

Plan security hardening for extranet environments (Windows SharePoint Services)

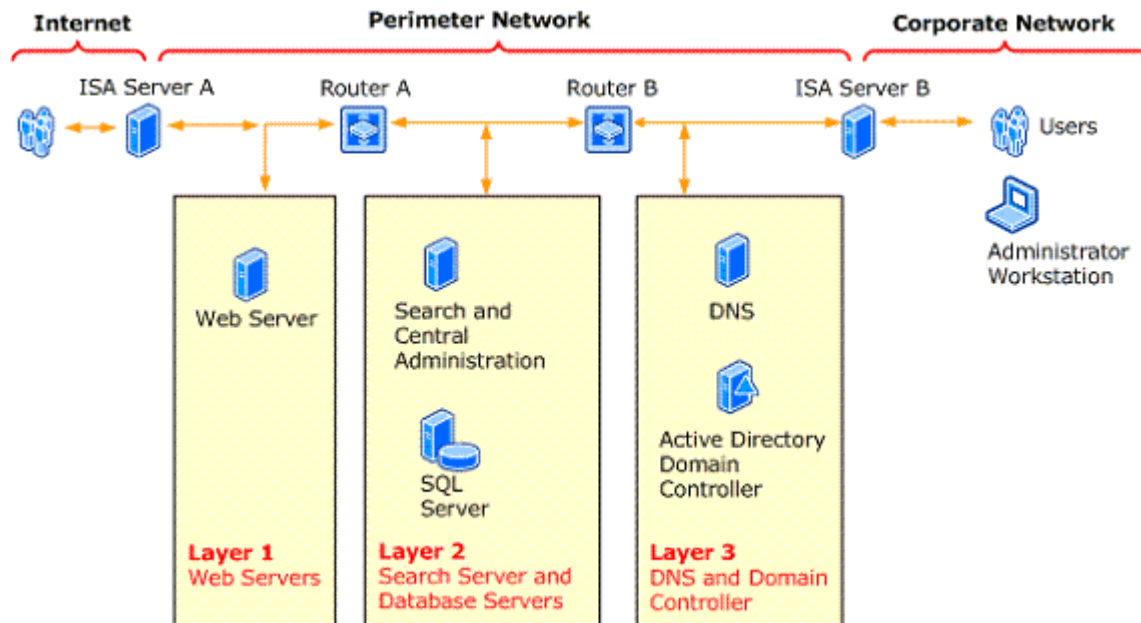
In this article:

- [Network topology](#)
- [Domain trust relationships](#)
- [Communication with server-farm roles](#)
- [Communication with infrastructure server roles](#)
- [Active Directory communication between network domains](#)

This article details the hardening requirements for an extranet environment in which a Windows SharePoint Services 3.0 server farm is placed inside a perimeter network and sites are available from the Internet or from the corporate network.

Network topology

The hardening guidance in this article can be applied to many different extranet configurations. The following figure shows an example implementation of a back-to-back perimeter network topology that illustrates the server and client roles across an extranet environment.



The purpose of the figure is to articulate each of the possible roles and their relationship to the overall environment. The Central Administration site can be installed to either a Web server or to the Search server (pictured). The routers illustrated can be exchanged for firewalls.

Domain trust relationships

The requirement for a domain trust relationship depends on how the server farm is configured. This


section discusses two possible configurations.

Server farm resides in the perimeter network

The perimeter network requires its own Active Directory directory service infrastructure and domain. Typically, the perimeter domain and the corporate domain are not configured to trust each other. However, to authenticate intranet users and remote employees who are using their domain credentials (Windows authentication), you must configure a one-way trust relationship in which the perimeter domain trusts the corporate domain. Forms authentication and Web SSO do not require a domain trust relationship.

Server farm is split between the perimeter network and the corporate network

If the server farm is split between the perimeter network and the corporate network with the database servers residing inside the corporate network, a domain trust relationship is required if Windows accounts are used. In this scenario, the perimeter network must trust the corporate network. If SQL authentication is used, a domain trust relationship is not required. The following table summarizes the differences between these two approaches.

	Windows authentication	SQL authentication
Description	<p>Corporate domain accounts are used for all Windows SharePoint Services 3.0 service and administration accounts, including application pool accounts.</p> <p>A one-way trust relationship, in which the perimeter network trusts the corporate network, is required.</p>	<p>Windows SharePoint Services 3.0 accounts are configured in the following ways:</p> <ul style="list-style-type: none"> • SQL authentication is used for every database that is created. • All other administration and service accounts are created as domain accounts in the perimeter network. • Web servers and search servers are joined to the perimeter network. <p>A trust relationship is not required but can be configured to support client authentication against an internal domain controller.</p> <div style="border: 1px solid black; padding: 5px;"> <p> Note</p> <p>If search servers reside in the corporate domain, a one-way trust relationship, in which the perimeter network trusts the corporate network, is required.</p> </div>
Setup	<p>Setup includes the following:</p> <ul style="list-style-type: none"> • Windows SharePoint Services 3.0 administration and service accounts are created in the corporate domain. • Web servers and application servers are joined to the perimeter network. 	<p>Setup includes the following:</p> <ul style="list-style-type: none"> • All database accounts must be created as SQL login accounts in SQL Server 2000 Enterprise Manager or SQL Server 2005 Management Studio. These accounts must be created <i>before</i> the creation of any Windows SharePoint Services 3.0 databases, including the configuration database and the SharePoint_AdminContent database. • You must use the Psconfig command-line tool to create the configuration database and the AdminContent database. You cannot use the SharePoint Products and Technologies

	<ul style="list-style-type: none"> • A trust relationship is established in which the perimeter domain trusts the corporate domain. 	<p>Configuration Wizard to create these databases. In addition to using the -user and -password parameters to specify the server farm account, you must use the -dbuser and -dbpassword parameters to specify SQL authentication accounts.</p> <ul style="list-style-type: none"> • You can create additional content databases in Central Administration by selecting the SQL authentication option. However, you must first create the SQL login accounts in SQL Server 2000 Enterprise Manager or SQL Server 2005 Management Studio. • Secure all communication with the database servers using SSL. • Ensure that ports used for communication with SQL Server remain open between the perimeter network and the corporate network
Additional information	The one-way trust relationship allows the Web servers and application servers that are joined to the extranet domain to resolve accounts that are in the corporate domain.	<ul style="list-style-type: none"> • SQL login accounts are encrypted in the registry of the Web servers and application servers. • The server farm account is not used to access the configuration database and the SharePoint_AdminContent database. The corresponding SQL login accounts are used instead.

The information in the preceding table assumes the following:

- Both the Web servers and the application servers reside in the perimeter network.
- All accounts are created with the least privileges necessary, including the following recommendations:
 - Separate accounts are created for all administrative and service accounts.
 - No account is a member of the Administrators group on any computer, including the server computer that hosts SQL Server.

For more information about Windows SharePoint Services 3.0 accounts, see [Plan for administrative and service accounts \(Windows SharePoint Services\)](http://technet.microsoft.com/en-us/library/cc288210(printer).aspx) [[http://technet.microsoft.com/en-us/library/cc288210\(printer\).aspx](http://technet.microsoft.com/en-us/library/cc288210(printer).aspx)] .

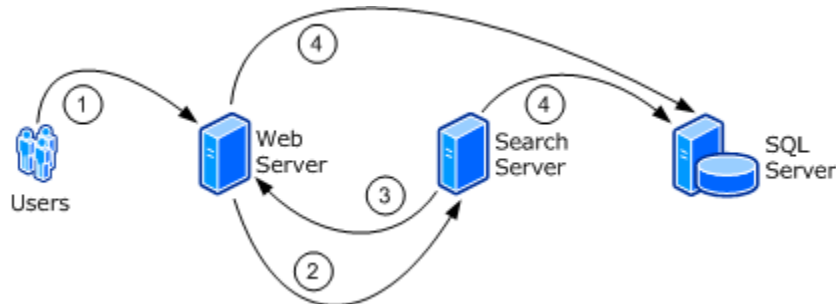
For more information about creating databases by using the Psconfig command-line tool, see [Command-line reference for the SharePoint Products and Technologies Configuration Wizard \(Windows SharePoint Services\)](http://technet.microsoft.com/en-us/library/cc288944(printer).aspx) [[http://technet.microsoft.com/en-us/library/cc288944\(printer\).aspx](http://technet.microsoft.com/en-us/library/cc288944(printer).aspx)] .

Communication with server-farm roles

When configuring an extranet environment, it is important to understand how the various server roles communicate within the server farm.

Communication between server roles

The following figure illustrates the communication channels within a server farm. The table that follows the figure describes the ports and protocols that are represented in the figure. The arrows indicate which server role initiates communication. For example, the Web server initiates communication with the database server. The database server does not initiate communication with the Web server. This is important to know when configuring inbound and outbound communication on a router or firewall.



Callout Ports and protocols

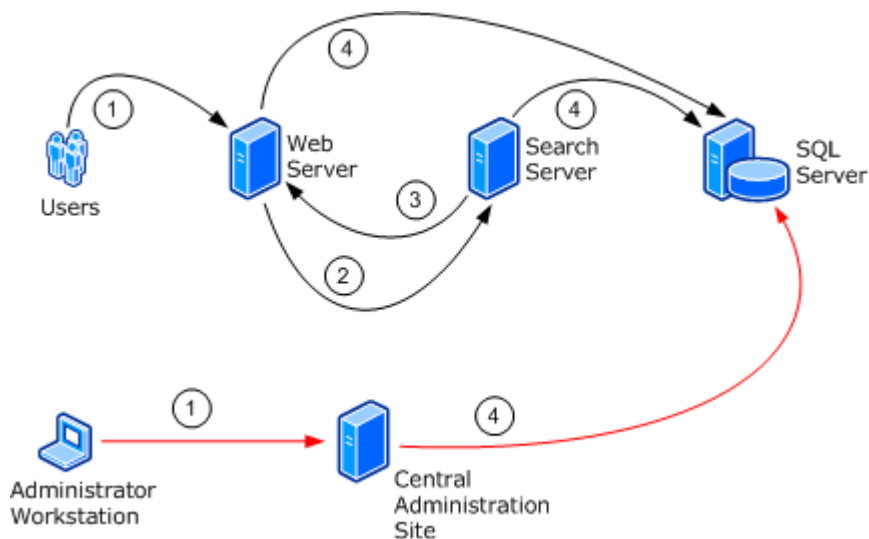
1	<p>Client access (including Information Rights Management (IRM) and search queries), one or more of the following:</p> <ul style="list-style-type: none"> • TCP port 80 • TCP/SSL port 443 • Custom ports
2	<p>File and printer sharing service — <i>Either</i> of the following:</p> <ul style="list-style-type: none"> • Direct-hosted server message block (SMB) (TCP/UDP 445) — Recommended • NetBIOS over TCP/IP (TCP/UDP ports 137, 138, 139) — Disable if not used
3	<p>Search crawling — Depending on how authentication is configured, SharePoint sites might be extended with an additional zone or Internet Information Services (IIS) site to ensure that the index component can access content. This configuration can result in custom ports.</p> <ul style="list-style-type: none"> • TCP port 80 • TCP/Secure Sockets Layer (SSL) port 443 • Custom ports
4	<p>Database communication:</p> <ul style="list-style-type: none"> • TCP/SSL port 1433 (default) for default instance (customizable) • TCP/SSL random port for named instances (customizable)

Communication between administrator workstations and Central Administration

The Central Administration site can be installed on any Web server or the search server. Configuration changes that are made through the Central Administration site are communicated to the configuration database. Other server roles in the farm pick up configuration changes that are registered in the configuration database during their polling cycles. Consequently, the Central Administration site does not introduce any new communication requirements to other server roles in the server farm. However, depending on which server you deploy the Central Administration site to, be sure to enable access from

administrator workstations.

The following figure includes the communication from an administrator workstation to the Central Administration site and the configuration database.



The following table describes the ports and protocols that are required for communication to and from the Central Administration site.

Callout	Ports and protocols
1	Central Administration site — One or more of the following: <ul style="list-style-type: none"> • TCP port 80 • TCP/SSL port 443 • Custom ports
4	Database communication: <ul style="list-style-type: none"> • TCP/SSL port 1433 (default) for default instance (customizable) • TCP/SSL random port for named instances (customizable)

Communication with infrastructure server roles

When configuring an extranet environment, it is important to understand how the various server roles communicate within infrastructure server computers.

Active Directory domain controller

The following table lists the port requirements for inbound connections from each server role to an Active Directory domain controller.

Item	Web Server	Search Server	Database Server
TCP/UDP 445 (directory services)	X	X	X

TCP/UDP 88 (Kerberos authentication)	X	X	X
Lightweight Directory Access Protocol (LDAP)/LDAPS ports 389/636 by default, customizable	X		

The Web servers require the use of LDAP/LDAPS ports only if LDAP authentication is configured.

DNS server

The following table lists the port requirements for inbound connections from each server role to a Domain Name System (DNS) server. In many extranet environments, one server computer hosts both the Active Directory domain controller and the DNS server.

Item	Web Server	Search Server	Database Server
DNS, TCP/UDP 53	X	X	X

SMTP service

E-mail integration requires the use of the Simple Mail Transport Protocol (SMTP) service using TCP port 25 on at least one of the front-end Web servers in the server farm. The SMTP service is required for incoming e-mail (inbound connections). For outgoing e-mail, you can either use the SMTP service or route outgoing e-mail through a dedicated e-mail server in your organization, such as a computer running Microsoft Exchange Server.

Item	Web Server	Search Server	Database Server
TCP port 25	X		

Active Directory communication between network domains

Active Directory communication between domains to support authentication with a domain controller inside the corporate network requires at least a one-way trust relationship in which the perimeter network trusts the corporate network.

In the example illustrated in the first figure in this article, the following ports are required as inbound connections to ISA Server B to support a one-way trust relationship:

- TCP/UDP 135 (RPC)
- TCP/UDP 389 by default, customizable (LDAP)
- TCP 636 by default, customizable (LDAP SSL)
- TCP 3268 (LDAP GC)
- TCP 3269 (LDAP GC SSL)
- TCP/UDP 53 (DNS)
- TCP/UDP 88 (Kerberos)
- TCP/UDP 445 (Directory Services)
- TCP/UDP 749 (Kerberos-Adm)
- TCP port 750 (Kerberos-IV)

When configuring ISA Server B (or an alternate device between the perimeter network and the corporate network), the network relationship must be defined as routed. Do not define the network relationship as Network Address Translation (NAT).

For more information about security hardening requirements related to trust relationships, see the following resources:

- [How to configure a firewall for domains and trusts](http://go.microsoft.com/fwlink/?LinkId=83470&clcid=0x409) [<http://go.microsoft.com/fwlink/?LinkId=83470&clcid=0x409>] (<http://go.microsoft.com/fwlink/?LinkId=83470&clcid=0x409>).
- [Active Directory in Networks Segmented by Firewalls](http://go.microsoft.com/fwlink/?LinkId=76147&clcid=0x409) [<http://go.microsoft.com/fwlink/?LinkId=76147&clcid=0x409>] (<http://go.microsoft.com/fwlink/?LinkId=76147&clcid=0x409>).