PortWise Security Options for 2X Application Services

Introduction

The aim of PortWise is to extend and enhance existing infrastructures, offering customers a flexible range of remote access and security options to complement their existing investment.

Where 2X services presently exist PortWise provides the option to extend their features and where 2X services are not deployed remotely PortWise offers the ability to do so without having to overly complicate the existing infrastructure. 2X services can be delivered securely whilst also being able offer other services such as true client-server services where required.

2X Authentication Options

PortWise is a comprehensive software based approach to identity and access management. It can enable a diverse user base completely secure remote access to a variety of internal 2X published applications, secured by a range of two factor authentication options. These include;

- SMS based One Time Passwords
- PortWise Soft Tokens
- PortWise WebID
- OATH compliant tokens
- RSA tags
- PKI Certificates
- RADIUS based solutions
- and numerous others

The PortWise platform brokers the authentication requests, providing granular access and control over user authentication, once successfully authentication the user can be presented with their access options.

PortWise TruID on iPhone (a mobile soft token)

PortWise Solution Summary

PortWise would become the point of entry, providing a range of two-factor authentication methods (integrated with other 3rd party solutions where required). Once the PortWise portal has authenticated the user by whichever method they selected the user can then be present with various different options for application delivery

- Standard PortWise Portal presenting both native services and 2X data services, the user then uses the standard 2X desktop client as normal to gain access to applications. The 2X web portal can also be presented as a option in the standard portal dashboard
- Redirection directly to the 2X web portal. In this mode PortWise is effectively just providing the additional authentication as well as securing the data traffic.
- Mixed mode resources, if required specific application icons can be presented within the PortWise portal to give direct access. This involves PortWise protecting the data traffic and starting specific applications via starting the local 2X client with the relevant command line options

PortWise traditionally provides the user with a standard dashboard of the resources they are authorised to access, be these purely web based such as an Intranet or fat client based such as Outlook. The user connects to the PortWise Access Point and is then authenticated and authorised based on the authentication method they choose and the access rules defined in the backend PortWise Policy and Authentication servers. The Access Points provide the SSL portal and dashboard and the backend servers provide the authentication and authorisation services.

In order to offer the choice of these authentication methods PortWise Access Points would be used to provide the user with the additional authentication options. Architecturally, PortWise Access Points and the 2X Web Portal are similar. Both provide an web gateway and both require session authorisation from the internal network .

The PortWise Access Points would sit in the DMZ, and can be branded identically with the 2X branding if required. The authentication dialogue would of course be different as all the available auth options would be presented to the user. These could be purely PortWise methods, third party options such as RSA or a combination of both.

Once authenticated PortWise SSO can be used to automatically log into the 2X web portal if required.

Solution Technical Overview

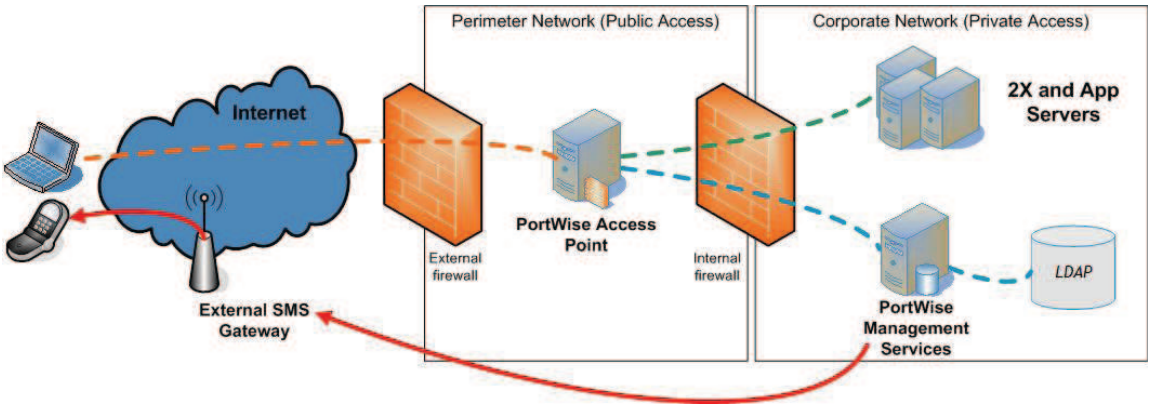
The PortWise solution consists of two types of server, the **PortWise Access Point** and the **PortWise Admin Server**. Together these servers provide an extremely secure end-to-end solution. The diagram below shows the positioning of these appliances into the company infrastructure.

Key points:

- The PortWise infrastructure is installed side-by-side, as a complementary solution.
- The PortWise Access Point and Admin servers deal with passing authentication requests relevant servers, either native PortWise services or third parties.
- The PortWise Access Point passes authentication requests to the PortWise Admin Server, which provides such two factor methods as Mobile Text and Soft-token authentication.
- The PortWise Access Points can be used to provide Single Sign On to the 2X portal if required
- The native 2X traffic is encrypted and tunnelled over the PortWise SSL VPN.

The user starts up their browser and types in the normal URL used to access PortWise and are presented with the authentication options available. This login page is delivered by the PortWise Access Points and no matter which authentication method is selected the credentials are passed back to the PortWise Admin server, which then performs the authentication, either directly to the PortWise Policy Service or to the third party backend servers. This means that all authentication traffic is held on the internal network.

Once authenticated, The PortWise Access Point can either redirect the browser to the 2X web portal or present the standard PortWise Portal. If redirecting to the 2X portal PortWise can transparently log the user into the web front end using PortWise Single Sign On if required. If PortWise cannot pass through the username and password from the initial login (i.e. using PortWise Synchronised where the lan password is not required) or does not have the user's credentials in secured storage, the user will be prompted for their credentials. These credentials will then be stored securely inside the PortWise User Storage, and the subsequent logins will be transparent until the username and password changes.



Option 1 – PortWise provides authentication and data tunnel for desktop client

If the 2X Web Portal is not being used PortWise can be deployed to deliver both the authentication and data tunnelling services.

Once the user has successfully authenticated they are presented with a standard PortWise portal page and 2X offered as a resource. When selected PortWise will push out the on-demand VPN client to protect and tunnel the application data. The local 2X client is then started for the user and they continue to work as if they where directly connected to the corporate network.

If the 2X Web Portal is being used it can also be defined as a standard web resource within the portal, giving access to all 2X options as well as standard resources.

Users then have the choice of using standard PortWise application delivery of web based services and client-server applications together with 2X.

Option 2 – PortWise provides authentication and data tunnel, 2X portal used

Where only authentication is required the PortWise Access Points can be configured to automatically start the VPN client and redirect to the 2X web portal once the user has passed the authentication process.

With this mode of working the user never sees the **Fel!Kontakt har inte definierats.** portal and all the PortWise specific pages needed for authentication can be branded to match the 2X portal.

Authentication and data traffic security are still handled by PortWise in the background but only the 2X portal is visible to the user.

PortWise Single Sign On can be used to transparently connect the user to the 2X portal.

Option 3 – Mixed mode PortWise Portal providing direct access to 2X apps

If complete flexibility is required the servers can be configured to offer not only access to the standard 2X desktop client and the web portal but can have individual 2X applications configured within the PortWise standard portal.

By utilising the options present in the 2X local client the PortWise portal can be configured to offer direct access to the 2X published applications.

The user authenticates to the standard PortWise portal where they are present with resource icons that will automatically start the local 2X client and the specific application. PortWise still handles both authentication and data encryption but also allows the user to access standard PortWise resources, the full 2X client or simply single applications published via 2X.

Portal Resources Example

The screenshot below shows the standard PortWise portal offering a variety of resources, these consist of :-

- **2X Desktop client** – a data tunnel is opened and the local 2X client opened on the PC allowing the user to select published applications from there
- **2X Portal** – the 2X web portal is opened in a separate window and the user is automatically logged in using PortWise Single Sign On
- **Fileshare** – a standard PortWise data resource where the users is presented with a fileshare on a remote fileserver
- **Notepad (via 2X)** – rather than offering the full 2X client or web portal the user is automatically delivered the published Notepad application from the 2X servers. The local 2X client is started automatically and told to connect to the specific application
- **OWA** – standard PortWise web based resource giving access to Outlook Web Access
- **Outlook Full Client** – a standard PortWise data resource where the local Outlook traffic is securely passed to the remote Exchange servers

This example PortWise portal shows 2X full client access, 2X web portal access and 2X specific application access as well as standard PortWise web and data resources. The user in this case has maximum flexibility in application delivery and is able to choose exactly how there resources are securely delivered.