

# Path Builder SSL Gateway<sup>™</sup>

CoreStreet Path Builder SSL Gateway is designed to secure web server access through certificate validation and path discovery

## Overview

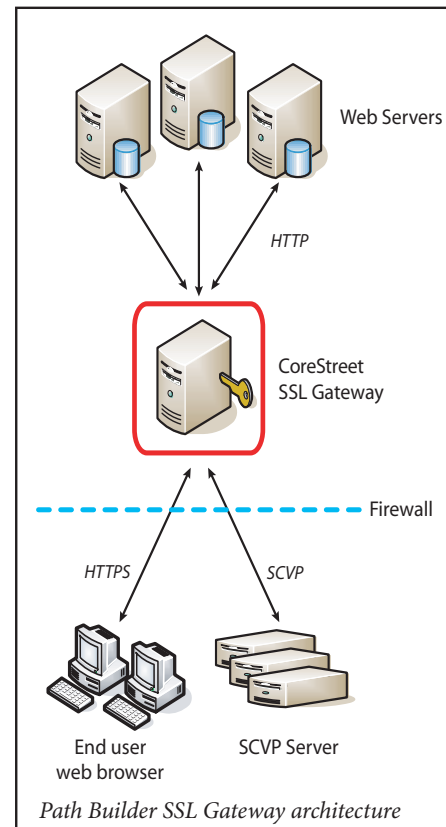
Although many organizations have deployed Public Key Infrastructures (PKIs), there have been no standards-based solutions for trust between disparate entities. As a result, government and industry were forced to rely on time-consuming and expensive, paper-based systems or struggle with incompatible electronic options.

The Path Builder SSL Gateway addresses this need by providing a standards-based approach for web-based access control in federated PKI environments. The SSL Gateway serves as an intermediary between a client and a secure web server in order to validate client SSL certificates and manage the path discovery necessary for certain validation functions.

The Path Builder SSL Gateway offers a unique approach in the market because of its ability to eliminate numerous false positive and false negative scenarios that exist in current environments, including “no path” false negatives, “invalid path” false negatives, and “valid path” false positives.

Organizations tend to have many different types of web servers throughout their infrastructures. Rather than implement and manage specific plug-ins for each type of web-server, the Path Builder SSL Gateway has been designed to service any type of web server. This gives organizations a very cost effective strategy to deal with the various web servers that may be deployed within their environment. Rather than require an already overstretched IT group to perform a number of software installations on each web server, as is typically done, the Path Builder SSL Gateway allows for an easy single installation for an organization’s entire web server infrastructure.

As an intermediary, the SSL Gateway separates its transactions into two types –external (SSL Gateway to client) and internal (SSL Gateway to secure web server). This provides for greater security because external transactions are performed using an SSL (HTTPS) connection, while internal transactions are performed using an HTTP connection.



## Benefits

**Standards-based** The Path Builder SSL Gateway is a standards-based product that is compatible with any Delegated Path Discovery (DPD) based Server-based Certificate Validation Protocol (SCVP) server and any OCSP Validation Authority

**Flexible** The Path Builder SSL Gateway is designed to function within a homogeneous or heterogeneous web server environment

**Cost effective** The Path Builder SSL Gateway does not require purchasing and installing on many different types of web servers

## Product Use Scenario

- A Client web browser sends request to the Path Builder SSL Gateway for access to a resource on a secure server.
- The Path Builder SSL Gateway initiates the SSL “handshake,” including its certificate in the reply.
- During the SSL handshake, the Path Builder SSL Gateway requests the user’s digital certificate. The client sends the user’s certificate to the Path Builder SSL Gateway, and uses its private key to prove it is the owner of the certificate.
- The Path Builder SSL Gateway authenticates the user’s certificate, verifying that it chains to a trusted root, and then validates (using either CRLs or OCSP) that there are no revoked certificates in the certification path, and that the certificate complies with any configured certificate policies and key usage restrictions. If necessary, Path Builder SSL Gateway uses SCVP to request a certification path from the remote SCVP server, and the remote server takes over the responsibility of path discovery in a centralized location.

### *Valid certificate*

- If the client certificate is valid, the Path Builder SSL Gateway opens an HTTP connection with the web server on behalf of the client. To maintain web server “anonymity,” all session traffic between the client and the web server passes through the Path Builder SSL Gateway, which presents the traffic to the client as though it came directly from the Path Builder SSL Gateway.

### *Invalid certificate*

- If an acceptable certification path is not available, the Path Builder SSL Gateway denies the request for access to the secure webpage. The Path Builder SSL Gateway can be configured to return an error page to the client providing details about the cause of the denial.
- Once the user is authenticated, the web server can then apply appropriate authorization rules to determine whether or not to provide access to the requester. In order to perform the authorization, the web server requires a trusted certificate. As part of the HTTP connection setup, the Path Builder SSL Gateway can be configured to forward this trusted certificate and a list of the valid certificate policies used to determine the trusted path.

## Requirements

### Software platform

- Microsoft® Windows Server® 2000 operating system, SP 4
- Microsoft Windows Server 2003 operating system, SP 1

### Minimum system requirements

- Microsoft Windows® Installer 2.0
- 10 MB free hard drive space

### Web server requirements

Path Builder SSL Gateway is compatible with any HTTP server, including:

- Apache HTTP Server
- Microsoft IIS
- BEA® WebLogic®
- Sun® Java™ System Web Server

### Related CoreStreet products

- CoreStreet Path Builder System™