Secure Bridge Setup

On this Page:

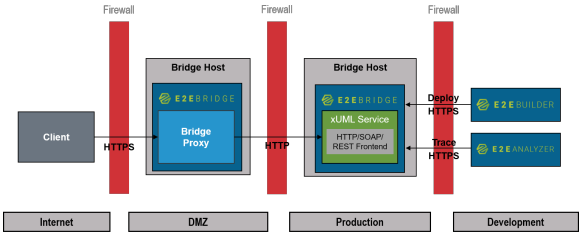
Related Pages:

- BRIDGE Hardening
- Testing Non-SOAP Services

Setup For Services Being Accessed From the Internet

As a main point for or a secure Bridge setup, we recommend to block all service control and service ports from inbound access within your firewall. Service access should only be possible via a proxy. A secure Bridge setup could look like:

Figure: Secure Bridge Setup for External Access

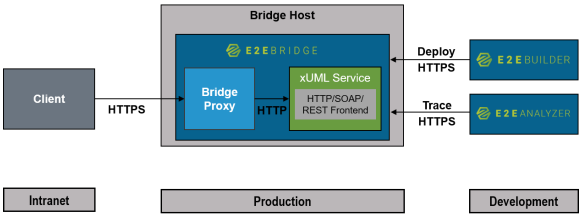


The firewall of the Bridge hosting the Bridge proxy should only have the proxy port open.
The firewall of the Bridge hosting the xUML services should allow only service ports and the Bridge control port (usually 8080).

Setup For Services Being Accessed From the Intranet

A reduced setup for Bridge services only being accessed from the intranet could look as depicted below.

Figure: Reduced Bridge Security Setup for Internal Bridge Access



The firewall of the E2E Bridge hosting the Bridge proxy and the xUML services should only have the proxy port open.

General Aspects

With both scenarios, you can still deploy services from your development environment, and you can also access your xUML services via the Analyzer for testing purposes as described on Testing Non-SOAP Services.

Please also consider the additional security settings that are described on BRIDGE Hardening.