ZENworks Mobile Workspace

Advanced Integration in High Availability Environments

Version 3.18.1 - November 2018

Table of Contents

Overview

This document aims to describe at a high level how ZENworks Mobile Workspace components can be used in high availability environments. If you intend to put in place such configuration, please contact your solution provider to define the best solution according to your needs.

Principle

The server is composed by the following components:

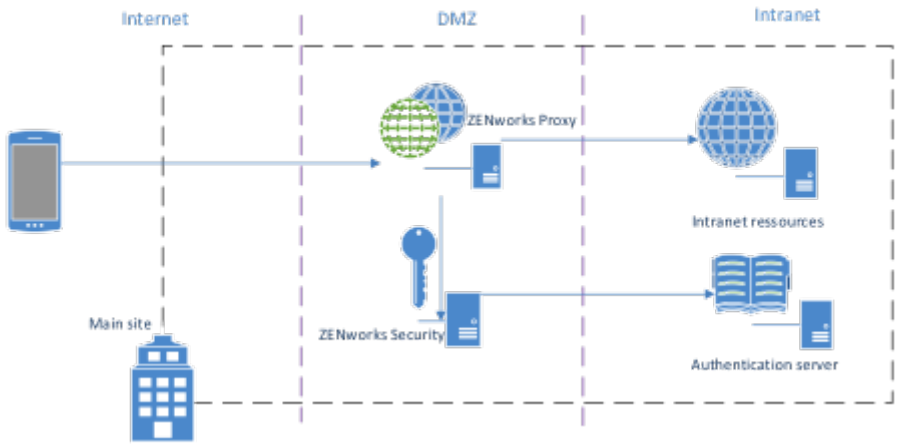

Figure 1. Overview

- ZENWorks Security server, this component is stateful since the existing sessions are in-memory. A session contains all the information's about the user, its credentials and the session key that is being generated to 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.
- ZENWorks Proxy server, this component is stateless. Multiple Proxy servers can be deployed per security server. A proxy server is responsible for:
  - Decrypt and encrypt inbound and outbound communications.
  - Requesting to the security server the validity of the session.
  - Validation of the app context.

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

Workflow

Below a schema to understand the interaction between all the different components of the solution:

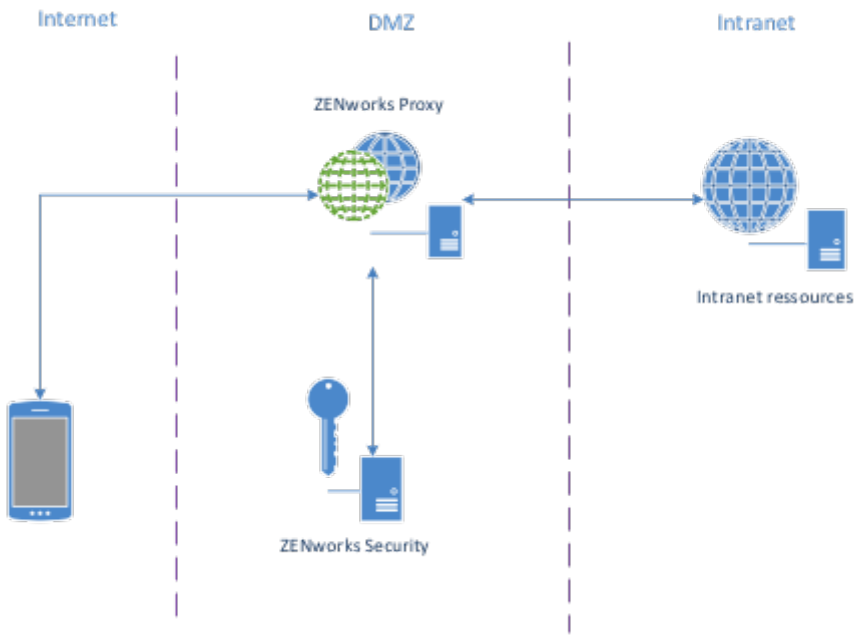

Figure 2. Workflow

The main steps to get access to backend resources from mobile devices is the following:

1. The mobile device establishes a secure channel to the ZENWorks Security server through the ZENWorks Proxy.
2. The ZENWorks Security server creates a session and send back the session ID to the device.
3. The device establishes a connection with the ZENWorks Proxy and gives the previously retrieved session ID.
4. The ZENWorks Proxy requests an authorization to the ZENWorks Security server according to the session ID.
5. The ZENWorks Security server grants access for the user according to the session ID.
6. The ZENWorks Proxy decrypt and open the access to the backend resources.

Fail Over

The security server is a critical component since a failure of it would temporarily prevent any Proxy to grant 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 its credentials with the failover instance.

The replication of the database that contains the shared keys can be done on 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:

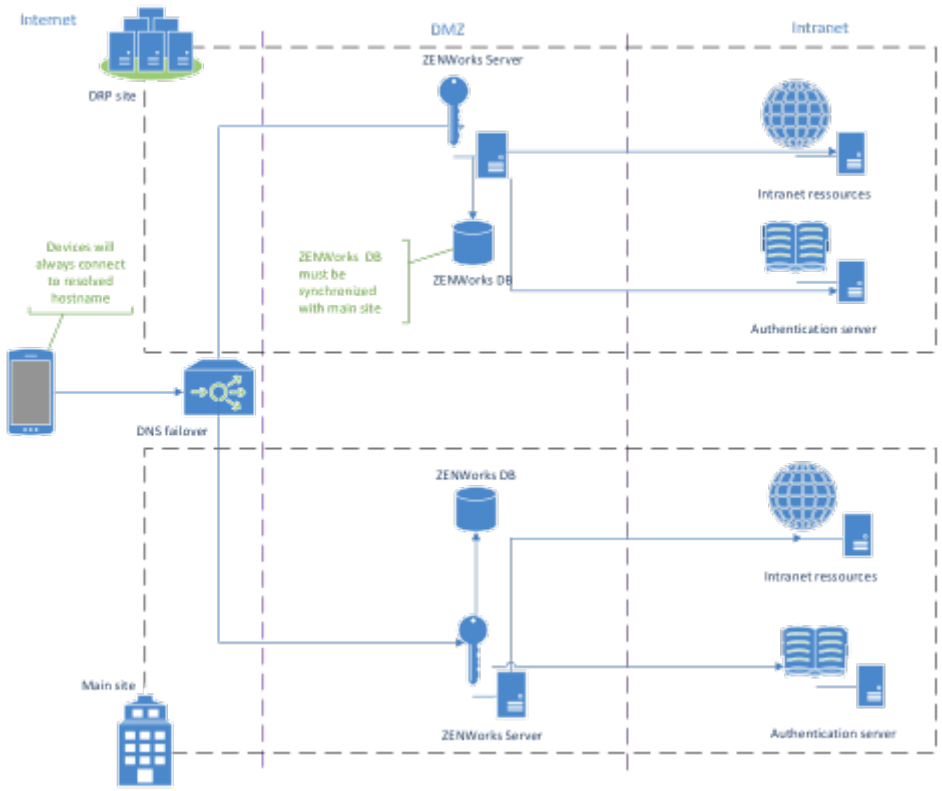

Figure 3. Failover

Data Recovery

To be able to recover quickly after a crash and to avoid users to re enroll, 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.

VM Snapshot

It’s the easiest way to backup the whole server but the service may be disrupted during the Snapshot (in case of heavy load). Also the copy of a VM Snapshot to a recovery site may take time.

Databases Export/Import

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

Live Synchronization

In critical environment, failover must almost be done instantly. ZENworks Mobile Workspace databse can work in master-slave mode so any change of the master will be replicated to the slave. Contact Sysmosoft support for such requirement.

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 Proxy. Most of the traffic will go through it that can overload it. A load balancer must be setup in front of a Proxy farm to guarantee load balancing and failover. Therefore, if a Proxy node in the farm fail, the charge will be dispatched among the others.

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

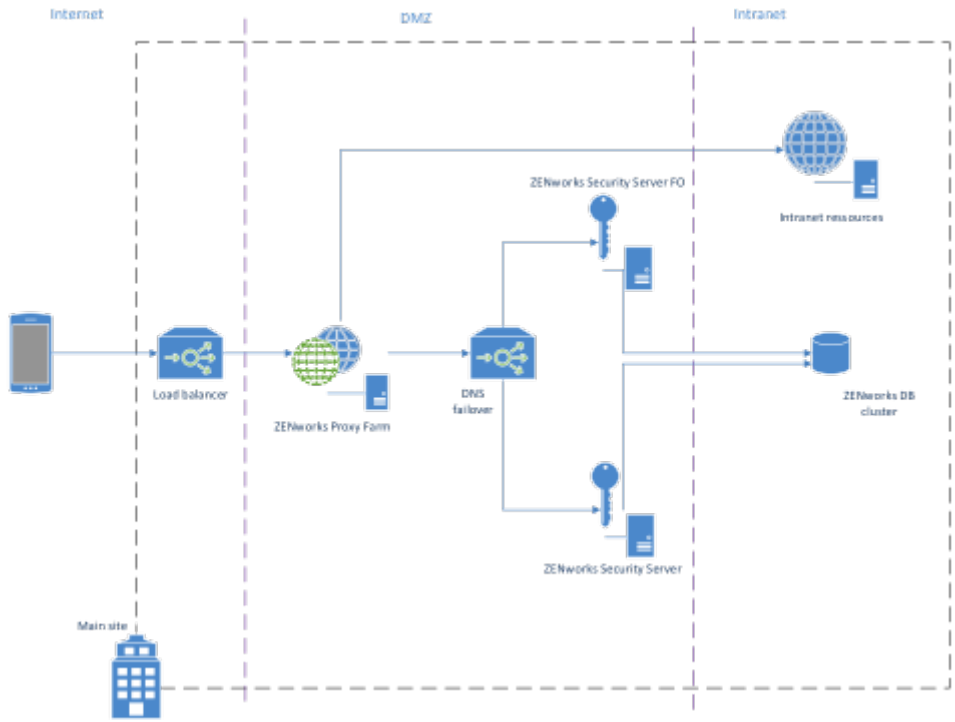

Figure 4. Load balancing

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 multisite company:

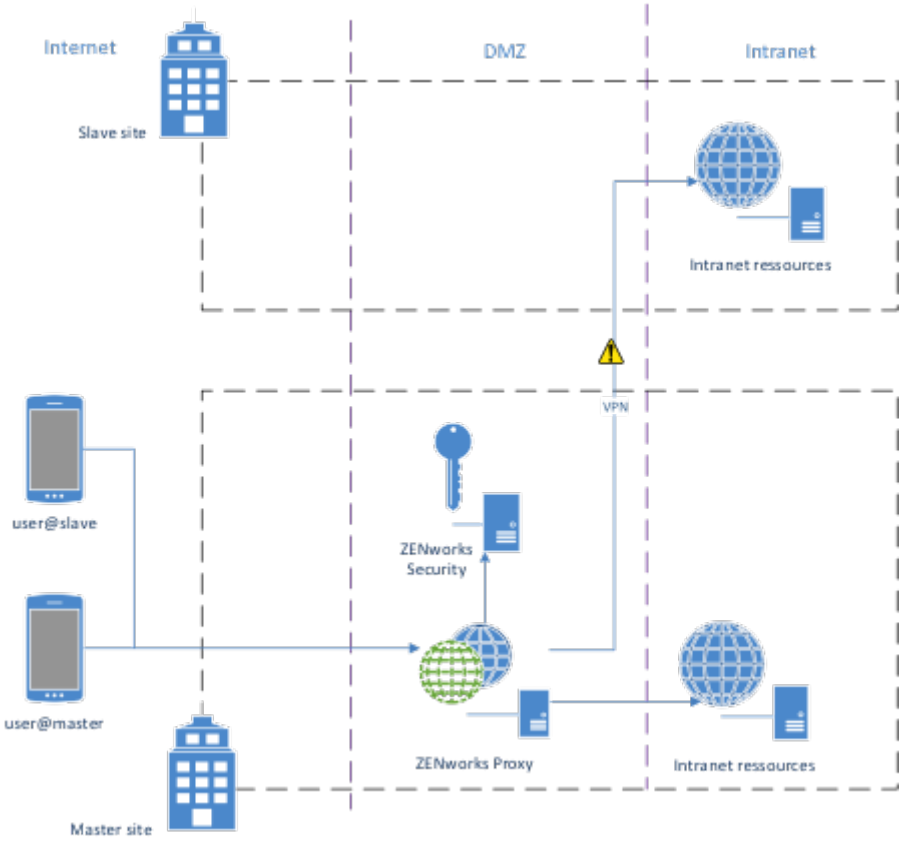

Figure 5. Common multisite

With ZENworks Mobile Workspace you can get as close as 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:

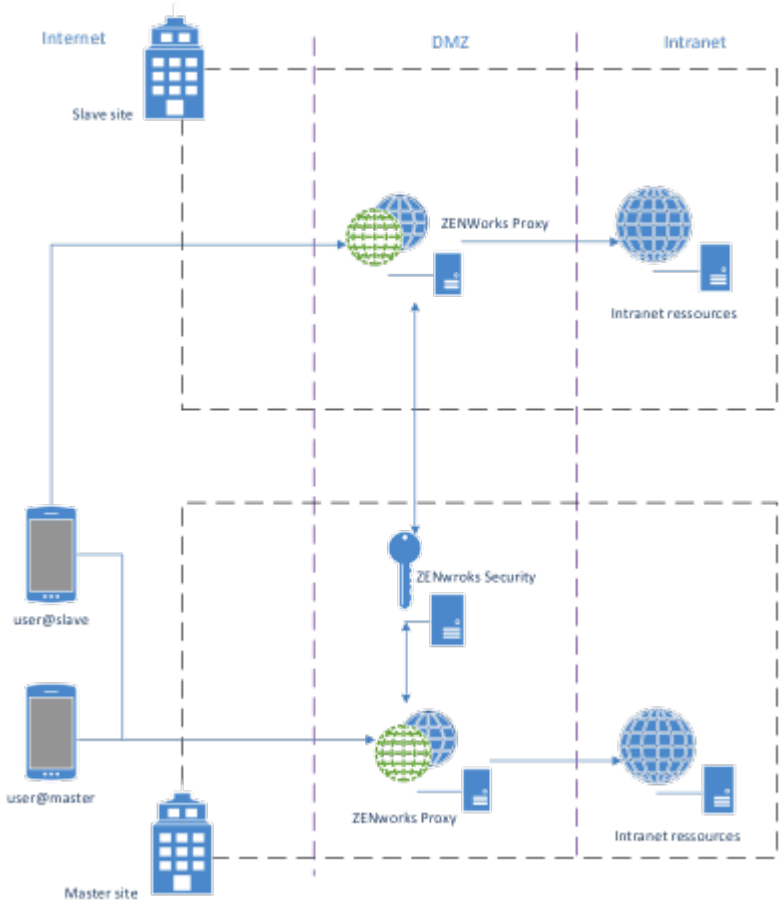

Figure 6. ZENworks Mobile Workspace multisite