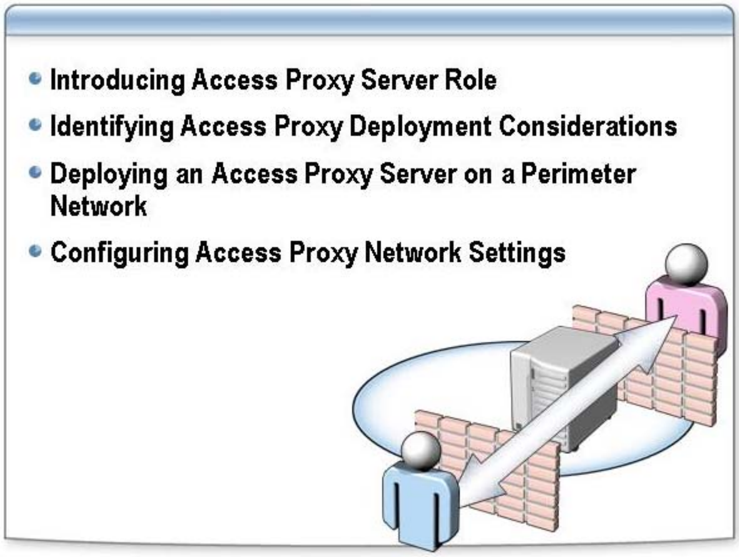
Microsoft®

Module 6: Installing an Access Proxy Server in Live Communications Server 2005 with Service Pack 1

Contents

Overview



- Introducing Access Proxy Server Role
- Identifying Access Proxy Deployment Considerations
- Deploying an Access Proxy Server on a Perimeter Network
- Configuring Access Proxy Network Settings

Introduction

After you deploy Microsoft® Live Communications Server 2005 with Service Pack 1 (LCS 2005 with SP1) Standard or Enterprise Edition, you may want to extend your organization's reach by providing secure external connections to your remote users, business partners, and customers.

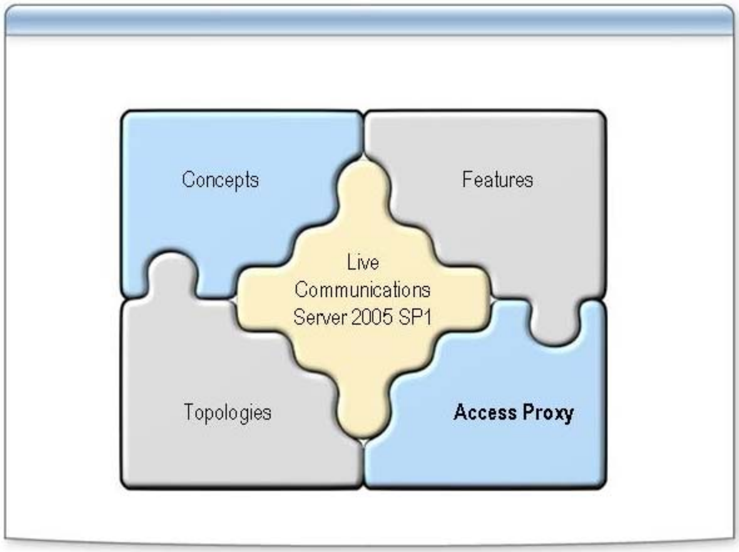
An Access Proxy server enables external connections by providing secure communications for both inbound and outbound traffic across Internet-facing firewalls.

Objectives

After completing this module, you will be able to:

- Describe concepts, features, and topologies of an Access Proxy server.
- List the requirements and recommendations for an Access Proxy server deployment.
- Deploy an Access Proxy server into an existing LCS 2005 with SP1 environment.
- Configure Access Proxy server network settings.

Lesson: Introducing Access Proxy Server Role



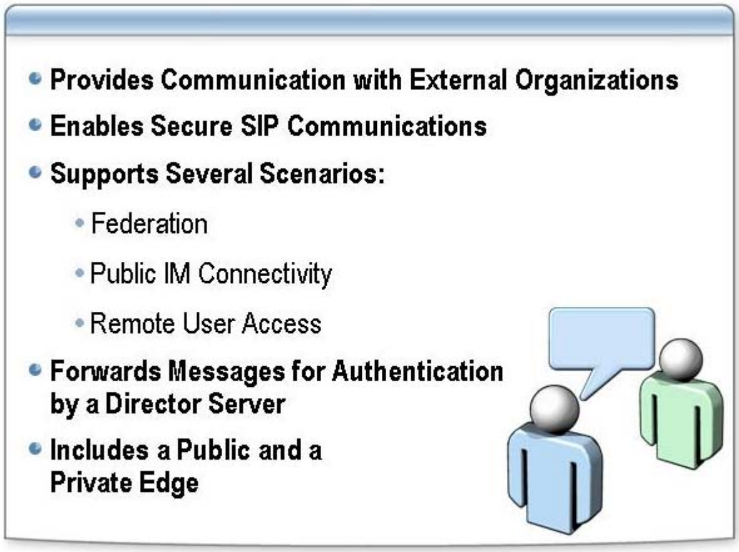
Lesson Objectives

This lesson introduces the Access Proxy server role, which you may want to install in either a Live Communications Server 2005 with SP1 Standard or Enterprise Edition environment. This lesson also describes the concepts, features, and topologies of an Access Proxy server.

After completing this lesson, you will be able to:

- Explain the purpose of an Access Proxy server role.
- List the features of an Access Proxy server.
- List each topology an Access Proxy server supports.
- Describe concepts, features, and topologies of an Access Proxy server.

What Is an Access Proxy Server?



- Provides Communication with External Organizations
- Enables Secure SIP Communications
- Supports Several Scenarios:
  - Federation
  - Public IM Connectivity
  - Remote User Access
- Forwards Messages for Authentication by a Director Server
- Includes a Public and a Private Edge

Introduction

The Access Proxy server is a new server role in Live Communications Server 2005. The Access Proxy provides a single, trusted connection point through which both inbound and outbound Session Initiation Protocol (SIP) traffic can cross Internet firewalls.

Scenarios

An Access Proxy server role is a prerequisite if you want to enable external communications for your LCS 2005 with SP1 deployment. External communications include the following scenarios:

- Federation with other businesses
- Connectivity with public IM networks such as MSN®, Yahoo!, or AOL
- Support for remote users

High Volume Environments

If your organization anticipates a high volume of external SIP traffic, you can deploy multiple Access Proxy servers in one or more arrays behind both external and internal hardware load balancers. You can configure each array as the sole connection point for some specified set of federated partners, remote users, or branch offices.

Authentication

Access Proxy servers do not provide authentication, although the Access Proxy does validate inbound message headers. Using a configured static route, it passes inbound traffic unchallenged to an internal next hop SIP server for authentication.

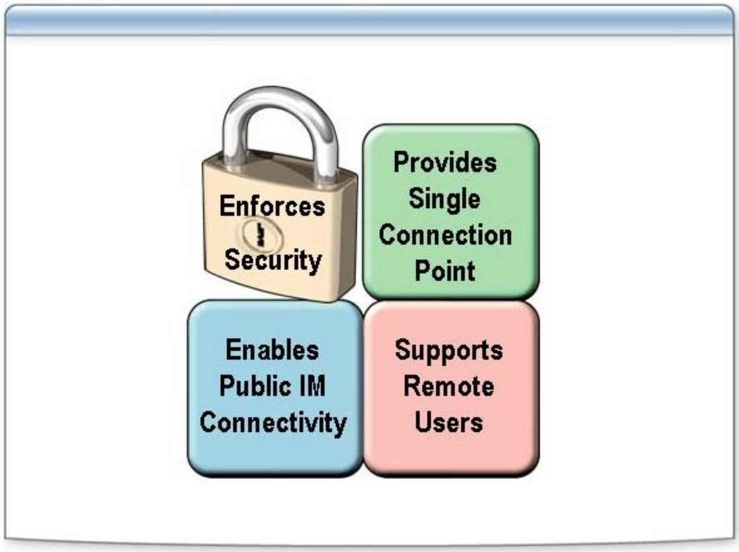
Important You may decide to use a Director server to provide authentication services. However, this is not a requirement for an Access Proxy implementation.

Public and Private Edge

Access Proxy servers always have two network interfaces. One network interface is the public (external) edge for accepting inbound SIP communications. The other network interface is the private edge, which supports outbound SIP communications from your internal network. Each edge will have a listening port and routing rules.

Important Microsoft only supports an Access Proxy server with two separate network interface cards. Each network interface card must be configured on different subnets.

What Are the Benefits of an Access Proxy Server?


Enforces Security
Provides Single Connection Point
Enables Public IM Connectivity
Supports Remote Users

Introduction

In the information worker age, individuals can work from home, office, car, and plane. Access to up-to-date information is critical. LCS 2005 with SP1 provides encrypted communications between your LCS 2005 with SP1 users and their external business partners. The LCS 2005 with SP1 Access Proxy role provides this additional security, and creates a single connection point between your organization and its affiliates.

Network Protection

The Access Proxy server implementation protects the internal network. Security risks are reduced because the internal network does not have a direct entry point.

Important You can install an Access Proxy server directly on your internal network but this is not a recommended configuration. You should install the Access Proxy in a perimeter network.

Message Encryption

The Access Proxy server allows Mutual Transport Layer Security (MTLS) encryption for Server-to-Server communication. It also supports Transport Layer Security (TLS) for Client-to-Server communication such as Remote User Access.

MTLS and TLS are used by LCS 2005 with SP1 to provide encryption. Server-to-server traffic is required to be MTLS, both inside and outside of the internal network perimeter. Client-to-client traffic inside the internal network perimeter can be TLS.

MTLS and TLS require digital certificates to be installed on each Access Proxy server. If the Access Proxy server is installed in a perimeter network, a digital certificate is required for the public edge and private edge. All communication traffic is encrypted, and message content is protected while in transit across public networks.

Administrative Control

LCS 2005 with SP1 enhances security through effective administrative control. Administrators can enable or disable Public IM Connectivity on a per-user basis. Administrators can also secure the Public IM Connectivity by choosing which Public IM service providers to enable for communication purposes.

Enterprise to enterprise federation also maintains separate administrative control for each deployment of LCS 2005 with SP1. An example of administrative control includes the authorization or restriction of individual users who are participating in the federation.

Message Filtering

The Access Proxy server can also provide filtering of Spam over Instant Messaging (SPIM). Microsoft has included this new filtering mechanism to prevent unsolicited communications with users who run the Microsoft Office Communicator or Microsoft Windows® Messaging clients.

Single Connection Point

A single Access Proxy server can provide multiple connections to remote users, business partners, as well as to outside vendors. One Access Proxy server can support the following connectivity options:

- Federation (Enhanced and Direct)
- Public IM Connectivity
- Remote Users

Public IM Connectivity

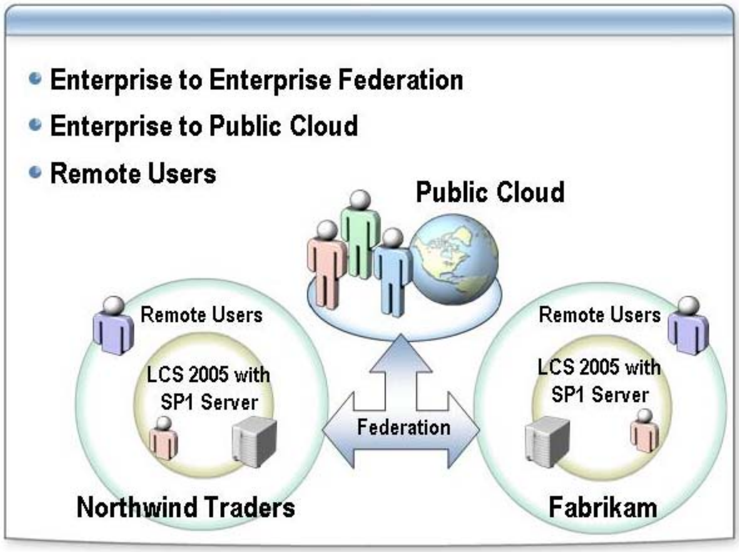
A new feature of an Access Proxy server is public IM connectivity or communication to a public IM cloud. An Access Proxy server supports communication between your organization's internal users and business partners or customers who use public instant messaging networks, such as MSN, Yahoo!, and AOL.

Remote User Support

Logistic vendors (shipping and delivery) are examples of remote users. Remote users could alert team members of potential delays by simply searching their roaming contact lists for presence information on their mobile phones. If a contact is online, they can IM an urgent notification of the delay.

Note LCS 2005 with SP1 does not require virtual private network (VPN) connectivity to support remote users.

Topologies Supported by Access Proxy Server



- Enterprise to Enterprise Federation
- Enterprise to Public Cloud
- Remote Users

Introduction

The Access Proxy role in LCS 2005 with SP1 supports the following basic topologies:

- Enterprise to Enterprise Federation through:
  - Enhanced Federation
  - Direct Federation
- Enterprise to Public Cloud
- Remote Users

Your organization can implement each topology separately based on the needs of the business.

Note The basic topologies do not require a Director server, although this is a recommended addition. A Director server provides authentication for remote users.

Federation

Federation is the capability to connect two or more enterprises to allow for extending presence information and instant messaging to business partners, suppliers, and customers. Federation enables efficient collaboration and provides a channel for connecting people in different geographical locations.

Enterprise to Enterprise Federation

Enterprise-to-Enterprise Federation provides secure connectivity between different LCS 2005 with SP1 enterprise deployments by maintaining trusted SIP connections between external networks and your internal organization. Users from different organizations can work together seamlessly as if they are in same SIP domain, with access to:

- Instant messaging
- Online presence information

You may configure Enterprise to Enterprise Federation in two ways:

- Enhanced Federation
- Direct Federation

Enhanced Federation is a new option in LCS 2005 with SP1, and reduces administration when you set up trusted SIP connections to other organizations. Enhanced Federation uses Domain Name Service (DNS) and service (SRV) records to find other SIP domains.

Important By default, Enhanced Federation requires you to configure a list of specified domains your organization wants to include in Enhanced Federation. This mode is Restricted Enhanced Federation. Unrestricted Enhanced Federation allows any SIP domain with a valid certificate to make a connection.

Direct Federation requires coordination with the administrator of the external SIP domain. Each administrator must specify the external organization's Access Proxy server name, the external destination domain, and possibly share certificates that have been privately generated.

Caution If your organization wants Direct Federation with 100 partners, then you must create 100 Direct Federation rules.

Enterprise to Public Cloud

Your organization may need to work with consultants, vendors and other individuals outside your network. These business partners provide critical real-time data. Public IM Connectivity allows an internal organization to communicate directly with public IM service providers such as MSN, Yahoo!, and AOL.

LCS 2005 with SP1 Enterprise to Public Cloud Federation enforces security and can archive business communication to outside business partners.

Note Enterprise to Public Cloud federation requires additional licenses, along with a LCS 2005 with SP1 CAL.

Remote Users

Telecommuters and remote users can take advantage of LCS 2005 with SP1 features. Remote LCS 2005 with SP1 users can:

- Maintain a roaming contact list.
- Use IM with co-workers.
- Search corporate IM users.
- Display Presence information.

This instant messaging information is encrypted and can be archived for compliance and tracking purposes.

Lesson: Identifying Access Proxy Deployment Considerations

- **Preparing DNS for an Access Proxy Server**
- **Considering Global Catalog Server Placement**
- **Planning for Certificates**

Introduction

Live Communications Server 2005 with SP1 Access Proxy server implementations requires a dependable underlying network infrastructure. These infrastructure requirements include DNS, Global Catalog servers, and certificates.

Without these infrastructure requirements, LCS 2005 with SP1 will not function correctly. Hence, it is important for you to review and configure the existing infrastructure before deploying an Access Proxy server.

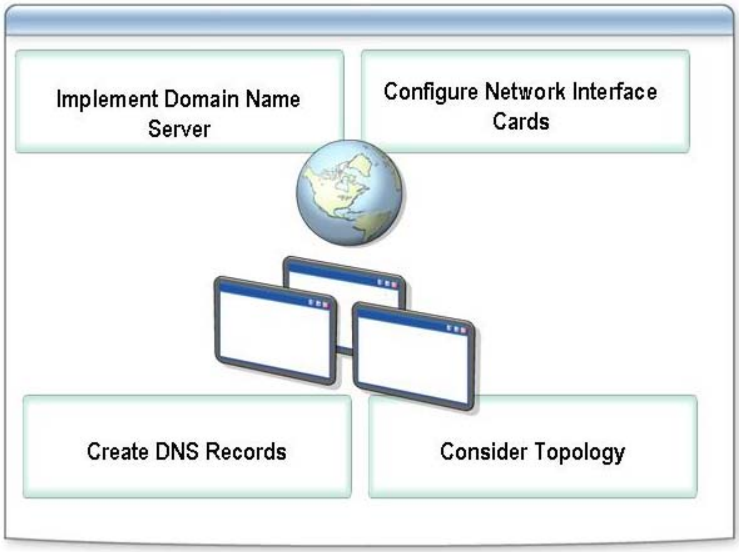
Lesson Objectives

After completing this lesson, you will be able to:

- Configure DNS for an Access Proxy server implementation.
- Determine strategic Global Catalog server installations.
- Plan for Access Proxy server certificates.
- List the requirements and recommendations for an Access Proxy server deployment.

If you deploy the Access Proxy server in a perimeter network, it should be a member of a workgroup. If the Access Proxy server is located on your internal network, join it to your Active Directory domain.

Preparing DNS for an Access Proxy Server


Implement Domain Name Server

Configure Network Interface Cards

Create DNS Records

Consider Topology

Introduction

An Access Proxy implementation relies specifically on DNS. To use DNS, you must configure your Access Proxy server with the IP address of one or more DNS servers. You also configure DNS on each Access Proxy server differently based on the topology you require, and whether you are setting up a Public Edge or a Private Edge.

Regardless of the topology you choose, you must create:

- An Address (A) record that maps to the IP address of the Access Proxy server for the Private Edge.
- An Address (A) record that maps to the IP address of the Access Proxy server for the Public Edge.

If you are planning to implement Remote User Access or Enhanced Federation, you will also create the following record depending on the topology you choose:

- A Service (SRV) record that maps to the A record for your Public Edge.

Network Interface Card

You must configure the network interface cards for your Public Edge or Private Edge to point to valid DNS servers. Your Private Edge will point to internal DNS servers while your Public Edge will point to one or more publicly accessible DNS servers.

Use the following steps to complete this task:

1. In **Control Panel**, select **Network Connections**.
2. In the **Network Connections** window, right-click the relevant **Local Area Connection** icon, and then click **Properties**.
3. In the **Network Connection Properties** dialog box, select **Internet Protocol (TCP/IP)**, and then click the **Properties** button.
4. Select **Use the following DNS server addresses**, and then enter the IP address of the relevant DNS server.

Note You are likely to have a fixed IP address for both the Public and Private Edges on the Access Proxy server.

A Records

DNS A records map a host name to an IP address. You must ensure that DNS contains an A record that maps to the correct IP address of your Access Proxy server's Public and Private Edge.

SRV Records

The SRV record allows a DNS client to locate a host that supports a particular service. For Access Proxy servers, you configure a SRV record for the SIP service, in the form:

_sip._tls.<domain>

This SRV record must then point to the host name for the relevant A record.

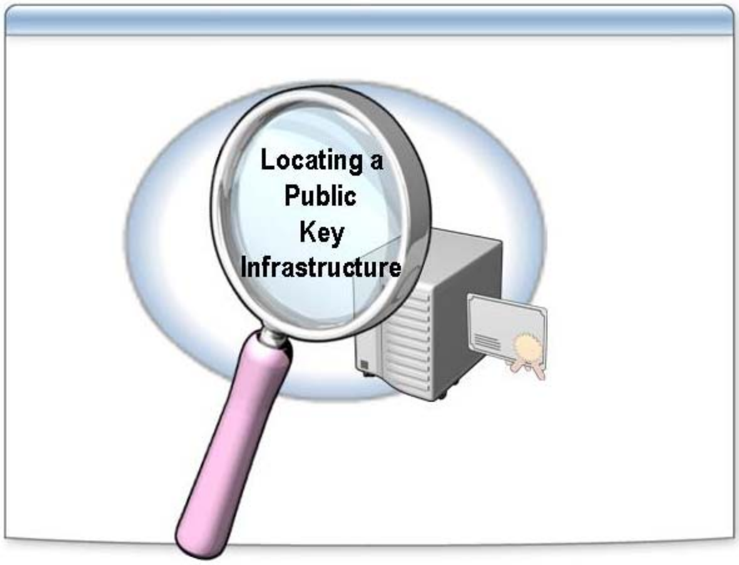
Topology Considerations

If you have decided to implement Enhanced Federation or Public IM Connectivity, you must configure an additional SRV record. Add a SRV record in the form:

_sipfederationtls._tcp.<domain>

This SRV record must also point to the A record.

Planning for Certificates



Introduction

Live Communications Server 2005 with SP1 requires each Access Proxy to have a digital certificate properly installed and configured.

You obtain these certificates from a Public Key Infrastructure (PKI). Your company might have an existing Windows 2003 certification authority (CA) infrastructure or use a third party CA.

Important An Access Proxy with only a single DNS name only requires one certificate. However, if you configure a Public Edge and Private Edge, each edge could have its own DNS name, which would requires two certificates

The certificate installation process depends on the location of the Access Proxy server.

Windows 2003 Certification Authority

If you have an existing Microsoft Windows 2003 CA, and you are deploying the Access Proxy server on the internal network, you can obtain a certificate from the existing Windows 2003 CA.

Third Party Certification Authority

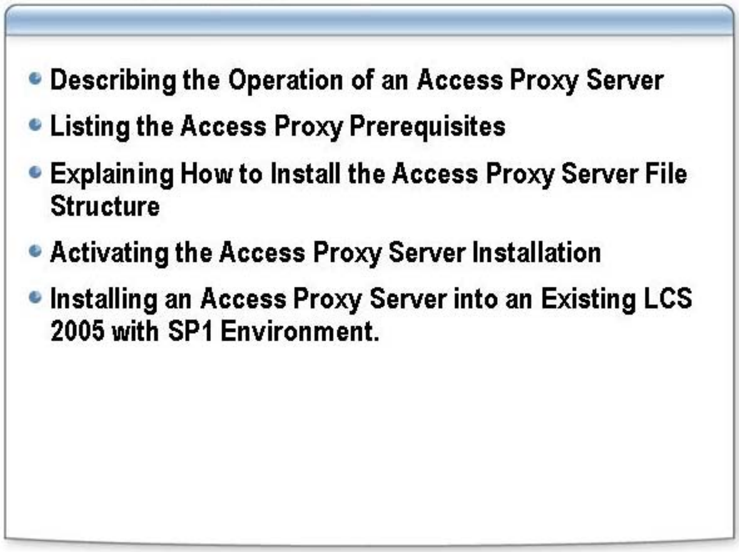
You may obtain a certificate from a third-party certificate authority in any of the following scenarios:

- Deploying an Access Proxy server in a perimeter network
- Implementing Public IM connectivity
- Using Enhanced Federation
- Configuring Direct Federation with many participating federation partners

Additional Resources

If you do not have an existing Public Key Infrastructure, review "Live Communications Server 2005 Document: Configuring Certificates" on the Microsoft Web site, at: www.microsoft.com/downloads/details.aspx?FamilyId=779DEDAA-2687-4452-901E-719CE6EC4E5A&displaylang=en

Lesson: Deploying an Access Proxy Server in a Perimeter Network



- Describing the Operation of an Access Proxy Server
- Listing the Access Proxy Prerequisites
- Explaining How to Install the Access Proxy Server File Structure
- Activating the Access Proxy Server Installation
- Installing an Access Proxy Server into an Existing LCS 2005 with SP1 Environment.

Introduction

If your company has decided to implement Live Communications Server 2005 with SP1 to support remote users and business partners, the following lesson will guide you through the installation process for an Access Proxy server.

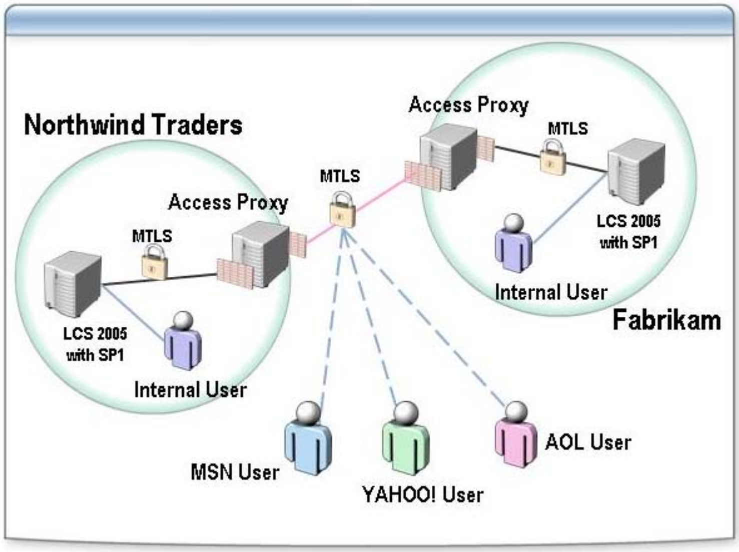
The same Access Proxy server can also support Enterprise to Enterprise Federations or Enterprise to Public IM Connectivity.

Lesson Objectives

After completing this lesson, you will be able to:

- Describe how to implement an Access Proxy Server.
- List the prerequisites before deploying an Access Proxy server.
- Explain how to install the Access Proxy server file structure.
- Activate the Access Proxy server installation for production usage.
- Install an Access Proxy server into an existing LCS 2005 with SP1 environment.

How to Implement an Access Proxy Server



Introduction

An Access Proxy server implementation requires an existing LCS 2005 with SP1 internal infrastructure. You will also want to provide a perimeter network where the Access Proxy server will be located.

MTLS Encryption

LCS 2005 with SP1 can use MTLS and TLS to provide encryption between any of the following:

- Access Proxy server and internal LCS 2005 with SP1 Standard Edition Server
- Access Proxy server and Enterprise Pool
- Access Proxy and the public IM service providers
- Access Proxy server and external Federation partners

Setup Procedures

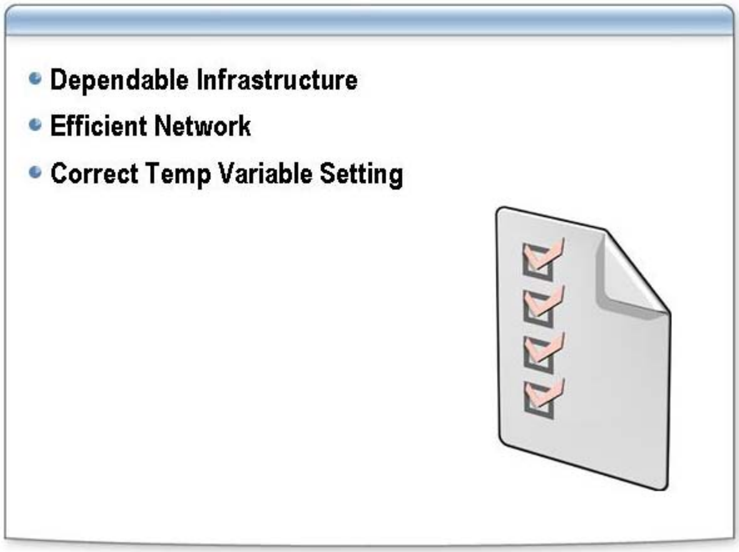
The following steps are required to implement an Access Proxy server successfully:

1. Verify prerequisites
2. Install the Access Proxy files
3. Activate the Access Proxy files
4. Complete post-setup procedures

The setup procedure automatically handles the creation of Access Proxy files, file structure, permission groups, service, and registry entries.

Important The Access Proxy service will not start until the configurations have been completed.

Reviewing Prerequisites



- Dependable Infrastructure
- Efficient Network
- Correct Temp Variable Setting

Introduction

You should review your current environment and verify that the infrastructure, network, and computers are prepared for an Access Proxy server implementation.

Important You need to decide if the Access Proxy server will be joined to a workgroup in your perimeter network or joined to your domain on your internal network. For more information, see the "How to Activate Access Proxy server" topic later in this module.

Infrastructure

You should verify that DNS is deployed and configured correctly. You also need to verify your PKI infrastructure.

Network

Verify that your firewall administrator has opened the SIP communication port. By default, the SIP port is 5061.

Note The network configuration is discussed later in this module.

Temp Variable

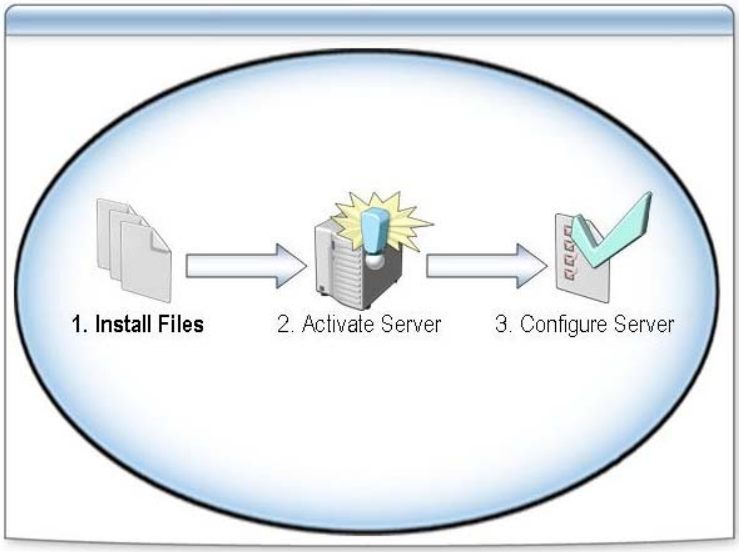
Access Proxy deployment requires validation of the %TEMP% environment variable. If the %TEMP% environment variable points to an encrypted folder, the graphical user interface (GUI) setup tool will not be able to deploy the Access Proxy server.

Complete the following steps to verify the Temp folder location:

1. Identify the %TEMP% folder by opening a command line and typing **Set**.
2. Navigate to the folder.
3. Review the Advanced properties of the %TEMP% folder in Windows Explorer and verify whether the **Encrypt content to secure data** option is selected.

4. If the Temp folder is encrypted, configure another folder and assign it to the %TEMP% environment variable. This can be completed in the command prompt by typing **SET %temp%=<drive>:\<directory>**.

Installing Access Proxy Files



Introduction

You deploy an Access Proxy server in three phases. The first phase is to copy the necessary files to the hardware you designate as an Access Proxy server.

Live Communications Server 2005 with SP1 includes a GUI setup tool to assist in the Access Proxy server installation. The GUI setup tool can:

- Explain the installation tasks.
- Generate warnings about disk space and other constraints.
- Provide Task Wizards to assist with the installation process.
- Analyze permissions for the installing account.
- Review prerequisites to ensure that all dependencies have been met.

Log on to Target Server

You must log on to the target server locally. Verify that your account is a member of the Administrators group.

Execute Setup.exe

The GUI setup executable setup.exe is located in the **i386** directory on the Live Communications Server 2005 with SP1 CD.

Install Access Proxy Files

The GUI setup tool lists several different server roles. Select the **Access Proxy** option, and then click **Install Files for Proxy**.

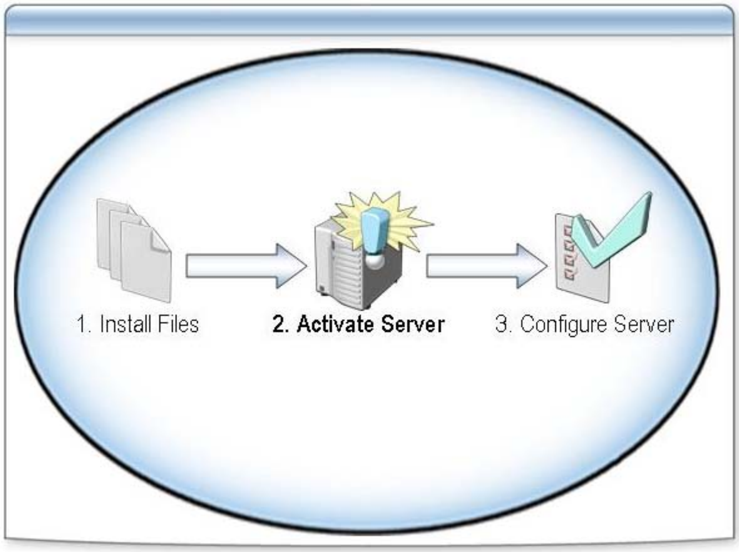
The wizard prompts you for the following information:

The wizard prompts you for license information, destination file location, and additional customer information.

After installation is complete, the following configuration tasks will have run:

- Installation of Access Proxy files
- Registration of Access Proxy files
- Creation of local groups
- Configuration of Windows Management Instrumentation (WMI) for Access Proxy

Activating Access Proxy Files



Introduction

The second phase of the Access Proxy server deployment is the activation process.

Note The activation process differs, depending on whether the Access Proxy server is in a workgroup or joined to a domain.

Log On to Target Server

You must log on to the target server locally, either through the console or over Terminal Services. Verify that your account is a member of the Administrator Group.

Run Setup.exe

The GUI setup tool that you will use is located in the **i386** directory on the Live Communications Server 2005 with SP1 installation CD.

Activate Access Proxy

The GUI setup tool lists several different server roles. You should select the **Access Proxy** option and then click **Activate Proxy**.

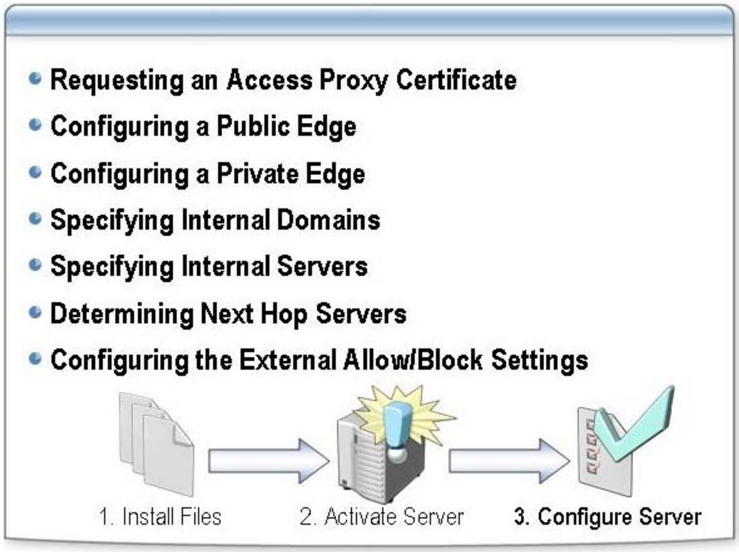
The wizard prompts you for a local service account (workgroup), whether to enable or disable archiving, and whether to start service after activation.

Tasks Completed (Workgroup)

If the Access Proxy server is in a workgroup, the installation carries out the following processes:

- Creates a local service account
- Sets archive options
- Configures service startup

Lesson: Configuring Access Proxy Settings



- Requesting an Access Proxy Certificate
- Configuring a Public Edge
- Configuring a Private Edge
- Specifying Internal Domains
- Specifying Internal Servers
- Determining Next Hop Servers
- Configuring the External Allow/Block Settings

Introduction

The last phase of deploying an Access Proxy server is the configuration phase. The location of an Access Proxy server determines the post-setup configuration process.

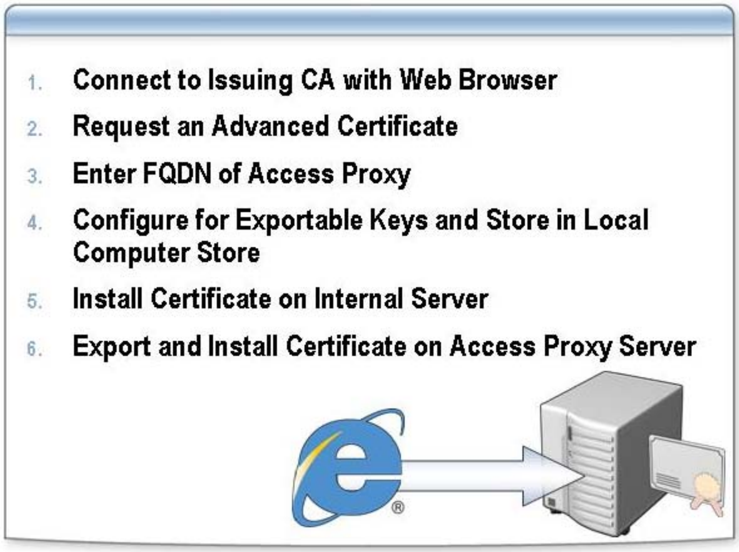
Important It is very important not to overlook this last step of the deployment, or issues may arise, such as services not starting correctly.

Lesson Objectives

After completing this lesson, you will be able to:

- Obtain an Access Proxy Certificate.
- Plan configuration of the Public Edge.
- Describe how to configure the Private Edge.
- Identify Internal Domains.
- Identify Internal Servers.
- Explain the Next Hop Internal Server.
- Configure the External Allow/Block Settings.
- Configure an Access Proxy server in a perimeter network.

Requesting an Access Proxy Certificate



1. Connect to Issuing CA with Web Browser
2. Request an Advanced Certificate
3. Enter FQDN of Access Proxy
4. Configure for Exportable Keys and Store in Local Computer Store
5. Install Certificate on Internal Server
6. Export and Install Certificate on Access Proxy Server

Introduction

To support MTLS encryption, you need to install one or more certificates on the Access Proxy server.

Windows 2003 Certificate Request

This example assumes you are obtaining a certificate from an internal Microsoft Windows 2003 certificate authority.

1. Log on to an internal LCS 2005 with SP1 server with administrative credentials.

Caution Do not log on to the Access Proxy at this time.

2. Select **Start**, and then click **Run**. Type **http://<Issuing CA Server Name>/certsrv**, and then click **OK**.
3. Select **Request a Certificate**.
4. Select **Advanced certificate request**.
5. Click **Create and submit a request to this CA**.
6. In the **Certificate Template** box, click the Web Server template that you duplicated as part of the enrollment procedure for the internal LCS server.
7. For the internal certificate, the Access Proxy will require a fully qualified domain name (FQDN) for the internal LCS servers to use when communicating with the Access Proxy. Type the FQDN in the **Identifying Information** box.
8. Accept the default value in **Key Options** and check that the **CSP** is set to **Microsoft RSA SChannel Cryptographic Provider**.
9. Select the **Mark keys as exportable** check box.
10. Select the **Store certificate in the local computer certificate store** check box, and then click the **Submit** button.
11. Select **Yes** if a **Potential Scripting Violation** message box appears.
12. Install the certificate on the internal server.

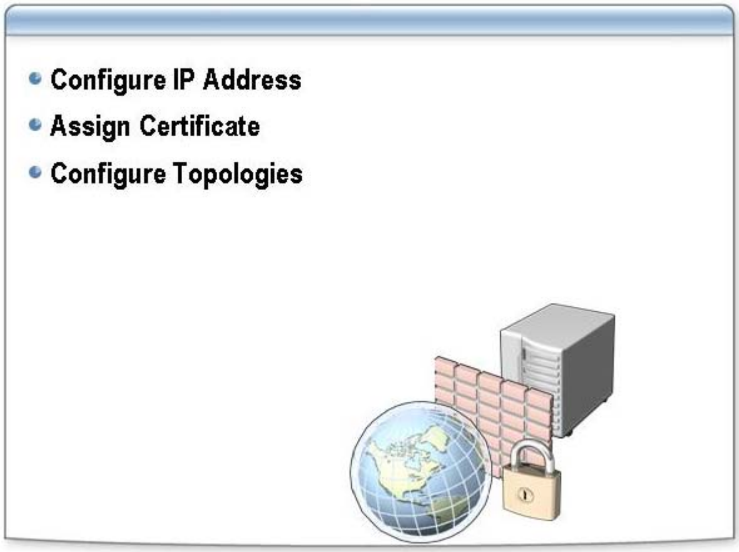
13. Export the certificate to the Access Proxy server.
14. Install the certificate on the Access Proxy server.

Note A second external certificate can be obtained for a Public Edge. The external certificate will be configured with the FQDN of the Public Edge.

Additional Resources

For more information about requesting a certificate from a third-party certificate authority, review “Live Communications Server 2005 Document: Configuring Certificates” on the Microsoft Web site, at: http://www.microsoft.com/downloads/details.aspx?FamilyId=779DEDAA-2687-4452-901E-719CE6EC4E5A&displaylang=en.

Configuring a Public Edge



- Configure IP Address
- Assign Certificate
- Configure Topologies

Introduction

A Public Edge is part of a defense-in-depth strategy that separates the Internet from your internal network. After you register your certificate(s), assign an IP address for your network interface card as well as a certificate.

Determine IP Address

You may need to work with your network infrastructure team to obtain an external IP address, which you then configure on the Access Proxy server.

Note The Public Edge must have a static IP address.

Complete the following steps to assign the IP address to the Public Edge:

1. Log on to the Access Proxy server with administrative permissions.
2. Access the Control Panel and review the properties of the Network Connections.
3. Right-click the network interface card that you want to configure, and then select **Properties**.
4. Click **Internet Protocol (TCP/IP)**, and then click **Properties**.
5. Review the **General** tab and click **Use the following IP address**.
6. Type the IP address you have designated for the Public Edge into the text box, and then click **OK**.

Assign Certificate

After you have configured the IP address, you can assign the certificate to the Public Edge:

1. Open the **Computer Management** console, and expand the **Services and Applications** node.
2. Right-click Microsoft Office Live Communications Server 2005, and then click **Properties**.
3. Click the **Public** tab.
4. Review the list of IP addresses and select the Public Edge IP address.

1. Click **Select Certificate**.
2. Select the certificate assigned to the Pubic Edge network interface card.
3. Click **OK**.

Important Before exiting from the Live Communications Server 2005 with SP1 properties, review the Configuring Topologies section below.

4. If you are not configuring topologies, click **Apply**.

Configuring Topologies

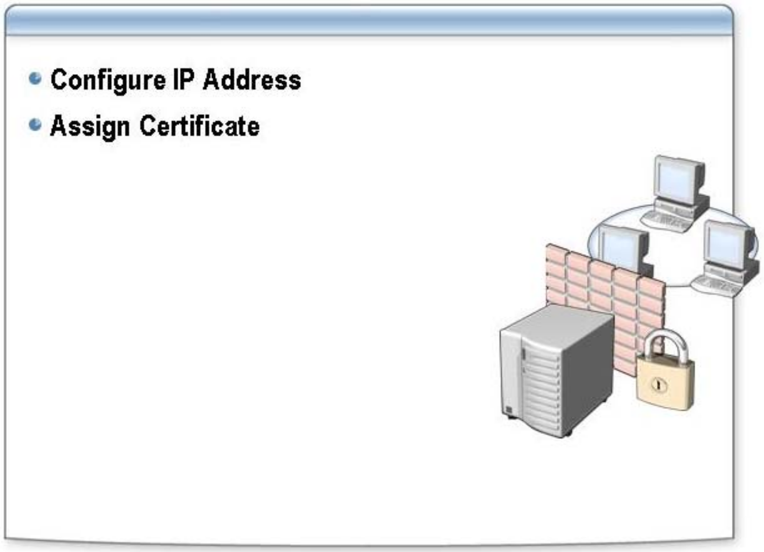
If you are planning to use multiple topologies, you can enable these features in the properties of the Live Communications Server 2005 on the Access Proxy server.

To enable Federation, select the **Allow Server connections for federation or branch office** check box.

To enable Remote Users, select the **Allow client connections for remote access** check box.

Important Remember to click **Apply** after selecting any check boxes.

Configuring a Private Edge



- Configure IP Address
- Assign Certificate

Introduction

A Private Edge supports the outbound SIP traffic from your corporate users. Once you have registered your certificate(s), assign an IP address for your network interface card as well as a certificate.

Note The IP address for the Private Edge must be static.

Determing IP Address

You may need to work with your network infrastructure team to obtain a static IP address which may be configured on the Access Proxy server.

Complete the following steps to assign the IP address to the Private Edge:

1. Log on to the Access Proxy server with administrative permissions.
2. Access the Control Panel and review the properties of the Network Connections.
3. Right-click the network interface card that you want to configure, and then select **Properties**.
4. Click **Internet Protocol (TCP/IP)**, and then click **Properties**.
5. Review the **General** tab and click **Use the following IP address**.
6. Type the IP address you have designated for the Private Edge into the text box, and then click **OK**.

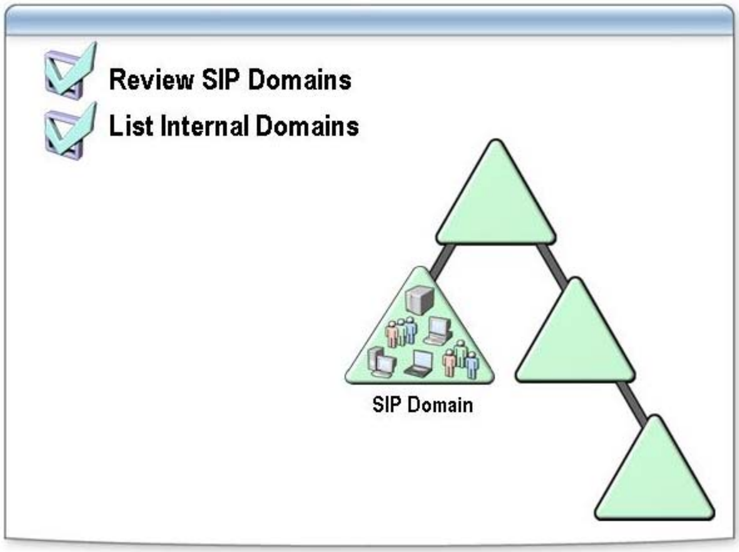
Assign Certificate

After you have configured the IP address, you can assign the certificate to the Private Edge:

1. Open the **Computer Management** console, and then expand the **Services and Applications** node.
2. Right-click **Microsoft Office Live Communications Server 2005**, and then click **Properties**.
3. Click the **Private** tab.
4. Review the list of IP addresses and select the Private Edge IP address.

5. Click **Select Certificate**.
6. Select the certificate assigned to the Private Edge network interface card.
7. Click **OK**.
8. Click **Apply**.

Specifying Internal Domains



☑ Review SIP Domains

☑ List Internal Domains

Introduction

Every Live Communications Server 2005 with SP1 deployment includes global settings. These global settings define the overall configuration of the system.

When you add an Access Proxy into the LCS 2005 with SP1 environment, you need to specify the internal SIP domain(s) manually. An Access Proxy server will not query Active Directory for the overall configuration information. It will not query Active Directory because it is designed to be joined to a workgroup instead of a domain.

Note If your Access Proxy is joined into a domain, it still will not query Active Directory information.

You can review the list of internal SIP domains(s) in the global settings.

Review SIP Domains

A Live Communications Server 2005 with SP1 infrastructure relies on your Active Directory configuration. You might have multiple LCS 2005 with SP1 domains in your Active Directory forest.

If you are not aware of all your internal SIP domains that include an installation of LCS 2005 with SP1, you may obtain the list by completing these steps:

1. Log on to a Live Communications Server on your internal network.

Note Do not carry out this procedure on the Access Proxy server.

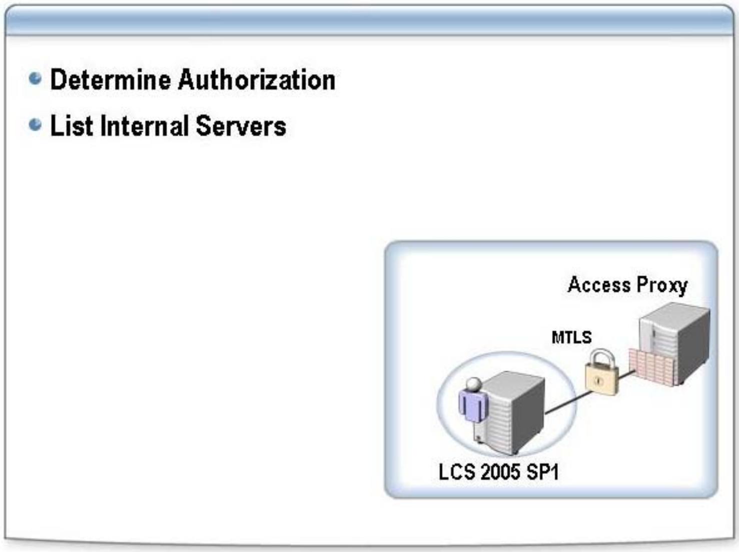
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Live Communications Server 2005**.
3. Right-click the **Forest** node, and then select **Properties**.
4. Review the **Internal** tab for the list of internal SIP domains.
5. Click **Cancel**.

List Internal Domains

If you have multiple internal domains, you must specify each one by completing the following procedures:

1. Log on to the Access Proxy server with administrative permissions.
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Computer Management**.
3. In the **Computer Management** console, expand the **Services and Applications** node.
4. Right-click **Microsoft Office Live Communications Server 2005**, and then click **Properties**.
5. Click the **Internal** tab.
6. Click **Add Domain** in the **Internal SIP domains supported by Live Communications servers in your organization** section.
7. Click **OK** to close the **Add SIP Domain** dialog box.
8. Repeat the **Add Domain** process until you have added each SIP domain.
9. Click **OK** to close the **Microsoft Office Live Communications Server 2005 Properties** dialog box.

Specifying Internal Servers



- Determine Authorization
- List Internal Servers

Introduction

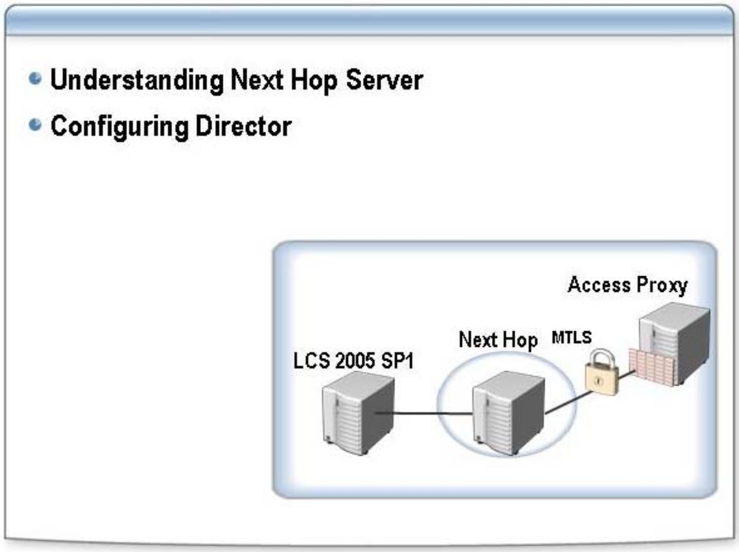
By design, an Access Proxy server enforces security because it is located in a perimeter network and maintains a list of internal servers authorized to communicate with it. You can specify which internal servers can connect directly with an Access Proxy server.

List Internal Servers

If you do have multiple internal servers, you need to specify each one by completing the following procedures:

1. Log on to the Access Proxy server with administrative permissions.
2. Open the **Computer Management** console, and then expand the **Services and Applications** node.
3. Right-click **Microsoft Office Live Communications Server 2005**, and then select **Properties**.
4. Click the **Internal** tab.
5. Click **Add Server** in the **Internal servers authorized to connect to this Access Proxy server** section.
6. Enter the **Server name** in FQDN form for the computer that is allowed to communicate with this Access Proxy server.
7. Click **OK** on the **Add Live Communications Server** dialog box.
8. Repeat the **Add Server** process until each designated internal SIP server is added.
9. Click **OK** to close the **Microsoft Office Live Communications Server 2005 Properties** dialog box.

Determining Next Hop Servers



- Understanding Next Hop Server
- Configuring Director

Introduction

When an Access Proxy server accepts incoming SIP traffic, this traffic must be delivered to the internal network. Instead of listing each internal LCS 2005 with SP1 server in the internal SIP server list, you can designate a Next Hop server.

Next Hop Server

A Next Hop server can be an internal LCS 2005 with SP1 server. Alternatively, the Next Hop server could host the new Director server role, introduced with Live Communications Server 2005 with SP1.

Director Server

A Director server can act as the second line of defense when deploying Federation or Remote Access to LCS 2005 with SP1. The Director server sits behind the corporate network perimeter between the Access Proxy and the pool server in the internal network. Directors are part of the corporate Active Directory infrastructure.

Important It is recommended that you implement a Director server to provide an extra layer of security.

If you decide to implement a Director, the Director provides authentication against Active Directory for traffic forwarded from the Access Proxy server.

Note A Director does not host users - its only function is for authentication purposes.

Configure Next Hop Server

To configure the Next Hop server, carry out the following procedure:

1. Log on to the Access Proxy server with administrative permissions.
2. Open the **Computer Management** console, and then expand **Services and Applications**.
3. Right-click **Microsoft Office Live Communications Server 2005**, and then click **Properties**.
4. Click the **Internal** tab.

5. Review the **Next hop network address** and then type either:

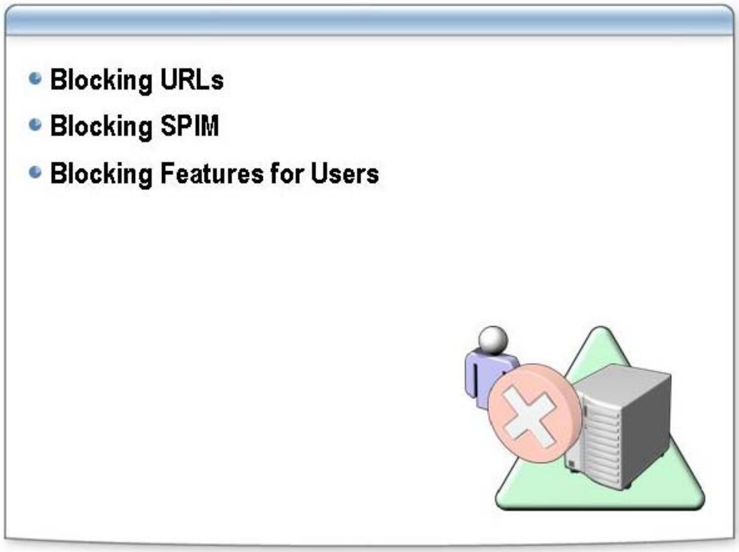
    a. The FQDN of the Director server.

    b. The FQDN of an internal LCS 2005 with SP1 server or Enterprise pool.

2. In the **Port** box, type **5061**.

3. Click **OK** to close the **Microsoft Office Live Communications Server 2005 Properties** dialog box.

Configure the External Allow/Block Settings



- Blocking URLs
- Blocking SPIM
- Blocking Features for Users

Introduction

Many security enhancements are available for an LCS 2005 with SP1 Access Proxy server. Security enhancements include:

- Blocking attacks
- Blocking unsolicited messages (SPIM)
- Blocking features at a user level

Blocking Attacks

The IM URL Filter Application (IMFilter.am) utility blocks URLs from being sent directly to a Microsoft Office Communicator or Windows Messaging client. You can install this utility on the following servers:

- LCS 2005 with SP1, Standard Edition
- LCS 2005 with SP1, Enterprise Edition
- Director
- Access Proxy

Note There is an improved version of the Intelligent Instant Message Filter available for download from the Microsoft.com Web site, at: http://www.microsoft.com/downloads/details.aspx?familyid=0ED13372-F3D2-40F0-BA5D-C880359A40F5.

Users can still send a URL that is intended for business use by including an underscore symbol (_) before the URL link. If an underscore and URL appears in an instant messaging conversation, the receiving user must:

- Start a browser session
- Copy the URL link
- Paste URL link into browser window
- Remove the underscore character

Important By default, the IM URL Filter utility is enabled. You are recommended to accept the default settings.

Blocking SPIM

You can control SPIM by filtering SPIM based on rules you define in a LCS 2005 with SP1 deployment. The SPIM filters can differ between the following topologies:

- Federation
- Public IM Connectivity

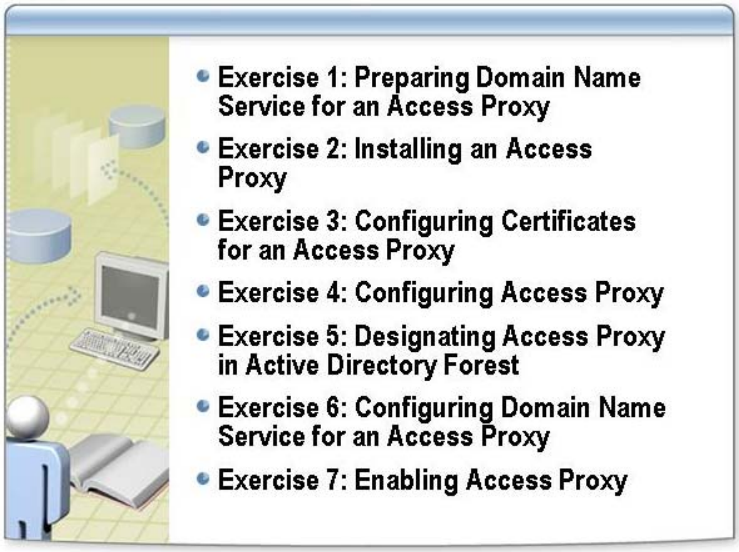
The Access Proxy server reviews the message filter settings and then accepts or rejects the incoming messages based on user verification of the sender.

Blocking Features for Users

There may be a requirement for you to block a user or group of users from using the features of LCS 2005 with SP1. To block users from participating in Federation, Public IM Connectivity, or Remote User access, perform the following steps:

1. Log on to an internal LCS 2005 with SP1 server.
2. Expand the **Forest** node, expand the **Domain** node, and then expand the domain that contains the users you want to configure.
3. Expand the **Live Communications servers and pools** node.
4. On either the Enterprise Pool or the LCS server node, select the **Users** container.
5. Right-click the user(s) you want to configure, and then click **Configure Users**. The **Configure Live Communications Server Users Wizard** appears.
6. Check **Configure Federation**, **Configure Remote Access** or **Configure Public IM Connectivity** as required.
7. For each selected option, select **Block Users**.
8. Click **Next**.
9. Check that the operation completes successfully, then click **Finish**.

Lab 6: Deploying an Access Proxy in LCS 2005 SP1



- Exercise 1: Preparing Domain Name Service for an Access Proxy
- Exercise 2: Installing an Access Proxy
- Exercise 3: Configuring Certificates for an Access Proxy
- Exercise 4: Configuring Access Proxy
- Exercise 5: Designating Access Proxy in Active Directory Forest
- Exercise 6: Configuring Domain Name Service for an Access Proxy
- Exercise 7: Enabling Access Proxy

Objectives

After you complete this lab, you will be able to:

- Prepare a Domain Name Service name for an Access Proxy server.
- Install an Access Proxy server for a LCS 2005 SP1 infrastructure.
- Configure certificate(s) for an Access Proxy server deployment.
- Configure the Public Edge, Private Edge, Next Hop and Topologies of an Access Proxy server.
- Designate the Access Proxy server in the Active Directory Forest.
- Configure DNS record for an Access Proxy server deployment.
- Enable the Access Proxy services.

Estimated time to complete this lab: 60 minutes

Important: At the end of this lab, leave all the VPC images running. DO NOT close the VPC images down, as the changes you make in this lab are required for Lab 7.

Introduction

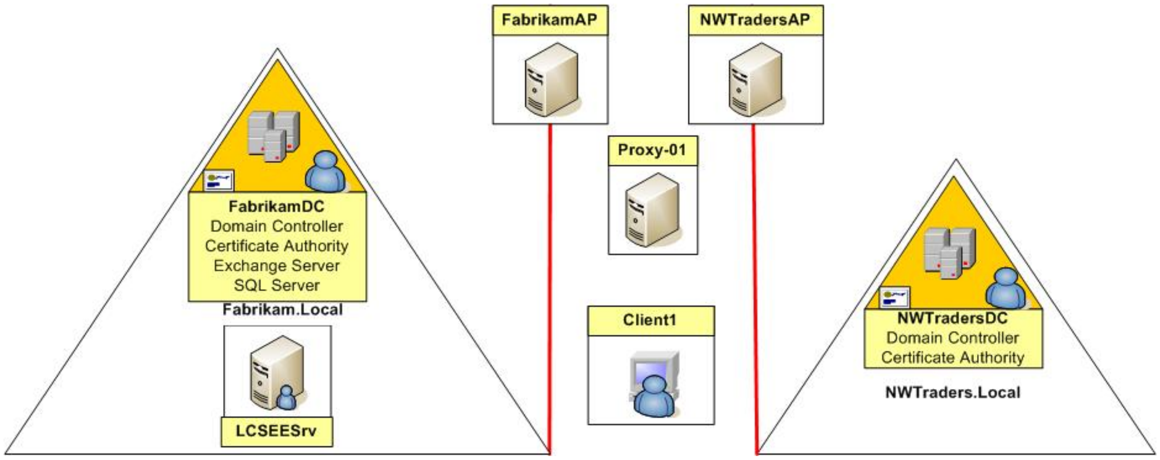
Fabrikam and NWTraders have now implemented LCS 2005 with SP1, and are now want to extend the reach of their networks to remote users. They also want to enable Federation with selected partners. To implement these facilities, Matt Dawson and Holly Holt both need to set up Access Proxies for their organizations.

In this lab, you will prepare the necessary Domain Name Service (DNS) records for an installation of an Access Proxy server. You will also install and activate the Access Proxy server. After installation is completed, you will configure the Access Proxy server.

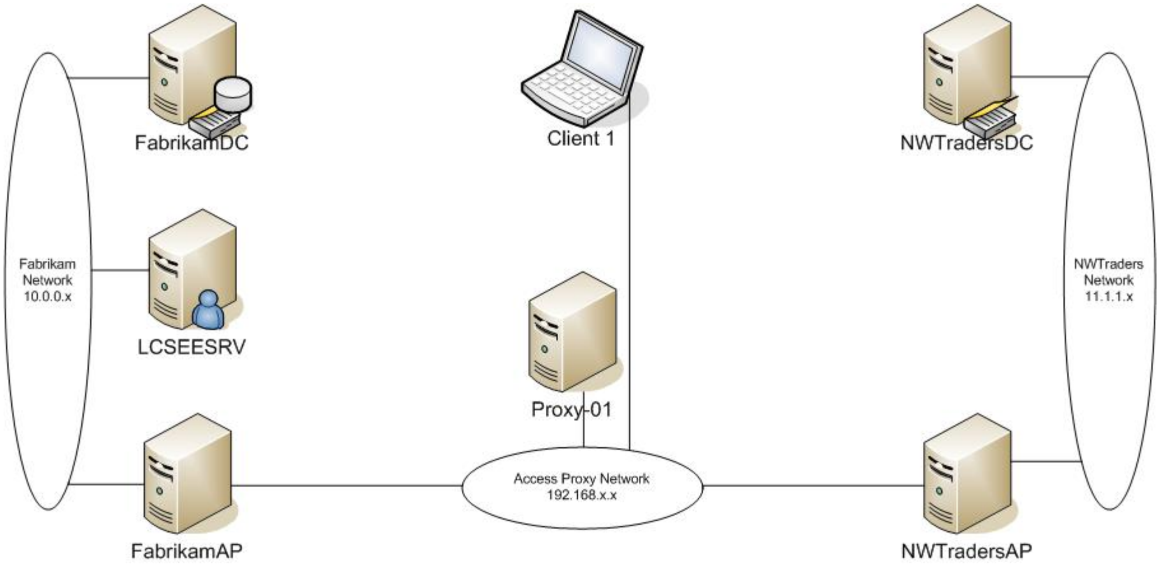
An Access Proxy server should only be deployed after a Standard or Enterprise Edition LCS 2005 with SP1 infrastructure has been implemented in your corporate network environment.

Network Topology

The labs in this course use virtual machines. To configure the virtual machines to be usable in a lab environment, the network topology has been substantially modified from a typical network configuration. The lab configuration combines many server roles in non-standard ways that are not recommended and are generally not viable in a production network. The network topology used in these labs is shown in the following figure.



Physical Network Topology



Virtual PC Image to Computer NetBIOS Name Mappings

The following table shows the mapping between the VPC images and the computer NetBIOS names for this lab. Please ensure you use the correct VPC image from the VPC console to start the lab.

VPC Configuration Name	Computer NetBIOS Name
7034A-FabrikamDC-B	FabrikamDC
7034A-FabrikamAP-B	FabrikamAP
7034A-LCSEESRV-B	LCSEESRV
7034A-NWTradersDC-B	NWTradersDC
7034A-NWTradersAP-B	NWTradersAP
7034A-Proxy01-B	Proxy-01

Important: You should start all these virtual PC images prior to commencing the labs in this module.

On 7034A-FabrikamDC-B and 7034A-NWTradersDC-B, a Service Control Manager message box may appear, with the following message: At least one service or driver failed during system startup. Use Event Viewer to examine the event log for details. If this message appears, click OK, and continue. The message refers to the Kerberos Key Distribution Center service. However, this service appears to start properly.

On 7034A-LCSEESRV-B, the Live Communications Server service may fail to start if FabrikamDC has not completely booted before starting LCSEESRV. Before you start the lab, check that the Live Communications Server service on LCSEESRV is running.

.

Exercise 1
Prepare Domain Name Service Records to Install Access Proxy

Scenario

Before Matt Dawson and Holly Holt can deploy their respective Access Proxies, they need to configure DNS information on the Access Proxy servers.

Description

In this exercise, you will prepare the DNS name of the Fabrikam and NWTraders Access Proxy servers. This is the first procedure you need to complete in order to prepare your environment for an Access Proxy deployment.

Tasks	Detailed Steps
⚠ **Important:** Perform Exercise 1 on the **7034A-FabrikamAP-B** virtual machine and Exercise 2 on **7034A-NWTradersAP-B** virtual machine.	
1. Prepare the DNS name of the Fabrikam Access Proxy server.	**a.** Log on to **7034A-FabrikamAP-B** as **Administrator** with a password of **pass@word1**. **b.** Click **Start**. **c.** Right-click **My Computer**. **d.** Click **Properties**. **e.** Click **Computer Name**. **f.** On the **System Properties** dialog box, click **Change**. **g.** On the **Computer Name Changes** dialog box, click **More**. **h.** In the **Primary DNS suffix of this computer** box, type **Fabrikam.local**. **i.** On the **DNS Suffix and NetBIOS Computer Name** dialog box, click **OK**. **j.** On the **Computer Name Changes** dialog box, click **OK**. **k.** On the **You must Restart this computer for the changes to take effect** dialog box, click **OK**. **l.** On the **System Properties** dialog box, click **OK**. **m.** On the **System Settings Change** dialog box, click **Yes** to restart the server.
2. Prepare the DNS name of the NWTraders Access Proxy server.	**a.** Log on to **7034A-NWTradersAP-B** as **Administrator** with a password of **pass@word1**. **b.** Click **Start**. **c.** Right-click **My Computer**. **d.** Click **Properties**. **e.** Click **Computer Name**. **f.** On the **System Properties** dialog box, click **Change**.

	g. On the **Computer Name Changes** dialog box, click **More**. **h.** In the **Primary DNS suffix of this computer** box, type **NWTraders.local**. **i.** On the **DNS Suffix and NetBIOS Computer Name** dialog box, click **OK**. **j.** On the **Computer Name Changes** dialog box, click **OK**. **k.** On the **You must restart this computer for the changes to take effect** dialog box, click **OK**. **l.** On the **System Properties** dialog box, click **OK**. **m.** On the **System Settings Change** dialog box, click **Yes** to restart the server.

Exercise 2
Install an Access Proxy server for a LCS 2005 SP1 infrastructure

Scenario

After Matt and Holly have configured DNS entries for the Access Proxies, they can proceed to install LCS 2005 with SP1. Fabrikam will install LCS 2005 with SP1 from the Enterprise Edition files, whereas NWTraders will install the same role from the Standard Edition files.

Description

In this exercise, you will create an Access Proxy server role on the FabrikamAP and NWTradersAP servers.

Tasks	Detailed Steps
⚠ **Important:** Perform this exercise on the **7034A-FabrikamAP-B** virtual machine.	
1. Install the installation files on the FabrikamAP Access Proxy server.	**a.** Log on to **7034A-FabrikamAP-B** as **Administrator** with a password of **pass@word1**. **b.** Click **Start**, and then click **My Computer**. **c.** Browse to **E:\Demo Files\LCS2005SP1\EE\Setup\I386**. **d.** Double-click **Setup.exe**. **e.** On the **Microsoft Office Live Communications Server 2005 with SP1 Enterprise Edition Deployment Tool** dialog box, click **Access Proxy**. **f.** Click **Install Files for Access Proxy**. **g.** On the **Welcome to the Setup Wizard for Microsoft Office Live Communications Server 2005** dialog box, click **Next**. **h.** On the **License Agreement** page, click **I accept the terms in the license agreement**, and then click **Next**. **i.** On the **Customer Information** page, accept the default entries, and then click **Next**. **j.** On the **Choose Destination Location** dialog box, accept the default entries, and then click **Next**. **k.** On the **Ready to Install the Program** page, click **Install**. **l.** On the **Setup Wizard Completed** page, click **Finish**. **m.** On the **Server Activation** dialog box, click **Yes**. **n.** On the **Welcome to the Activate Access Proxy Wizard**, click **Next**. **o.** On the **Select Service Account** dialog box, accept the default account information, and type **pass@word1 for the password field.**. **p.** Confirm by typing **pass@word1 in the confirm password field**, and then click **Next**. **q.** On the **Start Service Option** page, notice the **Start the service after activation** check box is unavailable, click **Next**. **r.** On the **Ready to Activate Access Proxy**, click **Next**.

s. On the **Activate Access Proxy Wizard has completed** page, click **View Log**.

t. If the **Information Bar** dialog box appears, click **OK**, click **Click here for options**, and then click **Allow Blocked Content**.

u. If a **Security Warning** dialog box appears, click **Yes**.

v. On the **Action** column, expand the **Execute Action** to review the log information.

The Execution Result column will list the results of each installation step.

w. Click **File**, and then click **Close** to exit the log information.

x. On the **Activate Access Proxy Wizard has completed** page, click **Finish**.

y. On the **Microsoft Office Live Communications Server 2005 with SP1 Enterprise Edition Deployment Tool** page, click **Close**.

z. On the **Microsoft Office Live Communications Server 2005 with SP1 Enterprise Edition Deployment Tool** page, click **Exit**.

The installation of the files and activation has been completed. To successfully start the Access Proxy server, you must configure the server.

Important: Perform this exercise on the **7034A-NWTradersAP-B** virtual machine.

2. Install the installation files on the NWTraders Access Proxy server.

a. Log on to **7034A-NWTradersAP-B** as **Administrator** with a password of **pass@word1**.

b. Click **Start**, and then click **My Computer**.

c. Browse to **E:\Demo Files\LCS2005SP1\SE\Setup\I386**.

d. Double-click **Setup.exe**.

e. On the **Microsoft Office Live Communications Server 2005 with SP1 Standard Edition Deployment Tool** dialog box, click **Access Proxy**.

f. Click **Install Files for Access Proxy**.

g. On the **Welcome to the Setup Wizard for Microsoft Office Live Communications Server 2005** dialog box, click **Next**.

h. On the **License Agreement** page, click **I accept the terms in the license agreement**, and then click **Next**.

i. On the **Customer Information** page, accept the default settings, and then click **Next**.

j. On the **Choose Destination Location** dialog box, accept the default settings, and then click **Next**.

k. On the **Ready to Install the Program** page, click **Install**.

l. On the **Setup Wizard Completed** page, click **Finish**.

m. On the **Server Activation** dialog box, click **Yes**.

n. On the **Welcome to the Activate Access Proxy Wizard**, click **Next**.

	o. On the **Select Service Account** dialog box, accept the default account information, and type **pass@word1 for the password field.**. **p.** Confirm by typing **pass@word1 for the confirm password field.** **q.** On the **Start Service Option** page, notice the **Start the service after activation** check box is unavailable, click **Next**. **r.** On the **Ready to Activate Access Proxy**, click **Next**. **s.** On the **Activate Access Proxy Wizard has completed** page, click **View Log**. **t.** If the **Information Bar** dialog box appears, click **OK**, click **Click here for options**, and then click **Allow Blocked Content**. **u.** If a **Security Warning** appears, click **Yes**. **v.** On the **Action** column, expand the **Execute Action** to review the log information. *The Execution Result column will list the results of each installation step.* **w.** Click **File**, and then click **Close** to exit the log information.. **x.** On the **Activate Access Proxy Wizard has completed** page, click **Finish**. **y.** On the **Microsoft Office Live Communications Server 2005 with SP1 Standard Edition Deployment Tool** page, click **Close**. **z.** On the **Microsoft Office Live Communications Server 2005 with SP1 Standard Edition Deployment Tool** page, click **Exit**. *The installation of the files and activation has been completed. To successfully start the Access Proxy server, you must configure the server.*

Exercise 3
Configure certificate(s) for an Access Proxy server deployment

Scenario

Matt and Holly have successfully installed LCS 2005 with SP1 Access Proxies. They now need to configure certificates on both Access Proxies for encrypted communications with other LCS 2005 servers. This process requires them to request and install a certificate chain into the Trusted Root certificates store, and to request a certificate that matches the name of the Access Proxy.

Description

In this exercise, you will install a certificate chain on the server and then request a certificate for both Fabrikam and NWTraders.

Tasks	Detailed Steps
⚠ **Important:** Perform this exercise on the **7034A-FabrikamAP-B** virtual machine.	
1. Install certificate chain on FabrikamAP.	**a.** Log on to **7034A-FabrikamAP-B** as **Administrator** with a password of **pass@word1**. **b.** On the taskbar, click **Start**, and then click **Run**. **c.** In the **Open** box, type **http://FabrikamDC/certsrv**, and then click **OK**. **d.** On the **Microsoft Certificate Services –SECA Welcome** page, under **Select a task**, click **Download a CA certificate, certificate chain, or CRL**. **e.** On the **Download a CA Certificate, Certificate Chain, or CRL** page, click **Download CA certificate chain**. **f.** On the **File Download** dialog box, click **Save**. **g.** On the **Save As** dialog box, in the **File name** box, type **C:\SE_Chain.p7b**, and then click **Save**. **h.** Close the Download complete dialog box. **i.** Close Internet Explorer®. **j.** On the taskbar, click **Start**, and then click **Run**. **k.** In the **Open** box, type **mmc**, and then click **OK**. **l.** On the **Microsoft Management Console**, click **File**. **m.** Click **Add/Remove Snap-in**. **n.** On the **Add/Remove Snap-in** page, click **Add**. **o.** In the **Available Standalone Snap-ins** list, click **Certificates**, and then click **Add**. **p.** Click **Computer account**, and then click **Next**. **q.** On the **Select Computer** dialog box, verify that **Local computer** is selected, and then click **Finish**. **r.** On the **Add Standalone Snap-in** dialog box, click **Close**. **s.** On the **Add/Remove Snap-in** page, click **OK**.

	t. On the **Certificates** console, expand **Certificates (Local Computer)**. **u.** Expand **Trusted Root Certification Authorities**. **v.** Right-click **Certificates**. **w.** Point to **All Tasks**, and then click **Import**. **x.** On the **Welcome to the Certificate Import Wizard** page, click **Next**. **y.** On the **File to Import** page, click **Browse**. **z.** In the **Open** box, type **C:\EE_Chain.p7b**, and click **Open**. **aa.** On the **File to Import** page, click **Next**. **bb.** On the **Certificate Store** page, under **Place all certificates in the following store**, ensure the **Trusted Root Certification Authorities** check box is selected, and then click **Next**. **cc.** On the **Completing the Certificate Import Wizard** page, click **Finish**. **dd.** On the **Certificate Import Wizard** message box, click **OK** to acknowledge that **The import was successful**. **ee.** Close the management console window without saving changes.
2. Request the Certificate on FabrikamAP.	**a.** On the **7034A-FabrikamAP-B** server taskbar, click **Start**, and then click **Run**. **b.** In the **Open** box, type **http://FabrikamDC/certsrv**, and then click **OK**. **c.** On the **Select a task** page, click **Request a certificate**. **d.** On the **Request a Certificate** page, click **advanced certificate request**. **e.** On the **Advanced Certificate Request**, click **Create and submit a request to this CA**. **f.** On the **Certificate Template**, click the **LCS2005EE** template. **g.** Under the **Identifying Information For Offline Template**, in the **Name** box, type **FabrikamAP.Fabrikam.local**. *The DNS name of the Access Proxy server was completed in Exercise 1.* **h.** Select the **Mark keys as exportable** check box. **i.** On the **Key Options** page, select the **Store certificate in the local computer certificate store** check box, and then click **Submit**. **j.** On the **Potential Scripting Violation** dialog box, click **Yes**.
3. Install the certificate on the FabrikamAP server.	**a.** On the **Certificate Issued** page, click **Install this certificate**. **b.** If you receive a **Potential Scripting Violation** dialog box, click **Yes**. **c.** Close Internet Explorer.

⚠ **Important:** Perform this exercise on the **7034A-NWTradersAP-B** virtual machine.

1. Install certificate chain on NWTradersAP.	**a.** Log on to **7034A-NWTradersAP-B** as **Administrator** with a password of **pass@word1**. **b.** On the taskbar, click **Start**, and then click **Run**. **c.** In the **Open** box, type **http://NWTradersDC/certsrv**, and then click **OK**. **d.** For the **Microsoft Certificate Services – SECA Welcome** page, under **Select a task** options, click **Download a CA certificate, certificate chain, or CRL**. **e.** On the **Download a CA certificate, certificate chain, or CRL** page, click **Download CA certificate chain**. **f.** On the **File Download** dialog box, click **Save**. **g.** On the **Save As** dialog box, in the **File name** box, type **C:\SE_Chain.p7b**, and then click **Save**. **h.** Close the Download complete dialog box. **i.** Close the Internet Explorer window.
2. Install the certificate chain on the NWTradersAP Access Proxy.	**a.** On the taskbar, click **Start**, and then click **Run**. **b.** In the **Open** box, type **mmc**, and then click **OK**. **c.** On the **Microsoft Management Console**, click **File**. **d.** Click **Add/Remove Snap-in**. **e.** On the **Add/Remove Snap-in** page, click **Add**. **f.** In the **Available Standalone Snap-ins** list, click **Certificates**, and then click **Add**. **g.** On the **Certificates snap-in** dialog box, click **Computer account**, and then click **Next**. **h.** On the **Select Computer** dialog box, verify that **Local computer** is selected, and then click **Finish**. **i.** On the **Add Standalone Snap-in** dialog box, click **Close**. **j.** On the **Add/Remove Snap-in** page, click **OK**. **k.** On the **Certificates** console, expand **Certificates (Local Computer)**. **l.** Expand **Trusted Root Certification Authorities**. **m.** Right-click **Certificates**. **n.** Point to **All Tasks**, and then click **Import**. **o.** On the **Welcome to the Certificate Import Wizard**, click **Next**. **p.** On the **File to Import** page, click **Browse**. **q.** On the **Open** page, type **C:\SE_Chain.p7b**, and then click **Open**. **r.** On the **File to Import** page, click **Next**. **s.** On the **Certificate Store** page, under **Place all certificates in the following store**, ensure the **Trusted Root Certification Authorities** check box is selected, and then click **Next**. **t.** On the **Completing the Certificate Import Wizard** page, click

	Finish. **u.** On the **Certificate Import Wizard** message box, click **OK** to acknowledge that **The import was successful**.
3. Request the Certificate on NWTradersAP.	**a.** Remain logged on to the **7034A-NWTradersAP-B** server to complete this task. **b.** On the taskbar, click **Start**, and then click **Run**. **c.** In the **Open** box, type **http://NWTradersDC/certsrv**, and then click **OK**. **d.** On the **Welcome** page, under **Select a task**, click **Request a certificate**. **e.** On the **Request a Certificate** page, click **Advanced certificate request**. **f.** On the **Advanced Certificate Request**, click **Create and submit a request to this CA**. **g.** On the **Certificate Template**, click the **LCS2005SE** template. **h.** Under the **Identifying Information for Offline Template**, in the **Name** box, type **NWTradersAP.NWTraders.local**. The DNS name of the Access Proxy server was completed in Exercise 1. **i.** Select the **Mark keys as exportable** check box. **j.** On the **Key Options** page, select the **Store certificate in the local computer certificate store** check box, and then click **Submit**. **k.** On the **Potential Scripting Violation** dialog box, click **Yes**.
4. Install the certificate on the NWTradersAP server.	**a.** On the **Certificate Issued** page, click **Install this certificate**. **b.** If you receive a **Potential Scripting Violation** dialog box, click **Yes**. **c.** Close Internet Explorer.

Exercise 4

Configure the Public Edge, Private Edge, Next Hop Server and Enable Topologies for an Access Proxy Server

Scenario

After requesting certificates, both Matt and Holly need to secure their respective Public Edge and Private Edges. They also need to enter a Next Hop server that acts as a secure communication end point for the Access Proxy server.

Description

After the Public Edge and Private Edge are configured, you will need to set up the Access Proxy server to forward incoming SIP traffic to the Next Hop server. You will also enable Public IM Connectivity and Federation, and update LCS 2005 SP1 global settings.

Tasks	Detailed Steps
⚠ **Important:** Perform this exercise on the **7034A-FabrikamAP-B** virtual machine.	
1. Configure Public Edge.	**a.** Log on to **7034A-FabrikamAP-B** as **Administrator**. **b.** Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Computer Management**. **c.** On the **Computer Management** console, expand **Services and Applications**. **d.** Right-click **Microsoft Office Live Communications Server 2005**, and then click **Properties**. **e.** On the **Microsoft Office Live Communications Server 2005 Properties** page, on the **Public** tab, in the **Network address** list, click **192.168.0.10**, and then click **Add**. **f.** On the **Add Listening Port** dialog box, verify that both check boxes are cleared, and then click **OK**. **g.** On the **Public** tab, click **Select Certificate**. **h.** On the **Select Certificate** dialog box, click the **FabrikamAP.Fabrikam.local** certificate, and then click **OK**.
2. Configure the Private Edge.	**a.** On the **Microsoft Office Live Communications Server 2005 Properties** page, click the **Private** tab. **b.** In the **Network Address** list, click **10.0.0.50**, and then click **Select Certificate**. **c.** On the **Select Certificate** dialog box, click the **FabrikamAP.Fabrikam.local** certificate, and then click **OK**.
3. Configure Internal SIP Domain List and Next Hop Server.	**a.** On the **Internal** tab, click **Add Domain**. **b.** On the **Add SIP domain** dialog box, in the **SIP domain** box, type **Fabrikam.local**, and then click **OK**. **c.** On the **Internal Servers Authorized to Connect to this Access Proxy**

	server, click **Add Server**. **d.** On the **Add Live Communications Server** dialog box, type **EEPool1.Fabrikam.local**, and then click **OK**. **e.** On the **Internal** tab, in the **Next hop network address** box, type **EEPool1.Fabrikam.local**. **f.** In the **Port** box, leave the default value of **5061**. **g.** On the **Microsoft Office Live Communications Server 2005 Properties**, click **OK**.
4. Configure the Host File to resolve the IP address of the Enterprise Edition pool	**a.** On the taskbar, click **Start**, and then click **Run**. **b.** In the **Open** box, type **%windir%\system32\drivers\etc\**, and then click **OK**. **c.** In the **Etc** folder, open the **hosts** file in Notepad. **d.** On the line under the localhost entry, add the following entry on one line: **10.0.0.10 EEPool1.Fabrikam.local** **e.** Add the following entry on the next line: **192.168.0.20 NWTradersAP.NWTraders.local** **f.** Save the **hosts** file and exit Notepad.
5. Update Global Settings.	**a.** Log on to **7034A-FabrikamDC-B** as **Administrator** with a password of **pass@word1**. **b.** If you are prompted to log on to Windows Messenger, click **Cancel**, and close Windows Messenger. **c.** On the taskbar, click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Live Communications Server 2005**. **d.** In the Microsoft Office Live Communications Server 2005 console, right-click the **Forest** node, and then click **Properties**. **e.** On the **Live Communications Server Global Properties** dialog box, on the **Genearl** tab, click **Add**. **f.** On the **Add SIP domain** dialog box, in the **SIP domain** box, type **FabrikamAP.Fabrikam.local**, and then click **OK**. **g.** On the **Microsoft Office Live Communications Server 2005**, click **File** and then **Exit**.
⚠ **Important:** Perform this exercise on the **7034A-NWTradersAP-B** virtual machine.	
1. Configure Public Edge.	**a.** Log on to **7034A-NWTradersAP-B** as **Administrator** with a password of **pass@word1**. **b.** Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Computer Management**. **c.** On the **Computer Management** console, expand **Services and Applications**. **d.** Right-click **Microsoft Office Live Communications Server 2005**, and then click **Properties**. **e.** On the **Microsoft Office Live Communications Server 2005 Properties** page, on the **Public** tab, in the **Network Address** list, click **192.168.0.20**, and then click **Add**.

	f. On the **Add Listening Port** dialog box, verify that both check boxes are cleared, and then click **OK**. **g.** On the **Public** tab, click **Select Certificate**. **h.** On the **Select Certificate** dialog box, click the **NWTradersAP.NWTraders.local** certificate, and then click **OK**.
2. Configure the Private Edge.	**a.** On the **Microsoft Office Live Communications Server 2005 Properties** page, click the **Private** tab. **b.** On the **Private** tab, in the **Network Address** list, click **11.1.1.30**, and then click **Select Certificate**. **c.** On the **Select Certificate** dialog box, click the **NWTradersAP.NWTraders.local** certificate, and then click **OK**.
3. Configure Internal SIP Domain List and Next Hop Server..	**a.** On the **Internal** tab, click **Add Domain**. **b.** On the **Add SIP domain** dialog box, in the **SIP domain** box, type **NWTraders.local**, and then click **OK**. **c.** On the **Internal** tab, click **Add Server**. **d.** On the **Add Live Communications Server** dialog box, in the **Server name** box, type **NWTradersDC.NWTraders.local**, and then click **OK**. **e.** On the **Internal** tab, in the **Next hop network address** box, type **NWTradersDC.NWTraders.local**. **f.** In the **Port** box, leave the default value of **5061**. **g.** On the **Microsoft Office Live Communications Server 2005 Properties**, click **OK**.
4. Configure Host File.	**a.** On the taskbar, click **Start**, and then click **Run**. **b.** In the **Open** box, type **%windir%\system32\drivers\etc\**, and then click **OK**. **c.** In the **Etc** folder, edit the **hosts** file with Notepad. **d.** Under the localhost entry, add the following entries on separate lines: **11.1.1.10 NWTradersDC.NWTraders.local** **192.168.0.10 FabrikamAP.Fabrikam.local** **e.** Save the host file. **f.** Exit Notepad.
5. Update Global Settings.	**a.** Log on to **7034A-NWTradersDC-B** as **Administrator** with a password of **pass@word1**. **b.** If you are prompted to log on to Windows Messenger, click **Cancel**, and close Windows Messenger. **c.** On the taskbar, click **Start**, point to **Administrative Tools**, and then click **Live Communications Server 2005**. **d.** In the **Microsoft Office Live Communications Server 2005** console, right-click the **Forest** node, and then click **Properties**. **e.** On the **Live Communications Server Global Properties** page, click the **Access Proxy** tab, and then click **Add**. **f.** On the **Add Access Proxy** dialog box, type **NWTradersAP.NWTraders.local**, and then click **OK**.

	g. On the **Live Communications Server Global Properties** page, click **OK**, then close the Microsoft Office Live Communications Server 2005 console.

Exercise 5
Add the DNS record for the Access Proxy Server

Scenario

Matt and Holly must now add the correct DNS records for the Access Proxy server into their internal DNS. This internal DNS setting points to the IP address on the private edge of each Access Proxy. They would also configure external DNS settings that point to the IP address on the Public Edge.

Description

You will need to configure an “A” record for the FabrikamAP and NWTradersAP Access Proxy servers on your internal and external DNS servers. If DNS is not configured properly, your Access Proxy deployment will not function properly.

In this lab environment, the external routing and DNS addressing is handled by Proxy-01.

Tasks	Detailed Steps
⚠ **Important:** Perform this exercise on the **7034A-FabrikamDC-B** virtual machine.	
1. Configure DNS record for the FabrikamAP server..	**a.** Log on to **7034A-FabrikamDC-B** as **Administrator** with a password of **pass@word1**. **b.** On the taskbar, click **Start**, point to **Administrative Tools**, and click **DNS**. The DNS management console appears. **c.** Expand **FABRIKAMDC**, and expand **Forward Lookup Zones**. **d.** Right-click **fabrikam.local**. **e.** Click **New Host (A)**. **f.** On the **New Host** dialog box, in the **Name** box, type **FabrikamAP**. **g.** In the **IP address** box, type **10.0.0.50**. **h.** On the **New Host** dialog box, click **Add Host**. **i.** When prompted that the Host A record was successfully added, click **OK**. **j.** On the **New Host** dialog box, click **Done**. **k.** On the **DNS Console**, click **File**, and then click **Exit**.
⚠ **Important:** Perform this exercise on the **7034A-NWTradersDC-B** virtual machine.	
1. Configure DNS record for the NWTradersAP server..	**a.** Log on to **7034A-NWTradersDC-B** as **Administrator** with a password of **pass@word1**. **b.** If the **Sign In to a SIP Communications Service** dialog box appears, click **Cancel**. **c.** On the taskbar, click **Start**, point to **Administrative Tools**, and click **DNS**. The **dnsmgmt** management console appears. **d.** Expand **NWTRADERSDC**.

	e. Expand **Forward Lookup Zones**. **f.** Right-click **NWTraders.local**. **g.** Click **New Host (A)**. **h.** On the **New Host** dialog box, in the **Name** box, type **NWTradersAP**. **i.** In the **IP address** box, type **11.1.1.30**. **j.** On the **New Host** dialog box, click **Add Host**. **k.** When prompted that the Host A record was successfully added, click **OK**. **l.** On the **New Host** dialog box, click **Done**. **m.** On the dnsmgnt console, click **File**, and then click **Exit**.
⚠ **Important:** Perform this exercise on the **7034A-Proxy01-B** virtual machine.	
1. Configure external DNS entries for FabrikamAP and NWTradersAP.	**a.** Log on to **7034A-Proxy01-B** as **Administrator**. **b.** Click **Start**, point to **Administrative Tools**, and then click **DNS**. **c.** On the **dnsmgmt** console, expand **Forward Lookup Zones**. **d.** Right-click **Fabrikam.local**. **e.** Click **New Host (A)**. **f.** On the **New Host** dialog box, type **FabrikamAP**. **g.** In the **IP address** box, type **192.168.0.10**. **h.** On the **New Host** dialog box, click **Add Host**. **i.** On the **DNS** message box, click **OK**. **j.** On the **New Host** dialog box, click **Done**. **k.** Right-click **NWTraders.local**. **l.** Click **New Host (A)**. **m.** On the **New Host** dialog box, type **NWTradersAP**. **n.** In the **IP address** box, type **192.168.0.20**. **o.** On the **New Host** dialog box, click **Add Host**. **p.** On the **DNS** message box, click **OK**. **q.** On the **New Host** dialog box, click **Done**.

Exercise 6
Start the Access Proxy Service

Scenario

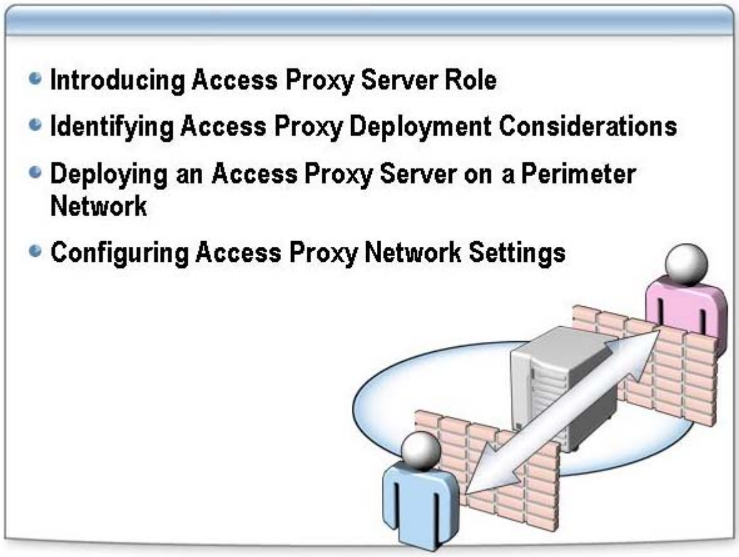
With the Access Proxies successfully configured, Matt and Holly can start the Access Proxy service on their respective servers.

Description

You will need to start the Access Proxy service on the Fabrikam and NWTraders servers. After you have started the service, review the Event Viewer and verify the Live Communications Server service has started on FabrikamAP and NWTradersAP.

Tasks	Detailed Steps
⚠ **Important:** Perform this exercise on the **7034A-FabrikamAP-B** virtual machine.	
1. Start the Live Communications Server service on FabrikamAP.	**a.** Log on to **7034A-FabrikamAP-B** as **Administrator** with a password of **pass@word1**. **b.** On the taskbar, click **Start**, point to **Administrative Tools**, and then click **Computer Management**. **c.** On the **Computer Management** console, expand **Services and Applications**. **d.** Right-click **Microsoft Office Live Communications Server 2005**, and then click **Start**. **e.** On the **Computer Management** console, expand **Event Viewer**. **f.** Click **Application**. Review Information Event Log entries with the source **Live Communications Server Proxy**. **g.** On the **Computer Management** console, click **Services**. **h.** Verify that the **Live Communications Server** service has started.
⚠ **Important:** Perform this exercise on the **7034A-NWTradersAP-B** virtual machine.	
1. Start the Live Communications Server service on NWTradersAP.	**a.** On **7034A-NWTradersAP-B**, click **Start**, point to **Administrative Tools**, and click **Computer Management**. **b.** On the **Computer Management** console, expand **Services and Applications**. **c.** Right-click **Microsoft Office Live Communications Server 2005**, and then click **Start**. **d.** On the **Computer Management** console, expand **Event Viewer**, and click **Application**. Review Information Event Log entries with the source **Live Communications Server Proxy**. **e.** On the **Computer Management** console, click **Services**. **f.** Verify that the **Live Communications Server** service has started. **g.** **DO NOT** close the VPC images, but leave them running for Lab 7.

Review



- Introducing Access Proxy Server Role
- Identifying Access Proxy Deployment Considerations
- Deploying an Access Proxy Server on a Perimeter Network
- Configuring Access Proxy Network Settings

In this module, you learned that the Access Proxy server is required to implement:

- Enhanced Federation to Federation
- Enterprise to Public IM Connectivity
- Remote User Access

Without an Access Proxy server, you will not be able to extend the features of Live Communications Server 2005 with Service Pack 1 for external connections.

It is recommended that you deploy an Access Proxy server in your perimeter network. A perimeter network will provide an extra layer of network security.

In the next Module, you will look at how an Access Proxy can provide support for Remote Users. Enabling Remote User Access gives your employees, clients and customers who are located outside the internal network the ability to use LCS 2005 with SP1 features without VPN access.