

The Relay Server

A Whitepaper from Sybase iAnywhere

TABLE OF CONTENTS

- 1 Benefits of the Relay Server
- 1 Relay Server Architecture
- 2 Security with the Relay Server
 - 2 MobiLink Security
 - 2 Afaia Security
 - 2 iAnywhere Mobile Office Security
 - 2 Sybase Unwired Platform Security
- 2 Summary

BENEFITS OF THE RELAY SERVER

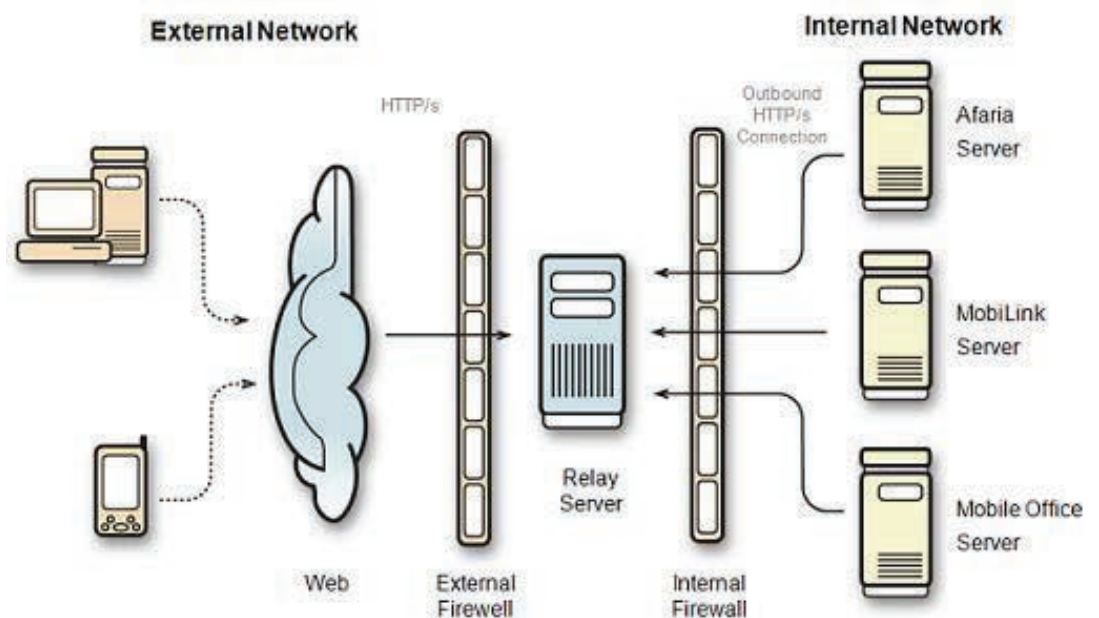
The Relay Server enables secure, load-balanced communication between mobile devices and MobiLink, Afaria, and iAnywhere Mobile Office servers through a web server. The Relay Server is also leveraged by the Sybase Unwired Platform (SUP) to provide secure transmission of Mobile Business Objects to backend enterprise systems.

The Relay Server:

- Facilitates communication between MobiLink, Afaria, iAnywhere Mobile Office and Sybase Unwired Platform clients with the appropriate backend server in a way that easily integrates into existing corporate Web and IT infrastructure
- Provides a mechanism to enable load-balanced and fault-tolerant environments for MobiLink, Afaria, Mobile Office and Sybase Unwired Platform servers
- Delivers a common communication architecture for Sybase iAnywhere products

RELAY SERVER ARCHITECTURE


The Relay Server is a set of Web server extensions designed for use with Microsoft Internet Information Services (IIS) 6.0 and Apache 2.2.8 Web servers. The Relay Server provides a secure multi-tenant load balancing and failover gateway for data transmission of Sybase iAnywhere products into corporate networks. It easily integrates with existing Web and IT infrastructure, providing a cost-effective way to secure a wide spectrum of services required for enterprise mobility.



The Relay Server supports MobiLink, Afaria, and iAnywhere Mobile Office backend servers. Support is provided for their corresponding clients including MobiLink, UltraLite, QAnywhere, Afaria, iAnywhere Mobile Office and other Sybase iAnywhere HTTP/S clients.

The Relay Server is also leveraged by Sybase Unwired Platform to allow Mobile Business Objects to efficiently synchronize in a secure manner with enterprise Web services, databases, or to applications such as SAP or Remedy, using a series of plug-in application connectors.

When integrating the Relay Server into existing Web and IT infrastructure there are no required changes to existing corporate firewalls and IT policies. The Relay Server is designed to handle incoming HTTP and HTTPS requests from the client, resulting in all communication coming from the Internet using port 80 or 443 to pass through the external corporate firewall.



A special connector call the Outbound Enabler facilitates all communication between the backend server and the Relay Server using HTTP or HTTPS. Given all communication with the Relay Server is established on an outbound connection from within the internal corporate firewall, there are no required ports to be open on the internal corporate firewall. This provides increased security as the internal corporate firewall remains intact, without the requirement of opening inbound ports for communication.

SECURITY WITH THE RELAY SERVER

The Relay Server is a set of Web extensions and relies on a Microsoft IIS or Apache Web server. Both Microsoft IIS and Apache support Transport Layer Security (TLS) for communication between the client and the Web server. All communication between the Relay Server and backend servers also supports TLS.

MobiLink Security

The MobiLink client uses HTTP or HTTPS to communicate with the Relay Server. With HTTPS, communication data is temporarily decrypted and re-encrypted as it is exchanged between the client and backend server. This is known as the WAP Gap.

To ensure completely secure communication through the WAP Gap, it is recommended to use MobiLink's end-to-end encryption feature to further protect data as it passes through the Relay Server.

MobiLink's end-to-end encryption feature provides protocol level encryption between MobiLink, UltraLite or QAnywhere clients and the MobiLink server. Both RSA and ECC encryption types are supported. TLS security can be used in combination with end-to-end encryption.

Afaria Security

Afaria uses both HTTP and HTTPS security when communicating with the Relay Server.

iAnywhere Mobile Office Security

Communication between iAnywhere Mobile Office clients and the Relay Server uses HTTP. iAnywhere Mobile Office provides end-to-end communication security, built on top of HTTP, by utilizing strong encryption algorithms for the data exchange between the iAnywhere Mobile Office server and client. It uses 1024-bit for the initial RSA key exchange and a 128-bit key for algorithm when 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 is only used to encode a secret key for the symmetric cryptography data exchange. iAnywhere Mobile Office uses a new symmetric AES key for every single message exchange with the server.

At no time during the communication are the messages decrypted inside the Relay Server.

Sybase Unwired Platform Security

Sybase Unwired Platform synchronization is built on MobiLink. In Sybase Unwired Platform, all communication between the MobiLink client and MobiLink server uses end-to-end encryption and HTTPS. As a result, all communication through the Relay Server is secure, even through the WAP Gap.

SUMMARY

The Relay Server is a cost effective way of integrating Sybase iAnywhere products through a common, secure gateway for data transmission that easily integrates into existing Web and IT infrastructure. The Relay Server provides multi-tenant load balancing and failover adding to the wide spectrum of services required for enterprise mobility.