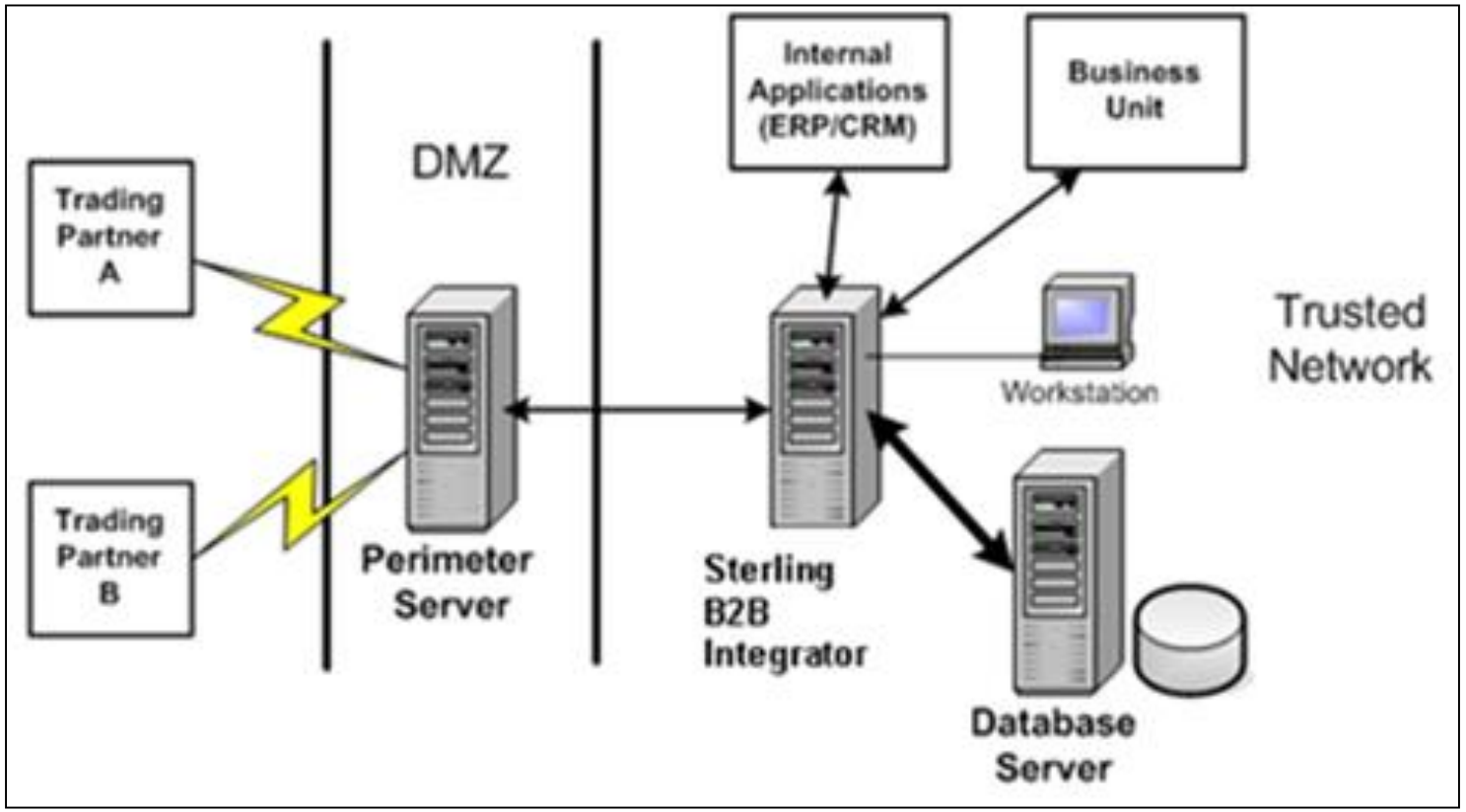
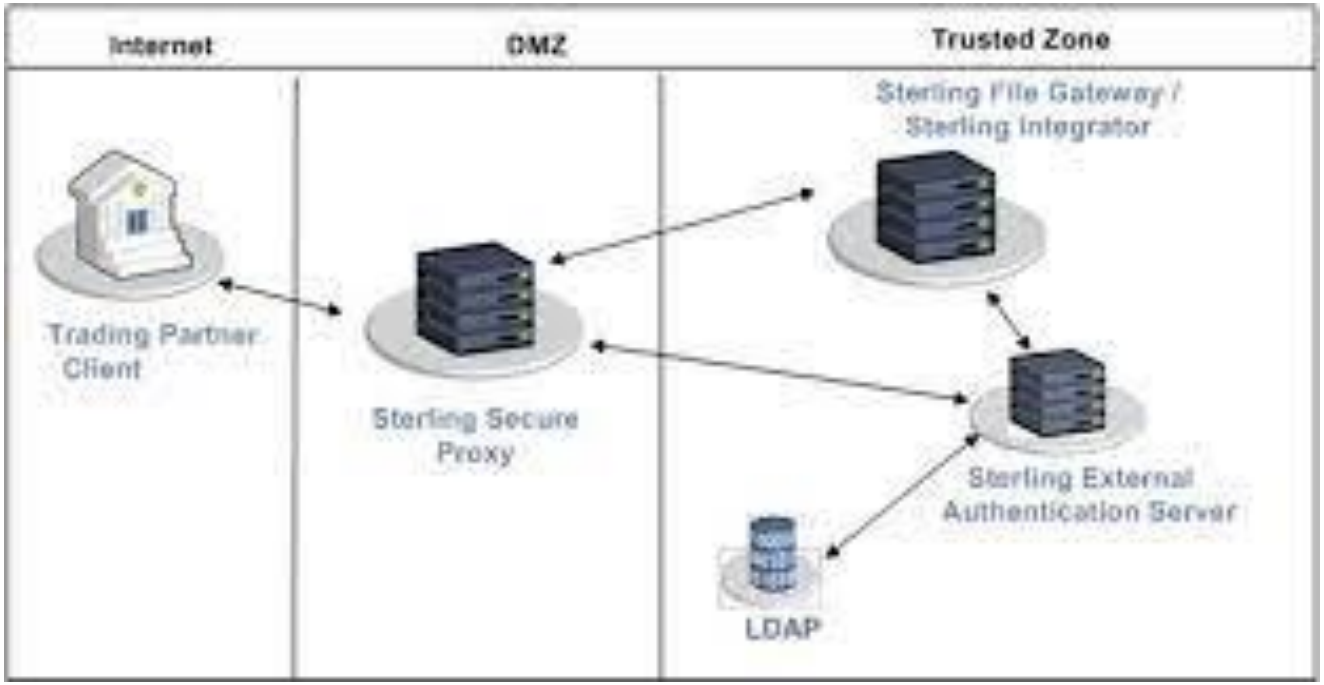
High-Level Architecture

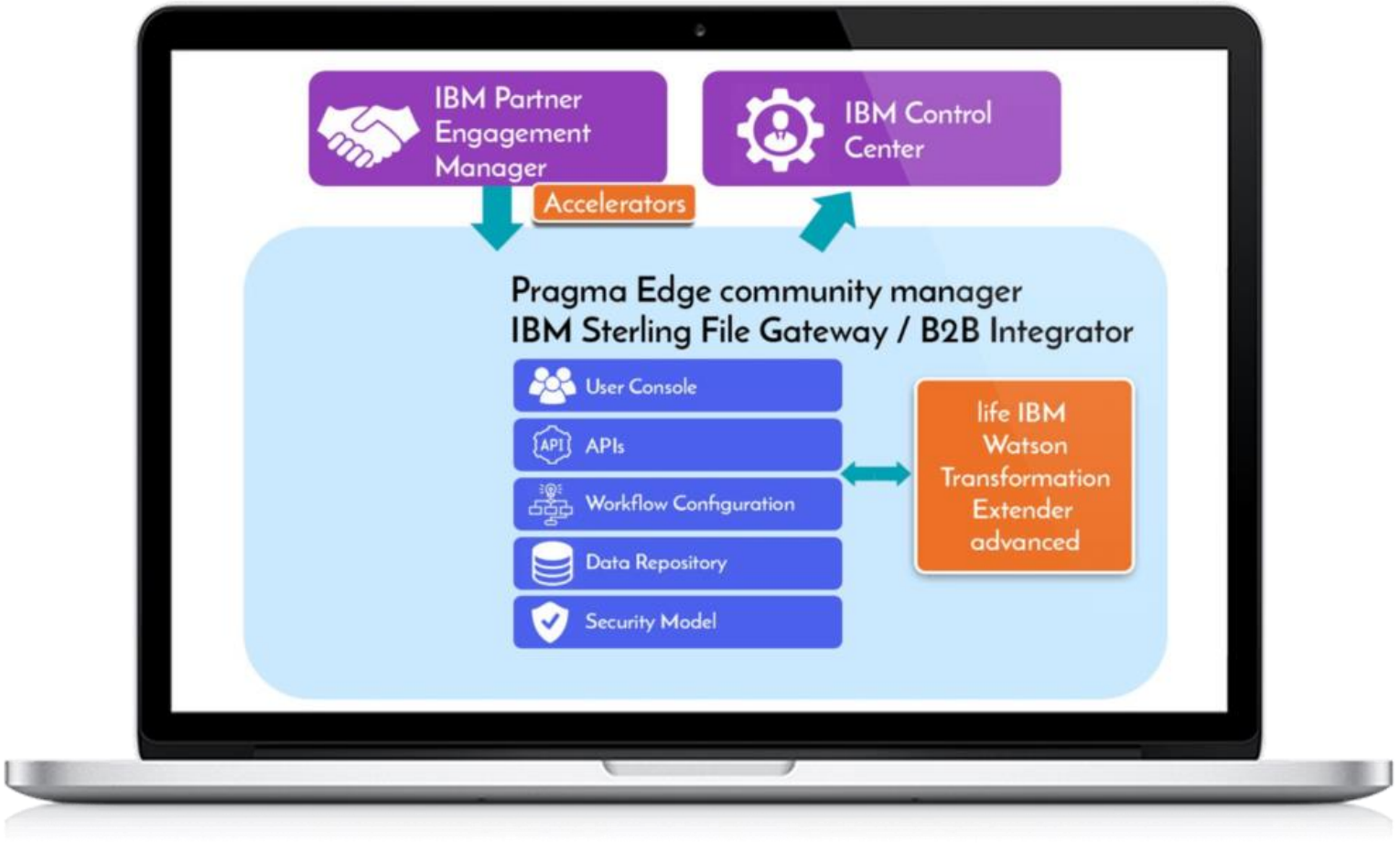
The Sterling B2B Integrator physical components architecture:



High-Level Architecture



High-Level Architecture



IBM Sterling B2B Integrator

- Sterling Integrator is a dynamic application that allows for real time integration between internal business units and external between you and your trading partners.

- It handles complex routing, translation and flexible integration.

Sterling File Gateway

- SFG is an application for transferring files between partners using different protocols, file naming conventions, and file formats.
- SFG utilizes the Sterling B2B foundation, which includes Sterling Integrator, Sterling Standards, and the Sterling platform.
- SFG can be accessed using unique application URL, provides single sign-on access to the Sterling Integrator administrative console through menu selection.
- It helps in transfer of high volume payloads with end-to-end visibility of file movement.

IBM Sterling® Partner Engagement Manager (PEM)

- Faster, automated partner onboarding
- Reduces the time and resources required to onboard new partners while managing and maintaining existing partners.
- Automated partner onboarding
- Partner self-service capability
- Enhanced visibility of onboarding process
- Single repository of partner data

IBM Sterling Control Center

- Sterling Control Center is a system management solution for managing file transfer activity across multiple instances of IBM® Sterling Connect:Direct®, IBM Sterling Connect:Enterprise®, and/or IBM Sterling B2B Integrator.
- Sterling Control Center can monitor several servers running different products and platforms.
- You can also monitor Sterling B2B Integrator using Sterling Control Center.
- Sterling Control Center provides centralized monitoring, management for improved quality of service, and better compliance with service level agreements (SLAs).

IBM Sterling Secure Proxy

- Companies all over the world rely on IBM Managed File Transfer (MFT) offerings to drive their mission-critical business processes.
- Data security, access management, and perimeter security are key considerations when moving data inside and outside of the organization.
- IBM Sterling Secure Proxy allows you to safely exchange data with partners, suppliers, and customers across the internet.

IBM Sterling Secure Proxy

- Sterling Secure Proxy is a DMZ-based application software proxy enabling secure and high-speed data movement over the internet.
- It provides increased perimeter security to protect the enterprise's trusted zone, as well as authentication services to prevent unauthorized access to your business-critical internal systems.
- It integrates with your existing security infrastructure to meet security and audit requirements while also supporting compliance regulations and incorporating industry standards and best practices.

Sterling External Authentication Server

- IBM® Sterling External Authentication Server allows you to implement extended authentication and validation services for IBM products, called client applications.
- Sterling External Authentication Server includes a server that client applications connect to and a GUI to configure Sterling External Authentication Server requirements.
- For SSL or TLS authentication, the connection between Sterling External Authentication Server and the client application is authenticated.

Sterling External Authentication Server

- Then, the client application sends a request with a certificate chain and/or a user ID and password.
- Sterling External Authentication Server uses the certificate validation or authentication definition referenced in the request to perform the requested operations.

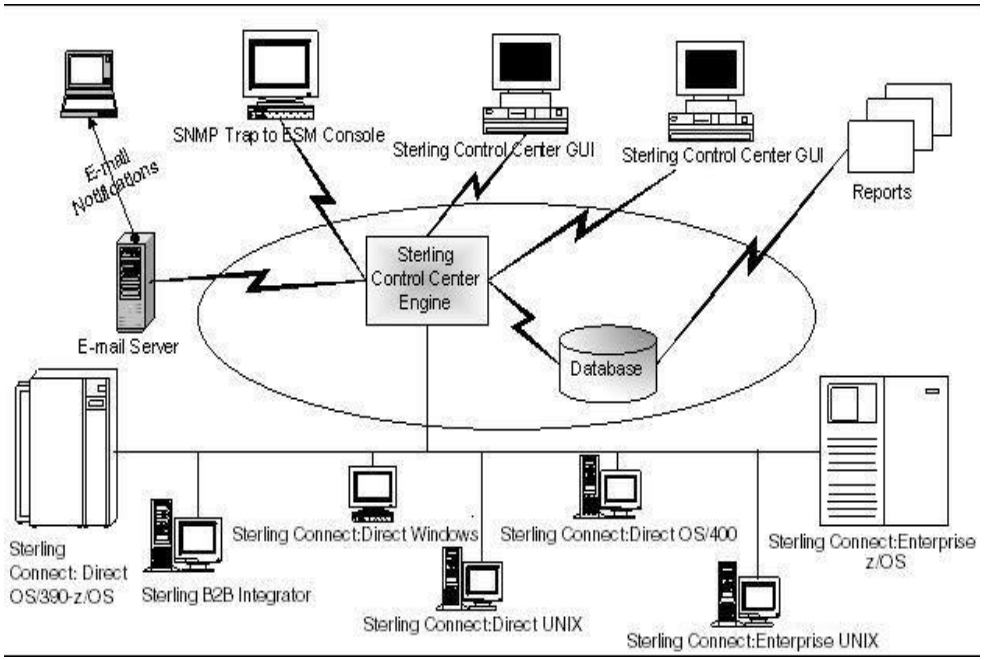
Sterling External Authentication Server

- For SSH authentication, the client application sends a request to Sterling External Authentication Server that contains a profile name, user ID, or SSH public key.
- Sterling External Authentication Server uses the configuration information in the profile to bind to an LDAP directory and look up the SSH key assigned to the user.
- It also performs an attribute assertion to match the key provided against the list of keys found in the LDAP directory.

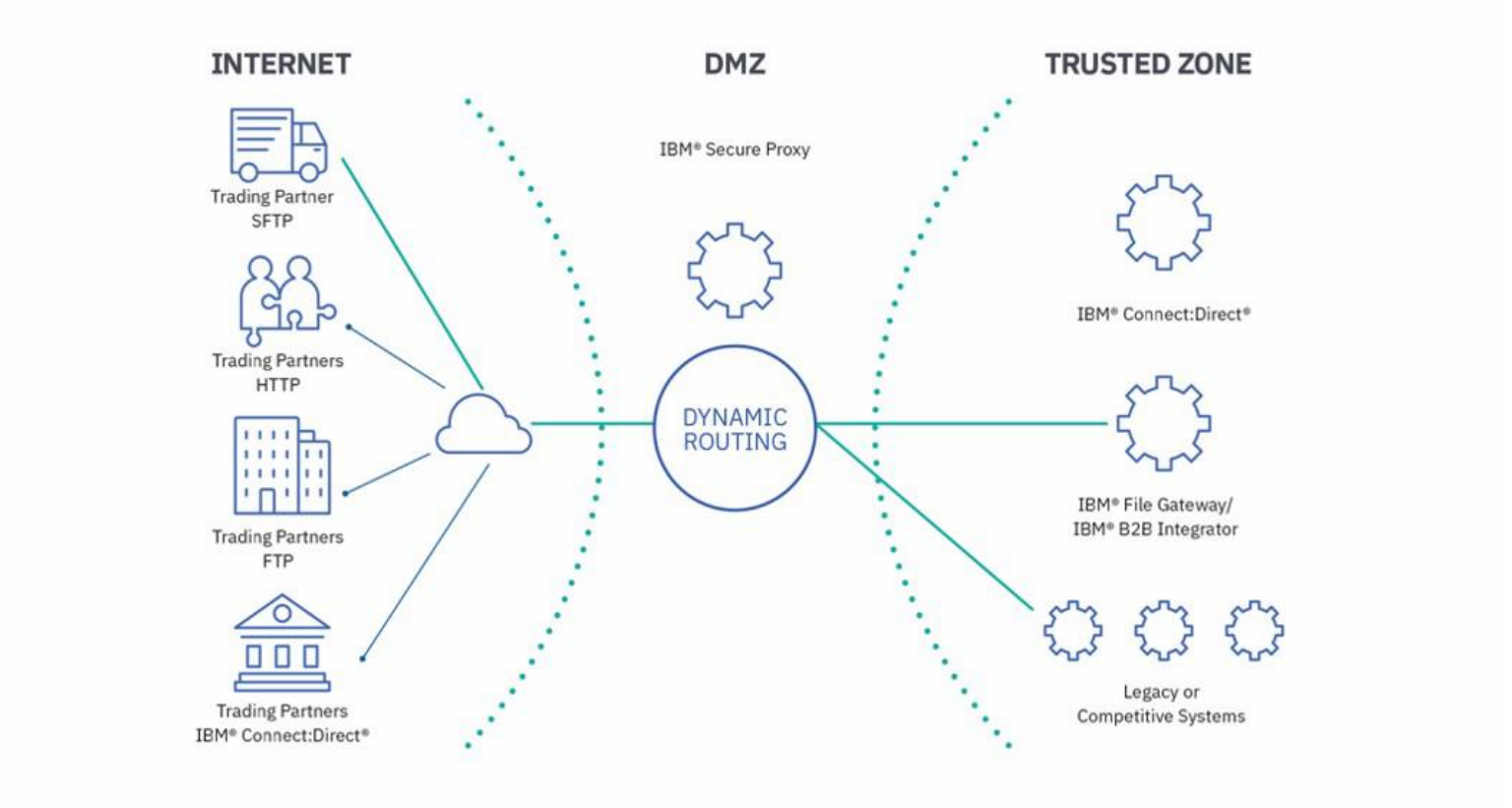
Sterling Control Center Components

The engine and GUI can be installed on computers with different operating systems.

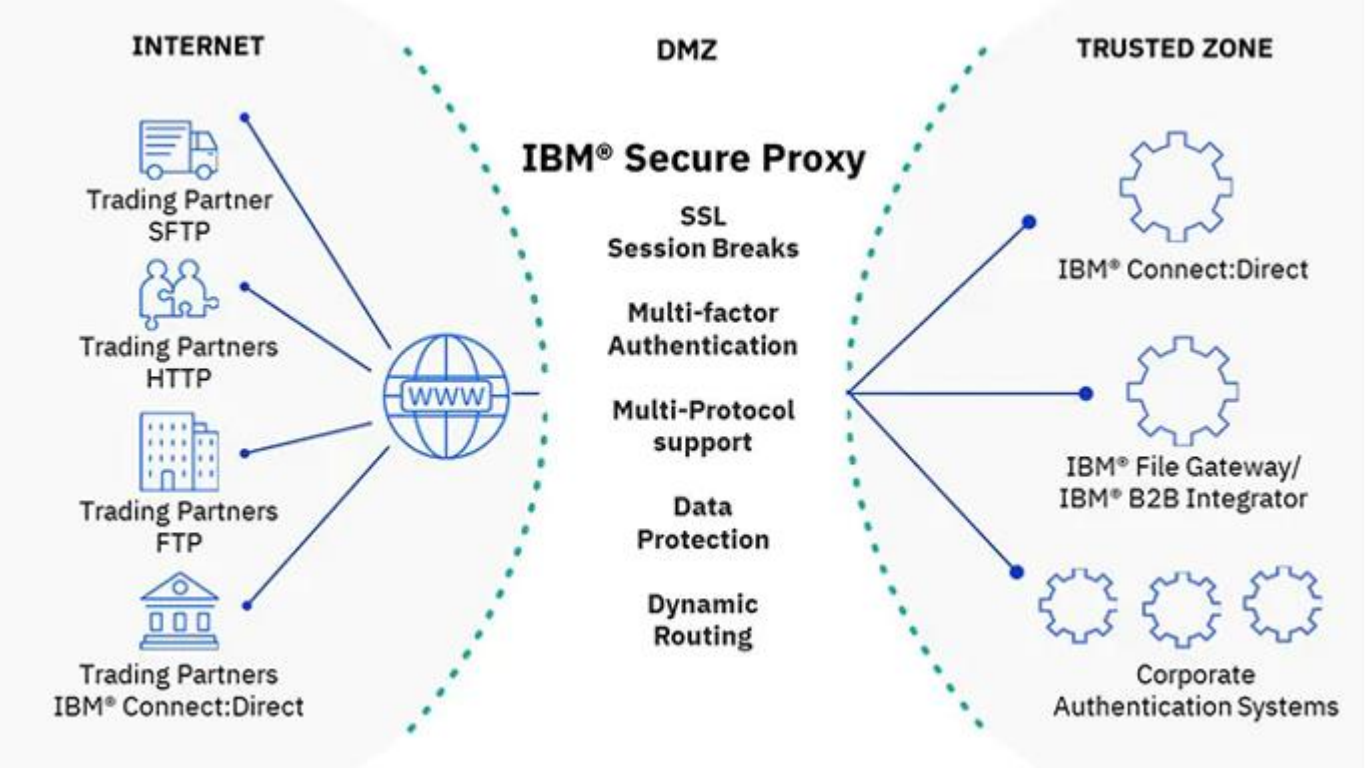
The following figure illustrates a Sterling Control Center environment:



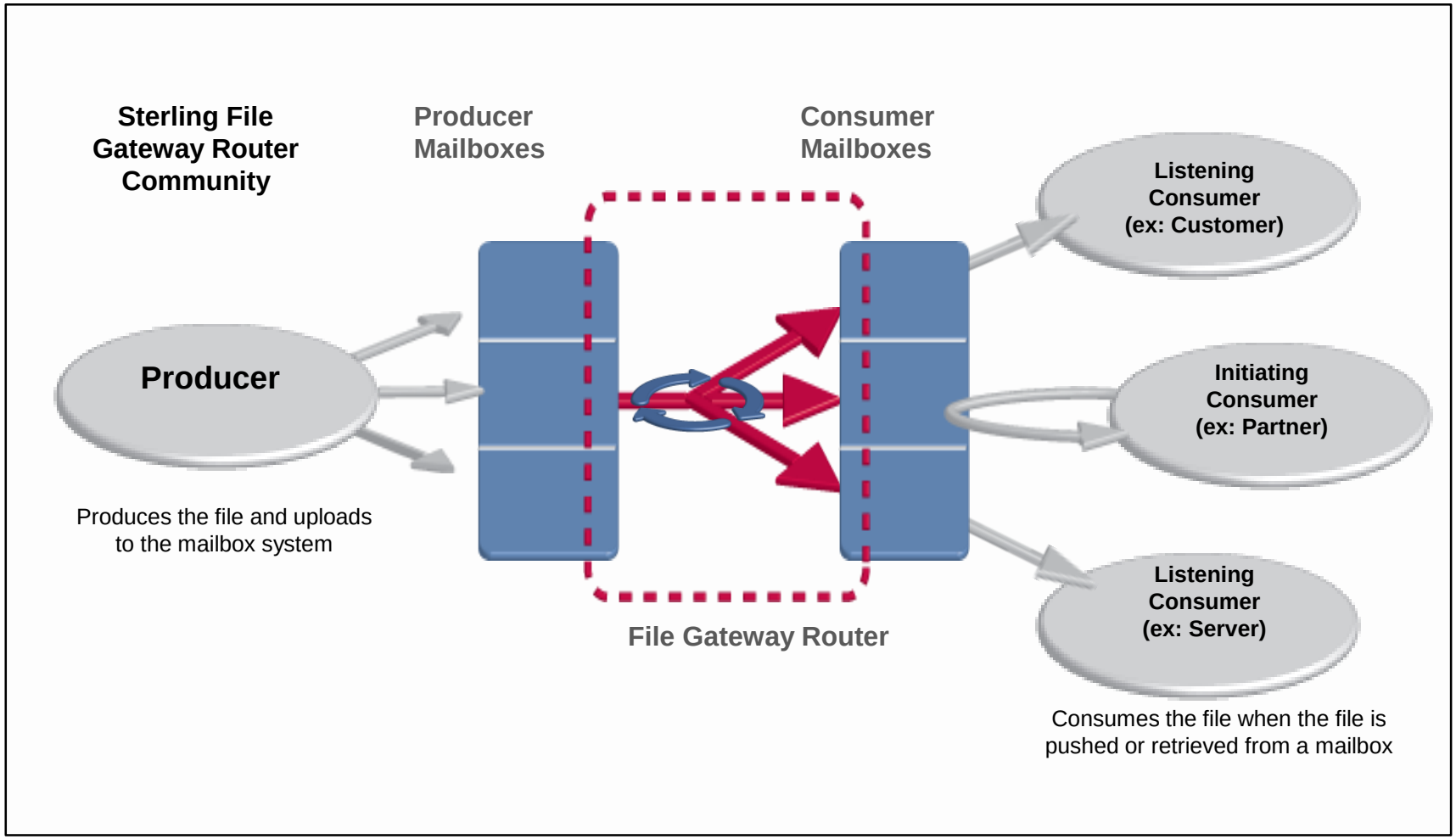
IBM Sterling Secure Proxy



IBM Sterling Secure Proxy



File Gateway is a Router



What is a Perimeter Server

A *perimeter server* is a software tool for communications management that can be installed in a DMZ.

The perimeter server manages the communications flow between outer layers of your network and the TCP-based transport adapters.

A perimeter server can solve problems with network congestion, security, and scalability, especially in high-volume, Internet-gateway environments.

A *perimeter network* is a computer network that is placed between a secure internal network and an unsecure external network to provide an additional layer of security. A perimeter server communicates with Sterling B2B Integrator through perimeter services.

Perimeter services is the subsystem supporting multihoming and secure perimeter network traversing for B2B communications protocols.

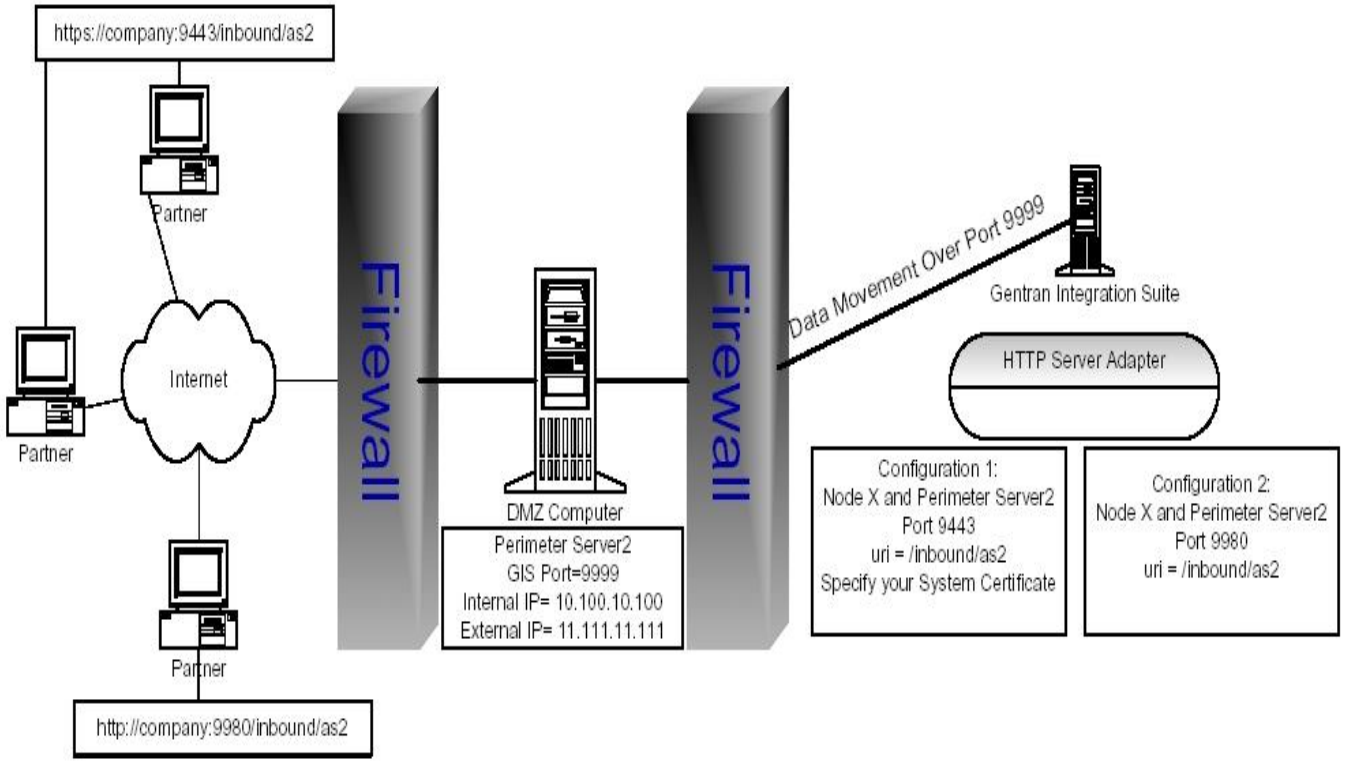
A perimeter server requires a corresponding perimeter client.

What is a Perimeter Server

Perimeter services consist of the following components:

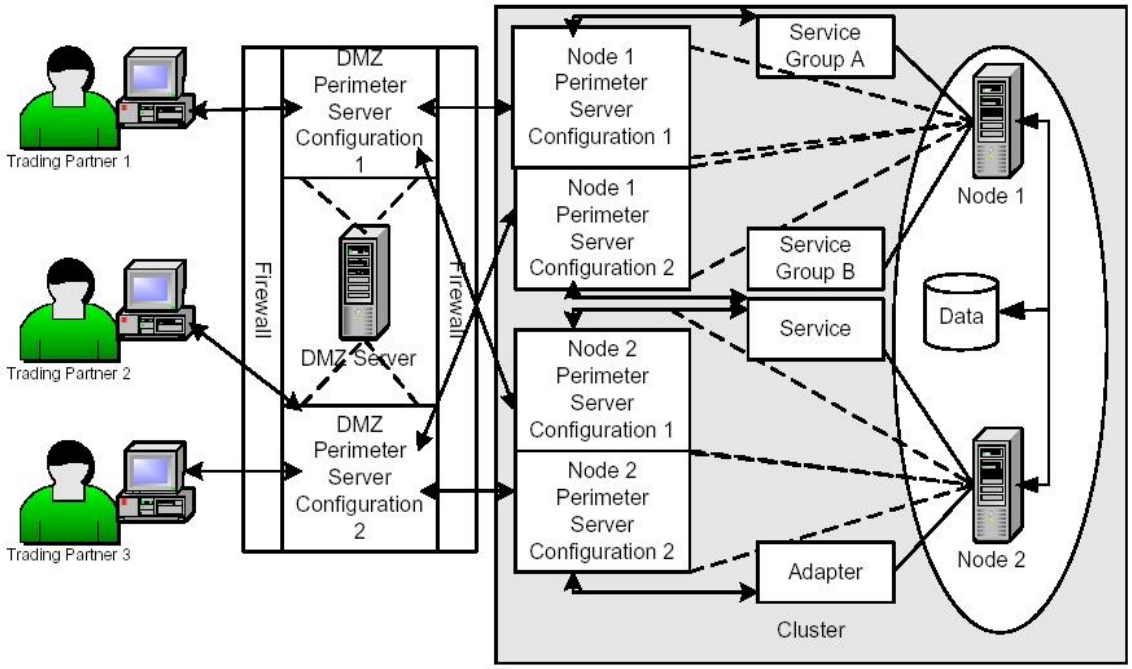
- Perimeter server you install on your DMZ computer or in a more secure network (remote perimeter server).
- Perimeter server pre-installed in Sterling B2B Integrator (local perimeter server).
- Perimeter services API that communications adapters in Sterling B2B Integrator use to use the perimeter servers (local and remote) for multihoming and perimeter network traversal functionality.
- Perimeter servers configuration management components in the Sterling B2B Integrator interface.

What is a Perimeter Server



Perimeter Servers and Clustering

The following figure shows a clustered environment running perimeter servers:



Perimeter Servers and More Secure Networks

The following figure shows this configuration: