Swivel Deployment

Contents

Swivel Deployment Overview

This document details the considerations to be made in the positioning of Swivel in a network.

Prerequisites

Swivel 3.x

Workflow

Initially a user is provisioned from a data source and may be automatically provisioned with a PIN and possibly a One Time Code, commonly the data source is Active Directory, and this provision process is fully automated. The user can be provisioned with a variety of authentication methods.

A user may connect in a variety of methods such as with their web browser or client software. The user then will be required to enter their username, password (if required), and One Time Code. Swivel supports an OTC that is pre-sent to the user, or on Demand and sent to the user when requested, or an OTC generated at the point of authentication such as with a hardware Token.

The Username, and password where required, and OTC are checked and authentication allowed or denied. If the authentication is in advance, the user is sent their next OTC. Depending on the integration Swivel may check the Username/OTC and Password, or the setup may be with primary/secondary authentication servers in a chained authentication.

Some variations exist on this such as where authentication uses Swivel as an Identity Provider (IDP) and is redirected to the Swivel IDP such as with Google or Two Stage authentication where the user is asked for a password and if correct the user can then enter their OTC.

Swivel supports the following Authentication Methods

Deployment Scenarios

Swivel needs to communicate with various services such as DNS servers and data sources such as Active Directory or LDAP, or have Single Channel Images requested by clients for authentication, and these may make an influence on where to deploy Swivel. For a list of ports and services required for a deployment see Swivel Install Information Notes for Engineers

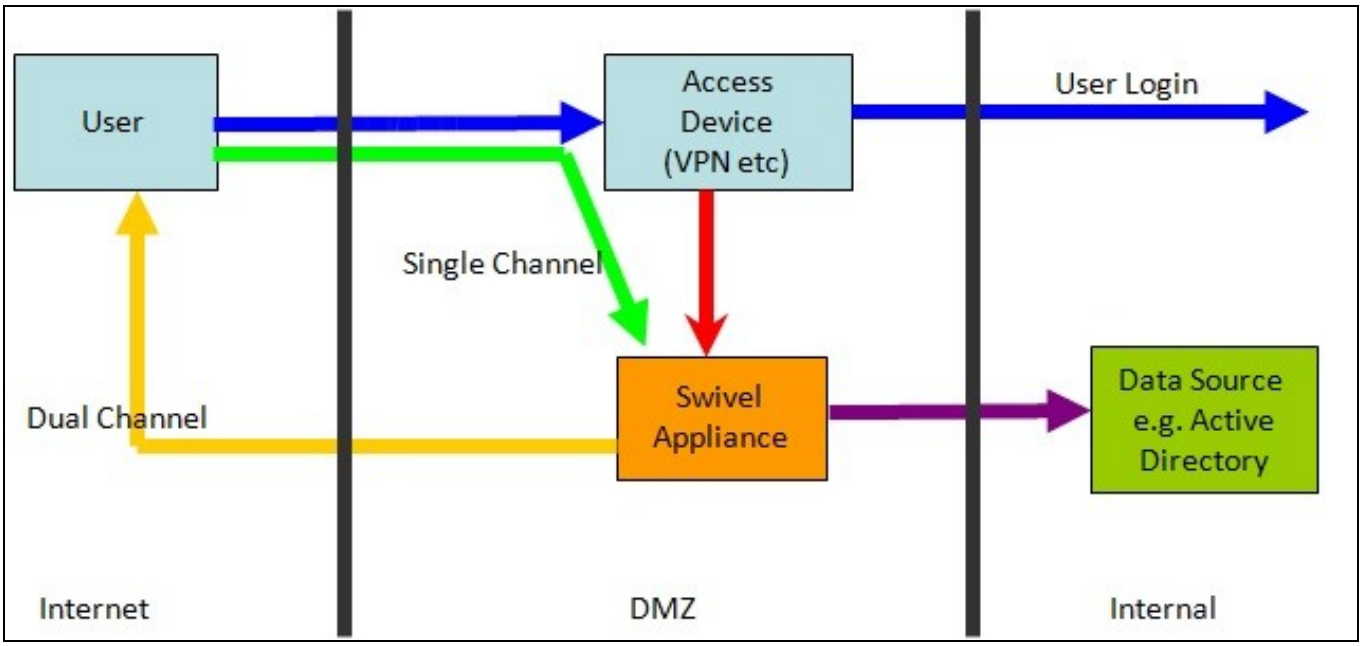
DMZ

Integrations may require clients external to an organisation, to make a request from the Swivel server or appliance, for security reasons Swivel is therefore usually deployed in the DMZ. Swivel appliances employ additional security by only allowing external connections to a proxy port. Reasons for making an external connection to the Swivel server include:

- TURing
- Pinpad
- Request a new SMS
- Security String Index
- Dual Channel Confirmed Message
- Taskbar
- ResetPIN
- Mobile Phone Clients

An exception to this is where the integration includes a device that proxies the request to the Swivel server so that there is no direct connection, this includes integrations such as OWA, ISA, TMG, Citrix Web Interface.

For security, by default Swivel appliances provide desperation between management on port 8080 and external requests using port 8443, although this can also be configured to accept requests on port 443 (see Using Port Address Translation (PAT) on the Swivel hardware or virtual appliance).



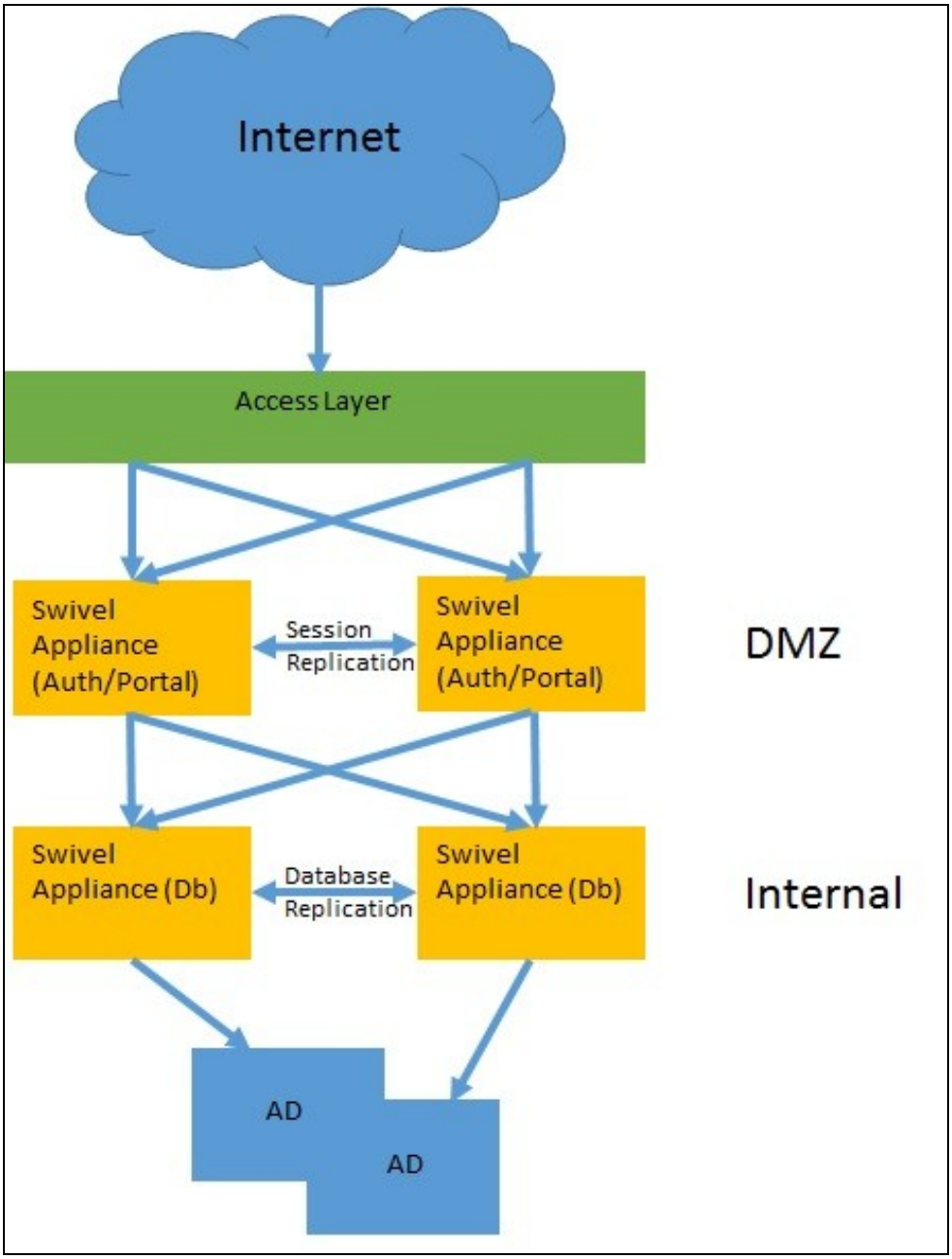
Internal

The general security principle for networks is that there should never be a connection from an external (untrusted) network to an internal (trusted) network. Where the Swivel server is used only for SMS authentication possibly using a GSM Modem or more commonly an SMS Gateway, using a hardware Token, or the clients are all located internally, it may be acceptable to place Swivel in the internal network.

Also where RADIUS responses are used for authentication such as using Challenge and Response new SMS requests can be made without the client making a direct request to Swivel.

Authentication and Database separation

For requirements where no data is to be stored within the DMZ, it is possible to separate the Authentication from the database using two Swivel A/A pairs, one pair for authentications and the second pair to hold the user data. The DMZ has Swivel Virtual or hardware Appliances as Authentication servers connecting to Swivel virtual or hardware Appliances acting as Database servers, or to use a database external to the Swivel appliance.



- VIP on Authentication servers provides resilience for single channel and Agent-XML authentication as well as security strings for mobile apps and User Portal functions such as ChangePIN Reset PIN
- RADIUS authentication is made using the real IP addresses of the DMZ Swivel virtual or hardware appliances
- Session replication provides resilience for sessions made on each authentication server
- VIP on Swivel database servers provides database resilience
- Swivel virtual or hardware appliances handle Database replication for resilience of data
- Swivel virtual or hardware appliances as Database servers import data into Swivel database from external data sources
- Two servers to import data from data source such as AD for resilience

Each Swivel server is configured with the same repositories, groups and transports. The Authentication servers define the Database servers as their database and not their local database.