Vidyo Conferencing in Firewall and NAT Deployments

Vidyo Technical Note Section 1

NAT Introduction:

The VidyoConferencing platform utilizes reflexive addressing to assist in setup of Vidyo calls. Reflexive addressing is used when the end user is using VidyoDesktop to make a call from behind a NAT. This happens automatically and transparently to the user.

Reflexive addressing requires the VidyoRouter have a public IP address in order to provide NAT traversal of the Vidyo endpoints. Therefore if the VidyoRouter itself is placed behind a NAT, reflexive addressing will not function properly. When the VidyoRouter is behind a NAT, the preferred configuration will use DNS to resolve properly to the server IP addresses. In some cases, a combination of the ICE and STUN protocols are used to determine the Public IP translated to the VidyoRouter. This document outlines how to configure the VidyoConferencing system to work when placed behind a NAT and still allow users to connect from the public Internet.

There are three basic areas that need to be addressed in order to configure the VidyoConferencing system to operate from behind a NAT. Those are below and will each be explained in detail in the following sections.

- Firewall/NAT Configuration
- DNS configuration
- Vidyo Server configurations

There are several options to deploy the VidyoConferencing equipment in order to provide a service for the entire organization:

- Place the VidyoPortal/VidyoRouter on a public Static IP address
- Place the VidyoPortal/VidyoRouter in a private network having a private Static IP address within the organization
- Place the VidyoPorta/VidyoRouter within the DMZ with a private Static IP address

This document describes how to configure scenarios 2 and 3 for purpose of FW and NAT traversal in section #3. In this section, we will focus on the first scenario.

When deployed with a public IP address and no “server side” firewall or NAT, the Portal and Router are reachable by either IP address or DNS name. This is the simplest scenario, since we are only concerned with the NAT and firewall at the far-end (client side).

Generally speaking, the client side firewall will most often permit any connection that initiates on the Private LAN to any outside network destination. In some cases, the local firewalls must be configured to allow each application from the inside to the Public Network.

Vidyo Conferencing Firewall Ports

Vidyo Technical Note Section 2

To register to the Vidyo Portal and place calls, the client side connection must be open to the VidyoPortal on these TCP/UDP ports:

VidyoDesktop and VidyoRoom connectivity to VidyoPortal and VidyoRouter		
TCP Port 80	HTTP: Outbound to Portal	Client to Portal authentication and GUI
TCP Port 443	HTTPS: Outbound to Portal (optional)	Optional for SSL connection to Portal
TCP Port 17992	EMCP: Outbound to Portal	Client connection to VidyoManager
TCP Port 17990	SCIP: Outbound to Portal	Client connection to VidyoRouter
UDP Ports 50,000 - 65,535	RTP/sRTP/RTCP: Bi-Directional to/from VidyoRouter	Audio and Video Media from participants (6 ports per participant). RTP and RTCP pair for each audio, video, and data collaboration stream.
UDP Timeout	General Comment	Change from Default (i.e. 0:02:00 2 minutes) to something larger (i.e. 3:00:00 – 3 hrs) to avoid call timeouts

NOTES:

1. *Some Firewalls have a UDP default timeout. On the Cisco PIX Firewall, for example, if the UDP timeout is not changed then the call will drop in exactly 2 minutes and the Vidyo client(s) would have to reconnect.*
2. *The VidyoPortal also has an embedded VidyoRouter running on the same appliance. It is possible these will share the same IP address.*
3. *Many newer Consumer home Firewalls have SPI (Statefull Packet Inspection) active by Default. This may need to be disabled for performance reasons.*

To enable remote management access to the Vidyo servers, the following TCP/UDP ports need to be opened through any server-side firewall or NAT:

Management Access to VidyoPortal, VidyoRouter, VidyoManager and VidyoGateway		
TCP Port 80	HTTP: Inbound to Server	Web Access to VidyoPortal and VidyoRouter
TCP Port 443	HTTPS: Inbound to Server (optional)	Secure Web Access to VidyoPortal and VidyoRouter
TCP Port 2222	SSH: Inbound to Server	SSH access to VidyoPortal and VidyoRouter

The following services are optional on the VidyoPortal, VidyoRouter and VidyoGateway, and require the following TCP/UDP ports if they are used:

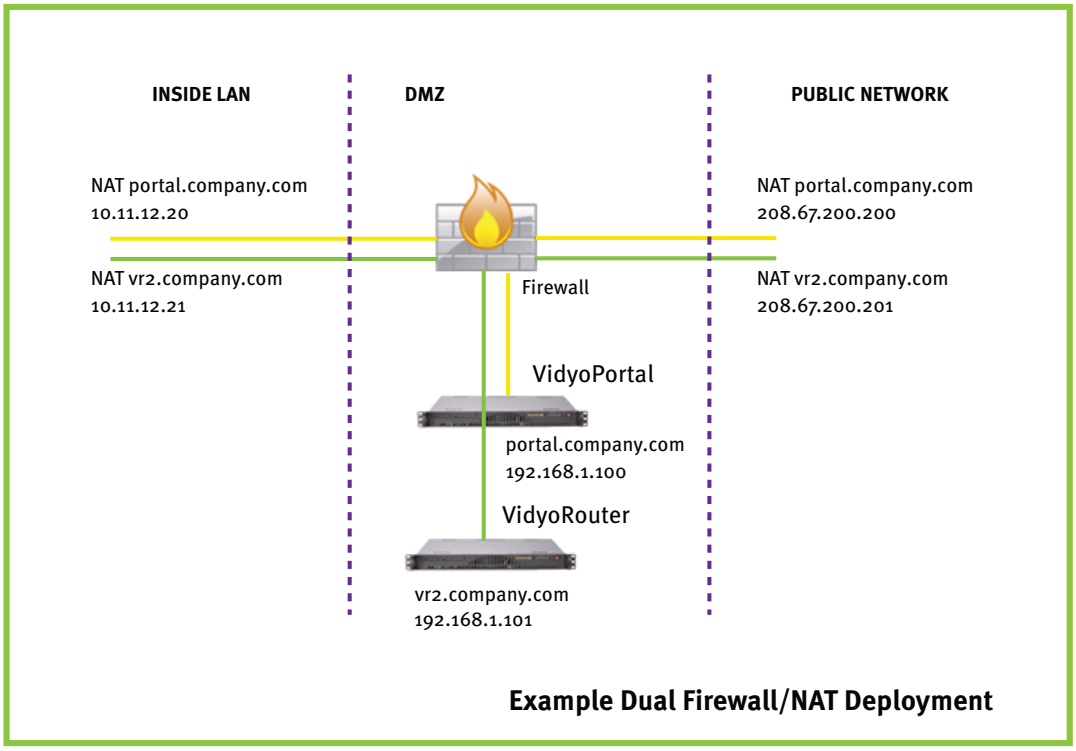
Other Services on VidyoPortal, VidyoRouter, and VidyoGateway		
UDP Port 123	NTP: Outbound from Server	Network Time Protocol
TCP Port 25	SMTP: Outbound from Server	Email notifications for new user accounts, lost passwords, and licensing notifications. VidyoPortal Only
TCP Port 3306	MySQL: Inbound to Server	Call Detail Record (CDR) access for billing systems. VidyoPortal Only
TCP PORT 389	LDAP: Outbound from Server	Optional authentication to LDAP/Active Directory
TCP Port 636	LDAPS: Outbound from Server	Secure LDAP. Optional authentication to LDAP/Active Directory
UDP Port 161 - 162	SNMP: Inbound to Server	Basic SNMP functions
TCP and UDP 3478	Stun: Bi-directional to/from Server	Optional only if using STUN for NAT traversal.

Steps to Configure VidyoConferencing in Firewall/NAT

Vidyo Technical Note section 3

Summary Introduction:

In this document, we will discuss the steps to configure the VidyoPortal and VidyoRouter in a NAT'd firewall or DMZ environment. For this, the Vidyo servers are installed either fully behind a firewall on the corporate LAN, or installed in the firewall DMZ with one or more NAT'd addresses and Static IP address. See the figure below for example Firewall/NAT topologies.



Example Dual Firewall/NAT Deployment

NOTE: *This document does not apply to deployments using VidyoProxy. If VidyoProxy is being used seperate instructions are available. The two deployment scenarios can coexist.*

For this configuration, there are three tasks to accomplish:

- Firewall/NAT Configuration
- DNS configuration
- Vidyo Server configurations

NOTE: *actual steps to configure the Firewall/NAT and DNS environments are outside the scope of this document, and will vary based on the Firewall/NAT and DNS servers to be used. This document will focus on the concepts only.*

Firewall/NAT Configuration:

Allocate an external (Public) Static IP address to use for the VidyoPortal/Routers and configure a one-to-one NAT statement to the desired private or DMZ Static IP address. In cases where the internal network is NAT'd to the DMZ, a similar static NAT must be configured from the Static private LAN to the Static DMZ server addresses.

With the NAT configured, we will need to permit access to the TCP and UDP ports needed by the Vidyo solution. In the firewall access-control list, be sure to open these ports as a minimum:

- Inbound TCP Port 80 - web access to the portal and administrative interfaces
- Inbound TCP Port 443 - optional for SSL secured web access and calls
- Inbound TCP Port 17992 - EMCP protocol client connection to VidyoManager/VidyoPortal (configurable)
- Inbound TCP Port 17990 - SCIP protocol client connection to VidyoRouter (configurable)
- Bi-Directional UDP Port 50000 – 65535 - RTP/SRTP media, one RTP/RTCP port pair for each audio, video, data sharing stream in the conference

Last, it's beneficial to check the UDP timeout for the firewall. Some firewalls will limit the duration of UDP port openings, and this may cause the calls to terminate prematurely.

DNS/FQDN Configuration:

For the firewall NAT traversal to properly communicate between servers and clients through the IP address translations, we will need to configure DNS properly for hosting the Vidyo servers in the DMZ or behind the NAT. In firewall deployments, Vidyo communicates based on DNS information rather than exposing IP addresses.

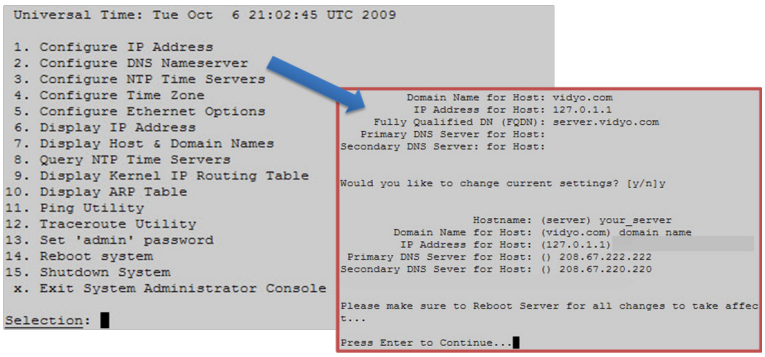
The DNS servers for both inside and outside networks (if different) will need to be configured for the Vidyo server's Fully Qualified Domain Name - FQDN. In our example, we are assuming the server is using the FQDN of portal.company.com.

Configure both public and private DNS records for the server FQDN. Regardless where the client resides, it needs to match the same hostname to the proper IP address, public Internet clients resolve to the outside NAT address, and internal WAN clients resolve to the inside IP address (either real IP or NAT inside address if double NAT is used) when they access the server URL. To test, from both the inside and outside subnets, ping to the server URL.

Vidyo Server Configuration:

With the firewall configured for the proper NAT statements, the required TCP and UDP ports opened, and the DNS entries configured, you can move on to the configuration in the Vidyo servers to enable using DNS and to route calls properly between the LAN and Public Network.

You must configure the VidyoPortal and Routers to be aware of their DNS hostnames. This is done in the system console menu, option #2.
Set the server local hostname and domain name as well as working DNS server addresses.

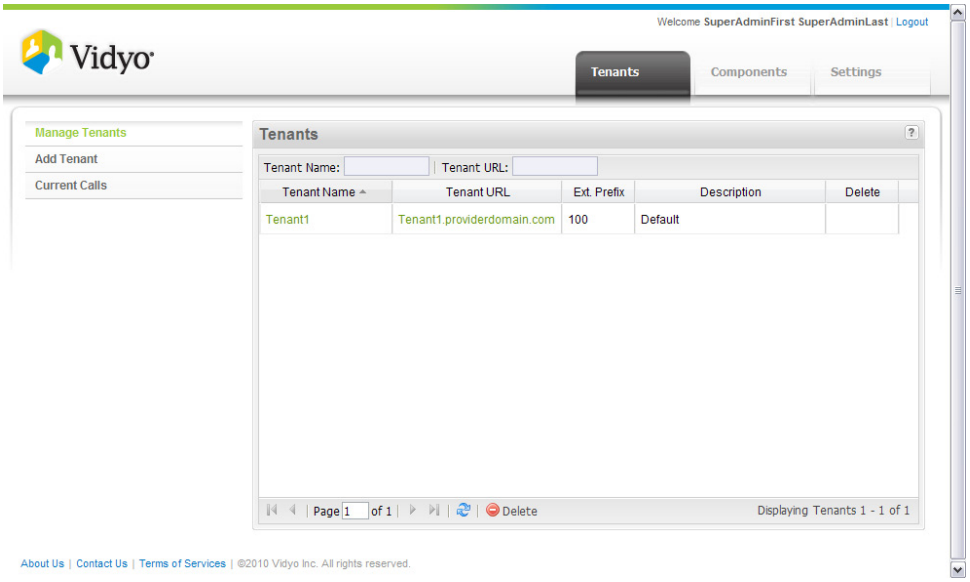


NOTE: *It's very important to note that the IP address listed in this screen (127.0.1.1) must remain intact for proper communications.*

In a firewalled installation, the VidyoManager, VidyoRouter(s) and VidyoProxy(s) need to be configured to use the server FQDN instead of the IP addresses.

Tenant URL(s):

- Login to the portal Super Admin pages, go to **Tenants** TAB / **Manage Tenants**:

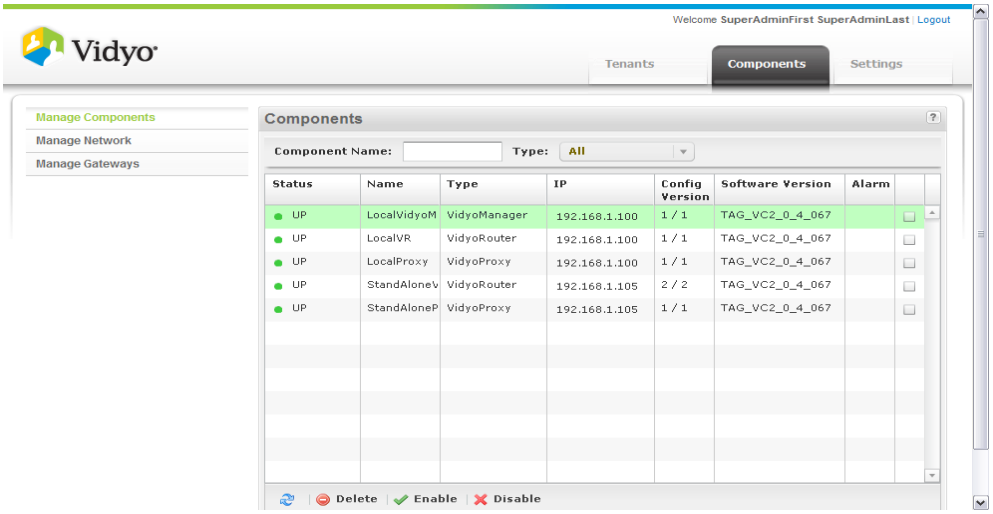


- Ensure that each Tenant (inluding the Default Tenant), is using a FQDN for **Tenant URL**.

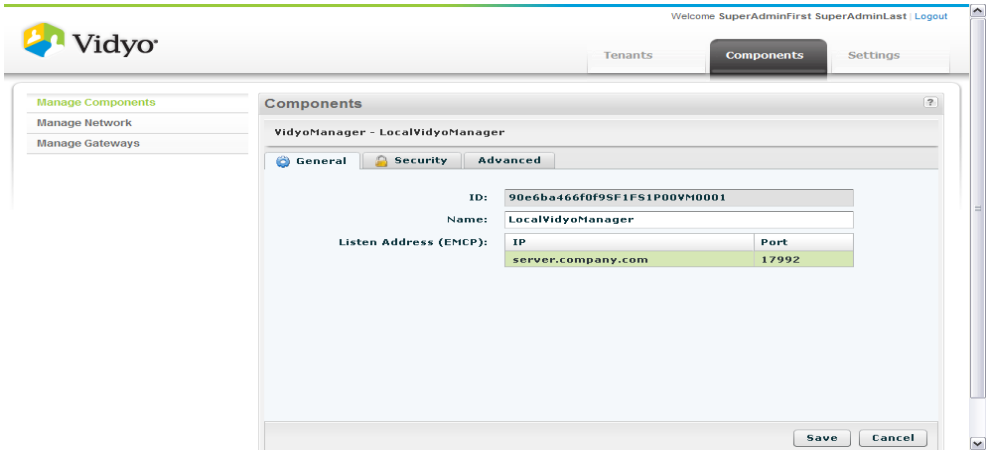
VidyoManager Configuration:

You will need to configure the Vidyomanager to be addressed by it's FQDN.

- Login to the portal Super Admin pages, go to **Components** TAB / **Manage Components:**



- Double-Click the **Status** of the VidyoManager entry:

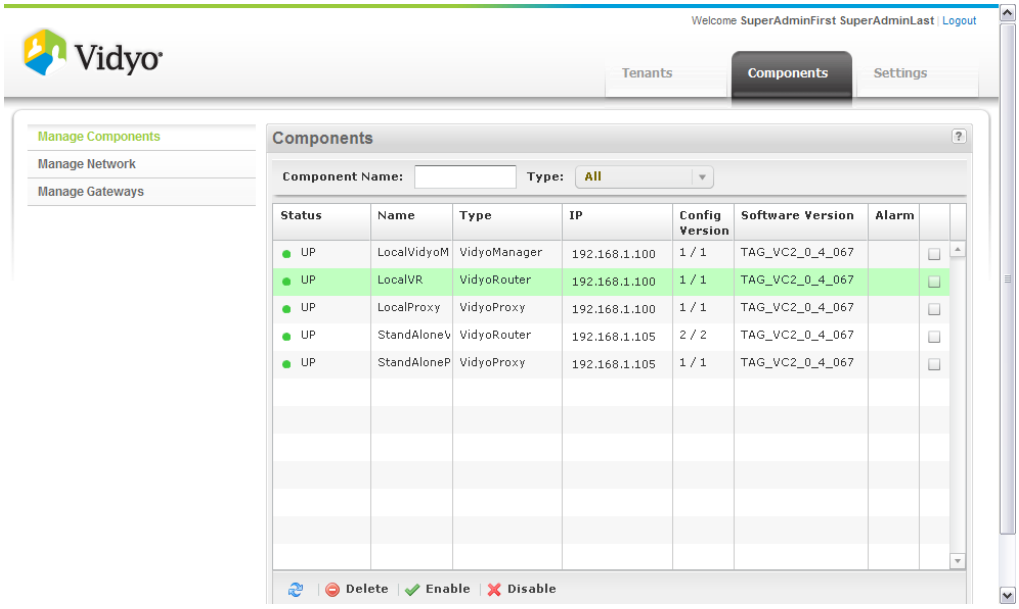


- Under **Listen Address (EMCP)**, edit EMCP address (VidyoManager address) by clicking the text in the **IP** column, and enter the server FQDN here - EX: portal.company.com**.**
- The EMCP **Port** column is where you can set the EMCP (VidyoManager) TCP Port. The default value for v2.0 is **17992**, the deafult in v1 was 10000. Edit the port according your needs and firewall rules.
- Click **Save** button.

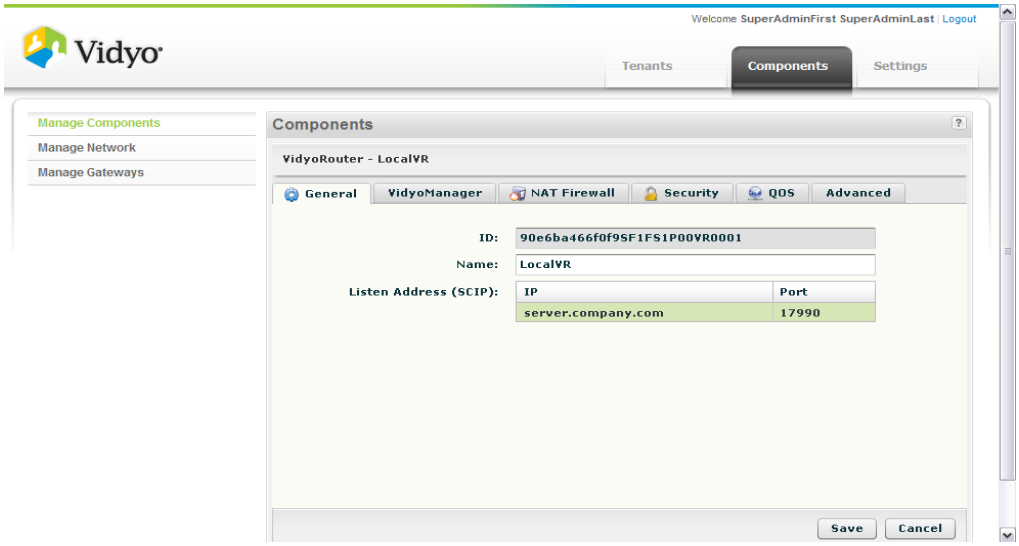
VidyoRouter(s) Configuration:

Next, you will need to configure each VidyoRouter to be addressed by it's FQDN.

- Return to the portal Super Admin pages, go to **Components** TAB / **Manage Components**:



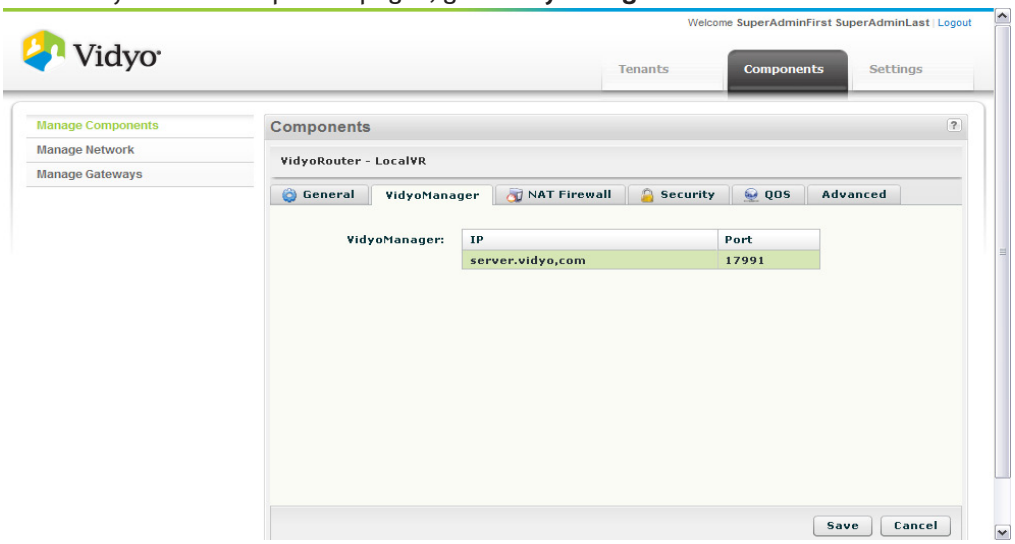
- Double-Click the **Status** of the local (embedded) VidyoRouter entry:



- Under **Listen Address (SCIP)**, edit SCIP address (VidyoRouter signaling address) by clicking the text in the **IP** column, and enter the server FQDN here - EX: portal.company.com.
- The SCIP **Port** column is where you can set the SCIP (VidyoRouter) TCP Port. The default value for v2.0 is **17990**, the deafult in v1 was 50000. Edit the port according your needs and firewall rules.

Next, you will need to configure the VidyoRouter to address it's VidyoManger by FQDN.

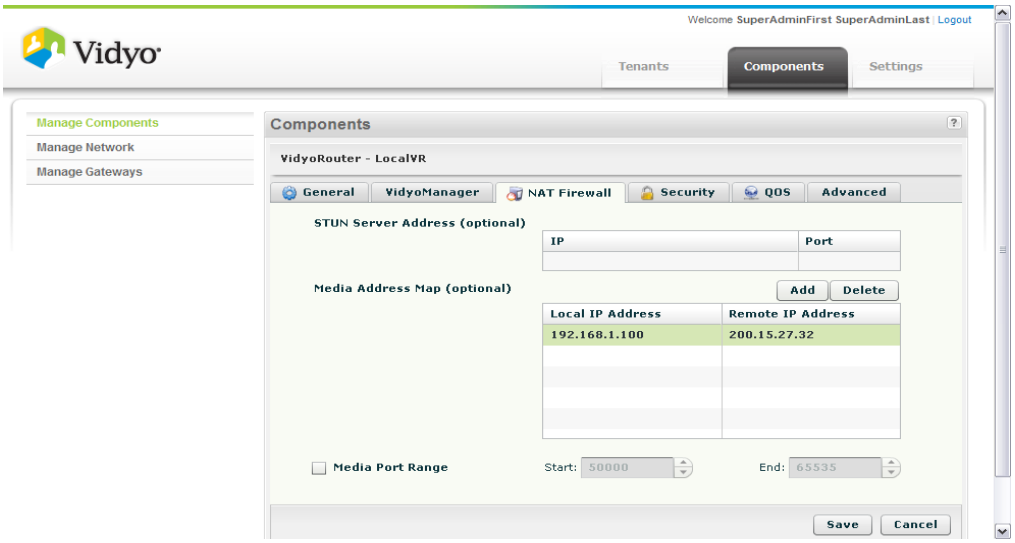
- In the VidyoRouter Component pages, go to **VidyoManger** TAB:



- Under **Vidyo Managers**, edit **IP** address by clicking the text in the **IP** column, and enter the server FQDN here - EX: portal.company.com.

Next, you will need to configure the VidyoRouter Media Mapping from private to public addresses.

- In the VidyoRouter Component pages, go to **NAT Firewall** TAB:



- Under **Media Address Map**, click **Add** button and enter each NAT translation required.
- For each NAT map, enter the **Local IP Address** (private) and **Remote IP Address** (public); the inside/outside NAT addresses needed.
- If there is a NAT from the private LAN towards the DMZ, you will need a media map rule for that.
- Click **Save** button.

In deployments where there is a dual NAT, one NAT from the Public Network to the server, and one from the private LAN to the server, there will be two Media Map statements.

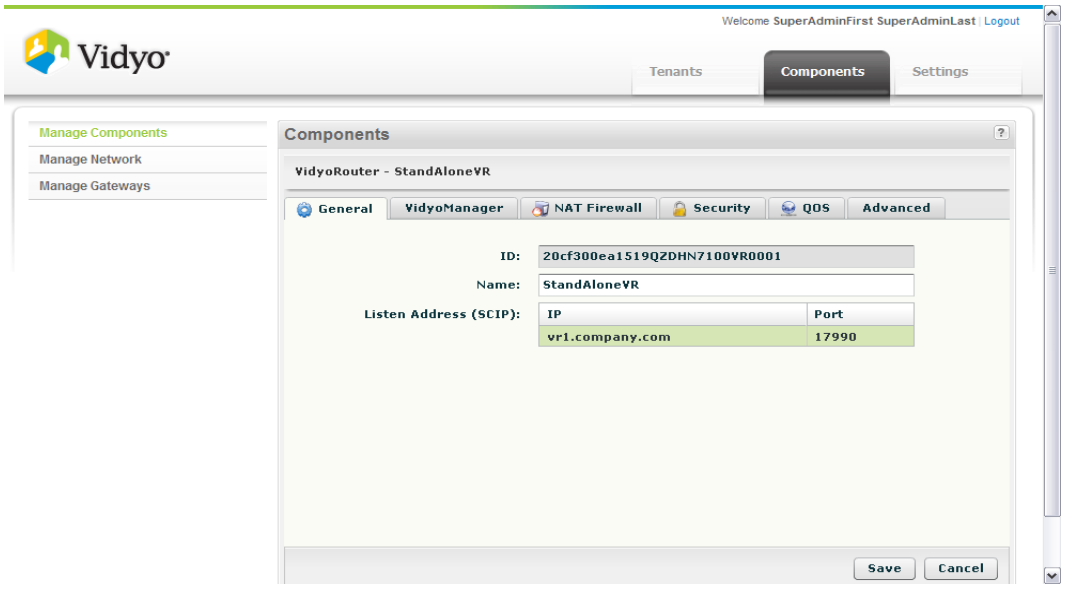
As an alternate method to Media Address Mapping, you can choose to use a public STUN server. To use a STUN server, enter the IP or URL and Port of the public STUN server you wish to use. The default STUN port is 3478. Vidyo hosts a public STUN server at: stunusa.vidyo.com. Using a STUN server instead of Media Address Maps is needed when the Vidyo server is hosted behind multiple layers of NATs.

DO NOT configure both Media Address Maps and STUN, only choose one method. Configuring both will cause your system to malfunction.

*REPEAT for each additional StandAlone VidyoRouter in your VidyoConferencing system.

Each StandAlone VidyoRouter server requires a unique and seperate FQDN to the Portal server. Use each server's unique FQDN for the SCIP address on each VidyoRouter configuration.

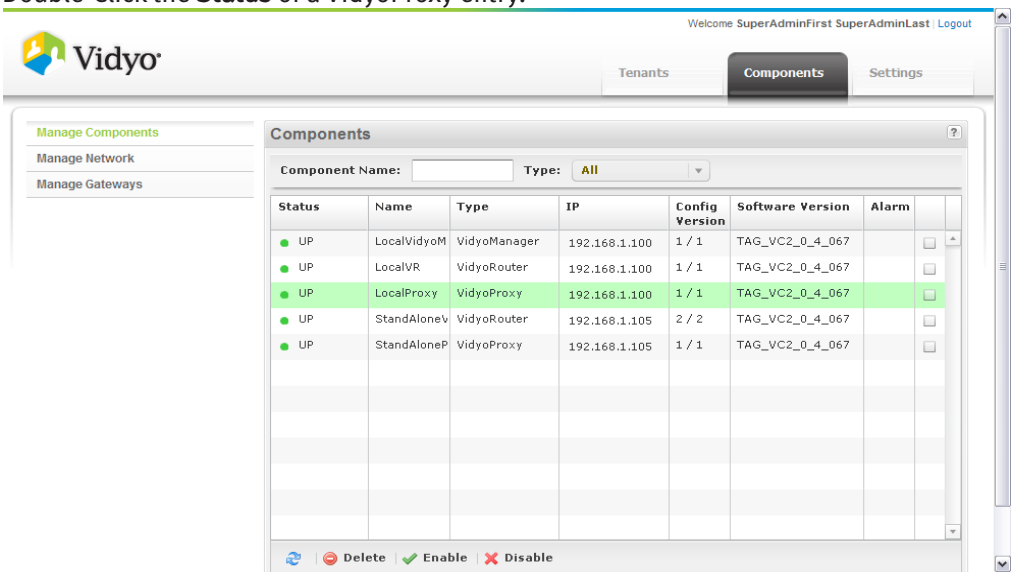
EX: vr1.company.com, vr2.company.com, etc.



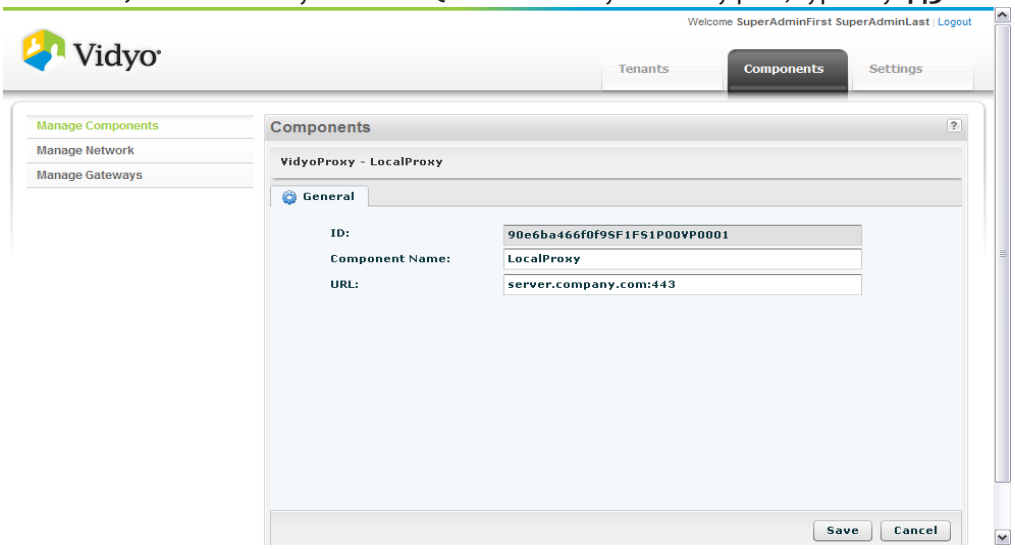
VidyoProxy(s) Configuration:

Next, you will need to configure each VidyoProxy to be addressed by it's FQDN.

- Return to the portal Super Admin pages, go to **Components** TAB / **Manage Components**:
- Double-Click the **Status** of a VidyoProxy entry:



- Under **URL,** enter the Proxy server's FQDN followed by the Proxy port, typically **443**.



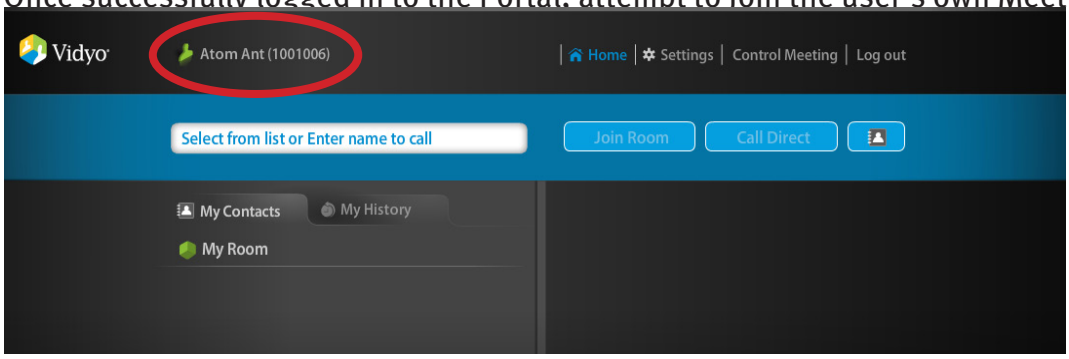
- Press **Save** button.

***REPEAT for each additional StandAlone VidyoProxy in your VidyoConferencing system.**

Use each server's unique FQDN for the address on each VidyoProxy configuration. You can use the same FQDNs as each StandAlone VidyoRouter uses that is hosting the Proxy - EX: vr1.company.com, vr2.company.com, etc.

With the Firewall/NAT, DNS and VidyoServer configurations completed, you can test the solution.

- From both sides of the firewall/NAT, attempt to login to the VidyoPortal as a Normal user account. If the EMCP is traversing properly, the person icon in the upper left of the portal user page will turn **green**. If the icon remains grey, then either the EMCP address or port is not configured properly in the VidyoManager configuration, or the port is not configured correctly at the firewall/NAT.
- Once successfully logged in to the Portal, attempt to Join the user's own Meeting Room



('My Room'). If a 'failed to Join conference' or 'failed to Join router' error message is received, then either the VidyoRouter SCIP address or port is not configured correctly in the VidyoRouter configuration, the port is not configured properly at the firewall/NAT, or the Portal server or client PC is unable to resolve the Router's FQDN.

- Ensure that media connections succeed (send and receive video). Once successfully joined to the meeting room, you should see loopback video if you are the only participant in the room, or the video from other participants. If you receive loopback video, then it means the media is traversing in both directions. If you receive another participant's video, ask them if they are receiving your video..if both sides are receiving each other's video, then that too means media traversal is working in both directions. If media traversal does not take place, then the UDP port range is not properly configured at the firewall/NAT.
- Be sure to test from both the Inside LAN and from the Public Network by using the same URL - EX: http://portal.company.com.
- Also if multiple Media Address Maps, test from each Remote network segment.