Network Security

This page describes the network security measures that must be implemented in order to protect your VoipNow infrastructure.

Networks

VoipNow Managed Firewall

VoipNow does not manage security. While it does its best to protect on the application stack level, it cannot guess your network topology and it cannot manage firewalls.

For convenience we included a node level firewall that is designed to help you deploy a basic network firewall on the host level.

A firewall installer is available on each VoipNow node. It will automatically detect the roles running on your node roles and apply only the corresponding access rules. Furthermore, it also contains a built-in safety feature to ensure you don't lose access to your server.

Installation

Trust some networks (optional)

You can always fully trust some networks. The installed firewall will never perform filtering for them (in/out).

Edit `/etc/voipnow/local.conf` and uncomment the TRUSTED_NET variable, replacing its value with your local network IP and netmask:

Access from these networks is always allowed (eg: TRUSTED_NET 10.10.34.12/32 10.10.33.1/24) # TRUSTED_NET NETWORK/MASK should be changed into something similar to:
Access from these networks is always allowed (eg: TRUSTED_NET 10.10.34.12/32 10.10.33.1/24) TRUSTED_NET 172.16.100.1/24
This must be done on all VoipNow nodes in the infrastructure.

Apply firewall (test mode)

Execute the following command:

/usr/local/voipnow/admin/sbin/voipnow_firewall -o apply -t true
Testmode enabled. If everything is working ok, please apply the firewall with /usr/local/voipnow/admin/sbin/voipnow_firewall --operation=apply --testmode=false
Your previous firewall has been saved in /tmp/iptables.20463
The firewall installer will:

- save your existing firewall rules into a temporary file (`/tmp/iptables.20463` in the above example)
- inspect the VoipNow Cloud Management for roles assigned to this role
- attempt to detect ports used by each role and apply the corresponding firewall rules
- install a "SafetyNet" consisting of a cron job which does a firewall flush after 3 minutes

You can see this safety net as a line in crontab:

*/3 * * * * /sbin/iptables -P INPUT ACCEPT; /sbin/iptables -P FORWARD ACCEPT;/sbin/iptables -P OUTPUT ACCEPT;/sbin/iptables -F;/sbin/iptables -X

Apply firewall (final mode)

Assuming that everything is ok, run the firewall script again with the `ok` parameter (this will remove the cron job and leave your newly generated firewall rules in place):

/usr/local/voipnow/admin/sbin/voipnow_firewall -o apply -t false

Private Network

The private network must be isolated. Only VoipNow nodes must be able to access it - it should not be shared with any other system. Furthermore, generic host level network firewalls must be configured to allow connection only on the ports that are opened on each role.

Public Network

The public network must be protected with firewalls. Connections must be allowed only on the ports configured to be accessed by customers' devices.

The sections below offer several recommendations on how to set up firewalls based on the role of the node.

Role Network Filtering

Functionaly Layer

Web Management Interface

Requires public network access, as well as private network access for management and database traffic. Traffic is encrypted; both private and public networks are required. Supports authentication and authorization methods. Could be protected with an application level firewall.

SIP

Requires public network access, as well as private network access for management and database traffic. Traffic can be encrypted with TLS as long as involved parties support this protocol otherwise its not encrypted; both private and public networks are required. Supports authentication and authorization methods. Could be protected with an application level firewall.

PBX

Requires public network access, as well as private network access for management and database traffic. Traffic can be encrypted (SRTP) as long as involved parties support the protocol otherwise traffic not encrypted; both private and public networks are required. Supports authentication and authorization methods.

Infrastructure Management

Infrastructure Controller

Requires private network access. Traffic is encrypted.

Worker

Task scheduler that does not listen on any port but requires private network access to connect to other roles.

Storage Layer

SQL

Traffic must be kept in the private network. Traffic is not encrypted; connection is made using authentication.

Distributed Database

Traffic must be kept in the private network. Traffic is not encrypted; connection is authenticated, but some basic operations to the database are possible without credentials.

Elasticsearch

Traffic must be kept in the private network. Traffic is not encrypted; connection is authenticated.

Amazon S3

Traffic is on the public network and is encrypted, connection is authenticated.