Extranet Topologies for SharePoint 2010 Products

Access scenarios

Remote employee

Remote employees can access corporate information and electronic resources anywhere, anytime, without requiring a virtual private network (VPN). Remote employees include:

- Traveling sales employees.
- Employees working from home offices or at customer sites.
- Geographically dispersed virtual teams.

External partner or customer

External partners can participate in business processes and collaborate with employees of your organization. You can use an extranet to help enhance the security of data in the following ways:

- Apply appropriate security and user-interface components to isolate partners and to segregate internal data.
- Authorize partners to use only sites and data that are necessary for their contributions.
- Restrict partners from viewing other partners' data.

You can optimize processes and sites for partner collaboration in the following ways:

- Enable employees of your organization and partner employees to view, change, add, and delete content to promote successful results for both companies.
- Configure alerts to notify users when content changes or to start a workflow.

Branded Internet sites

Publish branded, targeted content to partners and customers in the following ways:

- Target content based on product line or customer profile.
- Segment content by implementing separate site collections within a farm.
- Limit content access and search results based on audience.

This scenario works well with an extranet topology designed for content publishing and optimized for hosting static content.

Web hosting

Microsoft® SharePoint® 2010 Products include the capability to isolate and separate data from different Web sites while sharing service application resources across these same sites. This capability is called multi-tenancy.

- Multi-tenancy of services creates a true hosting environment and makes it possible to share service resources across customers (tenants), while partitioning data based on site subscriptions.
- Site subscriptions group tenant data across all site collections owned by the tenant, and provide the ability to separate and group each tenant's data in an otherwise shared environment.
- Administrators can centrally deploy and manage features and services, while giving tenants full control over the usage and experience.

Mobile phone access

SharePoint 2010 Products include access to SharePoint sites from mobile phones:

- Manipulate data on SharePoint sites: view, edit, add items
- Search (documents, lists, people, line-of-business data)
- Mobile document viewers (Word, Microsoft® Excel®, Microsoft® PowerPoint®)
- Alerts sent to mobile phones from SharePoint 2010 Products
- Solution development platform

Forefront Secure Access Solutions

Microsoft® Forefront® Unified Access Gateway (Forefront UAG) provides secure Web publishing of applications, using SSL. Forefront UAG provides access to internal resources for remote employees and partners.

Forefront UAG adds the following capabilities to the SharePoint 2010 Products extranet solution:

- **Secure access to SharePoint sites from mobile devices** - Authentication of mobile users using a dedicated interface for mobile devices.
- **Health-based endpoint authorization** - Access policies that are based not only on the user's identity and the information exposed, but also on the condition of the client endpoint.
- **Information leakage mitigation** - Cleanup of the client endpoint, including cache, temporary files, and cookies.
- **Authenticate directly from rich clients** – Use Microsoft Office Forms Based Authentication (MSOFBA) or basic authentication to enable rich client programs to directly access SharePoint sites.

Additionally, Forefront UAG DirectAccess provides remote users with the experience of a seamless connection to the internal network. When Forefront UAG DirectAccess is enabled, requests for internal network resources are directed securely, without the need to connect to a VPN.

If your organization has previously deployed ISA Server 2006 to publish earlier releases of SharePoint, you can continue to use this product or move to Forefront Threat Management Gateway (TMG) to publish SharePoint 2010 Products applications.

Feature	ISA 2006	Forefront TMG	Forefront UAG
Built-in features for configuring SharePoint publishing	✓	✓	✓
Network load balancing	✓	✓	✓
Array support	✓	✓	✓
Mobile access	✓	✓	✓
Rich authentication	✓	✓	✓
Endpoint health detection			✓
Granular access policies			✓
Information leakage mitigation			✓
Unified portal for publishing multiple line-of-business applications			✓
DirectAccess		✓*	✓

* DirectAccess is partially supported for Forefront TMG 2010

Extranet topologies

Topology

Internet

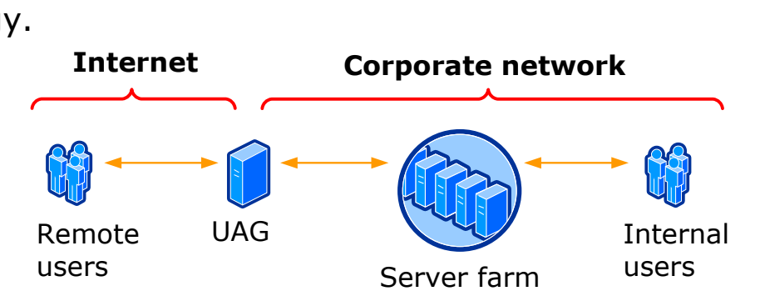
Perimeter network

Corporate network

Edge firewall

Description

This configuration uses a reverse proxy server on the border between the Internet and the corporate network to intercept and then forward requests to the appropriate Web server located in the intranet. By using a set of configurable rules, the proxy server verifies that the requested URLs are allowed based on the zone from which the request originated. The requested URLs are then translated into internal URLs. The following illustration shows an edge firewall topology.

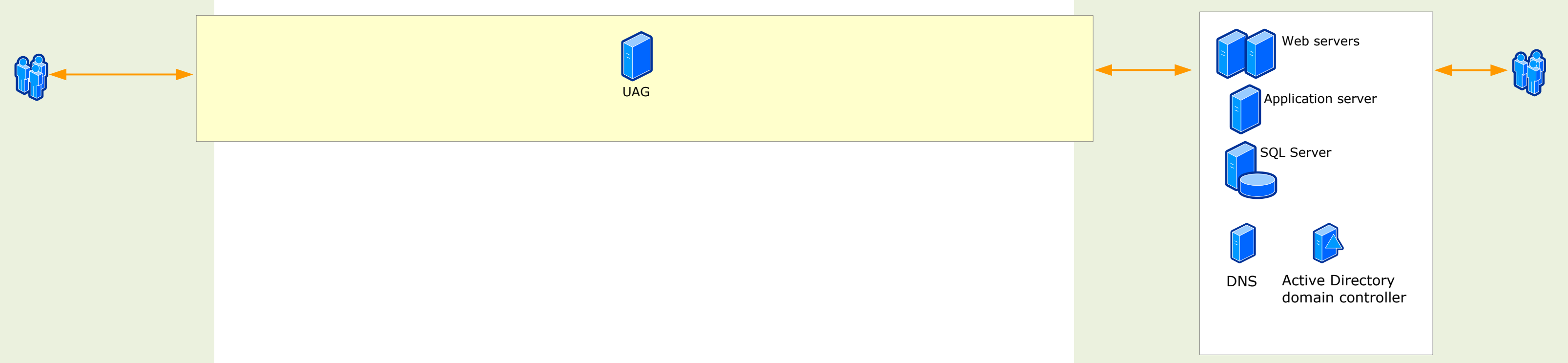


Advantages

- This is the simplest solution that requires the least amount of hardware and configuration.
- The entire server farm is located within the corporate network.
- There is a single point of data:
  - Data is located within the trusted network.
  - Data maintenance occurs in one place.
  - A single farm is used for both internal and external requests; this ensures that all authorized users view the same content.
- Internal user requests are not passed through a proxy server.
- UAG pre-authenticates users.

Disadvantage

- This configuration results in a single firewall that separates the corporate internal network from the Internet.



Back-to-back perimeter

Description

A back-to-back perimeter topology isolates the server farm in a separate perimeter network.

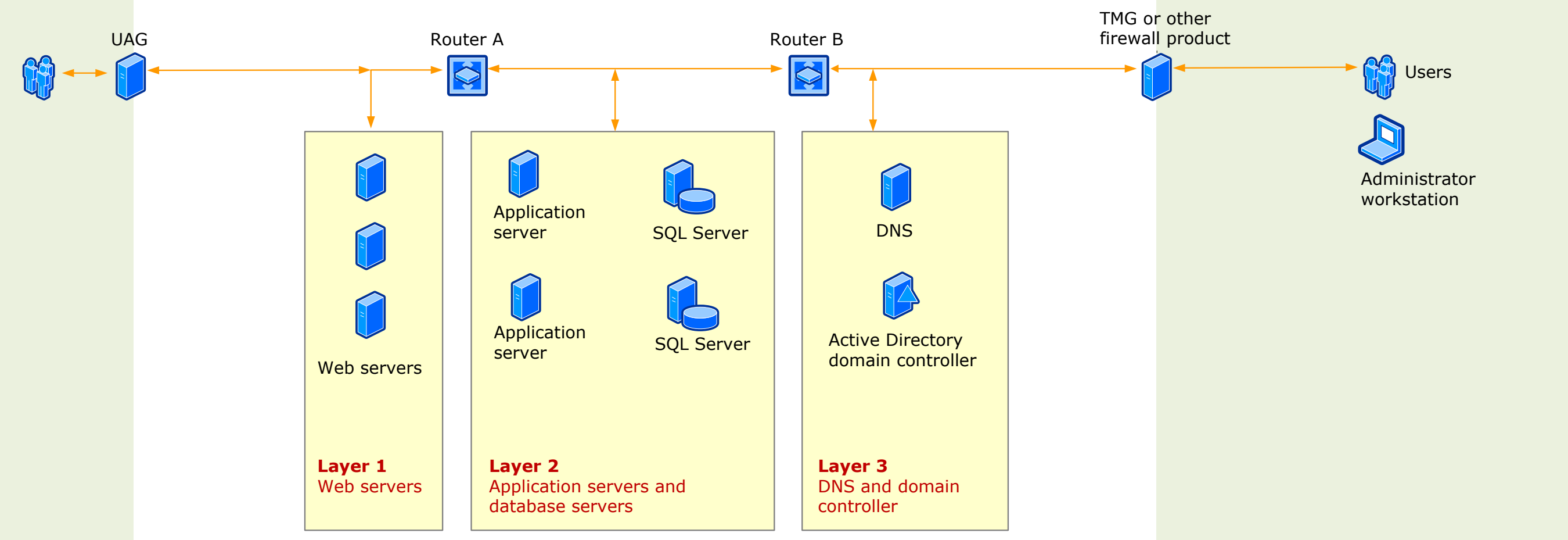
- All hardware and data reside in the perimeter network.
- The server farm roles and network infrastructure servers can be separated across multiple layers. Combining the network layers can reduce the complexity and cost.
- Each layer can be separated by additional routers or firewalls to ensure that only requests from specific layers are allowed.
- Requests from the internal network can be directed through the internal-facing ISA server or routed through the public interface of the perimeter network.

Advantages

- Content is isolated to a single farm on the extranet, simplifying sharing and maintenance of content across the intranet and the extranet.
- External user access is isolated to the perimeter network.
- If the extranet is compromised, damage is potentially limited to the affected layer or to the perimeter network.

Disadvantage

- The back-to-back perimeter topology requires additional network infrastructure and configuration.


UAG
Router A
Router B
TMG or other firewall product
Users
Administrator workstation
Web servers
Application server
SQL Server
Application server
SQL Server
DNS
Active Directory domain controller
Layer 1
Web servers
Layer 2
Application servers and database servers
Layer 3
DNS and domain controller

Back-to-back perimeter with cross-farm services

Description

In some scenarios, services are better optimized by sharing service applications across farms, even in extranet environments.

- A farm inside the corporate network hosts service applications that can be shared across farms.
- One or more farms in the perimeter network consumes service applications.

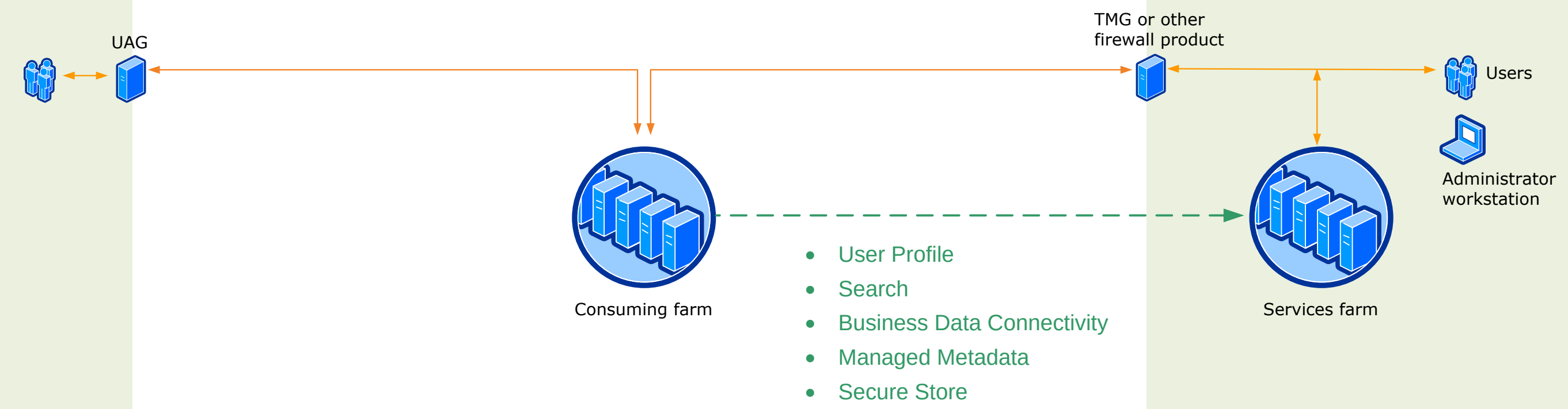
Advantages

- Services are centrally managed inside the corporate network.
- Service applications that involve many contributors, such as Managed Metadata, are located where the contributor accounts are located. Special access is not required for the perimeter network.

Disadvantages

- Some service applications require two-way trust between domains, for example, User Profile and Secure Store Service.

Note: Microsoft Project Server 2010 does not support cross-farm services.



Planning for services that access external data sources

Important: Service applications that access external data sources by using a delegated Windows identity (Excel Services, PerformancePoint Services, InfoPath Forms Services, and Visio Services) put additional requirements on the environment. External data sources must reside within the same domain as the SharePoint farm that hosts the service or the service application must be configured to use the Secure Store Service. If the Secure Store Service is not used and farm servers are split between two domains, the application servers must reside in the same domain as the external data sources. If external data sources do not reside within the same domain, authentication to the external data sources will fail.

Back-to-back perimeter with content publishing (and optional TMG caching)

Description

This topology adds content publishing to the back-to-back perimeter topology. By adding content publishing, sites and content that are developed inside the corporate network can be published to the server farm that is located in the perimeter network.

- Requires two separate farms — one in the corporate network and the other in the perimeter network.
- Publishing is one-way. Any content created or modified in the perimeter network is unique.

Advantages

- Customer-facing and partner-facing content is isolated in a separate perimeter network.
- Content publishing can be automated.
- If content in the perimeter network is compromised or corrupted as a result of Internet access, the integrity of the content in the corporate network is retained.

Disadvantages

- Additional hardware is required to maintain two separate farms.
- Data overhead is greater. Content is maintained and coordinated in two different farms and networks.
- Changes to content in the perimeter network are not reflected in the corporate network. Consequently, content publishing to the perimeter domain is not a workable choice for extranet sites that are collaborative.

Notes

The illustration shows the path of content deployment from the Central Administration site in the content staging farm to the Central Administration site in the destination farm. The Central Administration site is typically installed on one of the application servers. The illustration separately calls out the Central Administration site to show the role of this site in content deployment.

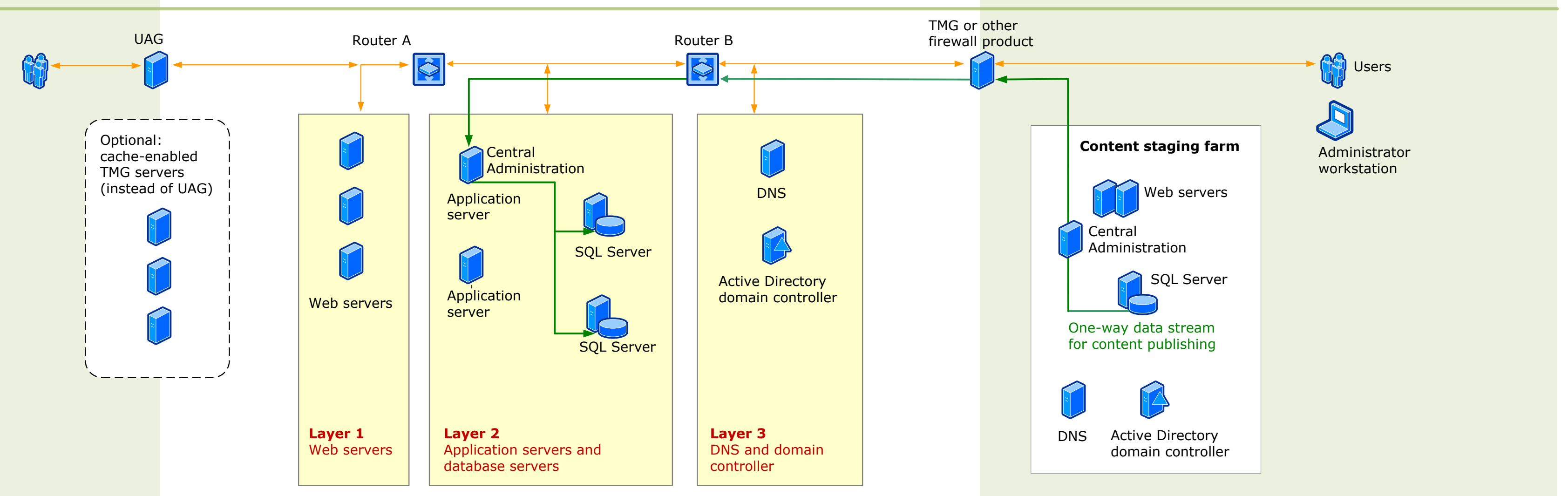
Using cache-enabled TMG servers

In environments where content does not require authentication, you can optimize performance by implementing caching features of Forefront TMG. TMG caching can be configured in addition to the caching features in SharePoint Server 2010.

TMG provide the following two types of caching:

- **Forward caching** Forward caching provides cached Web objects to internal users who make Web requests to the Internet.
- **Reverse caching** Reverse caching provides cached content to external Internet clients who make requests to internal Web servers published by TMG.

TMG caching enables you to scale out beyond the limits of a single farm by improving performance where Web servers might be a bottleneck. This enables you to improve performance when the maximum number of Web servers has been reached or to reduce the number of Web servers that are required.


UAG
Router A
Router B
TMG or other firewall product
Users
Administrator workstation
Optional: cache-enabled TMG servers (instead of UAG)
Web servers
Central Administration
Application server
SQL Server
Application server
SQL Server
DNS
Active Directory domain controller
Layer 1
Web servers
Layer 2
Application servers and database servers
Layer 3
DNS and domain controller
Content staging farm
Web servers
Central Administration
SQL Server
One-way data stream for content publishing
DNS
Active Directory domain controller

Split back-to-back

Description

This topology splits the farm between the perimeter and corporate networks. The computers running Microsoft SQL Server® database software are hosted inside the corporate network. Web servers are located in the perimeter network. The application server computers can be hosted in either the perimeter network or the corporate network.

If the server farm is split between the perimeter network and the corporate network, a domain trust relationship is required. In this scenario, the perimeter domain must trust the corporate domain.

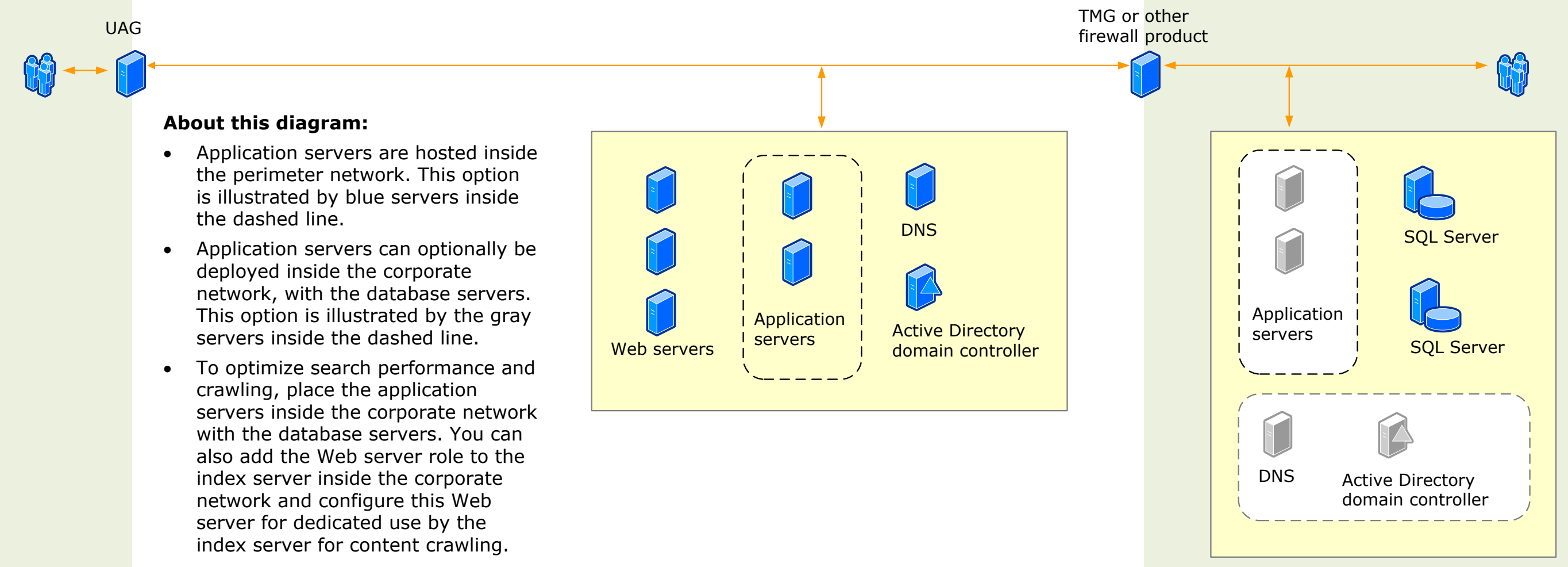
The only scenario in which a domain trust is not required is if the Web and application servers are in the perimeter network, the database servers are in the corporate network, *and* SQL authentication is used. However, if the Web and application servers are split between the networks and SQL authentication is used, a trust relationship is required.

Advantages

- Computers running SQL Server are not hosted inside the perimeter network.
- Farm components within both the corporate network and the perimeter network can share the same databases.
- Content can be isolated to a single farm inside the corporate network, which simplifies sharing and maintaining content across the corporate network and the perimeter network.

Disadvantages

- The complexity of the solution is greatly increased.
- Intruders who compromise perimeter network resources might gain access to farm content stored in the corporate network by using the server farm accounts.
- Inter-farm communication is split across two domains.


UAG
TMG or other firewall product
Web servers
Application servers
DNS
Active Directory domain controller
Application servers
SQL Server
SQL Server
DNS
Active Directory domain controller

About this diagram:

- Application servers are hosted inside the perimeter network. This option is illustrated by blue servers inside the dashed line.
- Application servers can optionally be deployed inside the corporate network, with the database servers. This option is illustrated by the gray servers inside the dashed line.
- To optimize search performance and crawling, place the application servers inside the corporate network with the database servers. You can also add the Web server role to the index server inside the corporate network and configure this Web server for dedicated use by the index server for content crawling.

Split back-to-back optimized for content publishing

Description

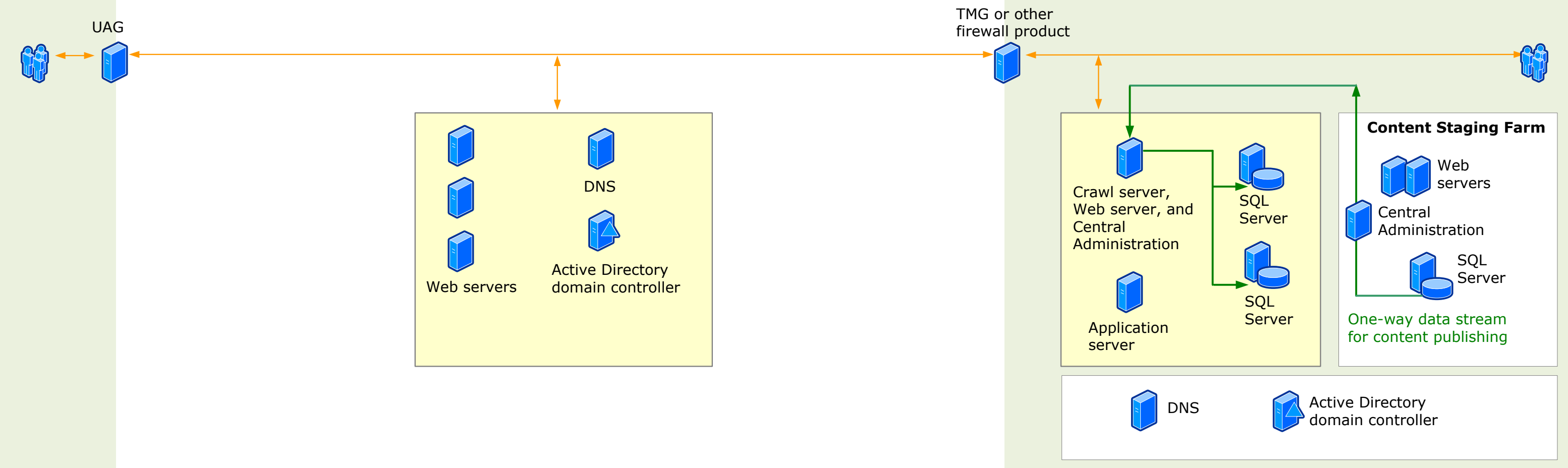
If you plan to publish content from a staging farm inside the corporate network to the database servers that host content for the extranet (also located inside the corporate network), you can optimize the farm by hosting the application servers, including the Central Administration site, inside the corporate network for the following reasons:

- The data stream for content publishing travels from the Central Administration site in the staging farm to the Central Administration site in the destination farm. If the Central Administration site is inside the corporate network, the content publishing data stream does not travel through the firewall between the perimeter network and the corporate network.
- Crawling takes place inside the corporate network.

Notes

The illustration shows the following choices:

- Application servers reside in the corporate network with the database servers. This requires a one-way trust relationship in which the perimeter domain trusts the corporate domain.
- The query role is installed in the same network as the databases, which optimizes performance of this role.
- The Central Administration site for the production farm is installed on the index server.
- The Web server role is installed on the crawl server for dedicated use by the crawl role.


UAG
TMG or other firewall product
Web servers
DNS
Active Directory domain controller
Crawl server, Web server, and Central Administration
SQL Server
SQL Server
Application server
Content Staging Farm
Web servers
Central Administration
SQL Server
One-way data stream for content publishing
DNS
Active Directory domain controller