ZENworks Mobile Workspace

Advanced Integration in High Availability Environments

May 2017

Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see https://www.novell.com/company/legal/.

Copyright © 2017 Micro Focus Software Inc. All Rights Reserved.

TABLE OF CONTENTS

1 Overview 3

2 Principle 3

3 Workflow 4

4 Fail Over 5

4.1 Data Recovery 6

5 Load Balancing 6

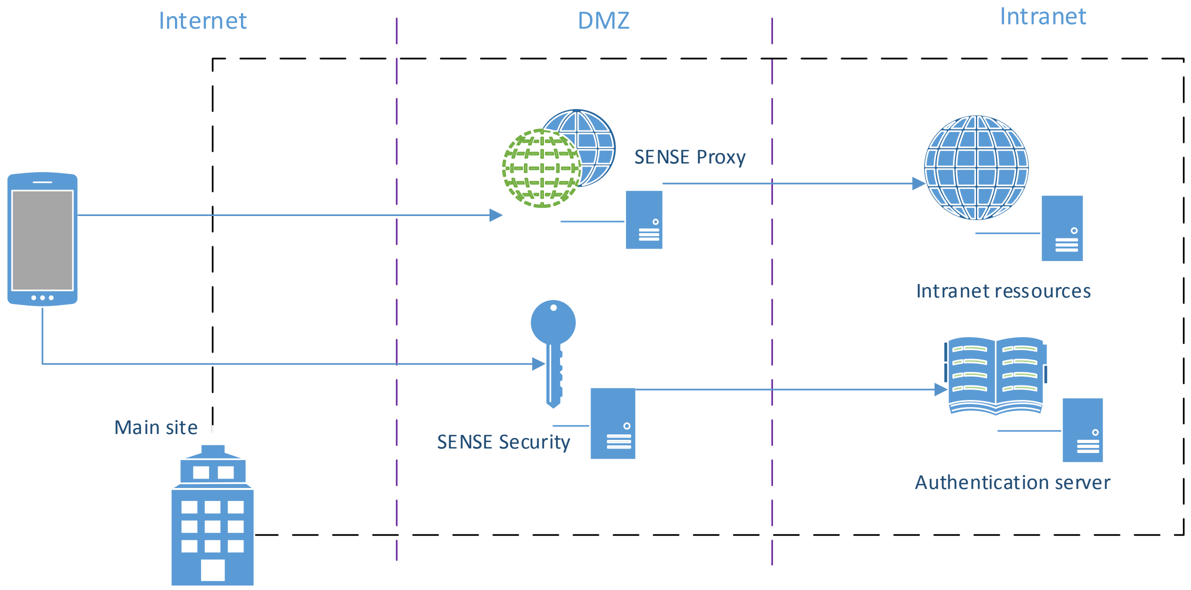
6 Multisite 7

1 OVERVIEW

This document aims to describe at a high level how ZENworks Mobile Workspace components can be used in high availability environments.

2 PRINCIPLE

The server is composed of the following components:



- Sense Security, this component is stateful since the existing sessions are in-memory. A session contains all the information about the user, its credentials and the session key that is being generated for each new session. A database is used to persist the shared keys between the apps and the server. The Security server is responsible for:
  - Synchronization and authentication of users;
  - Handling the shared keys between the clients and the server;
  - Creation and validation of sessions;
  - Handling the distribution and the update of the apps.

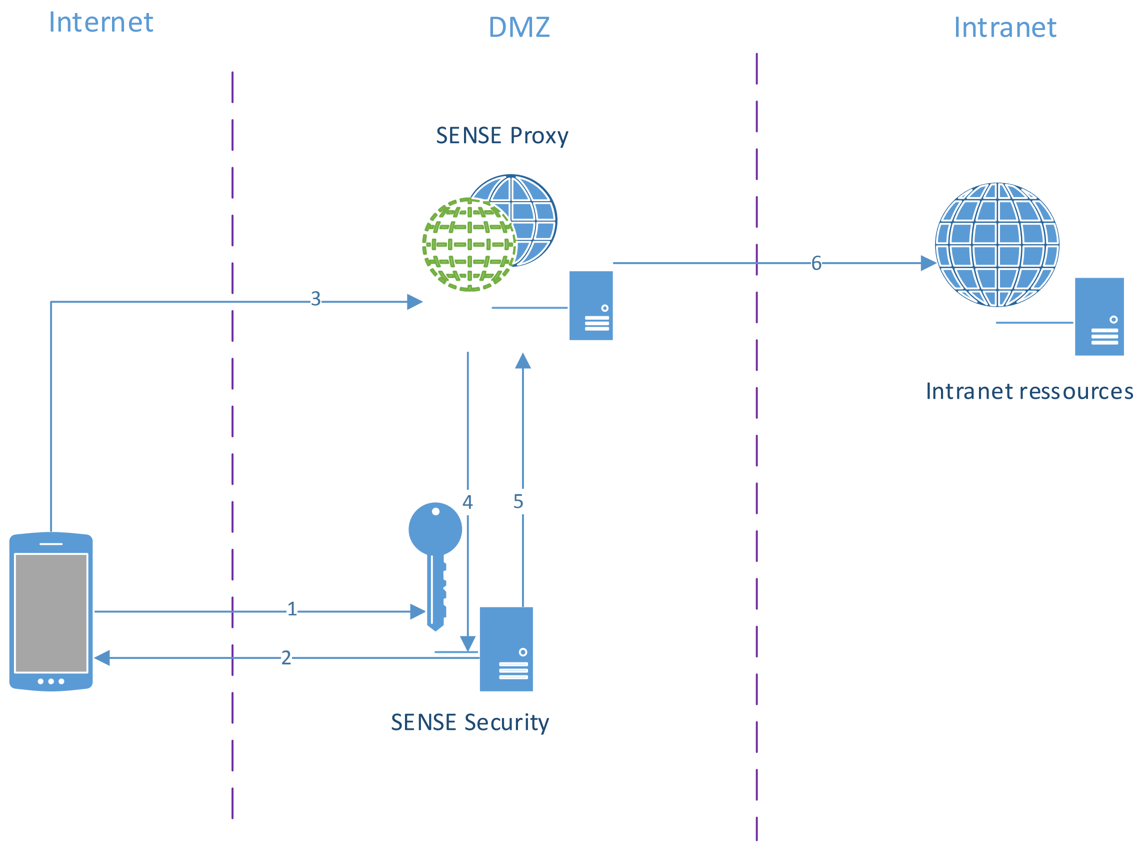
  To answer high availability constraints this server must be replicated as well as its database.

- Sense Proxy, this component is stateless. Multiple Proxy servers can be deployed per security server. A proxy server is responsible for:
  - Decryption and encryption of inbound and outbound communication
  - Sending a request to the security server for information about the validity of the session
  - Validation of the app context

To answer high availability constraints multiple Proxy servers can be deployed for every Security server in order to dispatch the processing charges.

3 WORKFLOW

The following workflow will enable you to understand the interaction between all the different components of the solution.



The main steps to get access to backend resources from mobile devices are as follows:

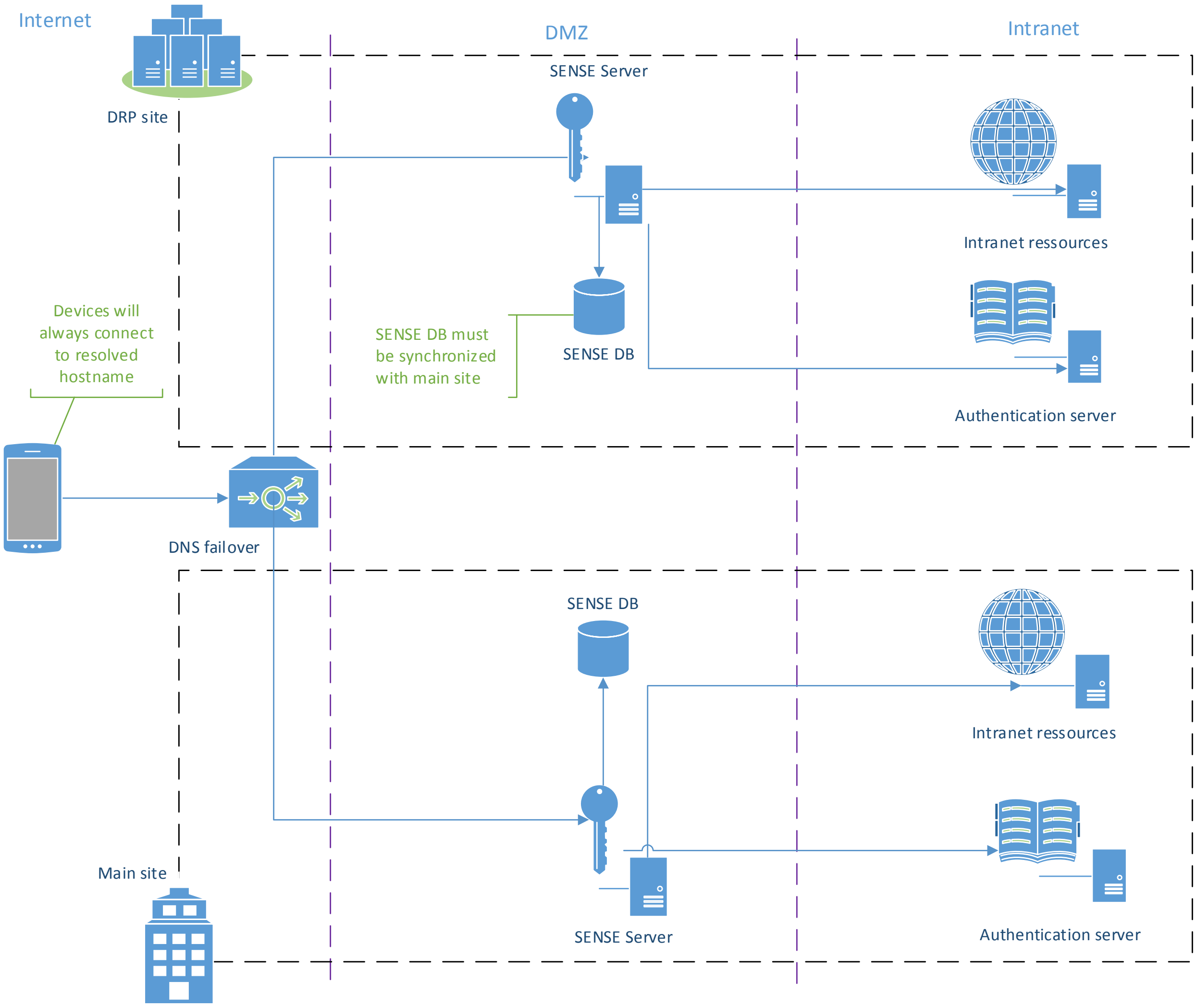
1. The mobile device establishes a secure channel to the ZENworks Mobile Workspace Security server.
2. The Security server creates a session and sends back the session ID to the device.
3. The device establishes a connection with the SENSE Proxy server and gives the previously retrieved session ID. Therefore, all further requests will go through the Proxy.
4. The Proxy server requests an authorization to the Security server according to the session ID
5. The Security server grants access to the user according to the session ID.
6. The Proxy decrypts and provides access to the backend resources.

4 FAIL OVER

The Security server is a critical component. If it fails it will temporarily prevent any Proxy from granting access to backend resources. However, a fail over mechanisms can be easily implemented by only replicating the database. In the case of a service interruption of the Security server, the end user would just have to re-open a session by entering his or her credentials with the failover instance.

Replication of the database that contains the shared keys can be done on a regular basis with SQL script or by using the database in master/slave mode.

The following schema explains how the failover instance can be setup:



4.1 Data Recovery

To be able to recover quickly after a crash and to avoid users from re-enrolling, the most important thing to backup is the Security server database. As installation of ZENworks Mobile Workspace may take less than 5 minutes, a full installation with database import can take less than 15 minutes.

To backup the database, 3 methods are available.

4.1.1 VM Snapshot

This is the easiest way to back up the whole server but the service may be disrupted during the Snapshot (in case of heavy load). Copying the VM Snapshot to a recovery site may take time.

4.1.2 Databases Export/Import

The most efficient way is to backup the database every 5 minutes on a remote folder. In case of a crash, you will be able install ZENworks Mobile Workspace again on the recovery site and import the database. You can follow the instructions from the “Backup and Restore” guide.

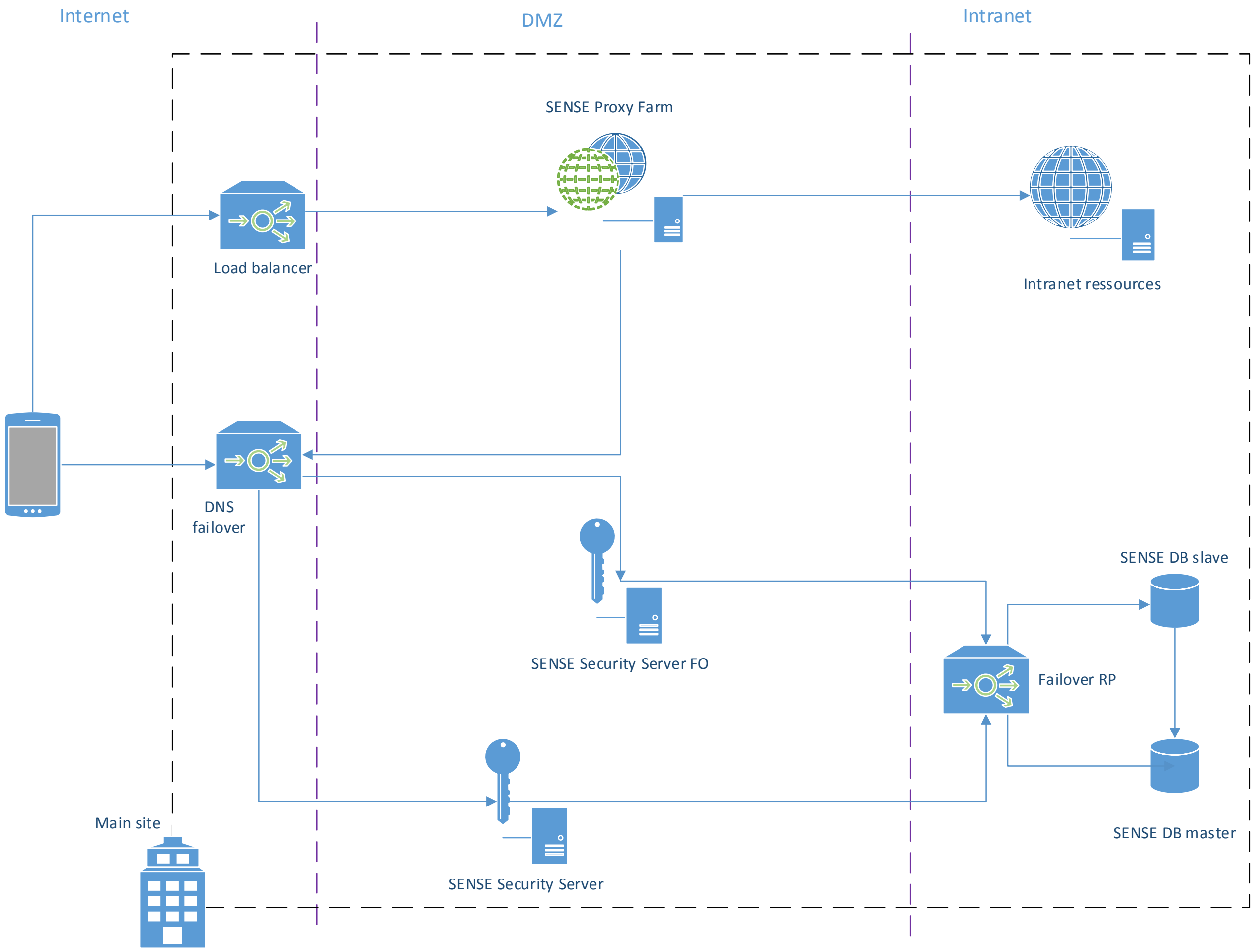
4.1.3 Live Synchronization

In a critical environment, failover must almost be done instantly. The ZENworks Mobile Workspace database can work in master-slave mode so any change of the master will be replicated on the slave.

5 LOAD BALANCING

The Proxy server relies on the Security server to grant access to backend resources, for this reason it is possible to deploy as much as needed of the Proxy. Most of the traffic will go through it and that can overload it. A load balancer must be set up in front of a Proxy farm to guarantee load balancing and failover. Therefore, if a Proxy node in the farm fails, the charge will be dispatched among the others.

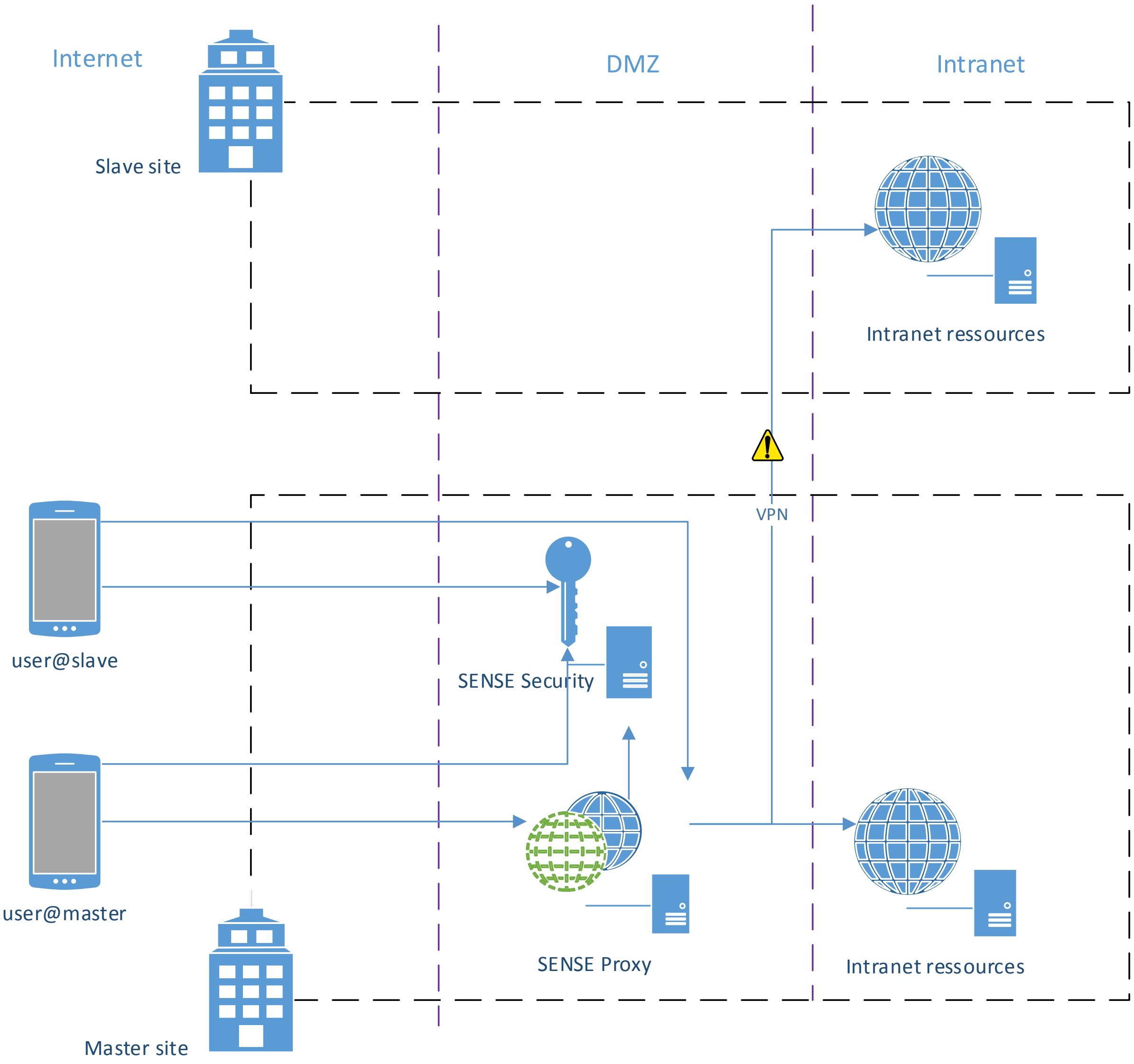
The following schema explains the architecture of both Proxy load-balancing and Security failover.



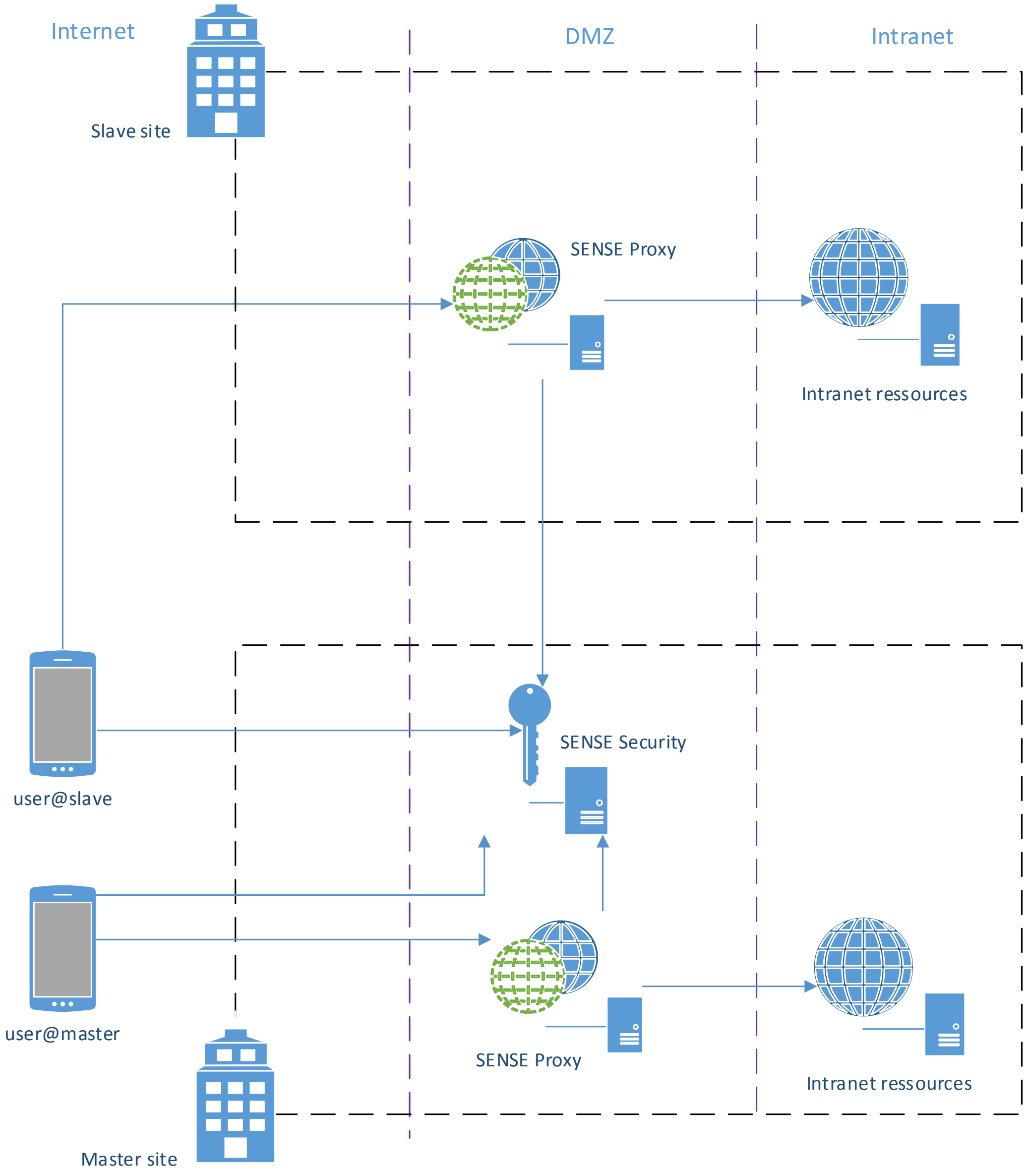
6 MULTISITE

Having a farm of Proxy can be also interesting to avoid overloading the intranet bandwidth.

The following scheme shows a common way to give access from devices to intranet resources of a multi-site company.



With ZENworks Mobile Workspace you can get close to your resources to avoid network equipment overload and faster access. Therefore, a different mobile client will be provided to allow the user to be authenticated against the main Security server but get access to its Proxy through another URL.


Internet
DMZ
Intranet
Slave site
SENSE Proxy
Intranet ressources
user@slave
SENSE Security
user@master
SENSE Proxy
Intranet ressources
Master site