ABP International, Inc.
1850 Crown Dr.
Suite 1112
Dallas, TX 75234

Phone (972) 831-1600
sales@abptech.com
support@abptech.com

NATPASS™

FIREWALL AND SESSION BORDER CONTROLLER
FOR SIP BASED VOIP NETWORKS

This Firewall & Session Border controller software is a product developed by Xcast Lab and is marketed as a standalone product by ABP International, Inc.

NATPass™ is a Trademark of ABP International, Inc.

Table of Contents

Introduction

The NATPass™ Firewall Controller is a session border controller designed to be a simple solution for VoIP service providers to deploy. NATPass™ addresses the need for customers who are behind Nets or firewalls to access communication services.

NATPass™, by design, is not a multi-protocol solution. It is bound only to SIP and uses specific features of SIP to increase performance, reliability, and ease of maintenance. NATPass™ is designed to work as an intermediary between endpoint devices such as SIP Phones and SIP Proxies also known as Registrars. NATPass™ supports T.38 allowing reliable faxing over IP. NATPass™ is a pure software solution, which provides unlimited scalability at the lowest cost.

How It Works

NATPass™ works much like a traditional SIP Proxy. It shares many of the same features, but utilizes SIP to bypass NAT. This is why it is often referred as Outbound Proxy in configuration of majority of end user devices. Firewall Controller's job is to discover the type of NAT that a device is behind and substitute SIP Headers as well as SDP parameters in order to bypass NAT in the most efficient way.

Diagram 1 VoIP Call Release Examples

Example A: Media Release to SIP Endpoints Located Behind Separate Firewalls

Example B: Media Release to SIP Endpoints Located Behind the Same Firewalls
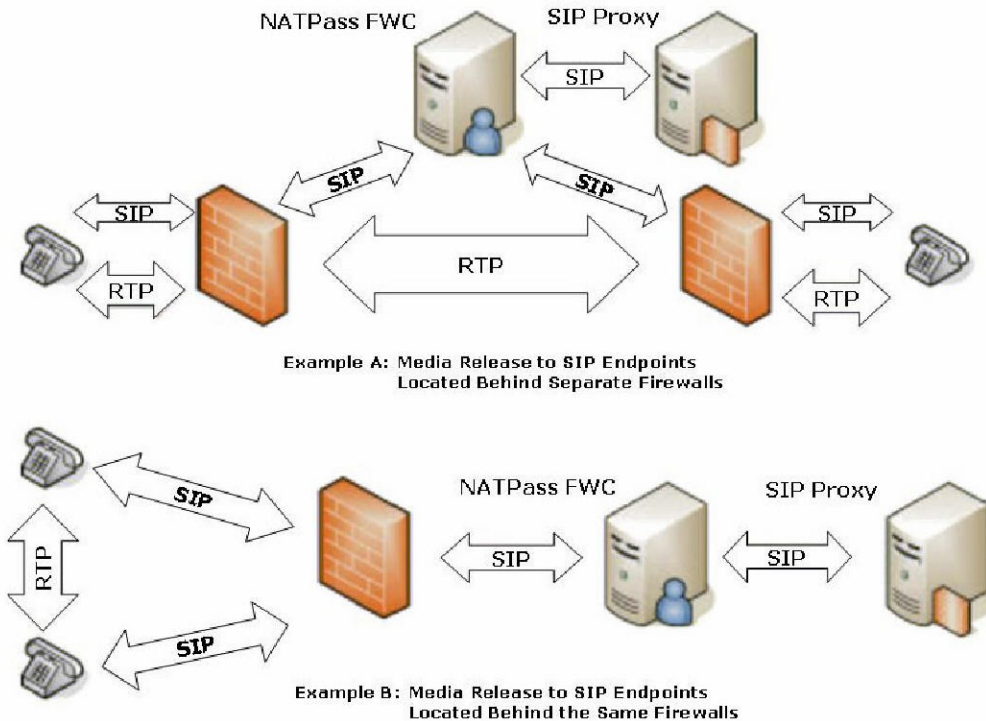
NATPass™ is optimized to release RTP stream to endpoint SIP devices whenever is possible. There are some conditions where releasing RTP is not possible. These conditions are usually related to certain types of NAT, IP phones or firewall configurations of calling parties. NATPass™ Firewall Controller handles these calls transparently to user. No changes in setup required since all call are individually checked for ability to release media and handled accordingly.

RTP stream released to endpoints is beneficial because voice traffic can be flowing between two devices using the shortest available route. In many cases it lets to improvement of quality of service especially if both parties are located on he same Local Area Network (LAN). At the same time very light SIP traffic is still flowing through the Firewall Controller and SIP Proxy allowing for applications to control call setup, disconnection, and routing (see Diagram 1).

When RTP stream is not released to endpoints it continues to flow through NATPASS™ together with signaling (see the diagram 2). This causes service provider additional bandwidth utilization and may create quality of service degradation due to latency introduced by going through additional hopes from user A to user B. Nevertheless, more often then not, benefits of traversing NAT Firewalls can outweigh the detriments listed above.

The other feature of NATPass™ is the ability to rectify SIP protocol bugs that appear in other vendors' devices and software. Engineers test and certify various SIP phones, IADs, gateways, etc… If they find the bug in the vendor's SIP implementation they can mangle the packets to correct the problem before it goes to actual proxies, applications, and other SIP endpoints. Devices that needed NATPass™ SIP correction are listed in the configuration file as broken devices until vendor doesn't release a fix (see more about broken devices in the Configuration section).

Diagram 2 Media is not Released to SIP Endpoints
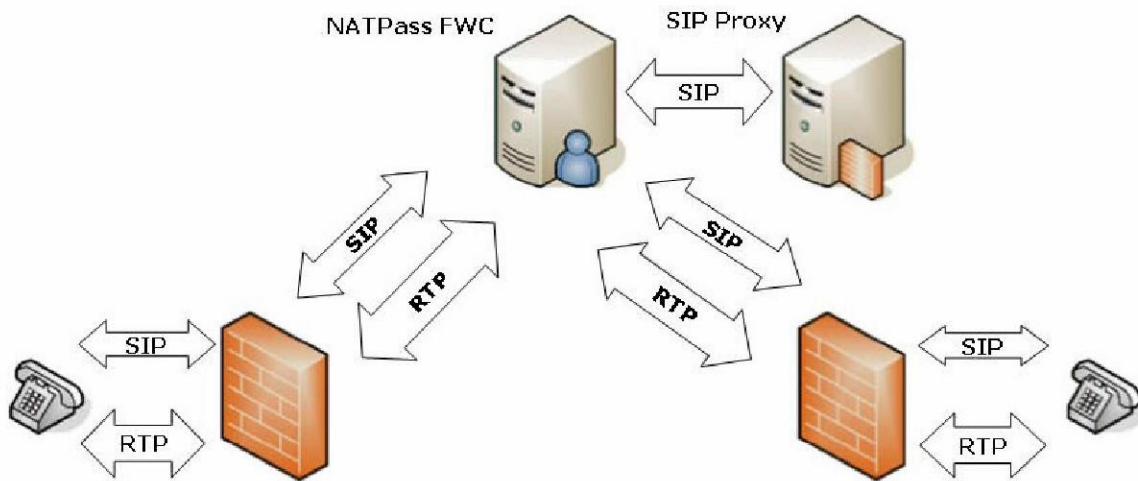
Example A: RTP Traffic is Forced to Travel
through NATPass Firewall Controller

In order for NATPass™ Firewall Controller to work properly, SIP PROXIES associated with this service should support SIP registration. The proxy could be specified as an IP or a domain name. In the latter case NATPass™ can perform simple DNS look ups or DNS SRV queries

☞ **Note:** *If your PROXY does not support registration, NATPass™ Firewall Controller will enable only outbound calls. You will **not** be able to receive inbound calls.*

Getting Started

NATPass™ runs on Linux all Red Hat and SUSE versions 9.0 or above. You need to become user *natpass* to perform administration on the Firewall Controller. And while it is possible to manage software as user *root,* it is not recommended for security reasons.

Installation

To Install

1. Download file NATPass.*LinuxVersion.PackageVersiion.*tgz from

   http://www.abptech.com (Products -> Nat traversal -> Far-End Nat traversal) or from http://www.natpass.com

2. Extract installation files by running:

   $ tar zxvf NATPass_LinuxVersion_PackageVersiion.tgz

```
drwxr-xr-x    2 root     root         4096 Jan 24  2003 src
[root@SipxchangePBX local]# tar zxvf NATPass_Redhat-05.06.27.tgz
NATPass_Redhat/
NATPass_Redhat/etc/
NATPass_Redhat/etc/rc.d/
NATPass_Redhat/etc/rc.d/init.d/
NATPass_Redhat/etc/rc.d/init.d/natpass-init
NATPass_Redhat/etc/logrotate.d/
NATPass_Redhat/etc/logrotate.d/natpass
NATPass_Redhat/misc/
NATPass_Redhat/misc/ld.so.extra
NATPass_Redhat/Readme.txt
NATPass_Redhat/natpass/
NATPass_Redhat/natpass/bin/
NATPass_Redhat/natpass/bin/natpass
NATPass_Redhat/natpass/bin/natpass_ctl
NATPass_Redhat/natpass/cfg/
NATPass_Redhat/natpass/cfg/natpass.cfg
NATPass_Redhat/natpass/lib/
NATPass_Redhat/natpass/lib/libACE.so.5.4.0
NATPass_Redhat/natpass/lib/libACE.so
NATPass_Redhat/natpass/logs/
NATPass_Redhat/natpass/logs/old/
NATPass_Redhat/natpass/rings/
NATPass_Redhat/natpass/rings/rbt.pcm
NATPass_Redhat/natpass/rings/r1.pcm
NATPass_Redhat/natpass/rings/ring.pcm
NATPass_Redhat/natpass/rings/24.pcm
NATPass_Redhat/natpass/rings/busy.pcm
NATPass_Redhat/uninstall-natpass.sh
NATPass_Redhat/install-natpass.sh
NATPass_Redhat/ChangeLog.txt
[root@SipxchangePBX local]# ll
```

Sample output for Redhat

3. Change directory to NATPass™ directory under /usr/local/

   On the example above would be "$ cd usr/local/NATPass_Redhat"

4. Become Super User (root) by running:

   $ su   (Enter the roots password at the prompt as requested)

5. Install software as a Super User (root) by running:

   # ./install-natpass.sh

```
-rwxr-xr-x    1 1000     users        300 Feb 23  2004 uninstall-na
[root@SipxchangePBX NATPass_Redhat]# ./install-natpass.sh
building file list ... done
./
bin/
bin/natpass
bin/natpass_ctl
cfg/
cfg/natpass.cfg
lib/
lib/libACE.so -> libACE.so.5.4.0
lib/libACE.so.5.4.0
logs/
logs/old/
rings/
rings/24.pcm
rings/busy.pcm
rings/r1.pcm
rings/rbt.pcm
rings/ring.pcm
wrote 6956984 bytes  read 164 bytes  1546032.89 bytes/sec
total size is 16658481  speedup is 2.39
building file list ... done
./
logrotate.d/
logrotate.d/natpass
rc.d/
rc.d/init.d/
rc.d/init.d/natpass-init
wrote 792 bytes  read 52 bytes  1688.00 bytes/sec
total size is 1277  speedup is 1.51
[root@SipxchangePBX NATPass_Redhat]#
```

Sample output for Redhat

6. Become user "natpass" by running:

   # su – natpass

7. Edit configuration file *natpass.cfg* in the directory

usr/local/NATpass_*LinuxVersion*/cfg/

Make sure that IP address in the file is a real IP address on interface eth0 of your server. Verify and add domains / IP addresses permissions (see Configuration Parameters for more details on this and other parameters). If you received License Key from the vendor uncomment *key* parameter by removing leading # and enter one space and the License Key string after as shown in the example below:

key = 44nfh56hljkyi57688787979sddfgg79799999999

If you have not received a key leave it commented as is, you'll have NATPass™ running in demo mode that allows you to have 5 sip devices only.

Don't forget to save changed configuration file.

8. To manually start / stop / restart NATPASS™ Firewall controller you need to run as either *root* or natpass:

> # /etc/rc.d/init.d/natpass-init start

> # /etc/rc.d/init.d/natpass-init stop

> # /etc/rc.d/init.d/natpass-init restart

9. NATPass™ is configured to automatically start during the Operating System boot.

To Uninstall

1. Follow directions from sections 2 through 4 of installation procedure above

2. Uninstall software by running:

> # ./uninstall-natpass.sh

Configuration

The simplicity of NATPass™ Firewall Controller is that no changes on the end-user's NAT/Firewall/Router is required. All configurations are done on the IP Phone device. In almost all cases the Outbound Proxy is set to the IP address and port of the NATPass™ Firewall Controller server.

☞ **Note:** *You do not need to specify any special NAT Features on the IP Phone settings. If your phone supports STUN, you will need to disable it prior to setting up NATPass™ Firewall Controller as the Outbound Proxy. If you have the option available to specify the voice codec on your phone, make sure one of the options is PCMU/G711uLaw. It is not necessary to specify it as the first option. It should be available as an option even though you may not use it.*

The product is codec independent and, in general, doesn't care about it. The only requirement that G.711 should be on supported codec list. It could be the last codec in prefer list, but has to be there.

Cisco 7940/7960: "NAT Enabled" should be set to "YES" and "NAT Address" should be set to "Unprovisioned". Cisco firmware does not allow you to change "NAT Address" back to "Unprovisioned" once it has been set. To reset it change the configuration file for the phone and load it through a TFTP Server.

Grandstream: The latest version of Grandstream's firmware has the option "Use Random Port". Set it to "NO"

NATPass™ Start Up Options

Firewall controller can be started up by command mentioned in Installation section, by running "*/usr/local/natpass/bin/natpass_ctl start*" or by running /usr/local/natpass/bin/natpass with the command line options mentioned below. The last option is not a standard way to run NATPASS™ and generally is only recommended for debugging purposes.

Default location of software /usr/local/natpass/bin is mentioned through the text. What else is needed?

-c <file>	Configuration file. Default: natpass.cfg
-i <ip.addr>	If your box has more than 1 IP Address, there is no default for this filed. You have to specify it.
-p <port>	Port. Default: 7060
-l <file>	Log file. Default: natpass.log
-f	Force "FULL mode" to "ON". *See explanation below.*
-?	Short help

Monitoring

The NATPass™ monitoring tools are a separate module that enables remote access to the system to display its status and various other important statistics using a regular web browser. With this tool, the system administrator or NOC agent can login and see, in real time, how many registered devices or concurrent calls NATPass™ is handling thru specific Proxies. Many statistics such us number of calls, minutes and ASR (Average completion rate) are available as well.

Login:

Status window:

name	calls24hr	mins24hr	ASR24hr	ACD24hr	calls1hr	mins1hr	ASR1hr	ACD1hr	REL24hr
statistics	944	35109	940	5.53	355	2325	1831	925	930

Total		2980	228	3	3	0	0	0	0	0	0	0

domain	reg	active	answe	RER	RES	FC	FT	FD	FF	FV	TR	TF
65.114.57.183	950	35	3	3	0	0	0	0	0	0	0	0
myauvi.siptalk.com	1280	110	0	0	0	0	0	0	0	0	0	0
mynero.siptalk.com	750	83	0	0	0	0	0	0	0	0	0	0

Configuration Parameters

The natpass.cfg file is a configuration file for NATPASS FIREWALL CONTROLLER and resides in /usr/local/natpass/cfg (as mentioned in Installation section)

Any line started with '#' or empty line is ignored. Line in configuration file has following syntax:

param = value

Every parameter appears in the configuration file only once, unless it is intentionally specified otherwise. Any duplicate parameters will be ignored.

Key	**License key**. Without key NATPASS™ will start as Demo version. It means that you will be able to register only two (2) PHONES.
	Note: Some SIP devices could have more then one phone line appearance. For example CISCO 7940 has two. Every line could have its own configuration and treated as separated PHONE. So it could happen that in Demo version you will be able to register only one physical device.
Domain	Using this parameter you can set up a list of allowed domains. It can be domain name or IP address. In case of domain name you can use '*' as wildcard to specify group of domains, but '*' could appear only as first character. For instance: domain = *.firewallcontroller.com
	Options (can be combined):
	- SRV: You can enable DNS SRV look up by adding SRV after the domain name. i.e. domain = *.myproxy.com SRV
	- FULL: You can force Full mode (see definition below) for specific domains by adding FULL after the domain name. i.e. domain = *.myproxy1.com FULL
	- PRSN: You can enable presence services (when supported by your proxy and endpoint) by adding PRSN after the domain name. i.e. domain = *.myproxy2.com PRSN
	i.e. domain = *.myproxy3.com SRV FUL PRSN
	Note: Any request received from non-specified domain will be denied. If you do not specify any domains NATPASS™ would start in unrestricted mode. It means that anybody can use it to provide services to their proxy.
	For each supported domain we recommend providing both domain and IP address; some devices prefer to use IP addresses instead of domain names.
Ipaddr	IP address. If your computer has internal and external IP addresses you have to specify external one here.
	Note: You cannot use name here, it should be "dotted decimal" Internet address.
Port	Main port. Pair of "**ipaddr:port**" is a point which you should specify as

	Outbound proxy then you configure your phones.
	Note*:* NATPASS™ uses five consecutive ports. For example if you do not specify a port setting it will be default to 7060. four consecutive ports 7061-7064) will also be used, if any of those ports are occupied by other application NATPASS™ would not start and an error message will be displayed.
Range	Range of ports for RTP. Default: 32768 – 65536
full_mode	**Default is: off. If you set it on NATPASS™ will not release RTP and will translate it.** ***Note:*** If you are going to set this parameter to **on** make sure that you have enough network bandwidth to translate all RTP traffic.
events_collector	If **Natpass monitoring tool** is used, the IP and port the application is listening should be specified here.
Log	**Log file location.**
log_level	**Options: full, short or off. Default is: full** ***Note:*** The log file can grow quite big in full mode. It is recommended that after product is installed and configured the logging is turned off As a side note a log rotation script is supplied in NATPASS™ installation package. This script performs a log rotation nightly. The script is named NATPASS™ and located in /etc/logrotate.d. This script uses logrotate facility contributed to public use by Redhat. Script can be customized to rotate logs more or less often and base NATPASS™ log rotation schedule either on time or on log file size.
Ring	**File with prerecorded ring or notification. Ring should be recorded as PCM 8K 16bits uLaw. That is why PHONE should have specific codex available.** **Note:** If you have the option available to specify the voice codex on your phone devices, make sure one of the options is PCMU/G711uLaw. It is not necessary to specify it as the first option. ***Note:*** In some condition when a call is placed, it is not possible to use internal (hardware) ring. NATPASS™ will play the ring tone to compensate. You can also record your own prompt. For example: "Thank you for using our service, please hold while we connect you"
register_timeout	**Time out in sec. for register. Default: 25 If you're going to use Microsoft RTC SIP stack set it to 30**
agent_name	**Substitute agent name (User-Agent:/Server:) in outgoing SIP messages**
Broken	**List of specific devices and their unsupported functions. It doesn't mean they are really BROKEN; they just need some special treatment.** ***Note:*** If you are not familiar with device issues please leave these setting untouched. If you believe that you have issues with some specific devices not listed here, please contact your distributor. **For now four types of defects can be described:**

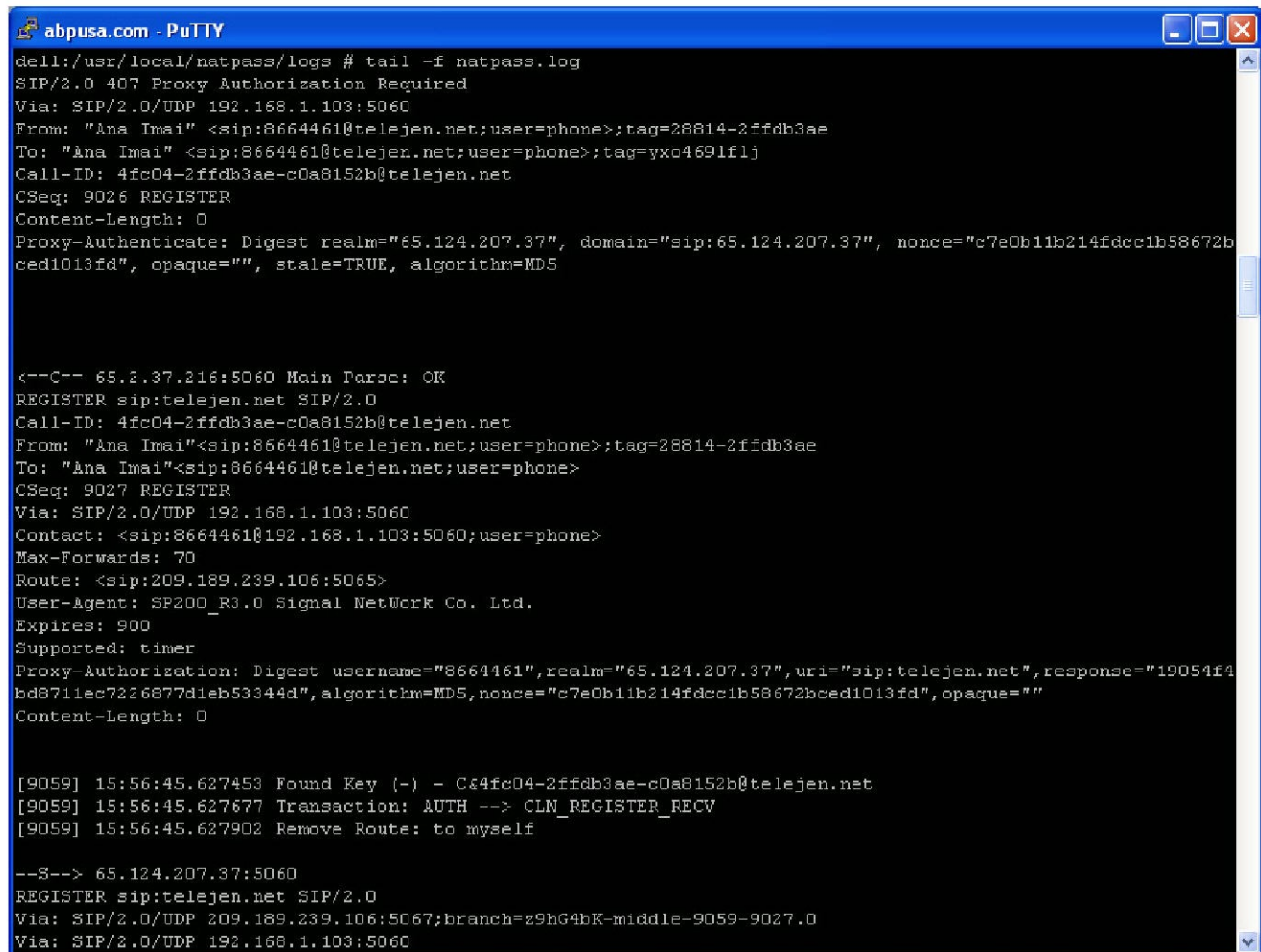|	- R – device doesn't support re-Invite - E – device can't correctly handle multiply early media response - S – device didn't send correct SDP after receiving early media - T – Tags provisional response 183 **Example:** broken = S Cisco ATA 18 broken = E Grandstream SIP UA 1.0.4

Logging Transactions and Errors

There is the only one log file natpass.log by default located in /usr/local/natpass/logs. This log, in full mode, displays all NATPASS™ transactions, errors, and a complete set of SIP/SDP headers for each transaction. The short mode, displays all NATPASS™ transactions, errors, but unless there is an error, it only displays the Request URI of each SIP transaction omitting all other headers.

You can see the current logs by issuing the following command:

> # tail –f /usr/local/natpass/logs/natpass.log

```
dell:/usr/local/natpass/logs # tail -f natpass.log
SIP/2.0 407 Proxy Authorization Required
Via: SIP/2.0/UDP 192.168.1.103:5060
From: "Ana Imai" <sip:8664461@telejen.net;user=phone>;tag=28814-2ffdb3ae
To: "Ana Imai" <sip:8664461@telejen.net;user=phone>;tag=yxo4691flj
Call-ID: 4fc04-2ffdb3ae-c0a8152b@telejen.net
CSeq: 9026 REGISTER
Content-Length: 0
Proxy-Authenticate: Digest realm="65.124.207.37", domain="sip:65.124.207.37", nonce="c7e0b11b214fdcc1b58672b
ced1013fd", opaque="", stale=TRUE, algorithm=MD5


<==C== 65.2.37.216:5060 Main Parse: OK
REGISTER sip:telejen.net SIP/2.0
Call-ID: 4fc04-2ffdb3ae-c0a8152b@telejen.net
From: "Ana Imai"<sip:8664461@telejen.net;user=phone>;tag=28814-2ffdb3ae
To: "Ana Imai"<sip:8664461@telejen.net;user=phone>
CSeq: 9027 REGISTER
Via: SIP/2.0/UDP 192.168.1.103:5060
Contact: <sip:8664461@192.168.1.103:5060;user=phone>
Max-Forwards: 70
Route: <sip:209.189.239.106:5065>
User-Agent: SP200_R3.0 Signal NetWork Co. Ltd.
Expires: 900
Supported: timer
Proxy-Authorization: Digest username="8664461",realm="65.124.207.37",uri="sip:telejen.net",response="19054f4
bd8711ec7226877d1eb53344d",algorithm=MD5,nonce="c7e0b11b214fdcc1b58672bced1013fd",opaque=""
Content-Length: 0


[9059] 15:56:45.627453 Found Key (-) - C&4fc04-2ffdb3ae-c0a8152b@telejen.net
[9059] 15:56:45.627677 Transaction: AUTH --> CLN_REGISTER_RECV
[9059] 15:56:45.627902 Remove Route: to myself

--S--> 65.124.207.37:5060
REGISTER sip:telejen.net SIP/2.0
Via: SIP/2.0/UDP 209.189.239.106:5067;branch=z9hG4bK-middle-9059-9027.0
Via: SIP/2.0/UDP 192.168.1.103:5060
```
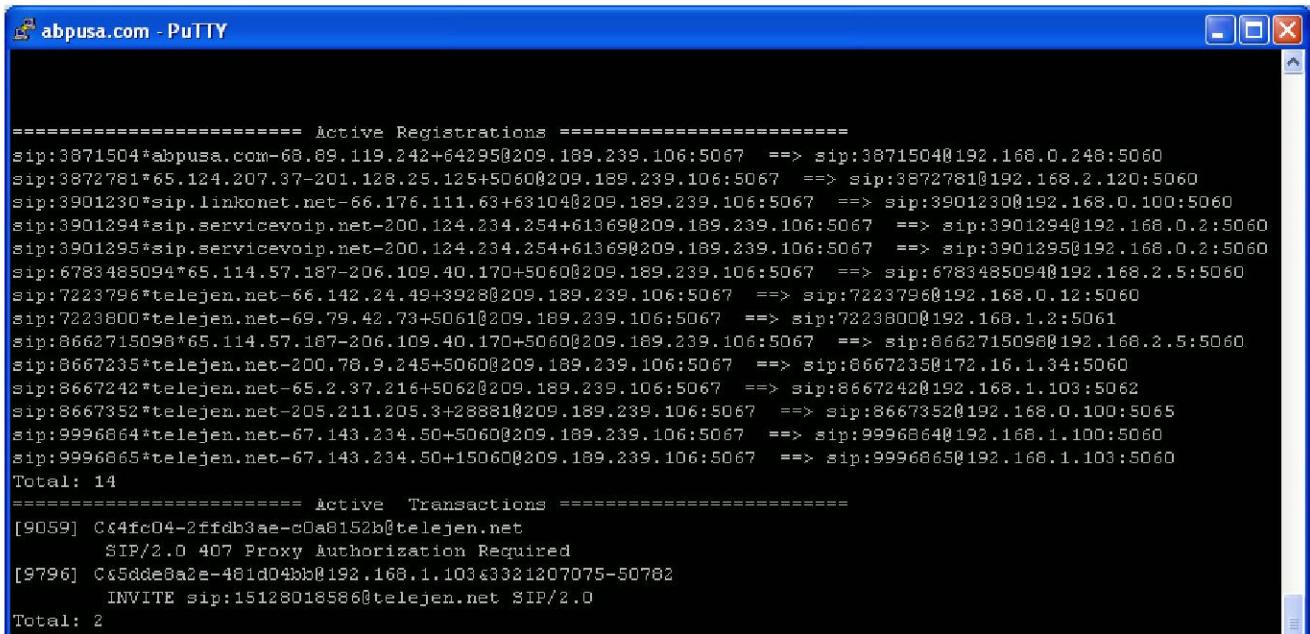
Stop the command with Ctrl+C

To find out process id of NATPASS™:
> # ps -ef | grep natpass

To force NATPass™ to display number of currently active SIP registrations and number of currently active SIP call transactions (when monitoring tools module is not used). Total number for each of the variable is displayed as well you need to initiate information writing into logs and display the logs from bottom. Use the following commands:

> # *kill -HUP <natpass process id discovered via previous command>*
>
> # *less /usr/local/natpass/logs/natpass.log*

```
abpusa.com - PuTTY                                                        _ □ X

========================= Active Registrations =========================
sip:3871504*abpusa.com-68.89.119.242+64295@209.189.239.106:5067  ==> sip:3871504@192.168.0.248:5060
sip:3872781*65.124.207.37-201.128.25.125+5060@209.189.239.106:5067  ==> sip:3872781@192.168.2.120:5060
sip:3901230*sip.linkonet.net-66.176.111.63+6310@209.189.239.106:5067  ==> sip:3901230@192.168.0.100:5060
sip:3901294*sip.servicevoip.net-200.124.234.254+61369@209.189.239.106:5067  ==> sip:3901294@192.168.0.2:5060
sip:3901295*sip.servicevoip.net-200.124.234.254+61369@209.189.239.106:5067  ==> sip:3901295@192.168.0.2:5060
sip:6783485094*65.114.57.187-206.109.40.170+5060@209.189.239.106:5067  ==> sip:6783485094@192.168.2.5:5060
sip:7223796*telejen.net-66.142.24.49+3928@209.189.239.106:5067  ==> sip:7223796@192.168.0.12:5060
sip:7223800*telejen.net-69.79.42.73+5061@209.189.239.106:5067  ==> sip:7223800@192.168.1.2:5061
sip:8662715098*65.114.57.187-206.109.40.170+5060@209.189.239.106:5067  ==> sip:8662715098@192.168.2.5:5060
sip:8667235*telejen.net-200.78.9.245+5060@209.189.239.106:5067  ==> sip:8667235@172.16.1.34:5060
sip:8667242*telejen.net-65.2.37.216+5062@209.189.239.106:5067  ==> sip:8667242@192.168.1.103:5062
sip:8667352*telejen.net-205.211.205.3+28881@209.189.239.106:5067  ==> sip:8667352@192.168.0.100:5065
sip:9996864*telejen.net-67.143.234.50+5060@209.189.239.106:5067  ==> sip:9996864@192.168.1.100:5060
sip:9996865*telejen.net-67.143.234.50+15060@209.189.239.106:5067  ==> sip:9996865@192.168.1.103:5060
Total: 14
========================= Active  Transactions =========================
[9059]  C&4fc04-2ffdb3ae-c0a8152b@telejen.net
        SIP/2.0 407 Proxy Authorization Required
[9796]  C&5dde8a2e-481d04bb@192.168.1.103&3321207075-50782
        INVITE sip:15128018586@telejen.net SIP/2.0
Total: 2
```

Frequently Asked Questions (FAQs)

Q. If NATPass™ can bypass my firewall does it mean that my firewall is broken or not secured enough?

A. No. It uses some SIP specific features to traverse through NAT/Firewall and only your SIP PHONE can use it. It does not compromise your network.

Q. Does it work with TCP?

A. No. It supports only UDP. But TCP support is on the roadmap.

Q. Can NATPass™ work with short form of SIP?

A. Yes, even if either PHONE or PROXY doesn't support short form of SIP. NATPASS™ receives SIP message in short form and forwards it in full form.

Q. What kind of firewall supported? Does it work with Symmetric NAT?

A. It should work with any type of firewall including Symmetric NAT.

Q. What is Symmetric NAT? Is my firewall Symmetric?

A. You can find classification of NAT in RFC 3489 – STUN http://www.faqs.org/rfcs/rfc3489.html. It should not mater what type of firewall you have.

Q. Is NATPass™ better then STUN?

A. They are two different solutions. STUN is less universal. NATPass™ works in many more situations where STUN alone does not work. STUN will not work if you are working behind new symmetric NAT routers. You can use STUN alone if you are familiar with configuring SIP devices to work behind NAT, if your PHONE supports STUN or if your NAT is not Symmetric.

If you don't know answer of any of above questions, or don't even want to know – use NATPASS™ Session Border / Firewall Controller

Recommended Platform

Hardware

- Intel based PC with Pentium III 500 MHZ Processor or above

- Recommended Memory 256 MB or more

- Hard drive 20 GB or more if the logging is enabled

- Operating system LINUX (Supported version RedHat 9 or SUSE 9.0)

Capacity / Performance Data

System should easily support 5000-10,000 UA on an adequate platform with sufficient bandwidth for devices that allow redirect of media. More exact performance data will be published once it becomes available for Version 3.0

Known Issues

- RTCP does not traversal through NAT

END USER SOFTWARE LICENSE AGREEMENT

This copy of Firewall Controller ("the Software Product") and accompanying documentation is licensed and not sold. This Software Product is protected by copyright laws and treaties, as well as laws and treaties related to other forms of intellectual property. Xcast Lab or its subsidiaries, affiliates, and suppliers (collectively "Xcast Lab") own intellectual property rights in the Software Product. The Licensee's ("you" or "your") license to download, use, copy, or change the Software Product is subject to these rights and to all the terms and conditions of this End User License Agreement ("Agreement").

Acceptance

YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT BY SELECTING THE "ACCEPT" OPTION AND DOWNLOADING THE SOFTWARE PRODUCT OR BY INSTALLING, USING, OR COPYING THE SOFTWARE PRODUCT. YOU MUST AGREE TO ALL OF THE TERMS OF THIS AGREEMENT BEFORE YOU WILL BE ALLOWED TO DOWNLOAD THE SOFTWARE PRODUCT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, YOU MUST SELECT "DECLINE" AND YOU MUST NOT INSTALL, USE, OR COPY THE SOFTWARE PRODUCT.

License Grant

This Agreement entitles you to install and use one copy of the Software Product. In addition, you may make one archival copy of the Software Product. The archival copy must be on a storage medium other than a hard drive, and may only be used for the reinstallation of the Software Product. This Agreement does not permit the installation or use of multiple copies of the Software Product, or the installation of the Software Product on more than one computer at any given time, on a system that allows shared used of applications, on a multi-user network, or on any configuration or system of computers that allows multiple users. Multiple copy use or installation is only allowed if you obtain an appropriate licensing agreement for each user and each copy of the Software Product.

Restrictions on Transfer

You may not assign your rights and obligations under this Agreement, or redistribute, encumber, sell, rent, lease, sublicense, or otherwise transfer your rights to the Software Product without first obtaining the express written consent of Xcast Lab.

Restrictions on Use

You may not use, copy, or install the Software Product on any system with more than one computer, or permit the use, copying, or installation of the Software Product by more than one user or on more than one computer. If you hold multiple, validly licensed copies, you may not use, copy, or install the Software Product on any system with more than the number of computers permitted by license, or permit the use, copying, or installation by more users, or on more computers than the number permitted by license. You may not decompile, "reverse-engineer", disassemble, or otherwise attempt to derive the source code for the Software Product. You may not use the database portion of the Software Product in connection with any software other than the Software Product.

Restrictions on Alteration

You may not modify the Software Product or create any derivative work of the Software Product or its accompanying documentation. Derivative works include but are not limited to translations. You may not alter any files or libraries in any portion of the Software Product. You may not reproduce the database portion or create any tables or reports relating to the database portion.

Restrictions on Copying

You may not copy any part of the Software Product except to the extent that licensed use inherently demands the creation of a temporary copy stored in computer memory and not permanently affixed on storage medium. You may make one archival copy, which must be stored on a medium other than a computer hard drive.

Disclaimer of Warranties and Limitation of Liability

UNLESS OTHERWISE EXPLICITLY AGREED TO IN WRITING BY XCAST LAB, XCAST LAB MAKES NO OTHER WARRANTIES, EXPRESS OR IMPLIED, IN FACT OR IN LAW, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OTHER THAN AS SET FORTH IN THIS AGREEMENT OR IN THE LIMITED WARRANTY DOCUMENTS PROVIDED WITH THE SOFTWARE PRODUCT.

Xcast Lab makes no warranty that the Software Product will meet your requirements or operate under your specific conditions of use. Xcast Lab makes no warranty that operation of the Software Product will be secure, error free, or free from interruption. YOU MUST DETERMINE WHETHER THE SOFTWARE PRODUCT SUFFICIENTLY MEETS YOUR REQUIREMENTS FOR SECURITY AND UNINTERRUPTABILITY. YOU BEAR SOLE RESPONSIBILITY AND ALL LIABILITY FOR ANY LOSS INCURRED DUE TO FAILURE OF THE SOFTWARE PRODUCT TO MEET YOUR REQUIREMENTS. XCAST LAB WILL NOT, UNDER ANY CIRCUMSTANCES, BE RESPONSIBLE OR LIABLE FOR THE LOSS OF DATA ON ANY COMPUTER OR INFORMATION STORAGE DEVICE. UNDER NO CIRCUMSTANCES SHALL XCAST LAB, ITS DIRECTORS, OFFICERS, EMPLOYEES OR AGENTS BE LIABLE TO YOU OR ANY OTHER PARTY FOR INDIRECT, CONSEQUENTIAL, SPECIAL, INCIDENTAL, PUNITIVE, OR EXEMPLARY DAMAGES OF ANY KIND (INCLUDING LOST REVENUES OR PROFITS OR LOSS OF BUSINESS) RESULTING FROM THIS AGREEMENT, OR FROM THE FURNISHING, PERFORMANCE, INSTALLATION, OR USE OF THE SOFTWARE PRODUCT, WHETHER DUE TO A BREACH OF CONTRACT, BREACH OF WARRANTY, OR THE NEGLIGENCE OF XCAST LAB OR ANY OTHER PARTY, EVEN IF XCAST LAB IS ADVISED BEFOREHAND OF THE POSSIBILITY OF SUCH DAMAGES. TO THE EXTENT THAT THE APPLICABLE JURISDICTION LIMITS XCAST LAB'S ABILITY TO DISCLAIM ANY IMPLIED WARRANTIES, THIS DISCLAIMER SHALL BE EFFECTIVE TO THE MAXIMUM EXTENT PERMITTED.

Limitation of Remedies and Damages

Your remedy for a breach of this Agreement or of any warranty included in this Agreement is the correction or replacement of the Software Product. Selection of whether to correct or replace shall be solely at the discretion of Xcast Lab. Xcast Lab reserves the right to substitute a functionally equivalent copy of the Software Product as a replacement. If Xcast Lab is unable to provide a replacement or substitute Software Product or corrections to the Software Product, your sole alternate remedy shall be a refund of the purchase price for the Software Product exclusive of any costs for shipping and handling.

Any claim must be made within the applicable warranty period. All warranties cover only defects arising under normal use and do not include malfunctions or failure resulting from misuse, abuse, neglect, alteration, problems with electrical power, acts of nature, unusual temperatures or humidity, improper installation, or damage determined by Xcast Lab to have been caused by you. All limited warranties on the Software Product are granted only to you and are nontransferable.

You agree to indemnify and hold Xcast Lab harmless from all claims, judgments, liabilities, expenses, or costs arising from your breach of this Agreement and/or acts or omissions.

U.S. Government Use

The Software is a "commercial item" as that term is defined at 48 C.F.R. § 2.101, consisting of "commercial computer software" and "commercial computer software documentation" as such terms are used in 48 C.F.R. § 12.212. Consistent with 48 C.F.R. § 12.212 and 48 C.F.R. §§ 227.7202-1 through 227.7202-4, Xcast Lab provides the Software to U.S. Government end users only pursuant to the terms and conditions herein.

Export Control

You agree and acknowledge that the Software is subject to U.S. export control law, and You will comply with all applicable laws and regulations in Your use of the Software under this Agreement, including without limitation all export laws and regulations of the U.S. Department of Commerce and all other U.S. agencies and authorities, including the Export Administration Regulations promulgated by the Bureau of Industry and Security (as codified in 15 C.F.R. Parts §§ 730-774). Without limiting the foregoing, you expressly agree not to export or re-export the Software in violation of such laws or regulations, or without all required licenses and authorizations.

Miscellaneous

Nothing contained herein will be construed to create any agency, employment, partnership, principal-agent relationship, or other form of joint enterprise between the parties. No waiver or modification of the Agreement will be valid unless signed by each party. The waiver of a breach of any term hereof will in no way be construed as a waiver of any other term or breach hereof. The headings in this Agreement do not affect its interpretation. You may not assign or transfer any of your rights or obligations under this Agreement to a third party without the prior written consent of Xcast Lab. Any attempted assignment or transfer in violation of the foregoing will be void from the beginning. Xcast Lab may assign this Agreement without consent to any third party. If any provision of this Agreement is held by a court of competent jurisdiction to be unenforceable, the remaining provisions of this Agreement will remain in full force and effect.

Notices to Xcast Lab must be sent to the following address, and will be deemed effective three (3) days after certified mailing, return receipt requested: Xcast Lab, 600 North Linn Street, Anamosa, IA 52205. This Agreement is governed by the laws of the State of California without reference to conflict of laws principles that would require the application of the laws of any other jurisdiction. The United Nations Convention on Contracts for the International Sale of Goods is specifically disclaimed. All disputes arising out of this Agreement will be subject to the exclusive jurisdiction of the state and federal courts located in San Francisco County, California, and the parties irrevocably consent to the personal and exclusive jurisdiction and venue of these courts. This Agreement is the final, complete, and exclusive agreement between the parties relating to the subject matter hereof, and supersedes all prior or contemporaneous understandings and agreements relating to such subject matter, whether oral or written.

Severability

If any provision of this Agreement shall be held to be invalid or unenforceable, the remainder of this Agreement shall remain in full force and effect. To the extent any express or implied restrictions are not permitted by applicable laws, these express or implied restrictions shall remain in force and effect to the maximum extent permitted by such applicable laws.

Setup and Configuration Files

Appendix A – Sample NATPASS™ Inventory

With natpass loaded in /usr/local/natpass/ directory.

```
# The actual binary
# /usr/local/natpass/bin/natpass

# Control file used to Natpass
# Usage: $0 {start | stop | restart}
# /usr/local/natpass/bin/natpass_ctl
A rc script used to start / stop / restart natpass. It also auto-starts middle on boot.
/etc/rc.d/init.d/natpass-init

# The configuration file
# /usr/local/natpass/cfg/natpass.cfg

# A library file used by natpass
# /usr/local/natpass/lib/LibACE.so

# The log file
# This file gets huge so either use logrotate or keep logging off.
# /usr/local/natpass/logs/natpass.log

# Old logfiles if logrotate is used
# /usr/local/natpass/logs/old/natpass.log.0.gz
# /usr/local/natpass/logs/old/natpass.log.1.gz
# /usr/local/natpass/logs/old/natpass.log.2.gz
# /usr/local/natpass/logs/old/natpass.log.3.gz
# /usr/local/natpass/logs/old/natpass.log.4.gz
# /usr/local/natpass/logs/old/natpass.log.5.gz
# /usr/local/natpass/logs/old/natpass.log.6.gz

# Files used to play Call Progress tones back to user if need be.
# /usr/local/natpass/natpass/24.pcm
# /usr/local/natpass/natpass/busy.pcm
# /usr/local/natpass/natpass/r1.pcm
# /usr/local/natpass/natpass/rbt.pcm
# /usr/local/natpass/natpass/ring.pcm

# Logrotate script used for logrotation of natpass.log
#/etc/logrotate.d/natpass
```

Appendix B – Sample Config File

```
# natpass.cfg
#
#
# License key - 32 bytes in hex
#
# Please don't uncomment the key without actual key available from your vendor!!!
#
#key =
key = 0b81_this_is_a_sample_key342sdfw4ff
#
# domain:
# '*' could appear only as first char.
# If there is no domain specification (or no config file) - Unrestricted mode.
# Examples of various services turned on per domain level
# SRV support
# domain = xyzsystems.com  SRV
#
# FULL mode per domain support
# domain = 123systems.com FULL
#
# Presence Services support
# domain = newdomain.net    PRSN
#
# All ofthe above
# domain = testdomain.com   SRV FULL PRSN

domain = *

#
# fuser
#
#fuser = 6165@fortuna.xcastlabs.com

# IP Address: Could be overwrited by option '-i xxx.xxx.xxx.xxx'
#
ipaddr = 209.189.130.106

# This is a feature that allows to discover address restricted cone
# firewalls.  Second routable IP address needs to be setup on the server
# before uncommenting the line below.
#
# second_ipaddr = 192.168.0.160

#
# Port: Could be overwrited by option '-p port'
#
port = 5065

#
```

```
# Range of ports for RTP. Default [32768-65536]
#
range = 50000 59999

#
# events_collector
#
# Events collector is a NATPASS monitoring application provided separately
# NATPASS sends information to specified address/port of the application if
# uncommented.
#
#events_collector = 127.0.0.1:1024
events_collector = 127.0.0.1:32802

#
#
# Full Mode: Could be forced to ON by option '-f'
#
#full_mode = ON

#
# Log File: Could be overwrited by option '-l file'
#
log = /usr/local/natpass/logs/natpass.log

#
# log_level = off, short, full
#
log_level = full

#
# Ring file ( PCM 8K 16bits uLaw )
#
#ring = 24.pcm
ring = /usr/local/natpass/rings/rbt.pcm

#
# TimeOut for resent REGISTER in sec. Default 30
#
#
register_timeout = 30

#
# If you don't like to see name 'Middle' as SIP User-Agent: header
# you could change it...
#
#agent_name = NATPass Firewall Controller

#
# List of Phones (User-Agent:/Server:) what do not support:
#       R - re-INVITE
```

```
#        E - Second Early Media
#      S - hold correct SDP after 183
#      T - Tag from provisional response 183

broken = S Cisco-CP7905/1.01
broken = S Cisco ATA 18
broken = ET CSCO/5
broken = E CSCO/6
broken = ETS Azacall200
#broken = R Cisco ATA 186  v2
#broken = R Cisco ATA 188  v2
broken = E Grandstream SIP UA 1.0.4
#broken = E Sipura/SPA2000
#broken = ER Some-Stranger Version/Modification
```

Appendix C – NATPASS™ Fail-Over HOW TO

When purchasing a redundant server license you'll receive help to implement this feature since the task might require some custom settings. NATPASS™ can be run in the redundant mode. This configuration has two servers involved. One of them is utilized as a primary node and the second is a hot standby. Servers monitor each other and network. If one of the servers fail, second one becomes a primary node. When the second server restored to normal running condition, it can be configured either stay as hot standby or take over to become a primary node again.

For the redundancy NATPASS™ utilizes standard Linux-HA project software with very minimal change (NATPASS™ service restart script added to facilitate restart during fail-over and / or recovery).

To obtain information about Linux-HA project please go to:

http://wiki.linux-ha.org/FrontPage?action=highlight&value=HomePage

To download latest stable version of heartbeat please go to:

http://www.ultramonkey.org/download/heartbeat/1.2.3/

Choose your OS for binary packages or get source code and compile on your own.

Installer will need to add a following script named natpass-init to /etc/ha.d/resource.d/ (or wherever resource.d directory located in your heartbeat installation)

```
######### natpass-init listing ###############

#!/bin/sh
# description: Natpass FWC
#
#

. /etc/ha.d/shellfuncs

BASEDIR=/usr/local/natpass
BINDIR=${BASEDIR}/bin
LOGDIR=${BASEDIR}/logs
CFGDIR=${BASEDIR}/cfg
RUNDIR=${BASEDIR}/run
LIBDIR=${BASEDIR}/lib
USERNAME=`id -un`
#USERID=`id -u`
CLUSTER_IP=`awk -F = '/CLUSTER_IP/ { print $2 }' $CFGDIR/cluster.conf | sed 's/\#.*//g'`

start() {

        if [ ! -f "${CFGDIR}/natpass.cfg" ]; then
           echo "$CFGDIR/natpass.cfg is missing ... "
```

```
        exit 1
    else
        stop
        cd ${RUNDIR}/natpass
        if [ ${USERNAME} = "root" ]
        then
            su -l xcast -c "ulimit -S -c 2000000;  ${BINDIR}/natpass -c  ${CFGDIR}/natpass.cfg  -i
${CLUSTER_IP} &"
        elif [ ${USERNAME} = "xcast" ]
        then
            ulimit -S -c 2000000; ${BINDIR}/natpass -c ${CFGDIR}/natpass.cfg  -i ${CLUSTER_IP} &
        else
            echo "You need to be either natpass or superuser"
            exit 2
        fi
    fi
}

stop() {
    cd $RUNDIR/natpass
    killall natpass
    sleep 2
    if [ -n "`ps h -o pid -C natpass`" ]; then
     killall -9 natpass
    fi
}

status() {
if [ -z "`ps h -o pid -C natpass`" -o -z "`ps -ef | grep natpass | grep -v grep | grep ${CLUSTER_IP}`" ];
then
    echo "natpass is stopped"
    ha_log "natpass is stopped"
else
    echo "natpass is running"
    proc_id=`ps h -o pid -C natpass`
    ha_log "natpass is running ($proc_id)"
fi
}


case "$1" in
    start)
        start
        echo "Natpass Started"
        ;;
    stop)
        stop
        echo "Natpass Stopped"
        ;;
    status)
        status
        ;;
    *)
        echo $"Usage: $0 {start | stop | status}"
        exit 3
```

esac
exit 0

############### end of natpass-init listing ##############################

Also the file cluster.conf has to be added to /usr/local/natpass/cfg (or wherever your natpass cfg directory is located).

##################### cluster.conf listing ####################################

CLUSTER_IP=xx.xx.xx.xx # VIrtual IP Address of the HA failover cluster

####################### end of cluster.conf listing #############################

Replace xx.xx.xx.xx with virtual IP defined in heartbeat configuration.

Change file natpass_ctl in /usr/local/natpass/bin/ (or wherever your natpass bin directory is located).

##################### listing of cluster aware natpass_ctl #######################

```
#!/bin/sh
#
# Natpass startup script

BASEDIR=/usr/local/natpass
BINDIR=${BASEDIR}/bin
LOGDIR=${BASEDIR}/logs
CFGDIR=${BASEDIR}/cfg
RUNDIR=${BASEDIR}/run
LIBDIR=${BASEDIR}/lib
USERNAME=`id -un`
CLUSTER_IP=`awk -F = '/CLUSTER_IP/ { print $2 }' $CFGDIR/cluster.conf | sed 's/\#.*//g'`
IS_VIRTUAL_IP=`/sbin/ifconfig | grep $CLUSTER_IP`

start() {

    if [ ! -f "${CFGDIR}/natpass.cfg" ]; then
      echo "$CFGDIR/natpass.cfg is missing ... "
      exit 1
    fi
      cd ${RUNDIR}/natpass
    case "$USERNAME" in
        root)
            if [ -n "$IS_VIRTUAL_IP" ]
            then
                su -l xcast -c "ulimit -S -c 2000000; ${BINDIR}/natpass -c ${CFGDIR}/natpass.cfg -i $CLUSTER_IP &"
            else
                su -l xcast -c "ulimit -S -c 2000000; ${BINDIR}/natpass -c ${CFGDIR}/natpass.cfg &"
            fi
            ;;
        xcast)
            if [ -n "$IS_VIRTUAL_IP" ]
            then
```

```
                    ulimit  -S  -c  2000000;  ${BINDIR}/natpass  -c  ${CFGDIR}/natpass.cfg  -i
$CLUSTER_IP &
              else
                    ulimit -S -c 2000000; ${BINDIR}/natpass -c ${CFGDIR}/natpass.cfg &
              fi
              ;;
        *)
            echo "You need to be either xcast or superuser"
            exit 2
      esac
}

stop() {
      cd $RUNDIR/natpass
      killall natpass
      sleep 2
      if [ -n "`ps h -o pid -C natpass`" ]; then
       killall -9 natpass
      fi
}

case "$1" in
      start)
            start
            echo "Natpass Started"
            ;;
      stop)
            stop
            echo "Natpass Stopped"
            ;;
      restart)
            stop
            echo "Natpass Stopped"
            sleep 3
            start
            echo "Natpass Started"
            ;;
        *)
            echo $"Usage: $0 {start | stop | restart}"
            exit 3
      esac
      exit 0

##################### end of listing of cluster aware natpass_ctl #####################
```

Your ha-resources file should look similar to this:

node1.mydomain.com xx.xx.xx.xx middle-init
Where you need to replace node1.mydomain.com with the right hostname and xx.xx.xx.xx
with your virtual cluster IP address.

Important !!!

Your license key is generated based on the IP address of your server. If you plan to set up heartbeat based redundancy you need to make sure that you give your vendor virtual IP address of the cluster and not the real IP of the server. At the same time, inside of the natpass.cfg of each cluster node the real first and second IP addresses of box need to be configured. So if your virtual cluster IP is 66.10.11.10 that is what given to vendor for licensing. If your 1st node of the cluster has real IP addresses as 66.10.11.11 and 66.10.11.12, those go into its natpass.cfg. And if your 2nd node has IP addresses 66.10.11.13 and 66.10.11.14, those go into 2nd node's natpass.cfg.

When heartbeat starts on one node it will look for the other node status and if the other node is down, become a primary node taking over virtual IP address and restarting Natpass to utilize this address and related licensing key. If the other node is running as a primary, newly started node either becomes secondary and starts Natpass in demo mode or, depending on the heartbeat configuration, will force primary node to become a secondary one and to release virtual IP address for its own use.