Pylon Anywhere™ Security Whitepaper

A whitepaper from iAnywhere Solutions, Inc., a subsidiary of Sybase, Inc.

Contents

Pylon Anywhere Introduction

Pylon Anywhere increases mobile worker productivity by delivering mobile and wireless access to Lotus Notes or Microsoft Exchange information including email, calendar, contacts, tasks and memos. It provides direct, server-based synchronization ensuring always available access to email and PIM information from the most popular mobile devices. With access to up-to-date information, even when a desktop or laptop is inaccessible, mobile workers can keep in touch no matter where the day takes them.

Pylon Anywhere consists of both server and client components. The server is the host to which mobile devices connect in order to synchronize data. The server controls functions such as security, authenticating users, communication, logging, and reporting, among others.

In addition, Pylon Anywhere provides client components that run on client computers and handheld devices, and facilitate interaction with the server.

Security Topics

This document outlines four of the major security concerns organizations have when deploying an email and PIM solution to mobile devices, and how Pylon Anywhere addresses these concerns.

Specifically, this document covers:

- **Communication Security** How does Pylon Anywhere protect the data in transit over the public Internet?
- **User Authentication** How does Pylon Anywhere authenticate end users?
- **Network Security** How does Pylon Anywhere minimize the risk of opening an organization's network to mobile devices?
- **On-Device Security** How can data on a mobile device be protected?

Communication Security

Communication Security Overview

Ensuring that communication over the public Internet is protected is an important aspect to an effective and secure mobile solution. This section provides an overview of the communication between a Pylon Anywhere client (an end user with a mobile device) and the Pylon Anywhere server.

Encrypted Data Within Standard Protocols

Pylon Anywhere clients communicate with the Pylon Anywhere server using standard HTTP or HTTPS. The benefit of using a standard protocol is the ability to leverage an organization's existing network security infrastructure, including firewall configuration. It is important to note that HTTP is used as the communication protocol to transport messages between client and server, but more importantly that the contents of these HTTP messages are fully encrypted by default. In addition, an organization has the ability to determine which encryption method to use, including:

- **SSL** Uses a secure socket connection to encrypt the data as it is transferred.
- **Triple DES** This FIPS 140-2 certified encryption offers 112-bit encryption strength using three 56-bit keys. It is a highly secure method, but can be inappropriate for very slow connections or mobile devices with limited processing power.
- **AES** This FIPS 140-2 certified encryption offers an advanced encryption method using 128-bit keys. It is optimized for wireless connectivity while providing a highly secure connection. This is the most commonly selected encryption method.
- **No encryption** This option should only be used for devices which do not connect through the public Internet or that connect via other secure methods.

Pylon Anywhere administrators are given the flexibility to allow different groups of users to communicate using different protocols.

Secure Key Exchange

Exchanging keys securely is an important component of an effective encryption policy. Pylon Anywhere uses Diffie-Hellman to negotiate session-based symmetrical keys. The Diffie-Hellman key agreement protocol, also known as exponential key agreement, allows the client and server to securely exchange a secret key over HTTP. By using this protocol, each client session has a unique symmetrical key, providing extremely tight and effective security between the client and server.

User Authentication

User Authentication Overview

All users who connect remotely to the Pylon Anywhere server must be able to authenticate with the server in order to establish a connection. Pylon Anywhere is designed to be flexible, and is easily configured to work within a wide variety of network environments. Choosing an authentication strategy is an important component of a mobile solution.

Pylon Anywhere authentication is handled on a user-by-user basis, and different authentication methods can be used for different users.

User Authentication Options

Pylon Anywhere provides flexibility when determining a user authentication strategy. There are four available approaches to authenticate users with the Pylon Anywhere server:

- Windows NT Domain Authentication
- Domino Authentication
- Pylon Anywhere Authentication
- LDAP Authentication

Windows NT Domain Authentication

For Exchange users, the default authentication approach is Windows NT Domain authentication. Authenticating against the user's Windows NT account is the most secure approach for authenticating with the Pylon Anywhere server, and later for accessing the Exchange server. With Windows NT Domain authentication, Pylon Anywhere authenticates users based on their Windows NT credentials. In order to connect, the user must provide the domain name, user ID, and password. For most situations, Windows NT Domain authentication is recommended for Windows NT users.

Domino Authentication

For Domino users, the default authentication approach is Domino authentication. When a user connects for the first time, Pylon Anywhere authenticates the user against the Domino server to automatically create a new user account. With other approaches to authentication, additional configuration is required to grant access to the Domino server. Domino authentication simplifies the process of granting access to the Domino server to retrieve email and PIM information.

Pylon Anywhere Authentication

With Pylon Anywhere authentication, users are authenticated against the Pylon Anywhere database. In order to use this authentication approach, you must have a Pylon Anywhere account set up for each user before the user attempts to connect for the first time. If the account has not been set up, the user cannot connect.

To provide access to Exchange or Domino, an administrator must enter additional information to facilitate that connection. Some organizations and end users prefer Pylon Anywhere authentication because it is simple and straightforward. It is a 'self-contained' solution, in that authentication relies entirely on the Pylon Anywhere database, eliminating the need to access other servers during the authentication process. With Pylon Anywhere authentication, the format for a user name can be simple. With NT Domain authentication, for example, the domain name must proceed the user name in order for the user to connect.

LDAP Authentication

With LDAP authentication, end users are authenticated against a specific LDAP source. This connection is easily configured from the Pylon Anywhere administration console. Similar to Pylon Anywhere authentication, an additional step is required to grant these users access to Exchange or Domino to retrieve email and PIM information.

Network Security

Network Security Overview

Pylon Anywhere can be installed to leverage an organization's existing architecture and security plan. This section outlines possible network configurations and provides details about how these configurations may fit in with your organization's architecture and security plan.

An organization has several options for placing Pylon Anywhere servers in relation to their perimeter network (also known as DMZ, demilitarized zone, or screened subnet) and corporate firewalls.

Organizational policy may dictate (at least to some degree) how Pylon Anywhere must be deployed within a network configuration. This section includes general information about network configuration, as well as some diagrams of typical network configurations. The default firewall ports referenced here may be different than those configured within an organization's environment.

Changing Communication Ports and Protocols

A common requirement for most organizations is that the network configuration should involve at least one port change and at least one protocol change. A straight pass-through of either ports, protocols, or both is not recommended.

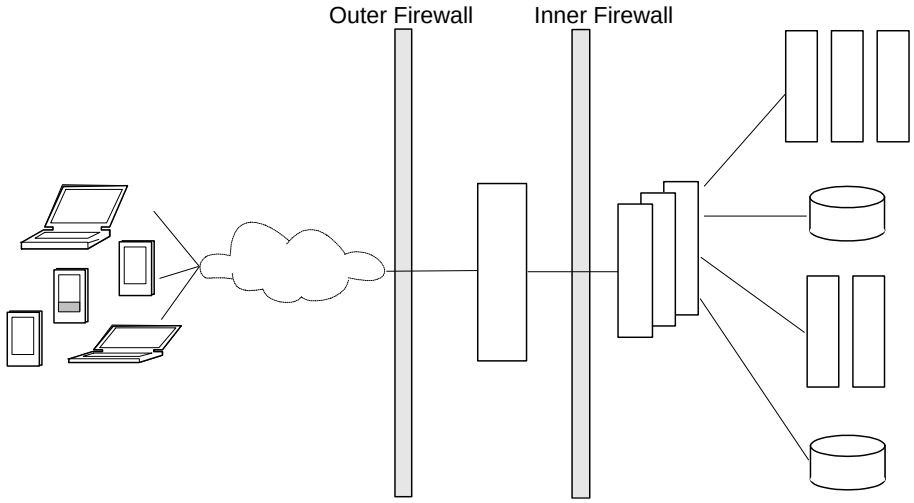

Figure 1: Straight pass-through (without changing ports or protocols) is not recommended

Instead, an organization can use a proxy server to make changes. Changing both ports and protocols is recommended. The following figure shows a typical

scenario using a proxy server to change both communication ports and protocols.

Figure 2: An example of changing ports and protocols

Sample Configurations

The pages that follow show some typical network configurations. To keep the diagrams simple, changing ports and protocols are not illustrated. The following configurations are covered in this section:

- Basic Configuration (Single Firewall)
- Reverse Proxy Server in the Perimeter Network (DMZ)
- Pylon Anywhere Mobile Gateway in the DMZ
- Combined Deployment in the DMZ
- VPN and RAS Connectivity
- IIS and ISAPI in the DMZ

Basic Configuration (Single Firewall)

The following diagram shows the basic structures for the deployment of Pylon Anywhere in a single firewall environment. In this scenario, all of the Pylon Anywhere components and the enterprise servers accessed by Pylon Anywhere are behind the corporate firewall. Access may be directly through the firewall, or proxy servers (such as Microsoft Internet Security and Access Server) can be used for added security.

Figure 3: Basic deployment behind a single firewall

Communication through the firewall takes place using HTTP or HTTPS. The default port settings are shown in the following table.

Note that your port settings may be different, depending on how your network is configured.

Default ports for communication through firewall

Communication Protocol	Default Port
HTTP	80
HTTPS	443

All communications are authenticated, encrypted, and compressed by the Pylon Anywhere servers.

Configuration notes (for single firewall)

- This configuration is the most basic configuration, showing the basic elements of a Pylon Anywhere solution.

- In this configuration, access can be directly through the firewall, or proxy servers (such as Microsoft Internet Security and Access Server) can be used for added security.

Reverse Proxy Server in the Perimeter Network (DMZ)

A reverse proxy server inside the DMZ is the preferred solution for most organizations as it offers a high level of port security, is extremely simple to deploy, and is highly scalable.

Figure 4: Reverse proxy server in a perimeter network (DMZ)

A reverse proxy server generally aggregates inbound IP requests to a single port in the firewall. Communication through the firewall takes place using HTTP or HTTPS.

The default port settings are shown in the following table. Note that your port settings may be different, depending on how your network is configured.

Default ports for communication through firewall

Communication Protocol	Default Port
HTTP	80
HTTPS	443

All communications are authenticated, encrypted, and compressed by the Pylon Anywhere servers.

Configuration overview (for reverse proxy server in DMZ)

The reverse proxy intercepts an inbound HTTP packet and depending on the configuration may do one of the following:

- authenticate the user
- inspect the packet against various rules
- direct the packet to an SSL port through a restricted enterprise port

Therefore, an organization can minimize the ports open in the corporate firewall, apply various alternate firewall security measures to that open port, and restrict communications with the open port to only the reverse proxy computer.

An example

Configuration of the reverse proxy server is best illustrated with an example. Assume the server address or the browsing web address of the Pylon Anywhere server is sync.acme.com. An organization would configure the reverse proxy server to intercept any requests for this address and to direct that address to the IIS server securely placed behind the firewall. The machine address and ports of this IIS server are not visible outside the firewall.

The DNS routing entry for external address resolution is configured to route any request to sync.acme.com to the reverse proxy server. Any request for sync.acme.com when the device is in the cradle or connected to the internal address would point to the IIS server for the Pylon Anywhere servers.

Configuration notes (for reverse proxy server in the DMZ)

- This configuration is the preferred solution for most organizations.
- This configuration helps ensure secure communication between the reverse proxy server and the Pylon Anywhere server because it restricts the number of open ports.
- Microsoft ISA server is an example of a reverse proxy server. Apache is another reverse proxy server that can be used.

Benefits of reverse proxy server in the DMZ

The benefits of the reverse proxy implementation include simplicity, robustness, flexibility, and security.

Simplicity

- Installation can take only a few minutes.
- A single port is open in the firewall, and it can be restricted to a single IP address.
- DNS routing makes the experience extremely simple whether the client is internal or external.

Robustness

- Using industry standard reverse proxy servers, an organization can deploy solutions that are engineered to be scalable and reliable.
- Reverse proxy servers can be deployed to minimize geographic distribution where users can connect one or many reverse proxy servers to a centralized Pylon Anywhere server.
- Reverse proxy servers do not significantly reduce performance.
- Configuring Secure ID or other external authentication sources is extremely simple when using a reverse proxy server.

Flexibility

- Because Pylon Anywhere server addresses are shielded from view, these servers can be deployed in a number of ways. The internal deployment can change with no effect on users and usability.

Security

- This deployment is highly secure. The number of ports open to the enterprise is minimized, and communications between the DMZ and the enterprise are highly controlled.

Pylon Anywhere Mobile Gateway in the DMZ

Another possible deployment approach involves placing the Pylon Anywhere Mobile Gateway inside an organization's perimeter network (DMZ).

Figure 5: Pylon Anywhere Mobile Gateway in a perimeter network (DMZ)

The Mobile Gateway is a communications infrastructure component of Pylon Anywhere. It is designed for secure and scalable communications between mobile devices and servers.

The Pylon Anywhere Mobile Gateway consists of two basic parts: an ISAPI extension that can be installed on an IIS server, and communications services that are usually installed on the Pylon Anywhere server.

The IIS server intercepts the HTTP requests from mobile devices and then routes these requests through TCP/IP to a specific port that has been defined. All traffic is encrypted end-to-end.

Configuration notes (for Mobile Gateway in the DMZ)

- This configuration is an option when WAP access to email is not required, and web access is using a Virtual Private Network (VPN) to connect to enterprise servers. WAP access is not available using this configuration.

Benefits of Mobile Gateway in the DMZ

The benefits of this deployment approach include robustness, performance, and security.

Robustness

- Installation consists of installing a single DLL and a property file.
- A single TCP/IP port is open in the firewall. It can be restricted to a single IP address.
- DNS routing makes the experience extremely simple whether the client is internal or external.

Performance

- This deployment model is an extremely simple approach that has minimal effect on system performance.
- The Mobile Gateway handles load-balanced connections to multiple Pylon Anywhere servers. The round-robin connections can be assigned based on 'next available' or based on server load.

Security

- This deployment approach is highly secure. The number of ports open to the enterprise is minimized, and communications between the DMZ and the enterprise are highly controlled.
- This configuration routes HTTP traffic to a different protocol and port, thereby restricting any pass-through attempts to the firewall.

Combined Deployment in the DMZ

Another approach is a hybrid approach, which includes elements of the previous two deployments. In the combined approach, the reverse proxy server handles web and WAP requests, and the IIS server running the ISAPI extension manages email and PIM synchronization.

VPN and RAS Connectivity

VPN or remote access server (RAS) connectivity is an appropriate choice for many organizations as it simplifies connection and DMZ configuration. It is currently a standard for mobile PCs, and VPN clients for Palm OS and Pocket PC handhelds are now available. Microsoft offers a VPN client on the Pocket PC 2002 operating system, and Certicom offers a handheld VPN client called Movian VPN.

Figure 6: Configuration with VPN or RAS

In this case, the VPN or RAS server communicates directly with the Pylon Anywhere servers through the inner firewall.

Configuration notes (for double firewall with VPN and RAS)

- This configuration can use either a single or double firewall.
- Before this configuration model is selected, the end user experience should be considered. Most likely, the user must provide a user ID and password to establish a dial-up connection, and then provide another user ID and password to establish a VPN connection. After successfully establishing both connections, the user can synchronize. After synchronization, the VPN connection must be disconnected, and then the dial-up connection must be disconnected.

IIS and ISAPI in the DMZ

Some organizations use a dual-firewall approach to network security, creating a perimeter network (or DMZ). This scenario covers locating the IIS server with the ISAPI component inside the DMZ.

Figure 7: IIS server with ISAPI component within the DMZ

In this scenario, the IIS server works as an intermediate server in the DMZ or isolated subnet, and then connects to a Pylon Anywhere server through an organization's internal network. This configuration adds another layer of security to the Pylon Anywhere installation.

This configuration may also be used in a two DMZ system where a reverse proxy server or a Layer 3 Switch is in use in the first DMZ and there is a need to change the port and protocol each time there is a pass through a firewall.

On-Device Security

On-Device Security Overview

Protecting the data that is on a device is just as important as protecting the information flowing between the device and the servers it interacts with. Device security is often something that is left up to the end user to implement and maintain. Although this is often driven by corporate policy, enterprises often look for ways to take this responsibility out of the hands of end users and place it under the enforceable control of an administrator.

Storing Credentials Securely

One piece of information that is extremely important to protect on the device is the user's credentials that are used by the Pylon Anywhere client to authenticate with the server to initiate synchronization. An administrator can decide whether to allow these authentication credentials to be stored on a device at all, or can choose a time period for which stored credentials are valid. If an administrator allows this information to be stored on the device and to never expire, someone who finds a lost device could initiate synchronization until the real user either changed the password on the server, or until the administrator made the account inactive.

In addition to security concerns, and administrator must understand the usability of the product when deciding on a password storage policy. For example, it may be cumbersome for an end user to enter their password every time they synchronize. To balance this with having a secure client application, an administrator may allow authentication credentials to be stored on the device, but to have them expire after 1 day. With this policy, an end user only needs to enter their password on their first synchronization of the day.

When a device synchronizes with the server for the first time, the user is prompted to enter their password during the encrypted session. At that time, the server encrypts the username, password, device ID, and an expiration date into a 'token'. This token is encrypted with 160-bit Blowfish encryption. This token is then sent to and stored on the mobile device, and is re-used until its expiration.

An important point to understand here is that since the server initially generated the token, the server is the only component that needs to know the encryption key. Therefore, only the server can decrypt the token. In addition, the token on the device is useless if moved to another device since the unique device ID is incorporated into the token.

Other On-Device Security Measures

In addition to ensuring that any credentials stored on the device are protected, there are other techniques that can be used to protect additional important data

that may be stored on the device.

Much like laptops, many mobile devices are equipped with a power-on password application. By taking advantage of this type of application, a user forces his or her device to prompt for a password when the device starts up. With this mechanism in place, someone who happens upon a misplaced device will not be able to access any data that is on the device.

Although the use of power-on passwords is most often part of an organization's mobile device security plan, it is something that is difficult to enforce. It is not easy for an administrator to force an end user to enable this specific security feature.

Pylon Anywhere offers a systems management add-on which is available and priced separately. This add-on can be configured to not allow any device to synchronize unless it has a power-on password enabled. Thus, an administrator can ensure that any users that are synchronizing their important information to their device will have device-level security in place to protect it.

While useful at providing a basic level of device protection, individuals with the time, tools, and desire to retrieve the data off of a mobile device can get past a power-on password. An additional level of security would provide the ability to delete all of the sensitive information from a device if lost or stolen.

The systems management add-on enables an administrator to delete sensitive information from a device if it is compromised. This can be performed in a number of ways.

First, the administrator can flag a specific device as lost or stolen, and if it attempts to connect to the server to perform a synchronization, the data can be deleted at that time. Although useful, this does not protect data that may already be on the device if the individual does not attempt to connect to the server.

For times when the individual does not attempt to connect to the server, the administrator has a second option of issuing a push message to the device, which instructs the device to wipe out all of the data. This option is only available for specific devices that can receive SMS messages or devices that are connected to the network.

Lastly, an administrator has the option of being proactive in the effort to protect sensitive data. An administrator can define a connection policy, which, for example, may require end users to connect to the server at least once a day. Then, if a device does not adhere to this connection policy, the account can be disabled, the PIM information can be deleted, additional data can be deleted, or the device can be wiped out entirely. The system administrator determines the connection policy and the associated action. The benefit of this capability is that the connection policy and action are stored on the device, meaning that even if the individual does not attempt to connect to the server, and if the device is not addressable, the data can still be deleted when the connection policy is violated.

Conclusion

Pylon Anywhere addresses the security concerns of an organization looking to deploy an email and PIM solution to mobile devices. Pylon Anywhere provides communication security to protect the transmission of sensitive information, a variety of user authentication options for authentication flexibility, network security to ensure that an organization can leverage its existing security infrastructure, and on-device security to protect sensitive information on mobile devices.

Legal Notice

Contact Us

iAnywhere Solutions Worldwide Headquarters One Sybase Drive, Dublin, CA, 94568 USA

Phone 1-800-801-2069 (in US and Canada)

Fax 1-519-747-4971

World Wide Web *http://www.ianywhere.com*

E-mail contact.us@ianywhere.com