Entrypoint®

Deployment Models and Security Protocols

Last updated February 2021

PHOENIX Software International®
SOLUTIONS FOR MAINFRAME AND PC PLATFORMS

Entrypoint Components

Application Studio

Entrypoint Server

Software Development Kit (SDK)

System Manager

Desktop Workstation

Network Protocol and Security

The Entrypoint Server exposes two ports with two separate protocols: HTTP for Web clients (either Web Services or Web Browsers) and EPXP for native Entrypoint Clients.

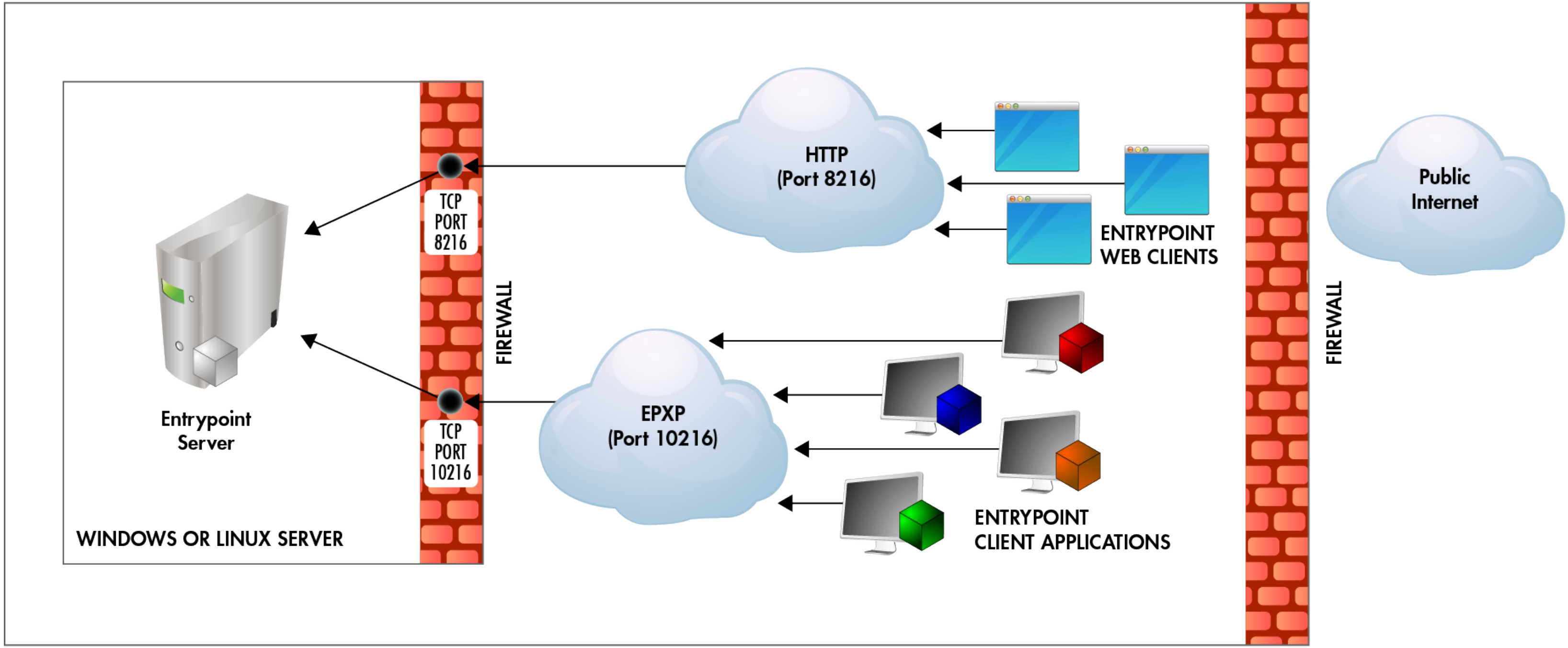
- HTTP can be secured using a reverse-proxy (such as Microsoft IIS or NGINX) installed on the same machine that the Entrypoint Server runs on. A reverse-proxy (with SSL/TLS offload) accepts incoming requests over HTTPS and then passes those requests using plain HTTP over port (8216) to the Entrypoint Server service.
- EPXP is a proprietary, bi-directional, message-oriented protocol that native (non-web) clients (Application Studio, Desktop Workstation, SDK Clients) use to connect to and interact with the Entrypoint server. Messages in EPXP are made up of a simple header, and an encrypted message body. Entrypoint uses the XTEA 128-bit block-cipher algorithm for the encryption of message bodies.

Authentication and Active Directory/LDAP

By default, the Entrypoint Server maintains a secure credential store and handles authentication internally. Optionally, users defined in an Entrypoint Server can be configured to use an Active Directory or other LDAP server for authentication and management of passwords. The connection between the Entrypoint Server and the Active Directory/LDAP server is handled using the LDAPS protocol, which secures the connection using SSL/TLS.

Default Deployment Model

The Default Deployment Model is a simple "Turn-key" model for small organizations that may not have a dedicated IT team. This deployment model prioritizes simplicity over security.

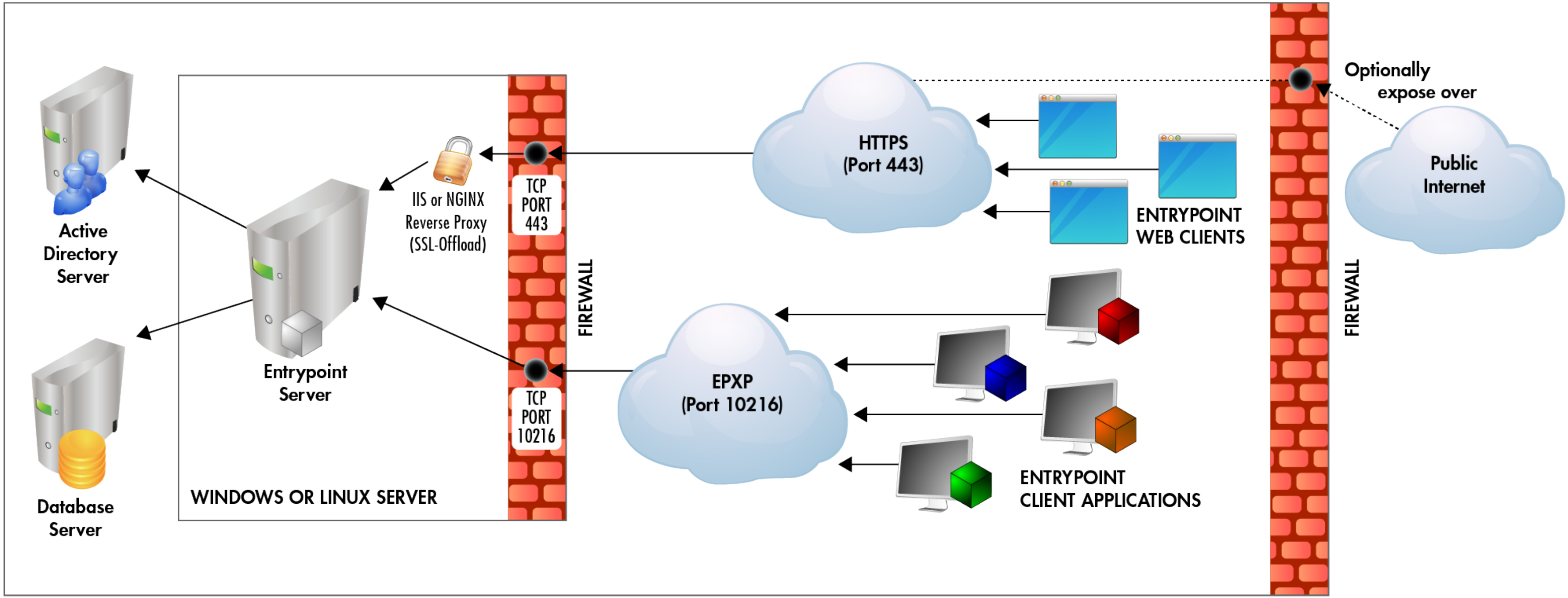


Default Deployment Model

- The Windows or Linux Server running the Entrypoint Server service opens inbound access to two firewall ports (8216 and 10216)
- Web Clients connect to the server using standard HTTP over the non-standard port 8216 (http://serveraddress:8216)
- Entrypoint native client applications connect directly to the server using the EPXP protocol over port 10216.
- The Entrypoint Server provides authentication of user credentials

Enterprise Deployment Model

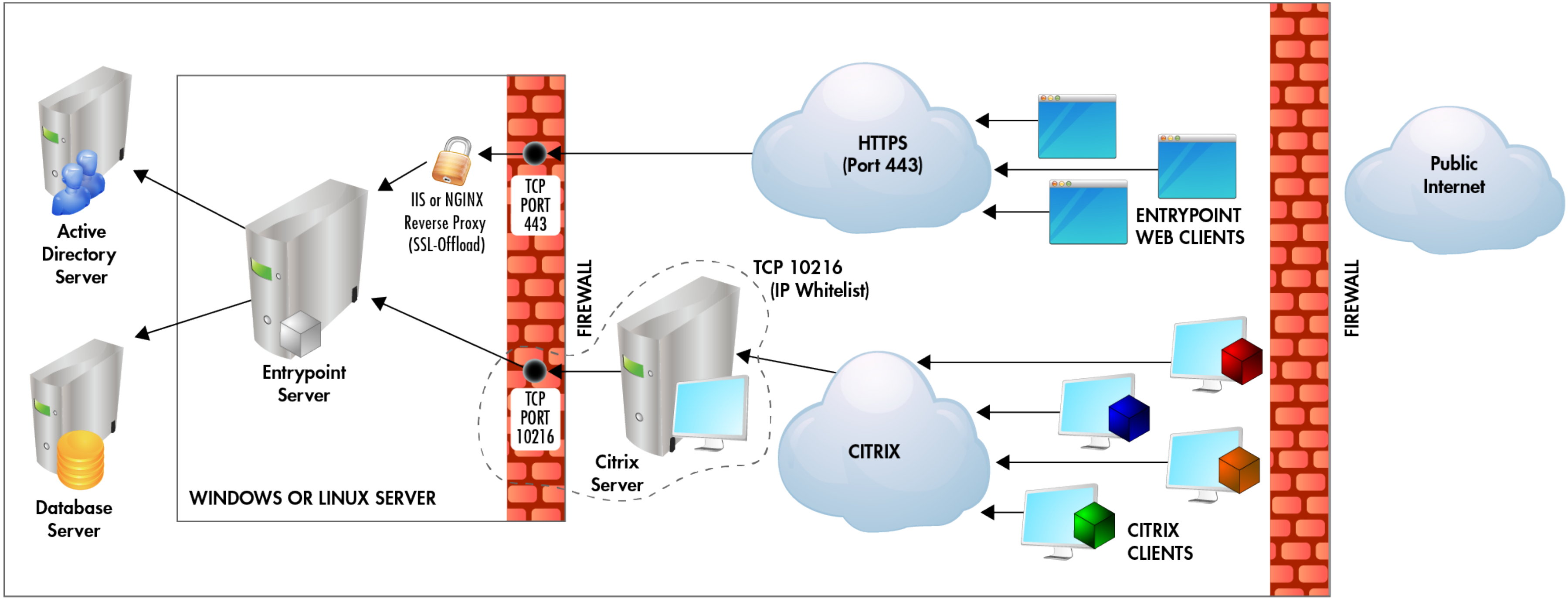
The Enterprise Deployment Model is more secure and flexible, and supports integration with existing infrastructure.



Enterprise Deployment Model

- The Windows or Linux Server running the Entrypoint Server service opens inbound access to two firewall ports (443 and 10216)
- A Reverse-Proxy with SSL/TLS Offload (such as Microsoft IIS or NGINX) provides standard HTTPS over port 443.
- Entrypoint native client applications connect directly to the server using the EPXP protocol over port 10216.
- The server utilizes an existing, external database server (such as Microsoft SQL Server, or PostgreSQL) rather than using the embedded database.
- The server (optionally) connects to an existing Active Directory server for authentication of user credentials.
- Optionally public Internet access to the Entrypoint Server web interface can be configured by allowing inbound connection through the organizations firewall and forwarding them to the Entrypoint Server on port 443.

High Security Deployment Model using Citrix



High Security Deployment Model using Citrix

- The Windows or Linux Server running the Entrypoint Server service opens inbound access to two firewall ports:
  - TCP Port 443 for HTTPS (web) traffic
  - 10216 using an IP Address whitelist, limiting access only to the Citrix server
- Entrypoint native client applications are installed and run within the Citrix server, which is the only machine permitted to connect to TCP port 10216 on the server
- A Reverse-Proxy with SSL/TLS Offload (such as Microsoft IIS or NGINX) provides standard HTTPS over port 443.
- The server leverages an existing, external database server rather than using the embedded database used in the default model
- The server (optionally) connects to an existing Active Directory server for authentication of user credentials

Learn more about Entrypoint

Entrypoint web page

Request a demo

Email us