WHITE PAPER

OneBridge® Security Overview

SYBASE®
iAnywhere®

OneBridge offers a variety of features to securely extend enterprise email and other applications to mobile and wireless devices.

In this growing mobile and wireless world, anytime, anywhere access to corporate data is becoming a necessity. Mobile workers are demanding access to mission-critical data in order to remain competitive in the market and efficient in their jobs. Now that corporate data can be accessed remotely and from a variety of devices, there are even more security challenges for the IT team. IT administrators must create and maintain corporate standards for secure mobile device access to corporate information.

OneBridge offers a variety of features to securely extend email and other enterprise applications to mobile devices in both wireless and wired environments. OneBridge offers a comprehensive solution for IT administrators to securely manage a variety of mobile devices under a single server. With OneBridge, mobile users can securely connect their devices from inside the enterprise and outside the firewall. The OneBridge security features can be broadly classified into three categories:

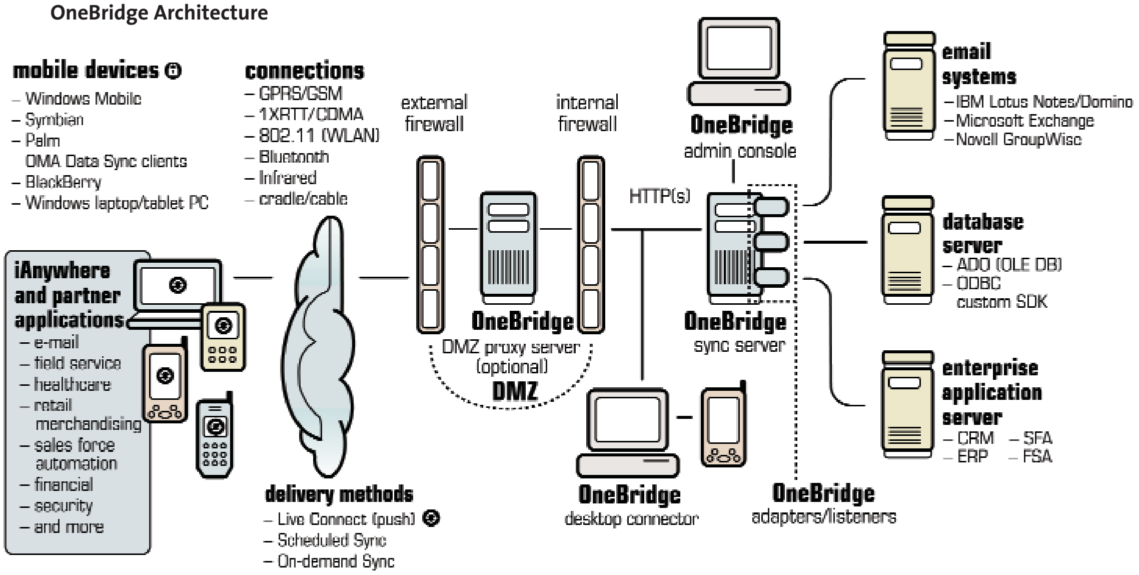
1. infrastructure security
2. data security
3. device security

INFRASTRUCTURE SECURITY

OneBridge is comprised of various components designed to provide a modular and distributed means for secure deployment.

- DMZ proxy—An application-specific HTTP proxy at the DMZ level.
- OneBridge Sync Service—Synchronization and device management services along with authentication of mobile devices. This server is typically installed inside the firewall.
- OneBridge desktop connector—Provides serial and USB connectivity to mobile devices.
- Outbound connection from the OneBridge sync server to the OneBridge DMZ Proxy Server - Eliminates the need to open an inbound port on the internal firewall

OneBridge Architecture



DMZ PROXY

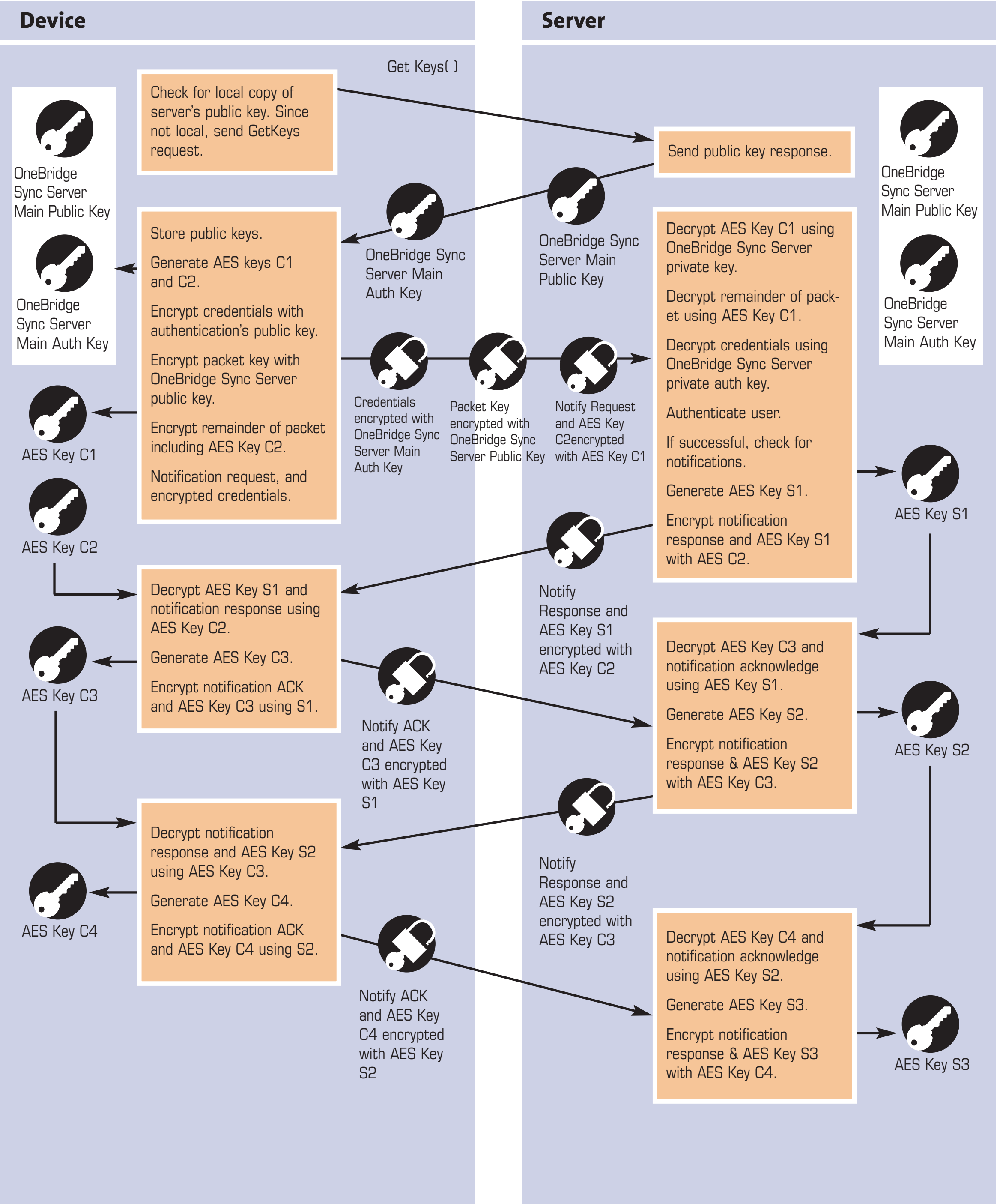
The OneBridge DMZ proxy acts as an application-specific HTTP proxy. Through a user-defined HTTP or HTTPS port, this proxy performs the necessary security and packet validation checks on connections from mobile devices before letting the incoming packet data through to OneBridge. This allows administrators to set up various types of filters to secure traffic through the firewall. The DMZ proxy has its own public key and private key pair used to decrypt the message header (this header has the session ID information and packet key). Additionally, all data in the packet is encrypted with an AES packet key and is not decrypted by the DMZ proxy. Both the OneBridge client and the OneBridge sync server initiate connections to the OneBridge DMZ Proxy Server, eliminating the need to open an inbound port on the internal firewall.

- Acts as an application-specific HTTP proxy at DMZ
- Validates incoming packet before allowing traffic through the firewall
- Uses HTTP(S) to communicate with OneBridge
- Does not decrypt the data portion of the packet
- Authentication mechanism is built-in to the OneBridge Proxy Server to validate OneBridge Sync servers that are connecting to the proxy.

AUTHENTICATION

With the DMZ proxy, OneBridge can be securely deployed inside the firewall. OneBridge also uses HTTP(S) to act as its transport protocol to communicate with rest of the OneBridge components. OneBridge has a two-tier authentication mechanism. The first tier is with the Windows NT/Active Directory, Lotus Domino, Database, RADIUS and SecureID. This tier is used to authenticate the user credentials and obtain the necessary group information to determine the actions that a user is authorized to run on OneBridge. The second tier provides authentication against groupware and database servers for synchronization. This two-tier authentication enables secure deployment of OneBridge and adapters at different locations.

- Uses HTTP(S) to communicate between DMZ proxy and adapters
- Deployed securely inside the firewall
- Provides two-tier authentication to validate user credentials
- First tier: Windows NT, Notes, Database, RADIUS and SecureID
- Second tier: Groupware and database servers
- Combined extended session and save password authentication functionality to enhance scalability



Device
Server
Get Keys( )
OneBridge Sync Server Main Public Key
OneBridge Sync Server Main Auth Key
OneBridge Sync Server Main Auth Key
OneBridge Sync Server Main Public Key
OneBridge Sync Server Main Public Key
OneBridge Sync Server Main Auth Key
Credentials encrypted with OneBridge Sync Server Main Auth Key
Packet Key encrypted with OneBridge Sync Server Public Key
Notify Request and AES Key C2encrypted with AES Key C1
AES Key C1
AES Key C2
AES Key S1
Notify Response and AES Key S1 encrypted with AES Key C2
AES Key C3
Notify ACK and AES Key C3 encrypted with AES Key S1
AES Key S2
Notify Response and AES Key S2 encrypted with AES Key C3
AES Key C4
Notify ACK and AES Key C4 encrypted with AES Key S2
AES Key S3

Check for local copy of server's public key. Since not local, send GetKeys request.

Send public key response.

Store public keys.

Generate AES keys C1 and C2.

Encrypt credentials with authentication's public key.

Encrypt packet key with OneBridge Sync Server public key.

Encrypt remainder of packet including AES Key C2.

Notification request, and encrypted credentials.

Decrypt AES Key C1 using OneBridge Sync Server private key.

Decrypt remainder of packet using AES Key C1.

Decrypt credentials using OneBridge Sync Server private auth key.

Authenticate user.

If successful, check for notifications.

Generate AES Key S1.

Encrypt notification response and AES Key S1 with AES C2.

Decrypt AES Key S1 and notification response using AES Key C2.

Generate AES Key C3.

Encrypt notification ACK and AES Key C3 using S1.

Decrypt AES Key C3 and notification acknowledge using AES Key S1.

Generate AES Key S2.

Encrypt notification response & AES Key S2 with AES Key C3.

Decrypt notification response and AES Key S2 using AES Key C3.

Generate AES Key C4.

Encrypt notification ACK and AES Key C4 using S2.

Decrypt AES Key C4 and notification acknowledge using AES Key S2.

Generate AES Key S3.

Encrypt notification response & AES Key S3 with AES Key C4.

LIVE CONNECT

Even with an always-on and automatic delivery of information through Live Connect technology, security is never compromised with OneBridge. IT can utilize the existing security policies in place to provide wireless "push" as the product supports most corporate authentication schemes like Windows ADS, RADIUS, RSA SECURE ID, etc. IT can also configure how long an authenticated session can last before users have to re-enter their credentials.

- Does not require saving password
- Supports RSA secure ID (HW/SW tokens)
- Administration configurable persisted sessions
- User authentication required for automatic delivery

ONEBRIDGE DESKTOP CONNECTOR

The OneBridge desktop connector serves as a desktop proxy and provides an easy way for users to connect their devices to OneBridge from their Windows desktops and laptop machines without the need for third-party software. This significantly reduces any security breaches because the access and management of information is controlled by the IT administrator rather than the mobile user. While device users can use any desktop connector to connect back to OneBridge, they are still required to input their credentials on the device to connect to OneBridge.

- Serves as a desktop proxy for mobile devices
- Eliminates the need for varying third-party desktop sync software
- User credentials are still required for connecting with OneBridge

DATA SECURITY

OneBridge provides end-to-end data security by encrypting the data between the server and the device. In addition, it does not stage or store data anywhere within OneBridge other than in the original data source. For encryption, OneBridge uses a combination of RSA for key exchange, and AES for encrypting the data. This combination of asymmetric and symmetric algorithms provides the best security and performance. Because public-key cryptography is more computationally expensive than symmetric cryptography, public-key cryptography will be used to encode a secret key for symmetric cryptography; then the system falls back on a faster symmetric cryptography system. With 128-bit encryption AES key, a widely embraced stream cipher, performs extremely well on mobile devices with limited processing power.

- End-to-end data security with 1024-bit RSA-OAEP key exchange and 128-bit AES-CFB symmetrical encryption
- Does not store or stage data outside of the data sources
- Sync engine uses a change-log-based algorithm, which does not store any data

DEVICE SECURITY

Device security essentially refers to securing the data within the device in the event the device is lost or stolen. OneBridge uses a variety of methods enabling IT administrators to protect data on devices. The administrator has the capability to force the device user to enter his credentials each time he/she connects to the server. Even in cases where the user is allowed to store credentials on the device, these credentials are encrypted with the server's public key thereby making it virtually impossible for unauthorized access. The IT administrator also can force the power-on password to be enabled. This requires users to key in their password to access their device.

- OneBridge administrators can force users to enter credentials each time the user connects
- All credential information (if allowed to be stored on the device) is encrypted with the server's public key
- OneBridge administrators can enforce power-on passwords on all devices (Palm, CE, Symbian, RIM)

For enhanced device-side security, enterprises can deploy Afaria Security Manager. This security solution provides administrator-defined password policy, on-device encryption and data fading, among other security capabilities. Data fading is the ability of administrators to define certain actions if a mobile device doesn't contact the server within a defined period of time, including hard resetting the device, forcing the device into administrative lock-down, or deleting files.

Finally, if a device is compromised or service is to be stopped, in addition to being able to block the device from connecting to the system, the administrator is able to send a "kill pill" directly to the device to wipe all encrypted data from it.

CONCLUSION

With the emerging "always-on" wireless devices and networks, it will be increasingly challenging to control devices and their access to enterprise applications. OneBridge provides IT an excellent opportunity to proactively control these devices by putting the right infrastructure in place to effectively monitor mobile usage without any user initiation. OneBridge research and development teams continue to actively work with these new technologies to ensure secure mobile device data access and synchronization.

OneBridge and Afaria are key components of the Information Anywhere Suite, a secure, scalable mobile software platform that addresses the converging IT requirements of enterprises today. By combining email, messaging, mobile device management, enterprise-to-edge security and back-office application extension capabilities, Information Anywhere enables organizations to empower employees to do the work they need to do anywhere, at anytime, on any device. For more information, please visit: www.ianywhere.com/iasuite

iANYWHERE SOLUTIONS, INC.
WORLDWIDE HEADQUARTERS
ONE SYBASE DRIVE
DUBLIN, CA 94568-7902
U.S.A.

FOR GENERAL INFORMATION:
CONTACT_US@iANYWHERE.COM
NORTH AMERICA
T 1-800-801-2069
1-519-883-6898

FOR SPECIFIC REGIONAL PRODUCT
INFORMATION:
EUROPE, MIDDLE EAST, AFRICA
+44 1628 597 100
ASIA PACIFIC
+852 2506 8700
JAPAN
+81 3 5210 6380
BENELUX
+31 (0)30 - 247 8444
FRANCE
+33 (0) 1 41 90 41 90
GERMANY
+49 (0) 7032 / 798 - 0
UNITED KINGDOM
+44 (0) 1628 597100

www.iAnywhere.com

SYBASE®
iAnywhere®