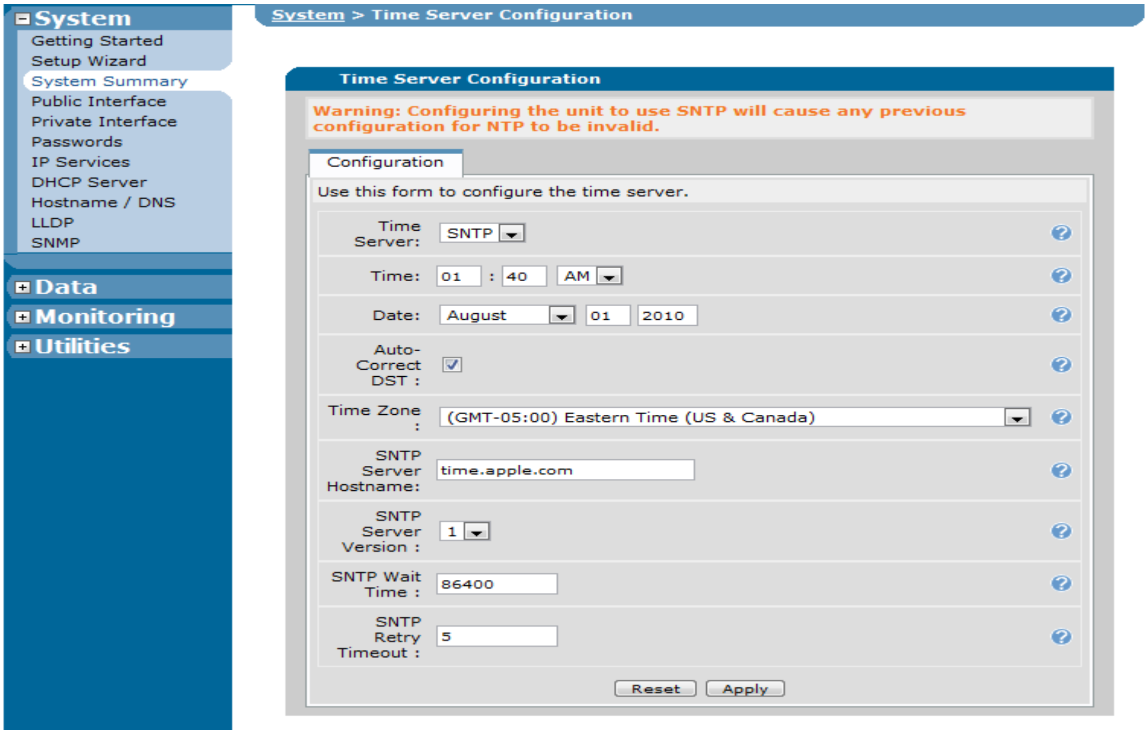
System Information

| | |
|---|---|
| **Hostname** | NetVanta3120 |
| **Firmware Version** | 17.08.01.00.E |
| **Part Number** | 1700601G2 |
| **Serial Number** | LBADTN0931AE064 |
| **System Uptime** | 4 days, 23 hours, 31 minutes, 21 seconds |
| **System Time** | 01:35:22 AM UTC |
| **System Date** | August 01, 2010 |
| **Memory** | Total Heap: 31,353,840 Bytes<br>Free Heap: 20,589,552 Bytes |
| **CPU Utilization** | System Load: 4.42%<br>1 Min Avg Load: 9.9%   5 Min Avg Load: 9.84%<br>Min Load: 0%   Max Load: 100%<br>Context Switch Load: 0.6% |
| **File System** | Total: 30,093,672 Bytes<br>Used: 10,199,728 Bytes<br>Free: 19,893,944 Bytes |
| **Time Server** | (Not Configured) |

Refresh in 4 seconds...

## SNTP Settings 2 of 2

**System → System Summary → Time Server** (Back to instructions)



Time Server Configuration

Warning: Configuring the unit to use SNTP will cause any previous configuration for NTP to be invalid.

Use this form to configure the time server.

| | |
|---|---|
| Time Server: | SNTP |
| Time: | 01 : 40 AM |
| Date: | August 01 2010 |
| Auto-Correct DST : | ☑ |
| Time Zone : | (GMT-05:00) Eastern Time (US & Canada) |
| SNTP Server Hostname: | time.apple.com |
| SNTP Server Version : | 1 |
| SNTP Wait Time : | 86400 |
| SNTP Retry Timeout : | 5 |

## Enable Remote Access

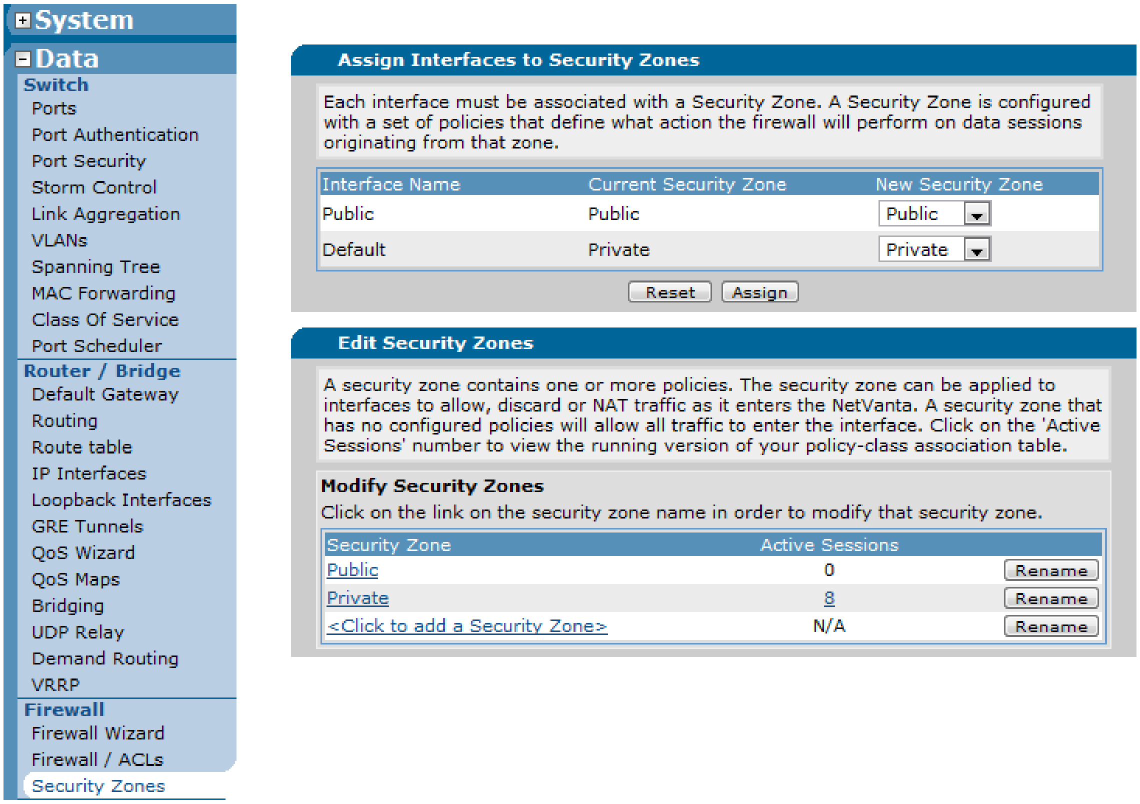
The ADTRAN 3120/3130 allows you to configure remote access to the GUI or command line interface.

Follow these steps to configure remote access:

1. In the left column select “Data”.
2. In the left column under “Firewall”, select “Security Zones”.
3. In the edit security zones section, click on “Public”. (Screenshot Public)
4. In the main screen click “Add Policy to Zone Public”. (Screenshot Add Policy)
5. In the main screen under “Policy Type:” select “Admin access” from the drop down. (Screenshot Policy Type)
6. You can set the description to something like “Remote Access”. The only other thing you’ll need to do is check “HTTPS” and if you want remote command line access check “SSH”. (Screenshot Remote Access)
7. At the bottom of the screen click the “Apply” button.
8. At the top of the screen click the “Save” button.

## Remote Access 1 of 4

**Data → Firewall → Security Zones** (Back to instructions)



**Assign Interfaces to Security Zones**

Each interface must be associated with a Security Zone. A Security Zone is configured with a set of policies that define what action the firewall will perform on data sessions originating from that zone.

| Interface Name | Current Security Zone | New Security Zone |
|---|---|---|
| Public | Public | Public |
| Default | Private | Private |

**Edit Security Zones**

A security zone contains one or more policies. The security zone can be applied to interfaces to allow, discard or NAT traffic as it enters the NetVanta. A security zone that has no configured policies will allow all traffic to enter the interface. Click on the 'Active Sessions' number to view the running version of your policy-class association table.

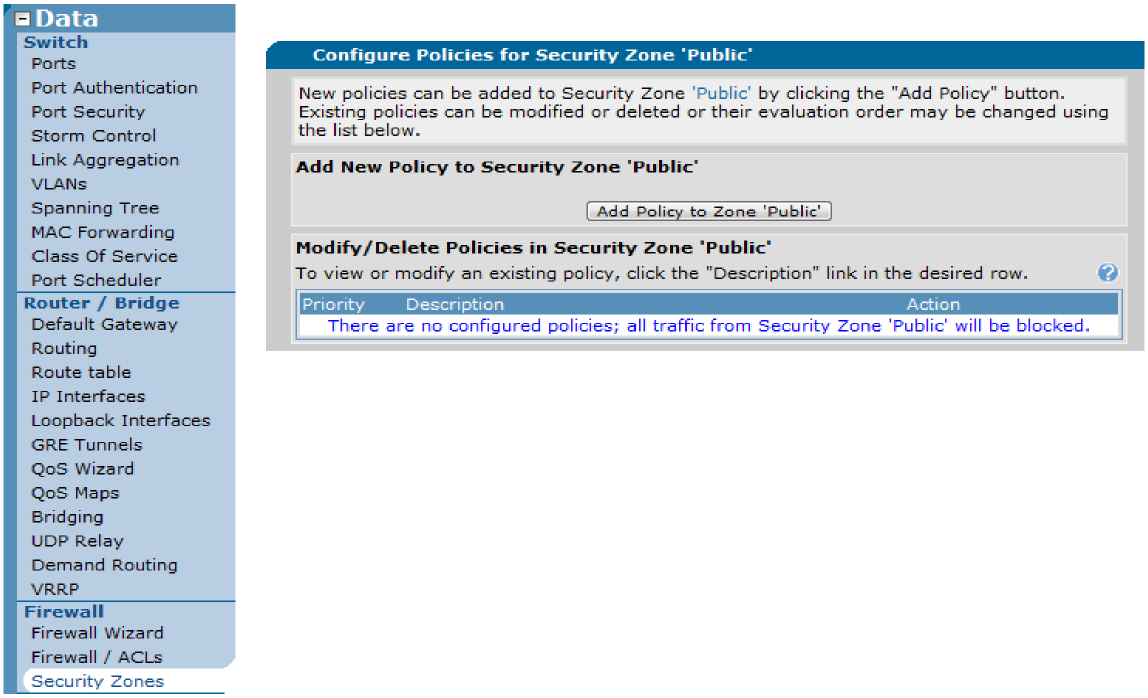
**Modify Security Zones**

Click on the link on the security zone name in order to modify that security zone.

| Security Zone | Active Sessions | |
|---|---|---|
| Public | 0 | Rename |
| Private | 8 | Rename |
| <Click to add a Security Zone> | N/A | Rename |

## Remote Access 2 of 4

**Data → Firewall → Security Zones → Public** (Back to instructions)



**Configure Policies for Security Zone 'Public'**

New policies can be added to Security Zone 'Public' by clicking the "Add Policy" button. Existing policies can be modified or deleted or their evaluation order may be changed using the list below.

**Add New Policy to Security Zone 'Public'**

**Modify/Delete Policies in Security Zone 'Public'**

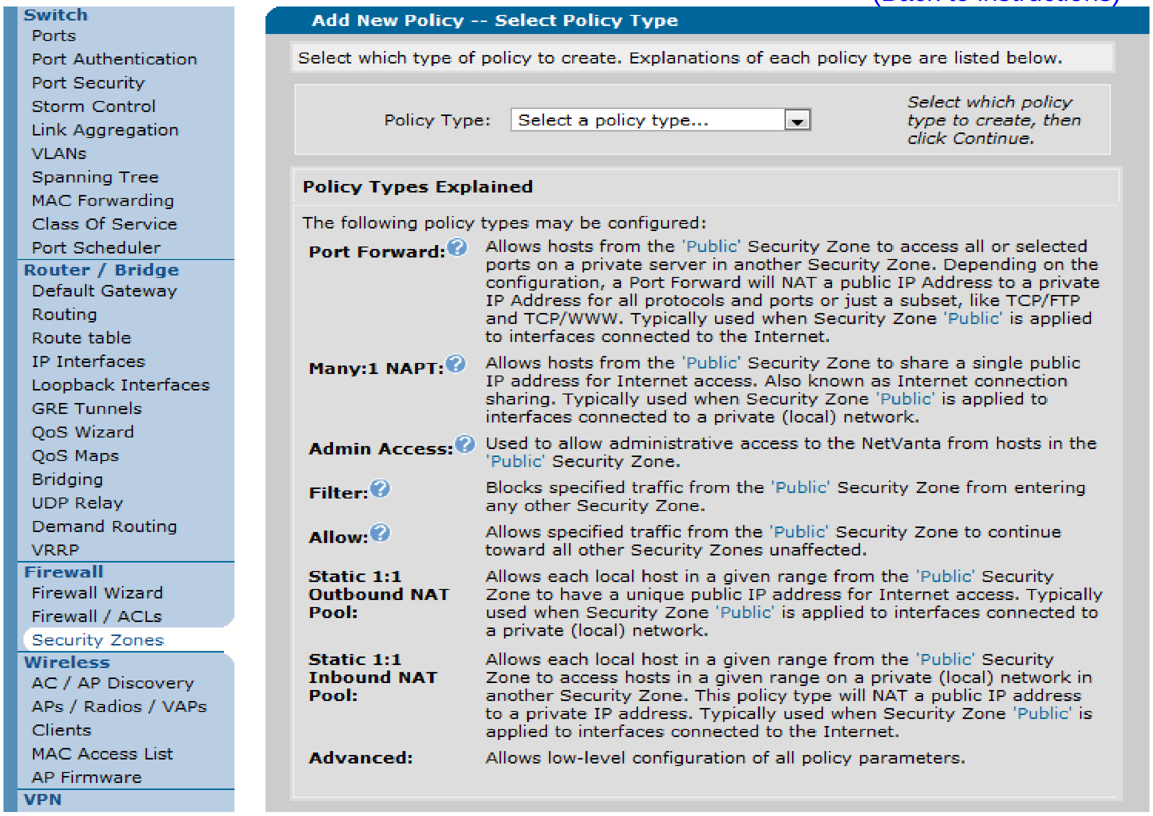
To view or modify an existing policy, click the "Description" link in the desired row.

| Priority | Description | Action |
|---|---|---|
| | There are no configured policies; all traffic from Security Zone 'Public' will be blocked. | |

## Remote Access 3 of 4

**Data → Firewall → Security Zones → Public → Add Policy to Zone Public**

(Back to instructions)



**Add New Policy -- Select Policy Type**

Select which type of policy to create. Explanations of each policy type are listed below.

Policy Type: Select a policy type...

*Select which policy type to create, then click Continue.*

**Policy Types Explained**

The following policy types may be configured:

**Port Forward:** Allows hosts from the 'Public' Security Zone to access all or selected ports on a private server in another Security Zone. Depending on the configuration, a Port Forward will NAT a public IP Address to a private IP Address for all protocols and ports or just a subset, like TCP/FTP and TCP/WWW. Typically used when Security Zone 'Public' is applied to interfaces connected to the Internet.

**Many:1 NAPT:** Allows hosts from the 'Public' Security Zone to share a single public IP address for Internet access. Also known as Internet connection sharing. Typically used when Security Zone 'Public' is applied to interfaces connected to a private (local) network.

**Admin Access:** Used to allow administrative access to the NetVanta from hosts in the 'Public' Security Zone.

**Filter:** Blocks specified traffic from the 'Public' Security Zone from entering any other Security Zone.

**Allow:** Allows specified traffic from the 'Public' Security Zone to continue toward all other Security Zones unaffected.

**Static 1:1 Outbound NAT Pool:** Allows each local host in a given range from the 'Public' Security Zone to have a unique public IP address for Internet access. Typically used when Security Zone 'Public' is applied to interfaces connected to a private (local) network.

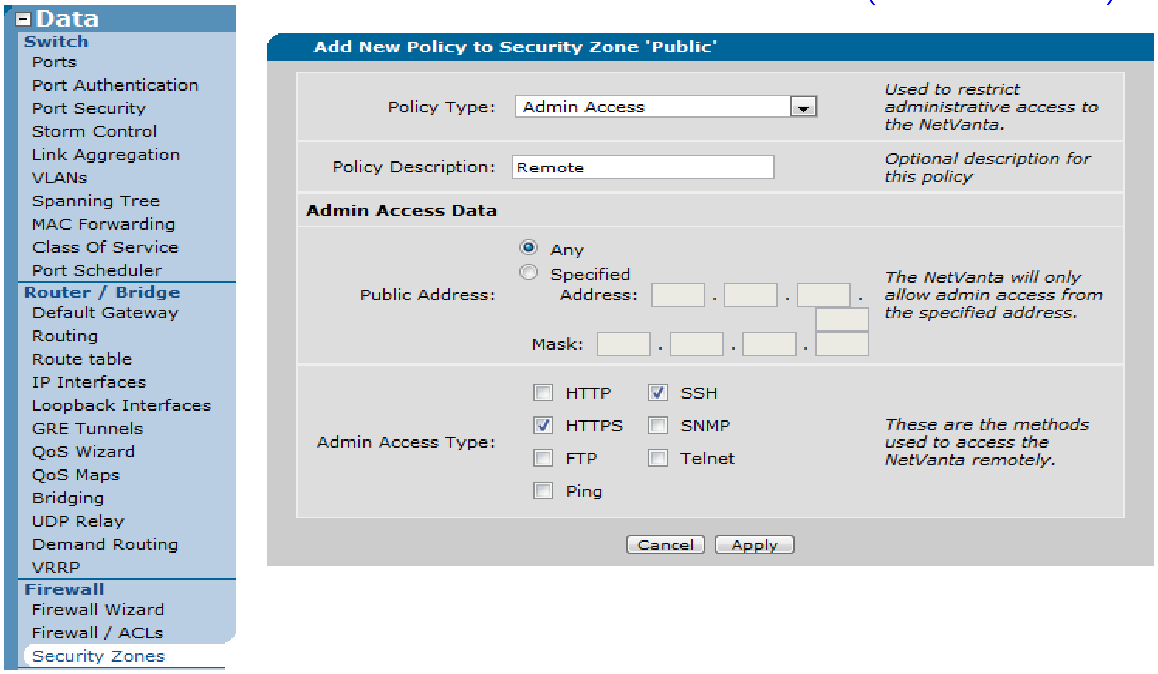
**Static 1:1 Inbound NAT Pool:** Allows each local host in a given range from the 'Public' Security Zone to access hosts in a given range on a private (local) network in another Security Zone. This policy type will NAT a public IP address to a private IP address. Typically used when Security Zone 'Public' is applied to interfaces connected to the Internet.

**Advanced:** Allows low-level configuration of all policy parameters.

## Remote Access 4 of 4

**Data → Firewall → Security Zones → Public → Add Policy to Zone Public → Admin Access**

(Back to instructions)



**Add New Policy to Security Zone 'Public'**

Policy Type: Admin Access — *Used to restrict administrative access to the NetVanta.*

Policy Description: Remote — *Optional description for this policy*

**Admin Access Data**

Public Address: ● Any ○ Specified Address: ___ . ___ . ___ . ___ Mask: ___ . ___ . ___ . ___ — *The NetVanta will only allow admin access from the specified address.*

Admin Access Type: □ HTTP ☑ SSH ☑ HTTPS □ SNMP □ FTP □ Telnet □ Ping — *These are the methods used to access the NetVanta remotely.*

## Technical Support

Technical support for FreedomIQ is available from 3:00 AM PST to 6:00 PM PST, Monday through Friday, Saturday from 6:30am PST to 3:30pm PST and can be reached either by phone or by email. Emergency support is available 24/7.

**Phone:** 888-955-3520 ext. 2

Use this number to reach a trained FreedomIQ technical support representative during normal support hours. If calling outside of normal hours, you will be provided the option to either leave a voicemail message or connect to the emergency support service (see below).

Numerous documents and support materials are available through the FreedomIQ Weblink. Please log into Weblink and select the support tab and review the documentation that is available online there.

**Support Email:** iqsupport@freedomvoice.com

Emails are automatically forwarded to our ticketing system. An auto-reply will be sent within a few minutes indicating the case number generated. Emails are generally returned within two hours during normal support hours, but may take longer depending on the current volume of tickets received. All emails should, however, be returned same day. For an issue that requires a faster turn-around time, please use the phone numbers listed above.