NetVanta 7000 Series Security Guide

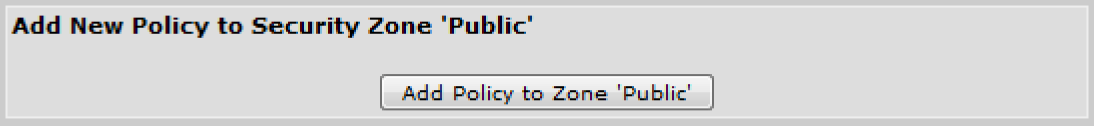
Overview

Securing the NetVanta 7000 Series IP PBX is an important part of the installation process and is often times overlooked when the unit has a public facing interface. An unsecured unit could result in a loss of data, customer downtime, or hijacked services. In an effort to keep operating costs at a minimum, securing a unit should be a primary objective. This document will give guidelines on how to configure basic security on the NetVanta 7000 Series.

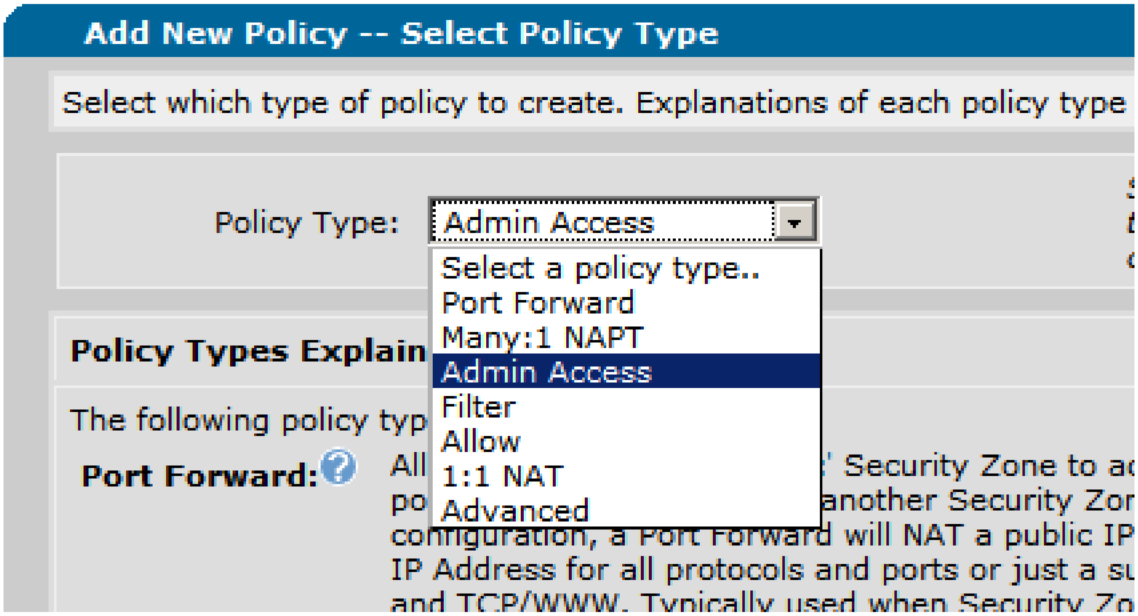
Restricting Services

Some services that run on the 7000 Series allow administrators to have access to the unit. Of these services, Telnet and HTTP do not use an encrypted authentication scheme. Therefore, a decision should be made on whether or not to disable these services completely. These services can be simply blocked by a policy class on the public interface.

Please refer to Knowledge Base Article 1968 for additional information on firewall configuration. After creating a security zone to apply on the WAN interface if you are not using the default Public security zone, you will need to create a new policy to allow the needed services. From the Security Zone Configuration Menu, you will need to click the “Add Policy to Zone 'Public'”. In this example, we are using a security zone named Public.


Add New Policy to Security Zone 'Public'

Since services are going to be allowed to be accessed through the WAN interface, Admin Access will be the type of policy added to the security zone. When prompted for the Policy Type, select “Admin Access” from the Policy Type drop down menu.



Add New Policy -- Select Policy Type

Select which type of policy to create. Explanations of each policy type

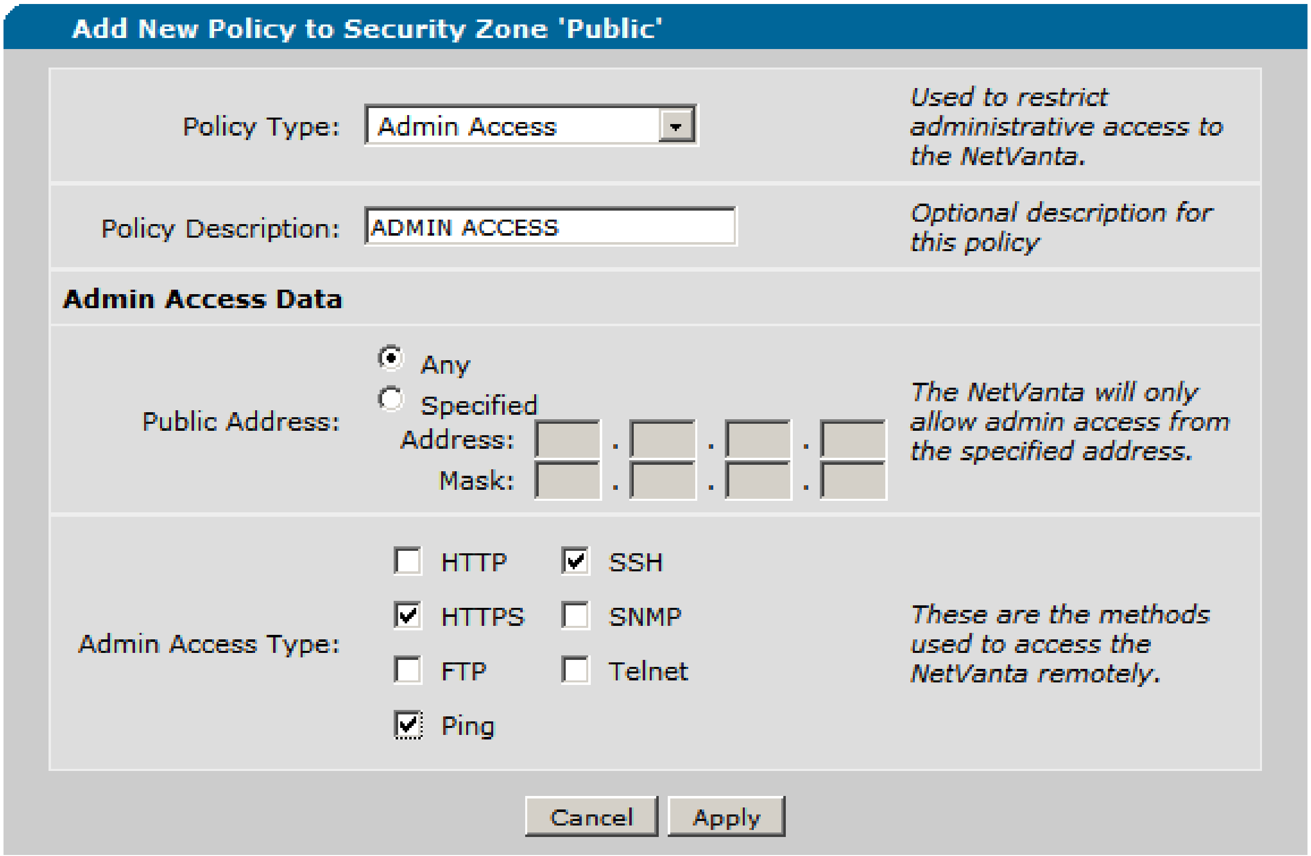
Policy Type: Admin Access ▾

Policy Types Explain

The following policy typ

Port Forward: All ' Security Zone to ac
po another Security Zor
configuration, a Port Forward will NAT a public IP
IP Address for all protocols and ports or just a su
and TCP/WWW. Typically used when Security Zo

When creating an Admin Access policy, one is able to limit the services accessed through the security zone. An administrator has the option of further limiting access to a specific address or range of addresses in which the traffic is sourced by utilizing the “Public Address” fields when creating the new policy. In the example below HTTPS, SSH, and PING are all allowed through the firewall sourced from any address.



Add New Policy to Security Zone 'Public'

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

Policy Description: ADMIN ACCESS — *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.

NOTE: Currently, the default configuration allows only HTTPS and SSH traffic through the Public security zone using the Admin extended access-list. In the web GUI, this policy will be labeled “Admin Access”. If your security standards require you to change the existing “Admin Access” policy, the default “Admin Access” policy should be removed if a new policy was created to be put in its place.

Leaving FTP unchecked will not affect remote phones from accessing the FTP service running on the unit as remote phones should have access to this service provided by the VPN Selectors. Please refer to Knowledge Base Article 2072 to check your configuration.

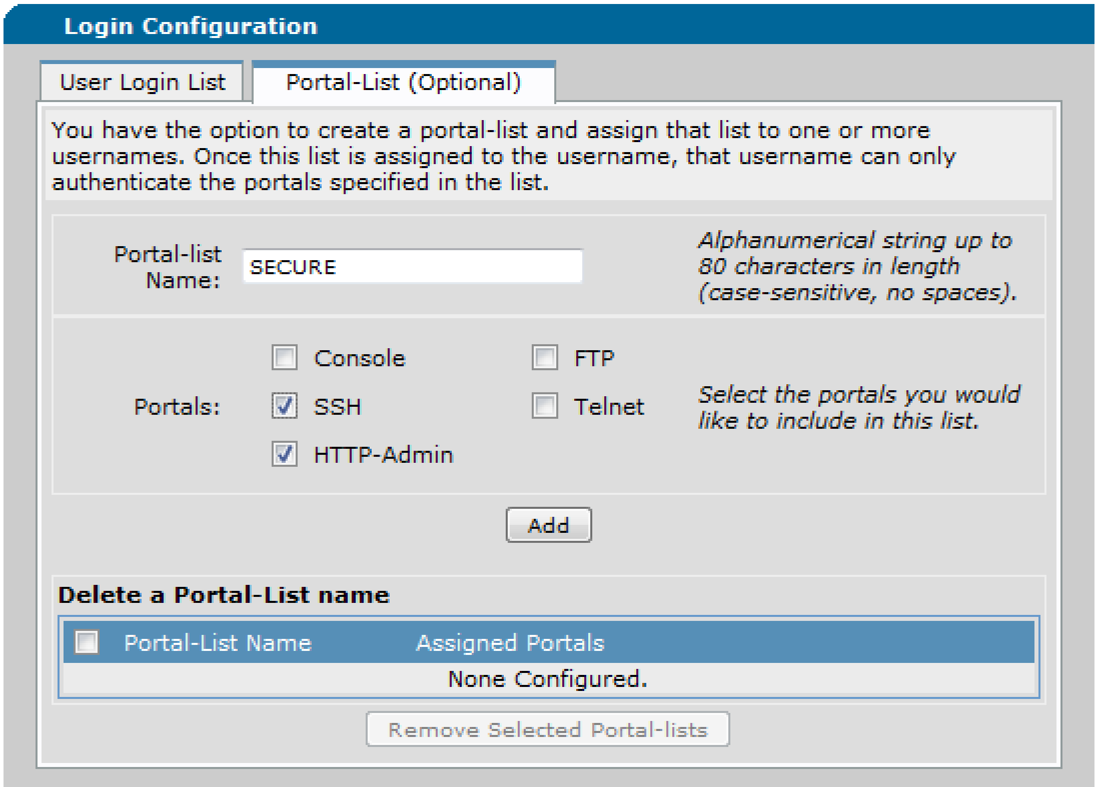
Featured below is the command line version of the extended access-lists and policy-class that would only allow SSH, HTTPS, and PING traffic for administrative access on the Public interface.

```
ip access-list extended ADMIN_ACCESS
  permit tcp any any eq ssh
  permit tcp any any eq https
  permit icmp any any
!
ip policy-class Public
  allow list ADMIN_ACCESS self
```

Using Secure Username/Password Practices

It is important to use passwords that are not based on dictionary words, as these can be easily cracked. However, phones that use FTP to download configuration files from the 7000 Series use the username/password combination `polycomftp/password`. By default, this password is configured globally in the unit's configuration. Portal-list can be utilized to segregate different username/password combinations for different services.

Portal-List configuration is under the Password Submenu of the System Menu in the web GUI. Under the Login Configuration section is the Portal-List tab. Under the Portal-List tab, an administrator can group different services to a particular Portal-List. In the examples below, the Portal-List `SECURE` was created to handle the usernames for SSH and HTTP-Admin access, and the Portal-List `PHONES` was created to handle the usernames for FTP access.



You have the option to create a portal-list and assign that list to one or more usernames. Once this list is assigned to the username, that username can only authenticate the portals specified in the list.

Portal-list Name: SECURE

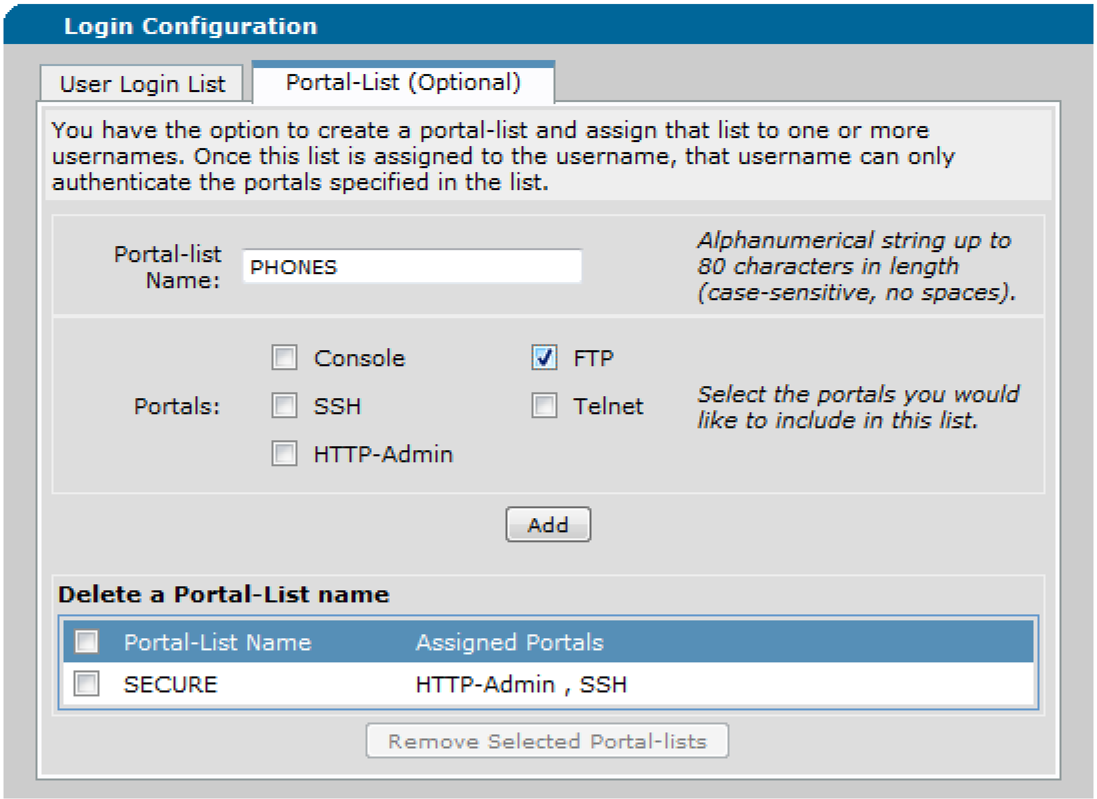
Alphanumerical string up to 80 characters in length (case-sensitive, no spaces).

Portals: □ Console □ FTP ☑ SSH □ Telnet ☑ HTTP-Admin

Select the portals you would like to include in this list.

Delete a Portal-List name

□	Portal-List Name	Assigned Portals
	None Configured.	



You have the option to create a portal-list and assign that list to one or more usernames. Once this list is assigned to the username, that username can only authenticate the portals specified in the list.

Portal-list Name: PHONES

Alphanumerical string up to 80 characters in length (case-sensitive, no spaces).

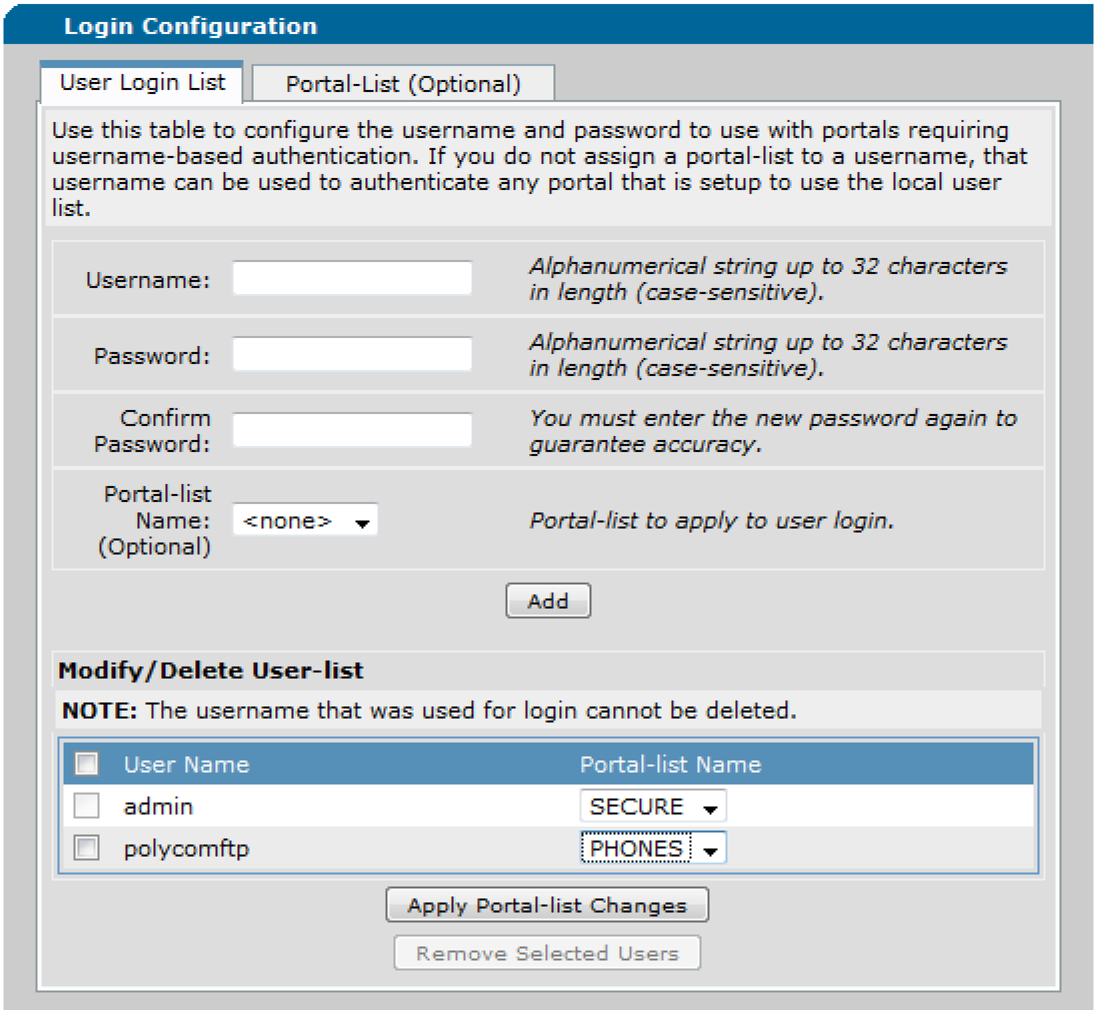
Portals: □ Console ☑ FTP □ SSH □ Telnet □ HTTP-Admin

Select the portals you would like to include in this list.

Delete a Portal-List name

□	Portal-List Name	Assigned Portals
□	SECURE	HTTP-Admin , SSH

Once the Portal-Lists are created, username/password combinations can be assigned to a particular service running on the unit. This is done under the Passwords Submenu of the System Menu. Under the User Login List tab, an administrator can assign a specific username to be used for authentication to the services listed under a specific Portal-List. In the example below, the username admin was added to the `SECURE` Portal-List, while the `polycomftp` username was added to a Portal-List called `PHONES`.



Use this table to configure the username and password to use with portals requiring username-based authentication. If you do not assign a portal-list to a username, that username can be used to authenticate any portal that is setup to use the local user list.

Username:		*Alphanumerical string up to 32 characters in length (case-sensitive).*
Password:		*Alphanumerical string up to 32 characters in length (case-sensitive).*
Confirm Password:		*You must enter the new password again to guarantee accuracy.*
Portal-list Name: (Optional)	<none>	*Portal-list to apply to user login.*

Modify/Delete User-list

NOTE: The username that was used for login cannot be deleted.

□	User Name	Portal-list Name
□	admin	SECURE
□	polycomftp	PHONES

Below is the command line configuration that would restrict the polycomftp/password to only be used on FTP and other logins to other services.

```
portal-list “PHONES” ftp
portal-list “SECURE” http-admin ssh
!
!
username admin portal-list “SECURE” password p4ssw0rd
username polycomftp portal-list “PHONES” password password
```

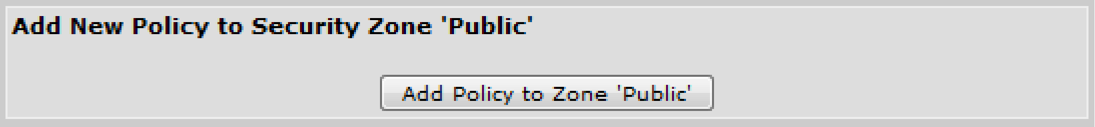
Allowing Only Known SIP User-Agents

It is possible for a malicious entity to hijack services on the 7000 Series if the SIP port is not restricted to only allow known user-agents. This is easily accomplished with an extended access-list. It is important to note that the AOS firewall can only use network addresses, host addresses, and hostnames to identify a source or destination. Some service providers will use SRV Records to identify their user-agents. The access-lists in AOS can use A Records but not SRV Records as a hostname. The command “show host” will allow you to see what the A Records the SRV Record is specifying if your service provider is using them. Below is an output of “show host” from the command line.

```
Name/address lookup uses domain name service
DNS Proxy is enabled
Default domain is test.network.adtran.com
Name servers are 10.19.211.34
Host                    Flags    Age       Type Priority  Address/Alias
_sip._udp.sip.test.n temp     267       SRV        20  sip1.adtran.com
_sip._udp.sip.test.n temp     267       SRV        30  sip2.adtran.com
sip1.adtran.com         temp     267       A           -  10.19.211.249
sip2.adtran.com         temp     267       A           -  10.19.211.245
```

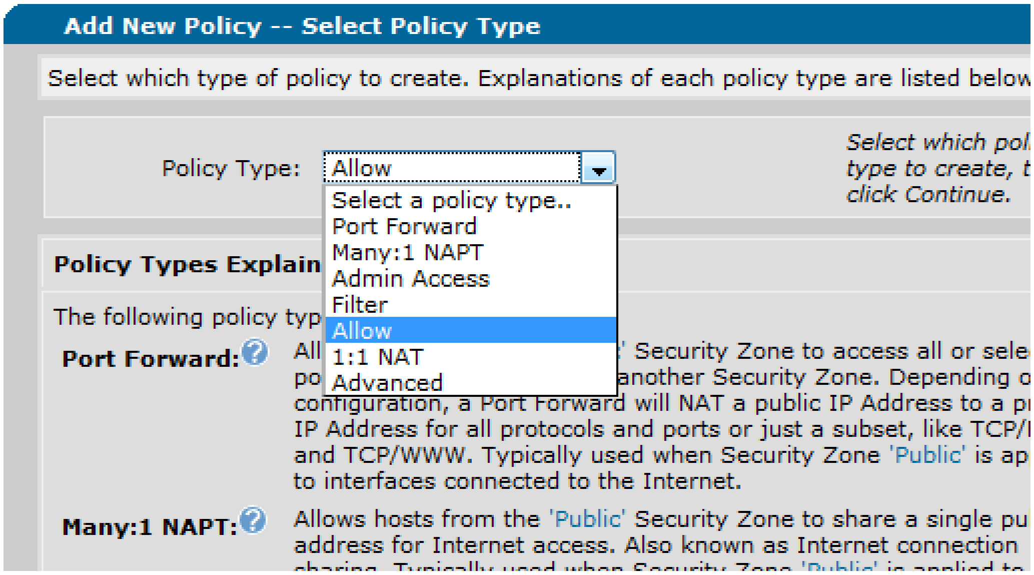
The output reveals that the SRV Record points to the two A Records: `sip1.adtran.com` and `sip2.adtran.com`. The two A Records can be used to formulate an extended access-list that will only allow these two SIP user-agents.

From the Security Zone Configuration Menu, the “Add Policy to Zone 'Public'” will need to be selected in order to begin adding a Policy for the SIP user-agents.



Add New Policy to Security Zone 'Public'

Since SIP user-agents are going to be allowed to be accessed through the WAN interface, an Allow will be the type of policy added to the security zone. When prompted for the Policy Type, select Allow from the Policy Type drop down menu.



Add New Policy -- Select Policy Type

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

Policy Type: Allow

Select which pol type to create, t click Continue.

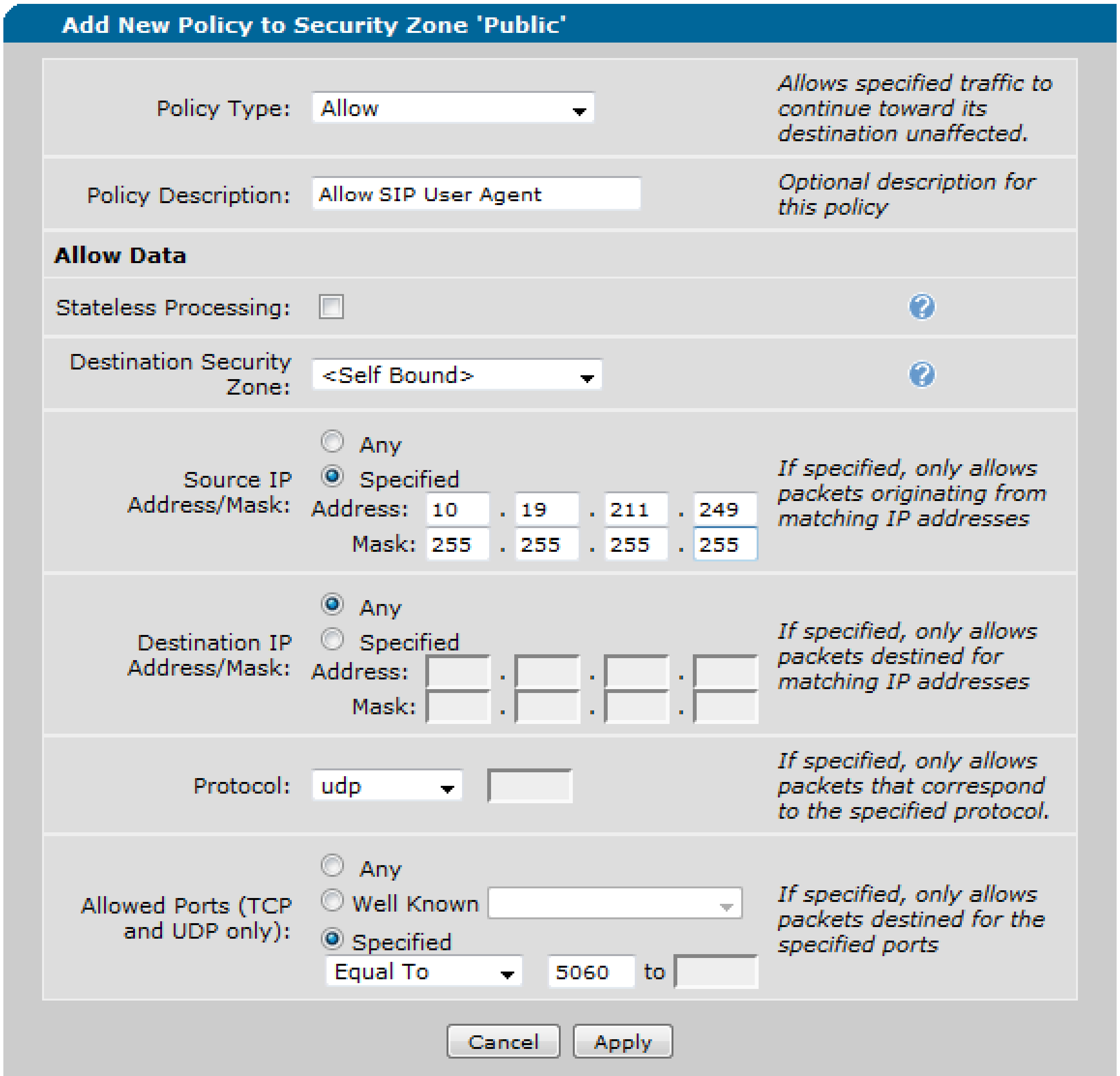
Policy Types Explain

The following policy typ

Port Forward: All ' Security Zone to access all or sele po another Security Zone. Depending o configuration, a Port Forward will NAT a public IP Address to a pr IP Address for all protocols and ports or just a subset, like TCP/I and TCP/WWW. Typically used when Security Zone 'Public' is ap to interfaces connected to the Internet.

Many:1 NAPT: Allows hosts from the 'Public' Security Zone to share a single pu address for Internet access. Also known as Internet connection

Below is an example of a Policy added to the Public security zone that would only allow communication with `sip1.adtran.com`. Note that from the web GUI, one can only specify an IP address when placing restrictions in a Policy. From the output of the “show host”, it was determined that sip1.adtran.com has an IP address of 10.19.211.249. Using this information, a <Self Bound> Policy was added to the Public security zone that allows traffic from host 10.19.211.249 on UDP port 5060.



Add New Policy to Security Zone 'Public'

Policy Type:	Allow	*Allows specified traffic to continue toward its destination unaffected.*
Policy Description:	Allow SIP User Agent	*Optional description for this policy*
Allow Data		
Stateless Processing:	□	
Destination Security Zone:	<Self Bound>	
Source IP Address/Mask:	○ Any ● Specified Address: 10 . 19 . 211 . 249 Mask: 255 . 255 . 255 . 255	*If specified, only allows packets originating from matching IP addresses*
Destination IP Address/Mask:	● Any ○ Specified Address: . . . Mask: . . .	*If specified, only allows packets destined for matching IP addresses*
Protocol:	udp	*If specified, only allows packets that correspond to the specified protocol.*
Allowed Ports (TCP and UDP only):	○ Any ○ Well Known ● Specified Equal To 5060 to	*If specified, only allows packets destined for the specified ports*

In this example with SRV records, the SRV record also list `sip2.adtran.com`. An additional Policy must then be added to allow communication to this server as well.

*NOTE: By default, the Public security zone allows SIP traffic from any source via the extended access-list SIP. This policy is named “SIP Service Provider Traffic” in the web GUI. After creating the needed policies to only allow SIP traffic from known user agents, the default “SIP Service Provider Traffic” policy should be removed.

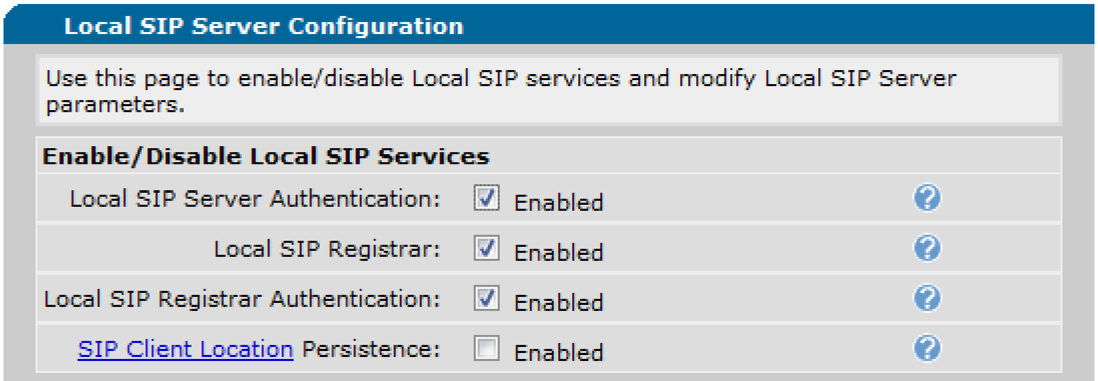
Below is an example of an extended access-list and policy-class that would only allow SIP traffic from these two user-agents done through the command line. Please keep in mind that network addresses, host addresses, or hostnames can be used when using the command line.

```
ip access-list extended SIP_TRUNKS
  permit udp hostname sip1.adtran.com any eq 5060
  permit udp hostname sip2.adtran.com any eq 5060
!
!
ip policy-class Public
  allow list ADMIN_ACCESS self
  allow list SIP_TRUNKS self
```

Using SIP Authentication

To further prevent hijacked services, the SIP Authentication framework can be utilized to more securely handle SIP transactions. The process uses the password configured for every SIP user. With SIP Authentication configured, the 7000 will challenge for the password for each request. It is important to note that prior to A2.04.00.E, the SIP Authentication Passwords were four character numeric values. In A2.04.00.E and higher, the password can be a sixteen character alpha-numeric value.

To enable SIP Authentication for both Registrations and Requests, the "Local SIP Server Authentication" and "Local SIP Registrar" check boxes must be selected under the "Local SIP Server Configuration" options under the "SIP Server Settings" Submenu of the Voice Menu.



Local SIP Server Configuration

Use this page to enable/disable Local SIP services and modify Local SIP Server parameters.

Enable/Disable Local SIP Services

Local SIP Server Authentication: ☑ Enabled

Local SIP Registrar: ☑ Enabled

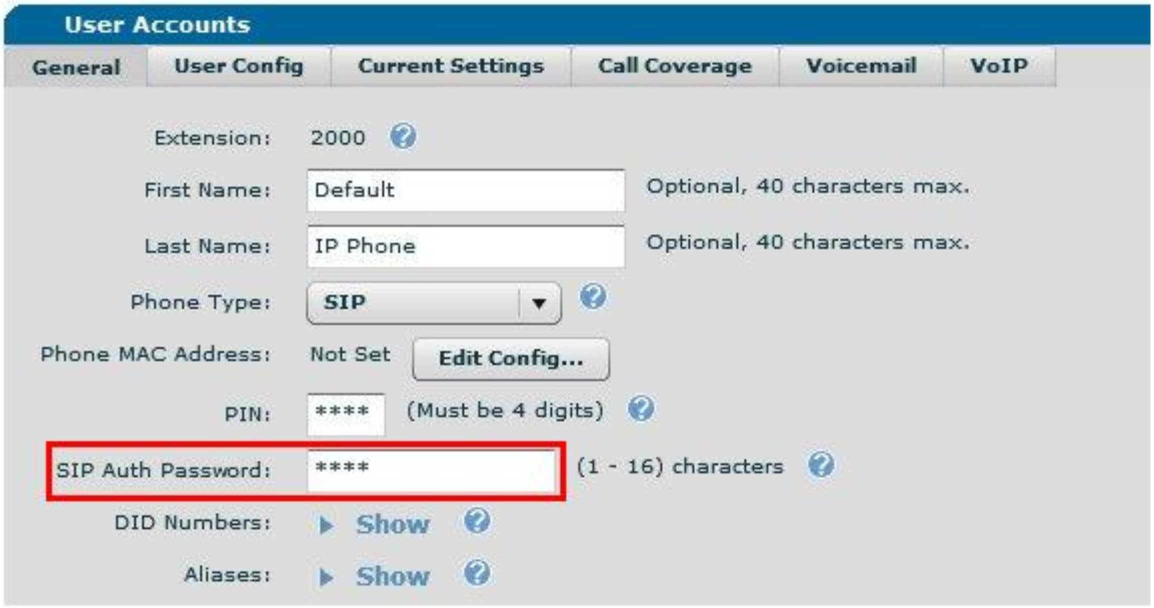
Local SIP Registrar Authentication: ☑ Enabled

SIP Client Location Persistence: □ Enabled

To configure the 7000 Series to use SIP Authentication via the command line, the following output needs to be added to the configuration.

```
ip sip authenticate
```

The authentication credentials for the phones are configured in the User Account Submenu of the Voice Menu. The image below shows the portion of the User Account page where the credentials are configured.



Extension: 2000

First Name: Default Optional, 40 characters max.

Last Name: IP Phone Optional, 40 characters max.

Phone Type: SIP

Phone MAC Address: Not Set

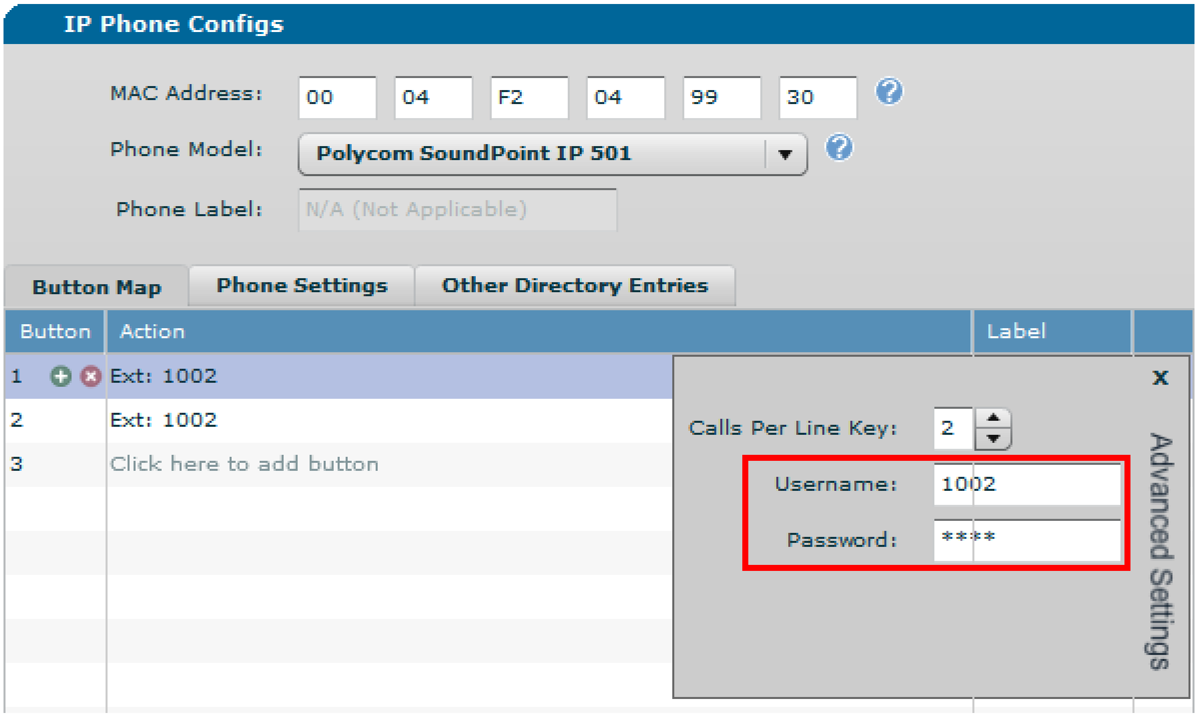
PIN: **** (Must be 4 digits)

SIP Auth Password: **** (1 - 16) characters

DID Numbers: ▶ Show

Aliases: ▶ Show

If the user account has a Phone Config associated with the User Account, the Authentication will need to be updated in the Phone Config that is associated with the User Account. SIP configurations can be edited under the IP Phone Configs Submenu of the Voice Menu. In the IP Phone Config page, the wrench shaped icon for the specific line will need to be clicked to display the Advanced Options. Below is an example of a Phone Config with the Advanced Settings displayed.



MAC Address: 00 04 F2 04 99 30

Phone Model: Polycom SoundPoint IP 501

Phone Label: N/A (Not Applicable)

Button	Action	Label
1	Ext: 1002	
2	Ext: 1002	
3	Click here to add button	

Calls Per Line Key: 2

Username: 1002

Password: ****