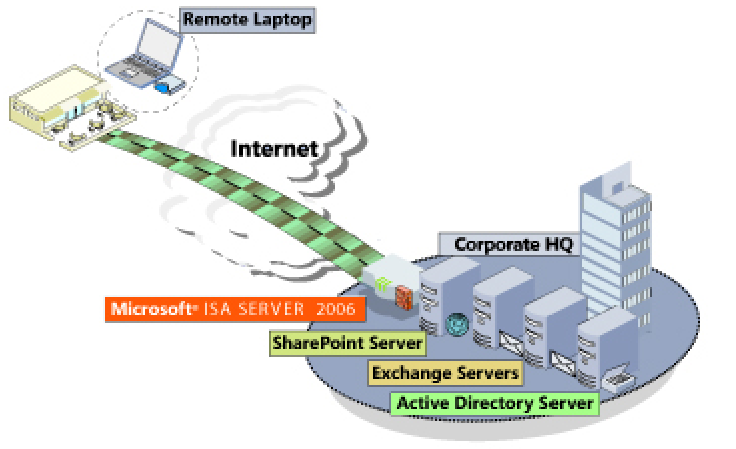
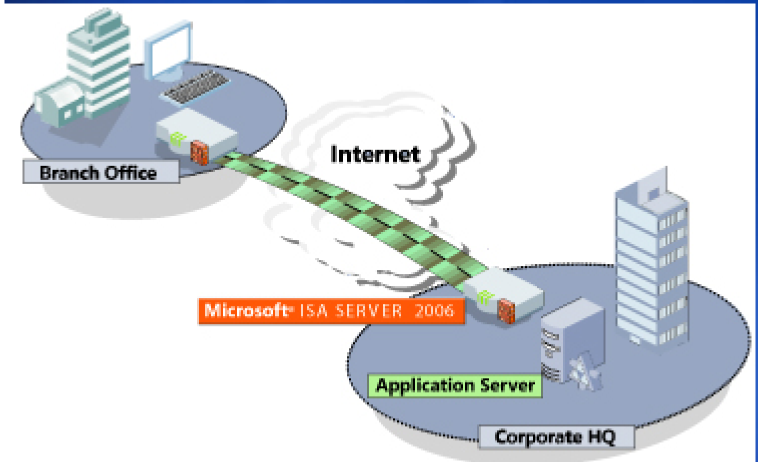
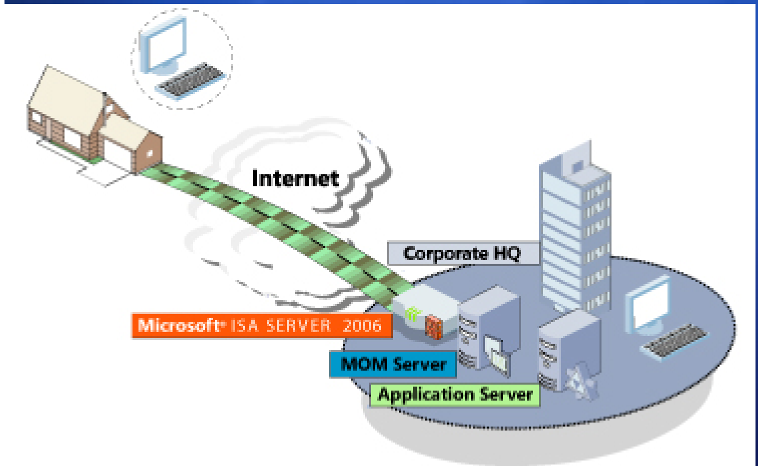
SEC 311

ISA Server 2006 中的新增功能

它是做什么用的？







安全的应用程序发布

分支机构网关

Internet访问保护

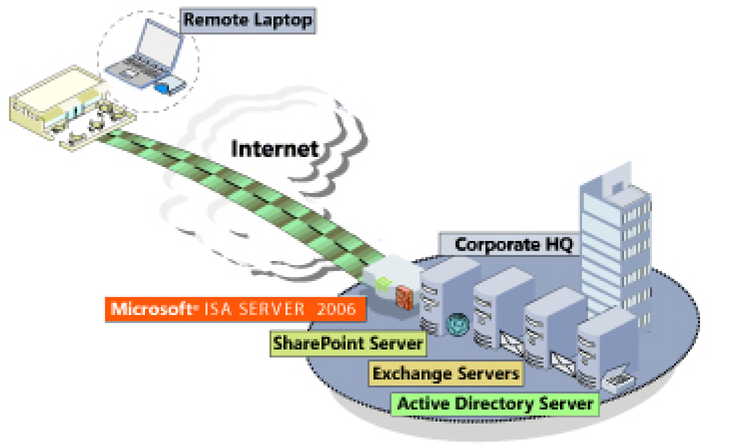
集成的安全性

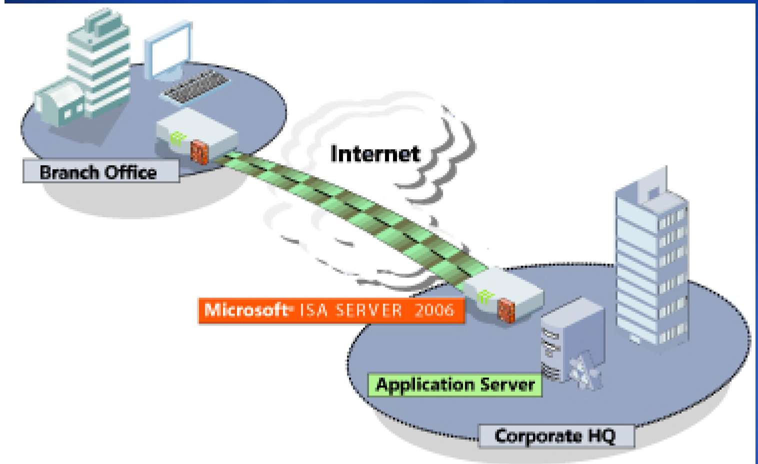
高效的管理

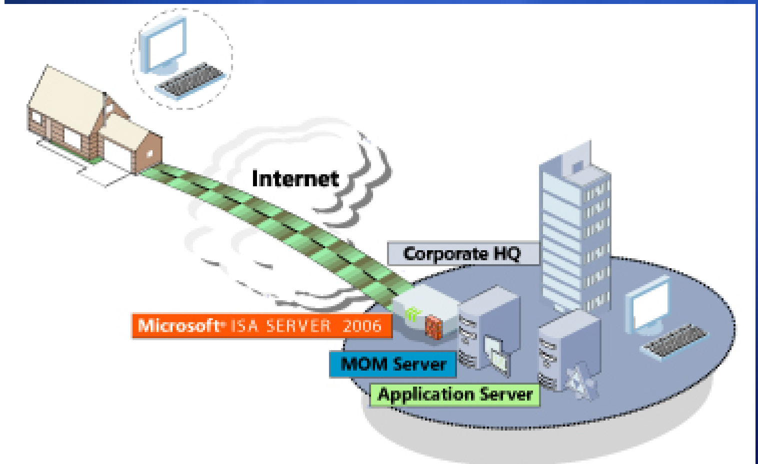
快速和安全的访问

安全的应用程序发布

集成的安全性	• 增强的多因素身份验证 • AD/LDAP 集成 • 可自定义的基于表单的预身份验证 • 增强的身份验证委托 • 改进的会话管理
高效的管理	• Web 发布负载平衡 • 用于 Exchange、SharePoint、其它 Web 服务器的自动化工具 • 更好的证书管理
快速、安全的访问	• 更多单点登录选择 • 自动的链接转换







安全的应用程序发布

分支机构网关

Internet 访问保护

集成的安全性

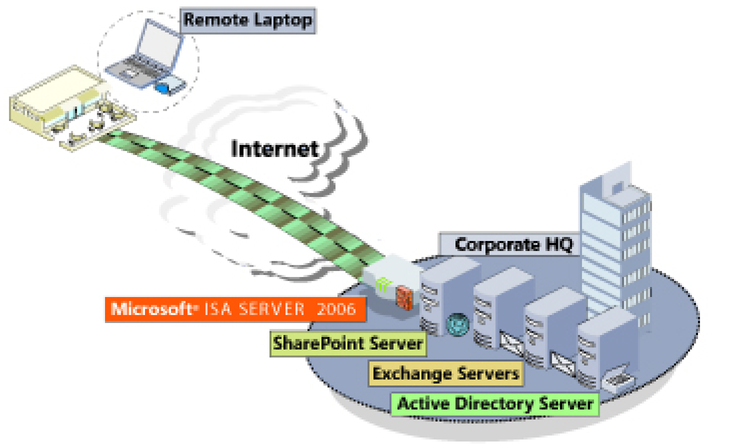
高效的管理

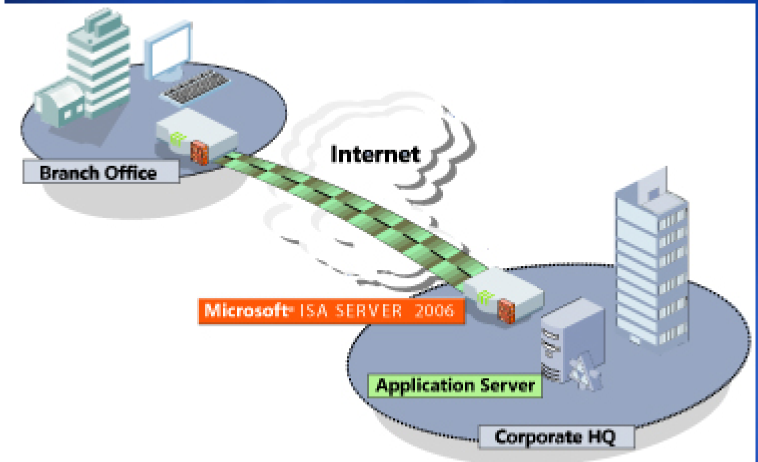
快速和安全的访问

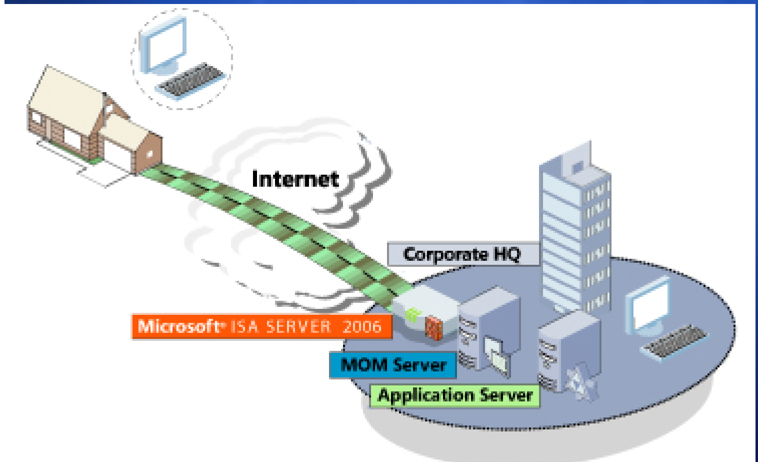
分支机构网关

集成的安全性	• BITS 缓存
高效的管理	• 自动化的 VPN 连接工具 • 可移动媒体上的应答文件 • 更快的企业策略传播
快速、安全的访问	• HTTP 流量压缩 • 考虑 DiffServ 信号

- BITS 缓存、HTTP 压缩和 DiffServ 与 ISA Server 2004 service pack 2 中的对应功能几乎相同







安全的应用程序发布

分支机构网关

Internet访问保护

集成的安全性

高效的管理

快速和安全的访问

Internet 访问保护

集成的安全性	• 增强的泛洪抑制 • 增强的蠕虫抑制 • 全面的警报触发器
高效的管理	• 增强的资源控制

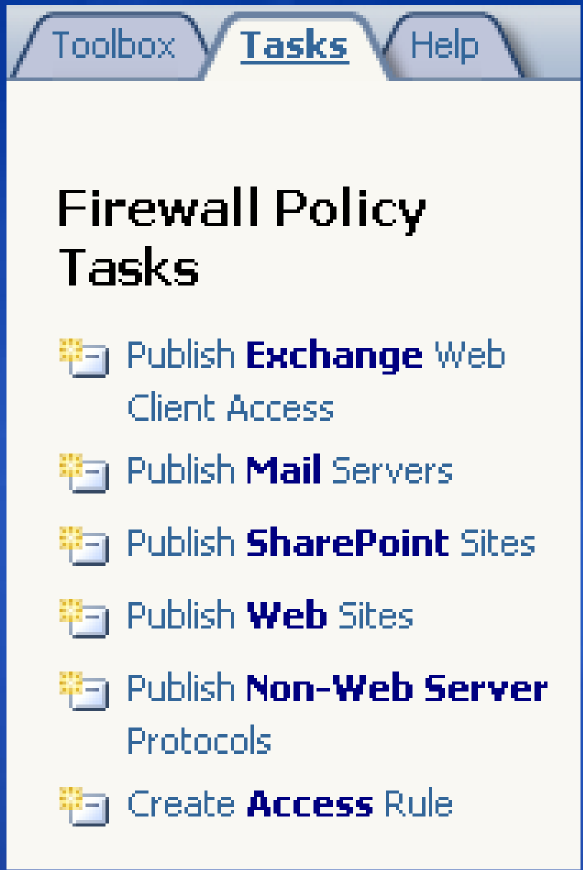
安全的发布

按数量

> 35%	未经授权的计算机资源访问
1:1	外部与内部攻击比率

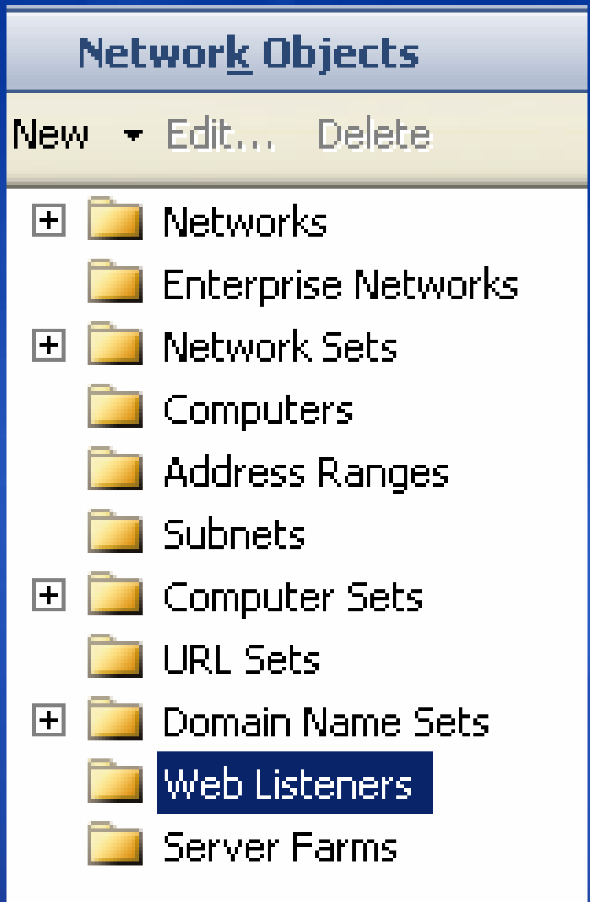
CSI/FBI 2005 报告

更多的向导



- 基于 Web 的项目
  - OWA
  - SharePoint
  - Web 服务器
  - 规则和网络对象
- 其它项目
  - SMTP 电子邮件
  - Exchange RPC
  - 自定义规则
- 向导根据需要创建网络元素并配置链接转换

Web 侦听器向导



- 身份验证
- 证书处理
- HTTP 压缩

身份验证属性

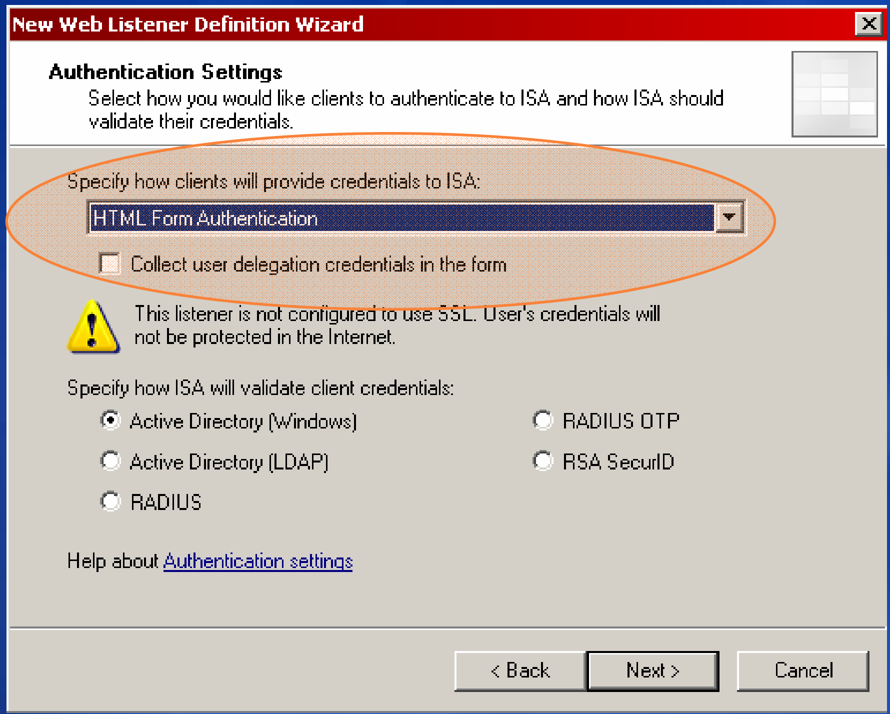
用户 ID

组成员资格

协议使用

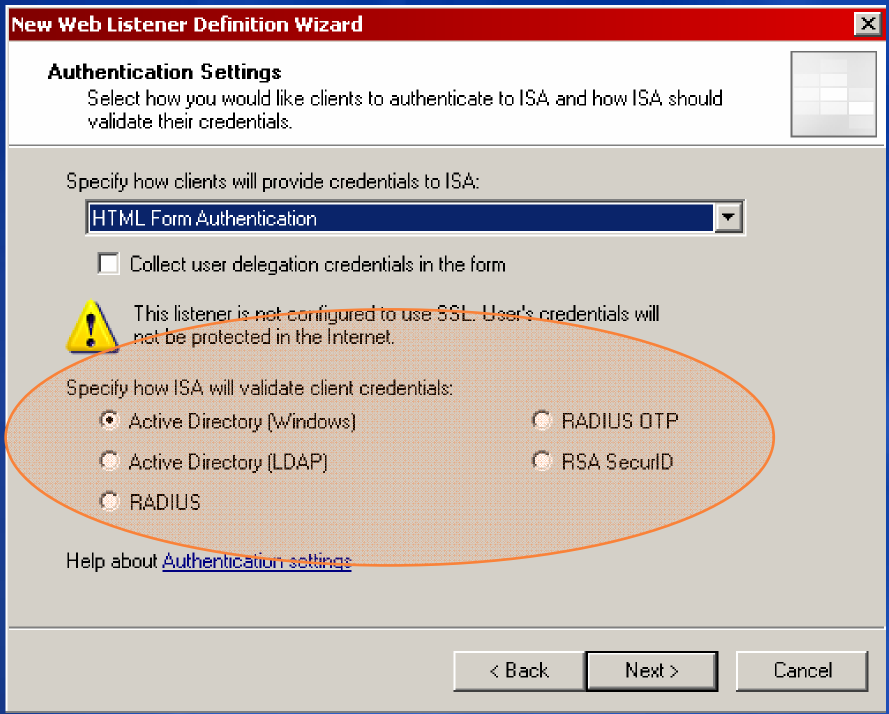
计划安排

身份验证：客户端对 ISA



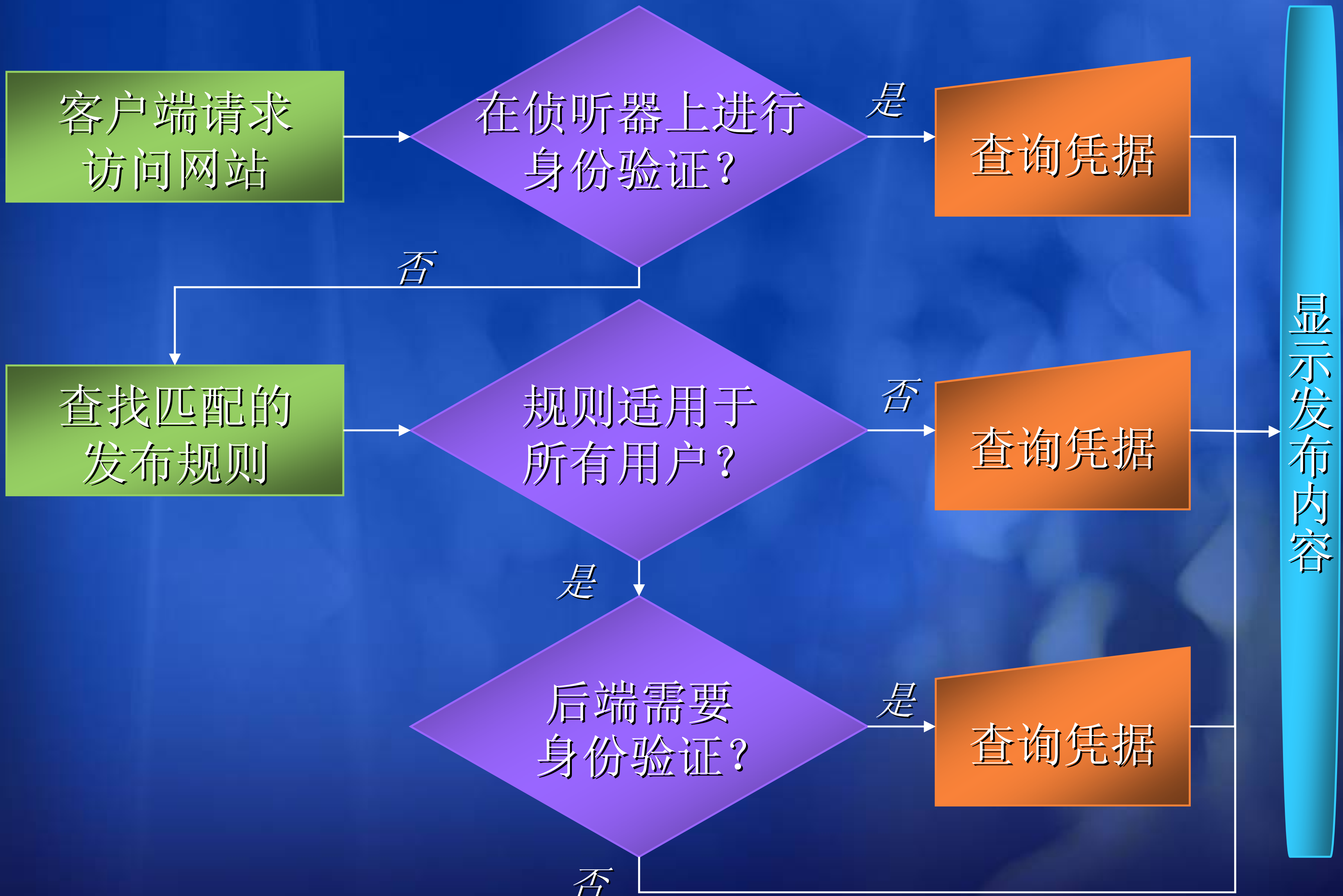
- HTML 表单
  - RADIUS
  - OTP
  - SecurID
- HTTP 基本身份验证
- 客户端 SSL
  - 与其他方法组合或故障切换到其他方法
- 无
- 第三方加载项

身份验证：ISA 对验证器



- Active Directory
  - Kerberos
  - LDAP
- RADIUS
- RADIUS OTP
- SecurID

身份验证流



客户端请求
访问网站
在侦听器上进行
身份验证？
是
否
查询凭据
查找匹配的
发布规则
规则适用于
所有用户？
否
查询凭据
是
后端需要
身份验证？
是
查询凭据
否
显示发布内容

身份验证方法

前端	HTTP	基本 摘要 协商
	客户端 SSL	忽略 接受 • 请求证书；若未提供则付诸侦听器的身份验证 要求 • 请求证书；若未提供则规则失败 • 结合侦听器身份验证的凭据要求，获得双因素身份验证
	HTML 表单	按侦听器或按规则；26 种语言 • 用户名 + 密码 • 用户名 + 通行码 • 用户名 + 密码 + 通行码 仅支持浏览器；非浏览器必须使用 HTTP 基本身份验证

身份验证方法

网关	Kerberos	ISA 属于域
	LDAP	ISA 独立 域为 Windows 2000 or 2003 非 AD LDAP 无法工作 可用性标志轮换
	RADIUS	ISA 独立 可用性标志轮换 Windows、FreeRADIUS、GNU RADIUS、其他
	OTP	ISA 独立 基于时间或计数器 提供 Cookie 以避免重新身份验证 Aladdin、Vasco、ActivCard、Secure

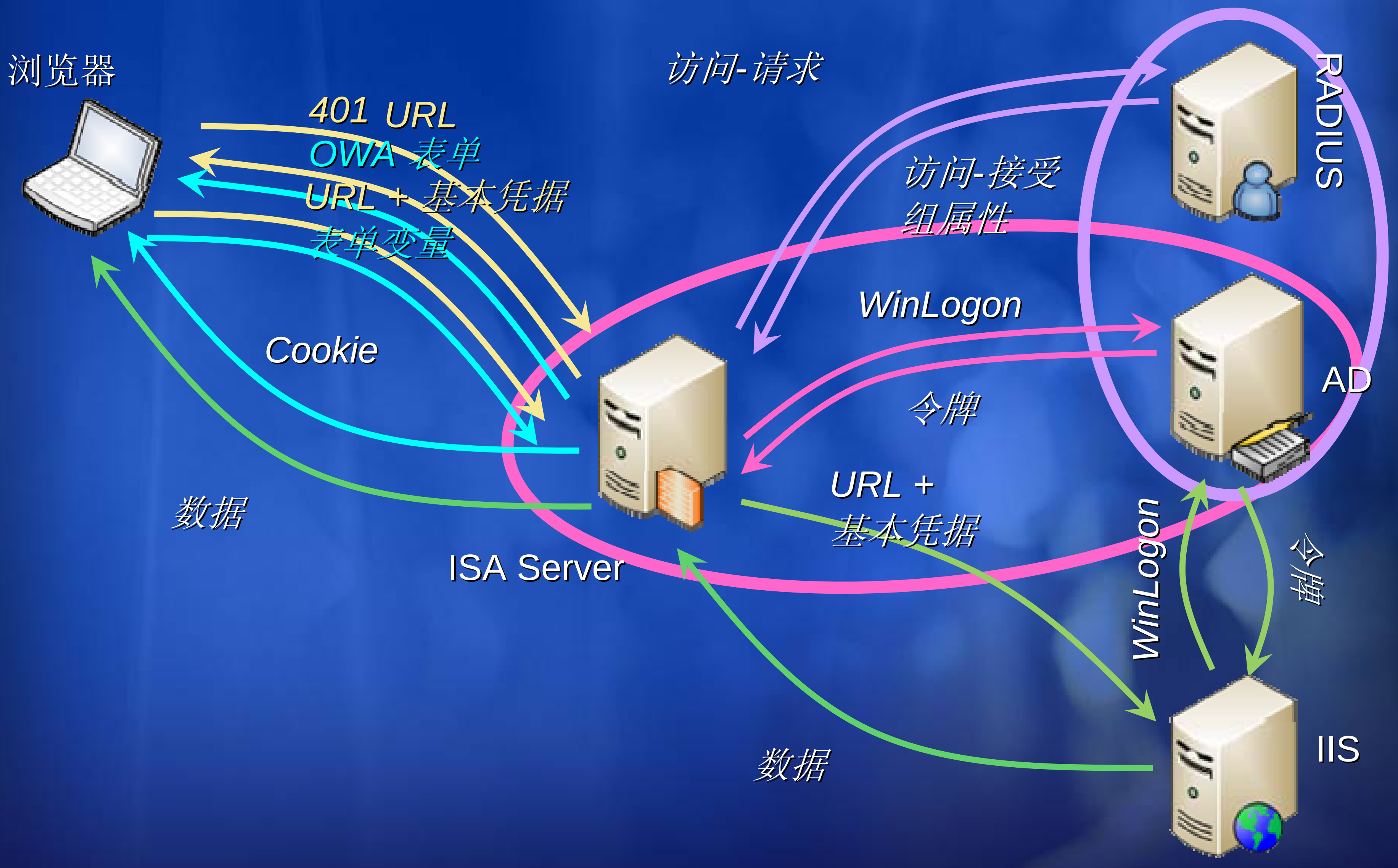
身份验证方法

后端	无	阻止
		通过
	HTTP	基本
		协商 • 尝试 Kerberos，然后故障切换回 NTLM
	Kerberos	支持 S4U2Proxy 委托 • 仅支持 Windows 2003 域

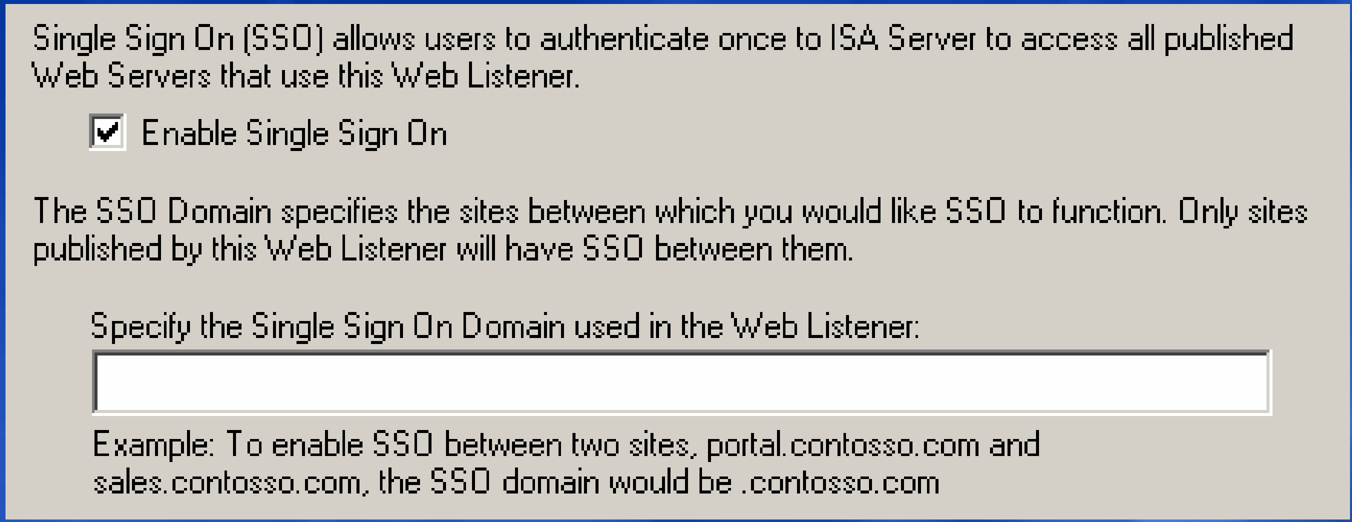
身份验证方法

增强的委托	前端接口	提供程序	后端委托	注释
	HTML 表单 HTTP 基本	WinLogon LDAP RADIUS	无（通过） 无（阻止） HTTP 基本 Kerberos S4U2Proxy 协商	• 支持 SSO • 双因素身份验证可能需要证书
	摘要集成	WinLogon	无（通过） 无（阻止）	
	带通行码的表单	SecurID	无（通过） 无（阻止） SecurID	• 支持 SSO
	带通行码和密码的表单	SecurID	无（通过） 无（阻止） HTTP 基本 Kerberos S4U2Proxy 协商 SecurID	• 支持 SSO
	客户端 SSL	WinLogon	n/a	• 与 SecurID 结合用于双因

委托过程

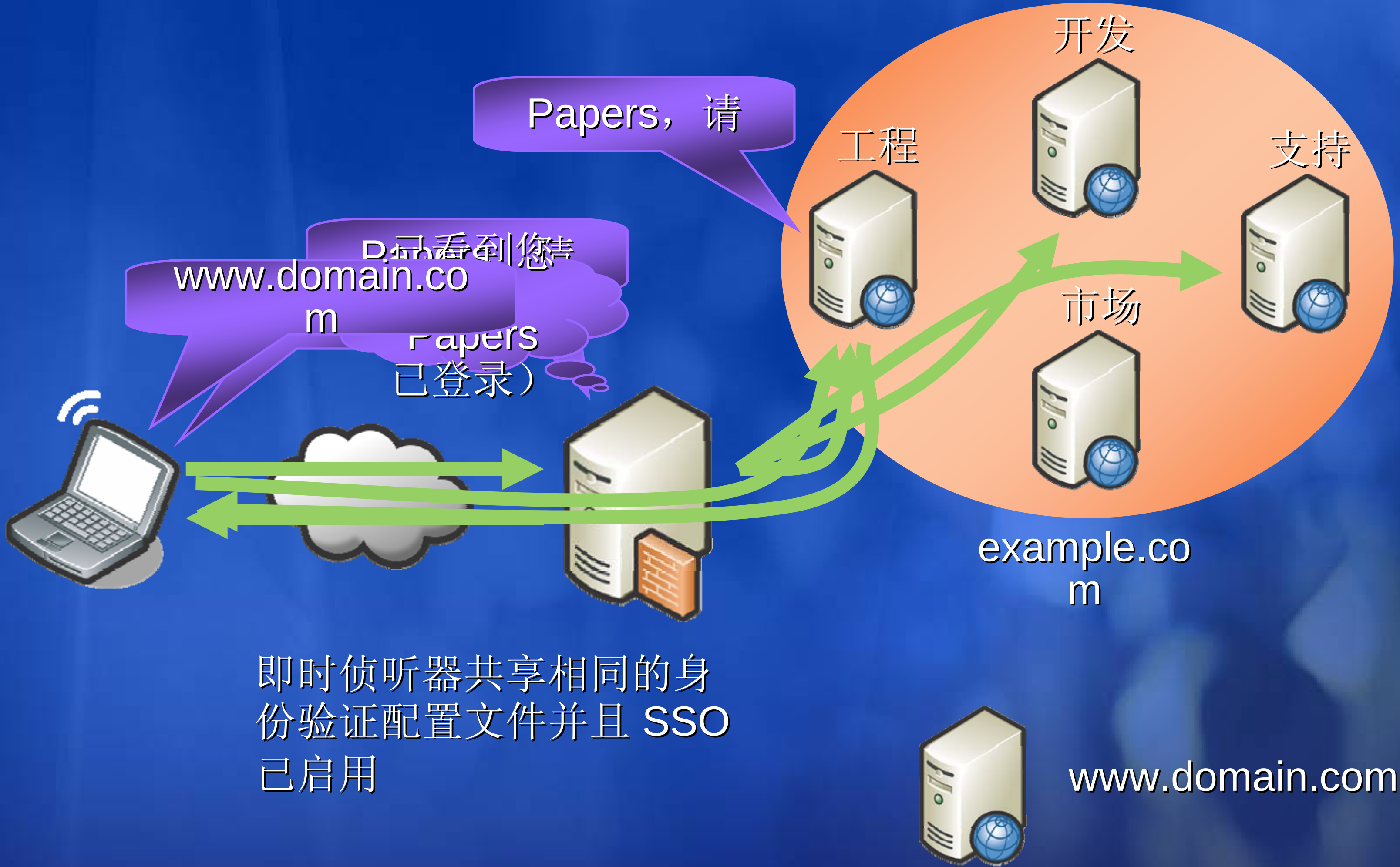

浏览器
401 URL
OWA 表单
URL + 基本凭据
表单变量
Cookie
数据
ISA Server
访问-请求
访问-接受
组属性
WinLogon
令牌
URL +
基本凭据
RADIUS
AD
WinLogon
令牌
IIS
数据

单点登录

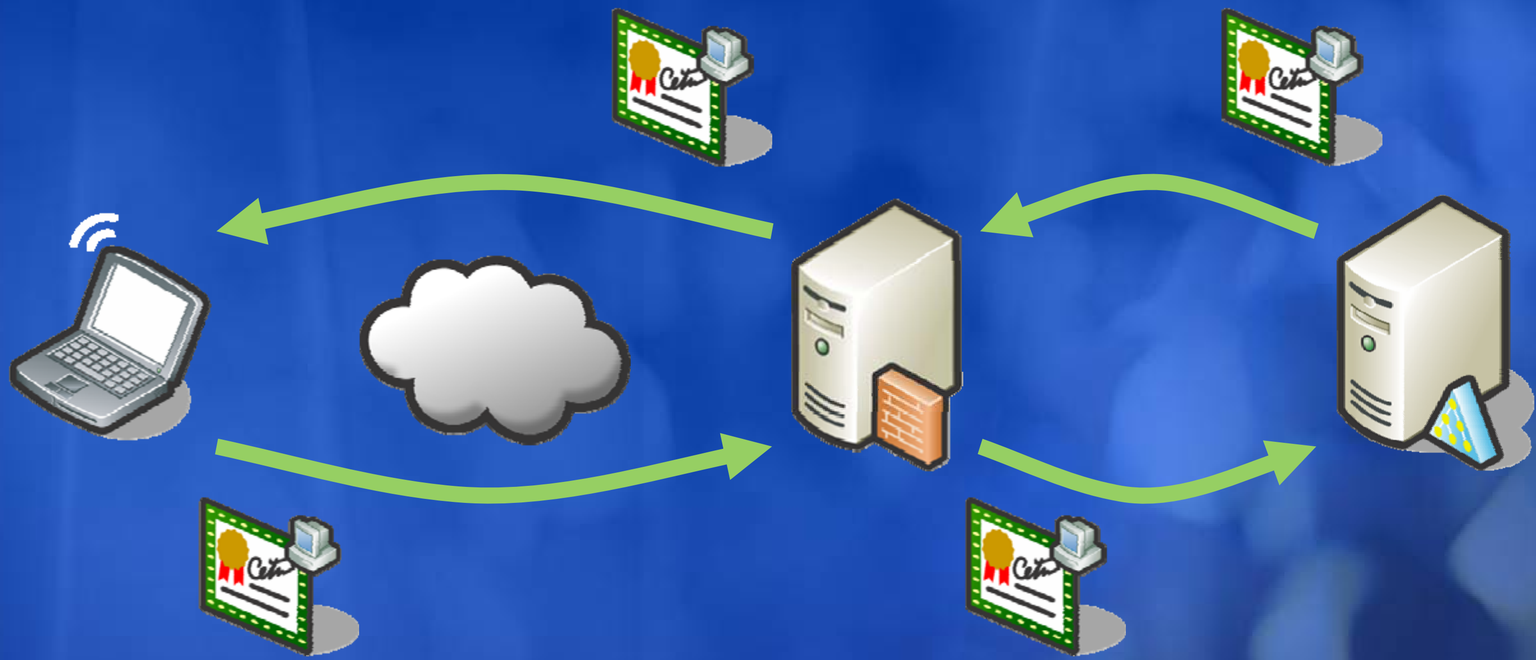


- 在单个侦听器上发布的所有应用程序之间自动进行
- 将侦听器视为由该侦听器中所有已发布站点共享的身份验证设置容器

单点登录流


Papers，请
www.domain.co
m
Papers
已登录）
开发
工程
支持
市场
example.co
m
即时侦听器共享相同的身份验证配置文件并且 SSO 已启用
www.domain.com

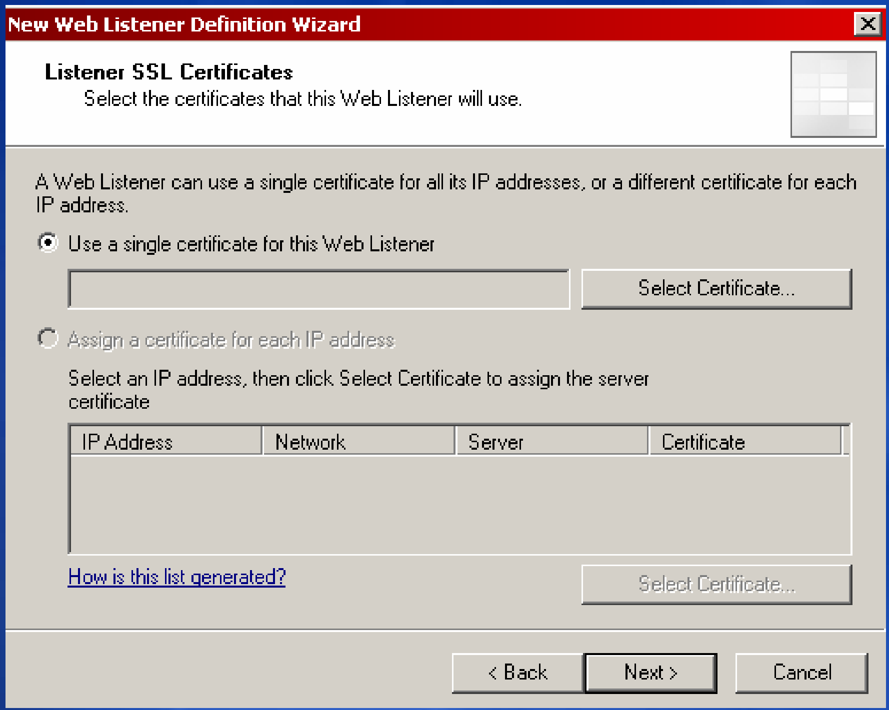
证书类型：检查中



证书类型

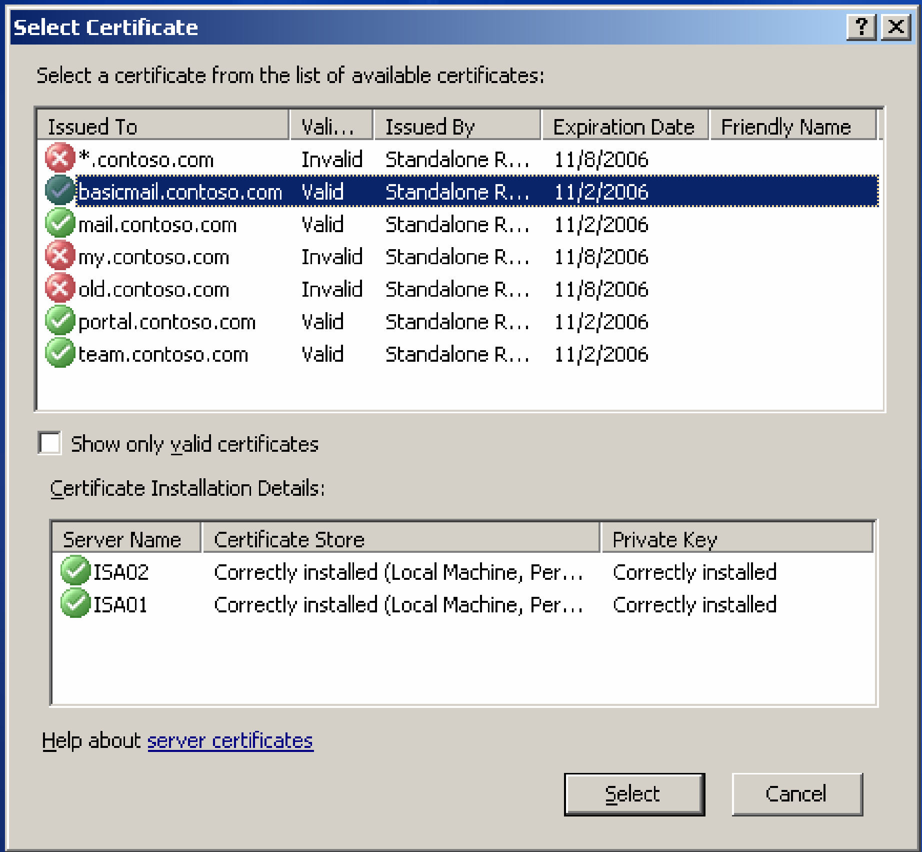
必需	
前端	验证 ISA Server 的身份验证并建立到远程客户端的 SSL 连接
后端	验证已发布服务器的身份验证并建立到 ISA Server 的 SSL 连接
可选	
ISA Server 客户端	向已发布的服务器验证 ISA Server 的身份
远程客户端	向 ISA Server 验证远程客户端的身份

证书处理



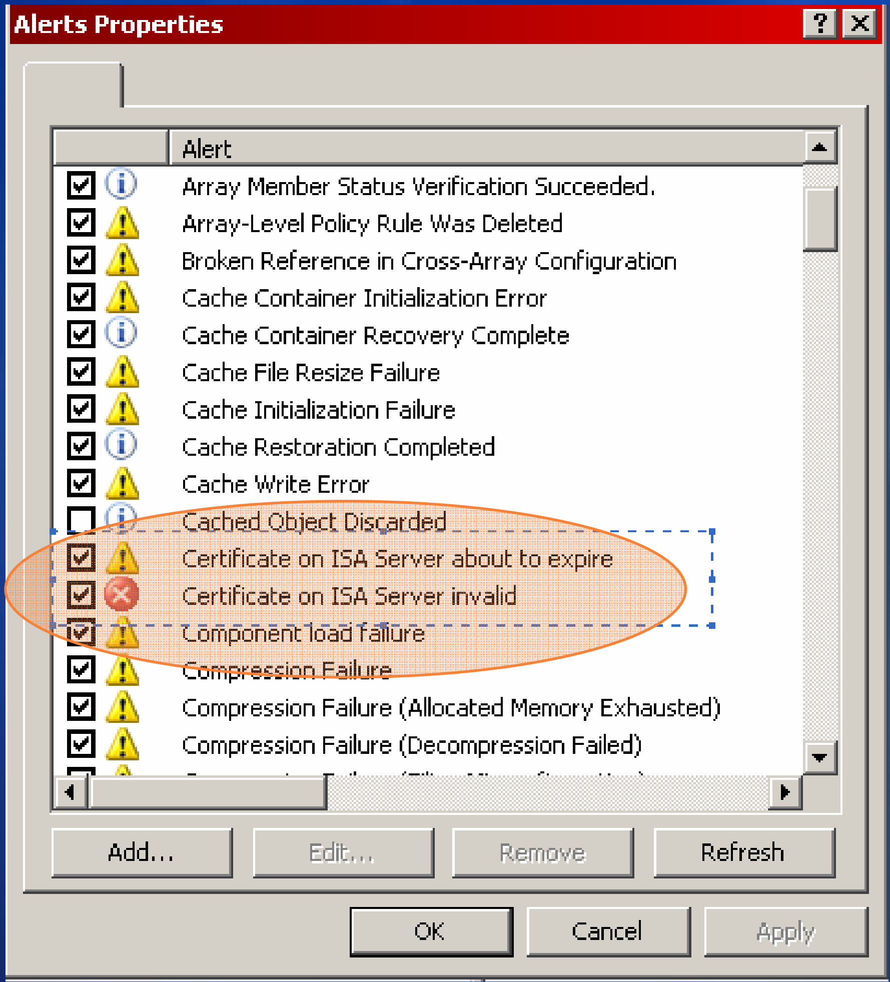
- 每个侦听器多个证书
  - 用于多个站点的单组身份验证设置
  - 消除使用通配符证书（成本更高）的需要
- 能够为阵列中的每个服务器选择不同的证书
  - 不必获取证书的指纹
- 建议：添加 SSL 硬件

证书状态



- 不正确地安装的证书
  - 在不正确的存储区中（必须在计算机而不是用户存储区中）
  - 缺乏私钥
- 每个阵列成员的状态
- 如果证书过期则发出警告

用于证书的管理警报



- 现在在管理警报中报告证书问题
- 比 ISA 2004 的通用“证书未安装”错误更好！

基于 HTML 表单的身份验证

- 适用于任何已发布的网站
  - 高级：带高级功能的浏览器
  - 基本：带有限功能的浏览器
  - 移动：低分辨率的浏览器
- 每个类别三个表单
  - 登录
  - 注销
  - SecurID
- 语言
  - 根据浏览器语言设置进行选择
  - 可重写

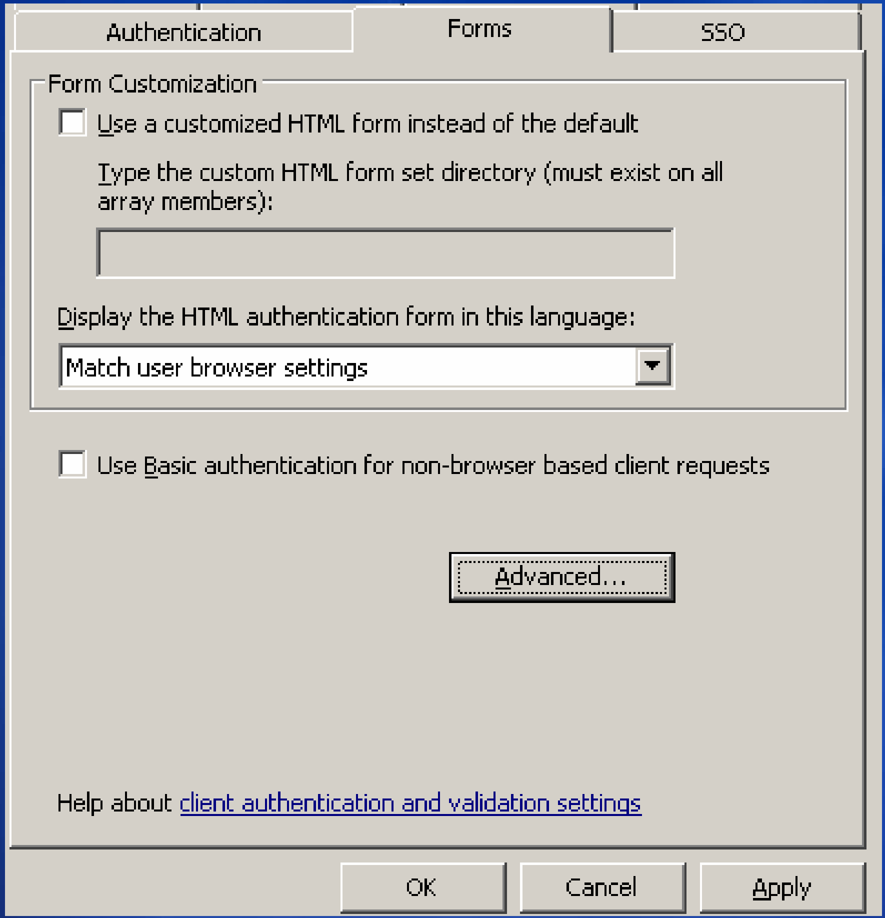
表单格式

- 用户名和密码
- 用户名和通行码
- 组合（同时输入两者）
  - ID+密码：用于 SecurID 或 RADIUS OTP
    - 由 ISA Server 验证
  - ID+密码：用于委托
    - 由后端验证
- 预定义的表单集（主要是登录）
  - 通用 ISA Server
  - Exchange

通用表单

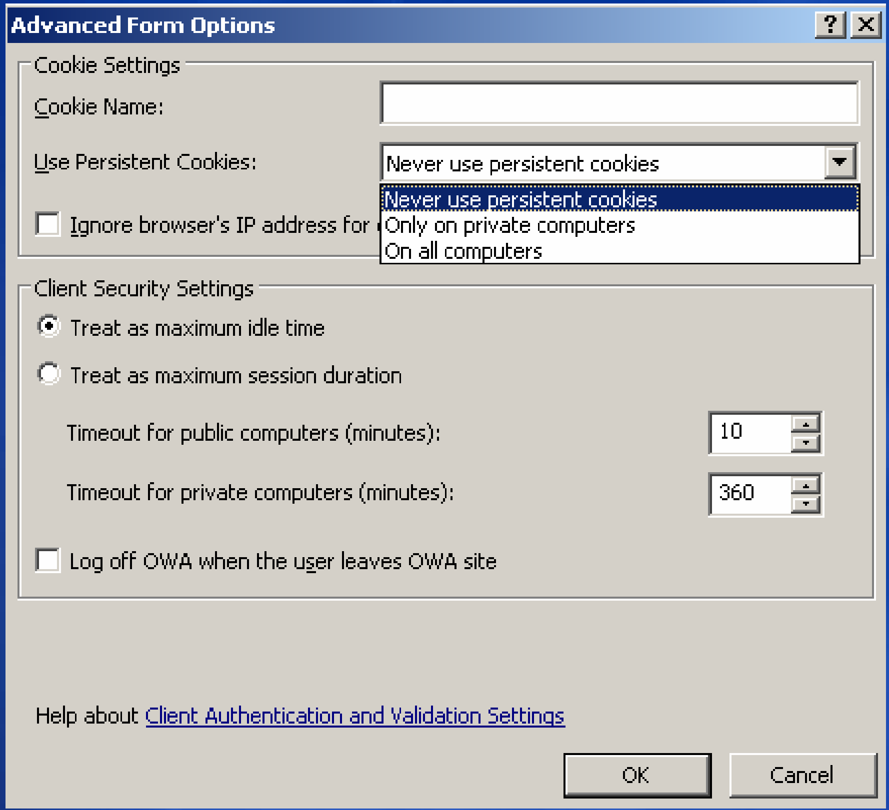
Microsoft®
ISA Server Web Access 2006
Security (show explanation)
This is a public or shared computer
This is a private computer
I am using a basic browser or have a slow Internet Connection
ISA Credentials (show explanation)
Domain\user name:
Passcode:
Web Server Credentials (show explanation)
Use A different username for the web server.
Password:
Log On

自定义表单集



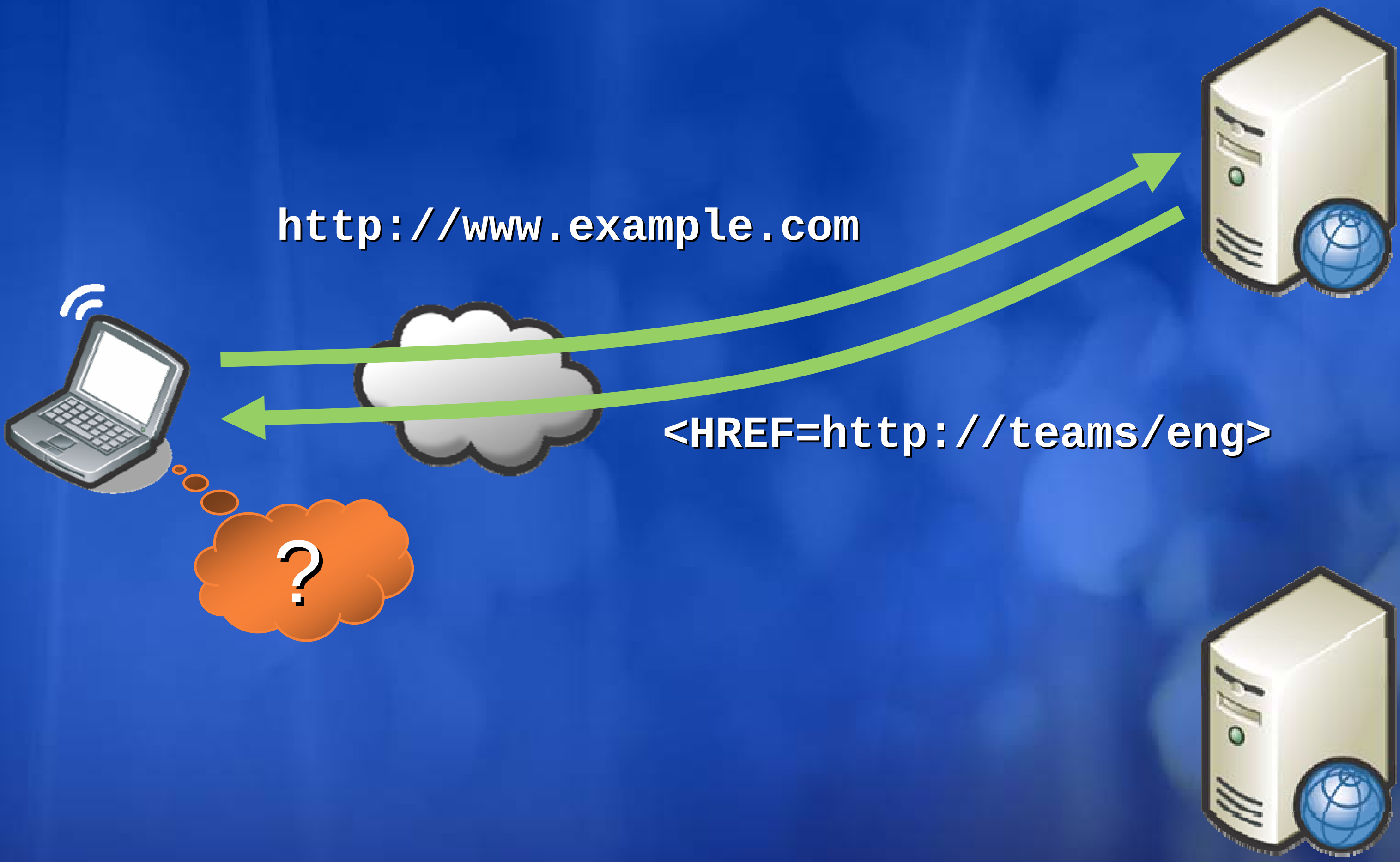
- 在每个侦听器上可以不同
- 发布规则可以重写侦听器表单

会话管理

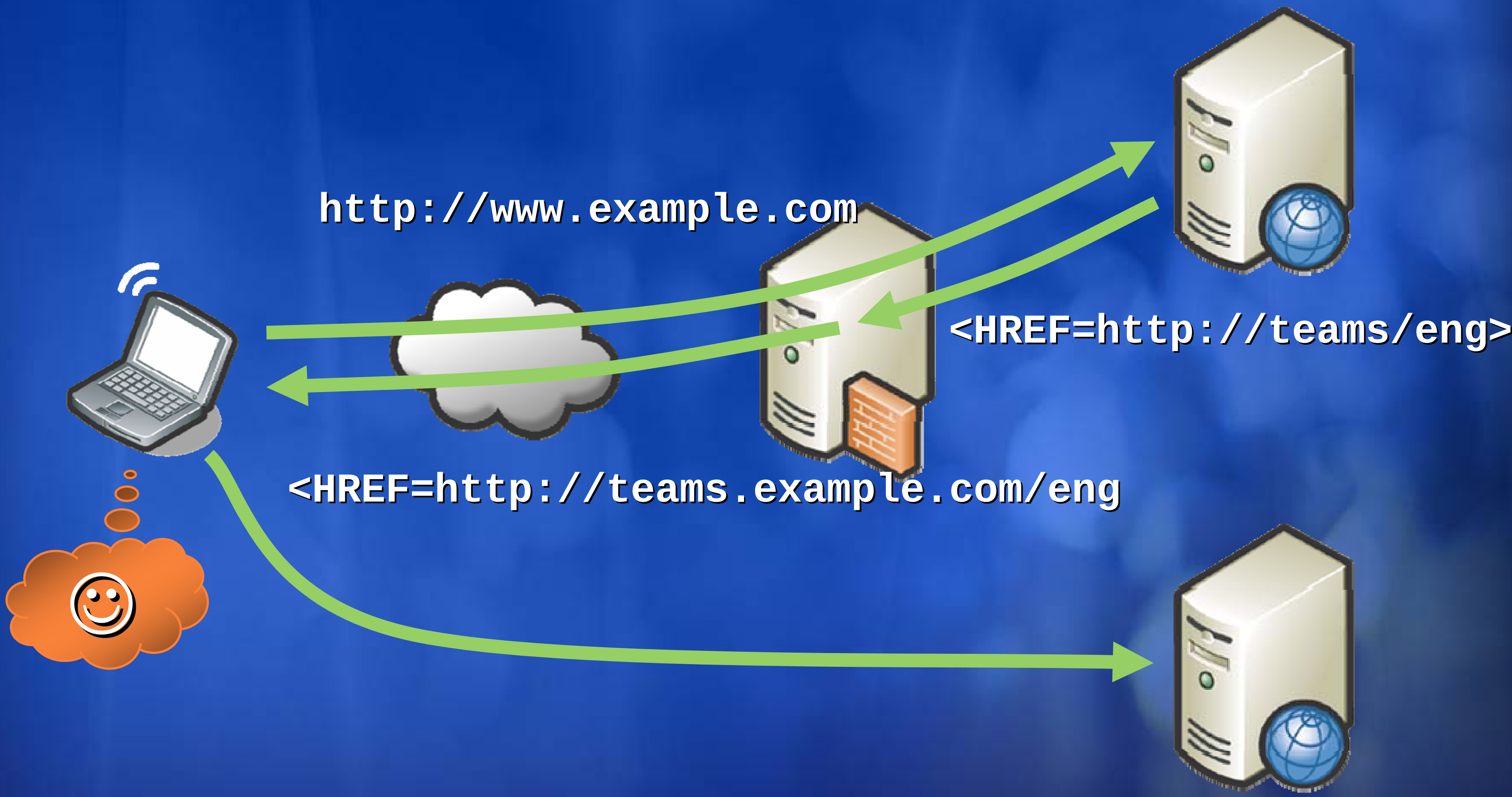


- Cookie
  - 持久
  - 会话
- 超时
  - 空闲时间
  - 会话期间
  - 非用户活动不会重设 Cookie 定时器
- 注销
  - 将注销 URL 添加到发布规则
  - 删除 Cookie；添加到撤销列表
  - 记录远程用户的身份

链接转换：检查中

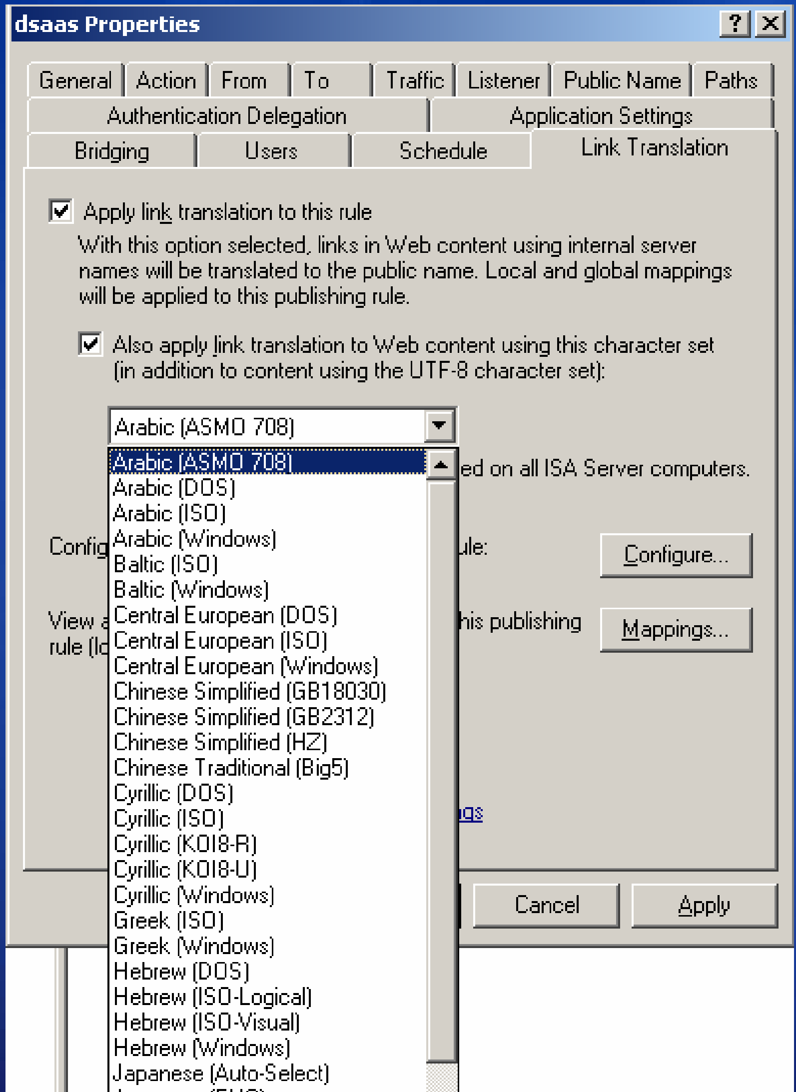


链接转换：检查中



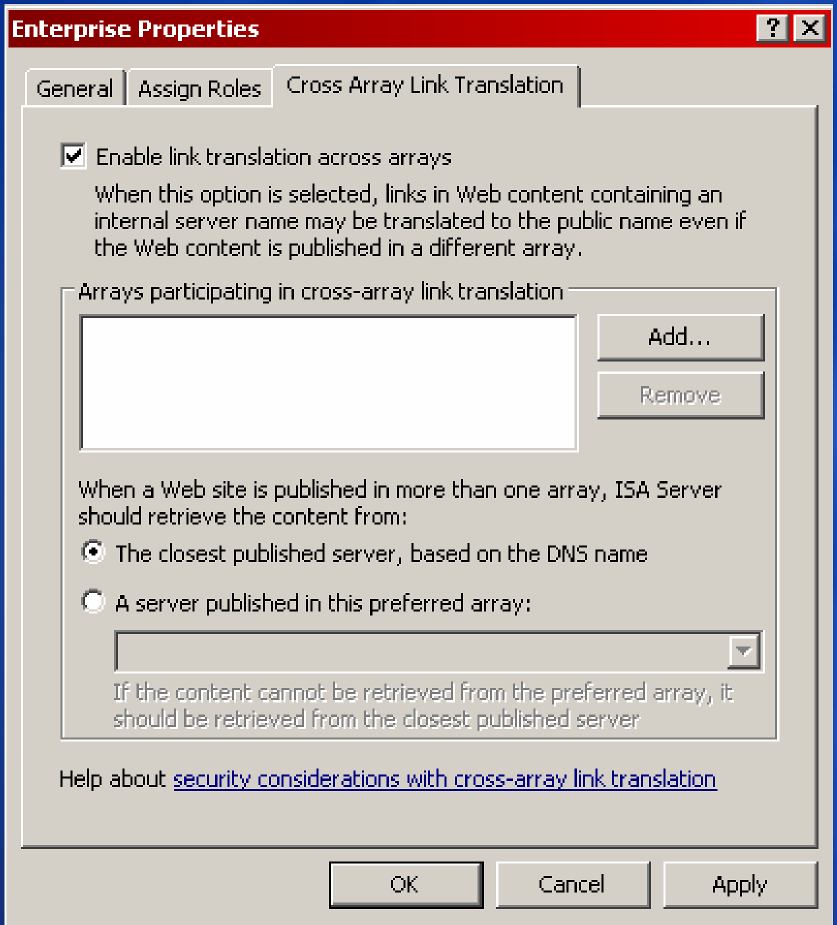
http://www.example.com
<HREF=http://teams/eng>
<HREF=http://teams.example.com/eng

链接转换



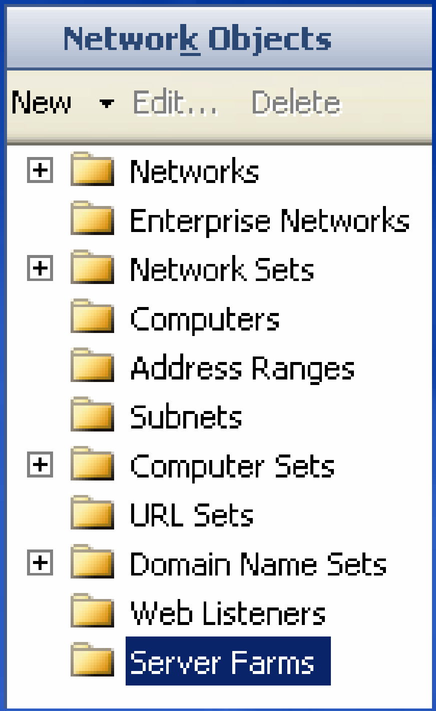
- 链接转换好在哪里？
  - 使内部详细信息保持隐秘
  - 允许外部用户访问链接而不必重新编写应用程序（节省金钱）
- 有何新功能？
  - 自动启用
  - 更快的转换引擎
  - 其方法全球通用

阵列中的链接转换



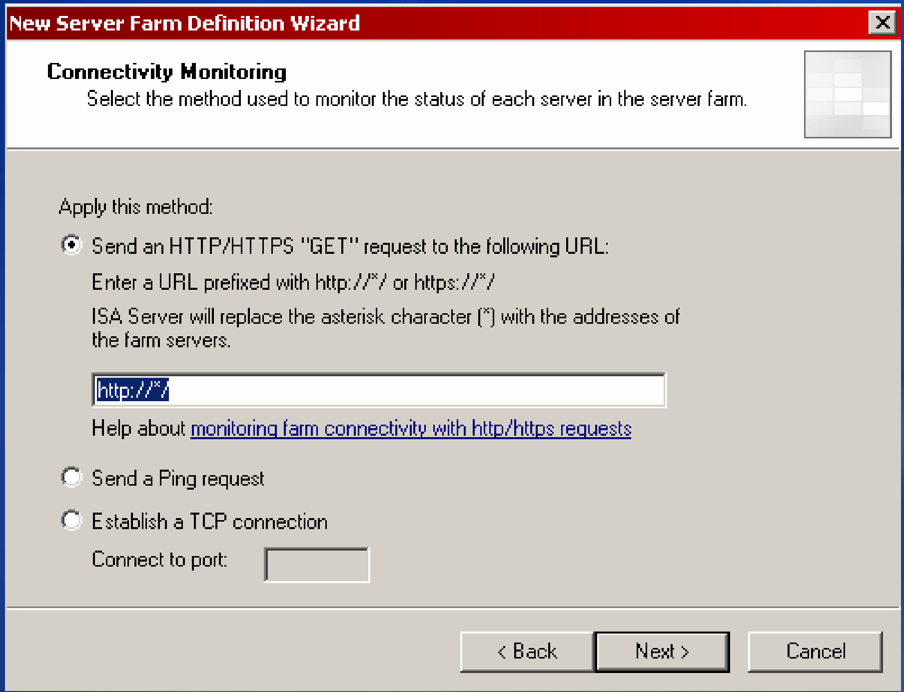
- 即使 Web 内容在其它阵列中也转换链接
- 帮助提高可用性
  - 如果一个地理区域的阵列失效，则移交给另一个地理区域

服务器场

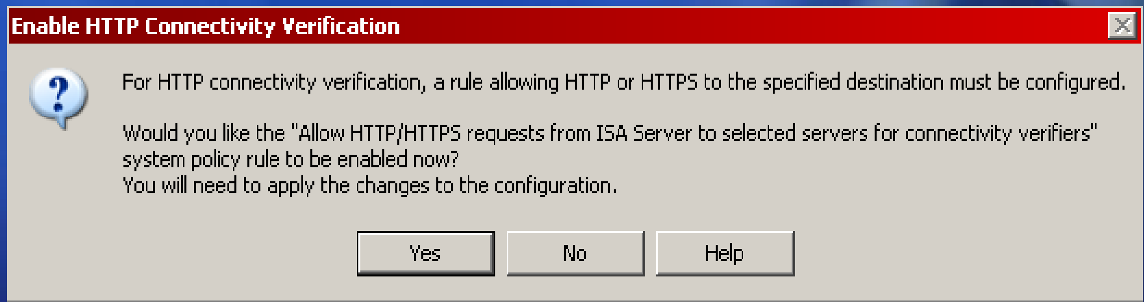


- 定义为一个网络对象，在您希望的任何发布规则中使用

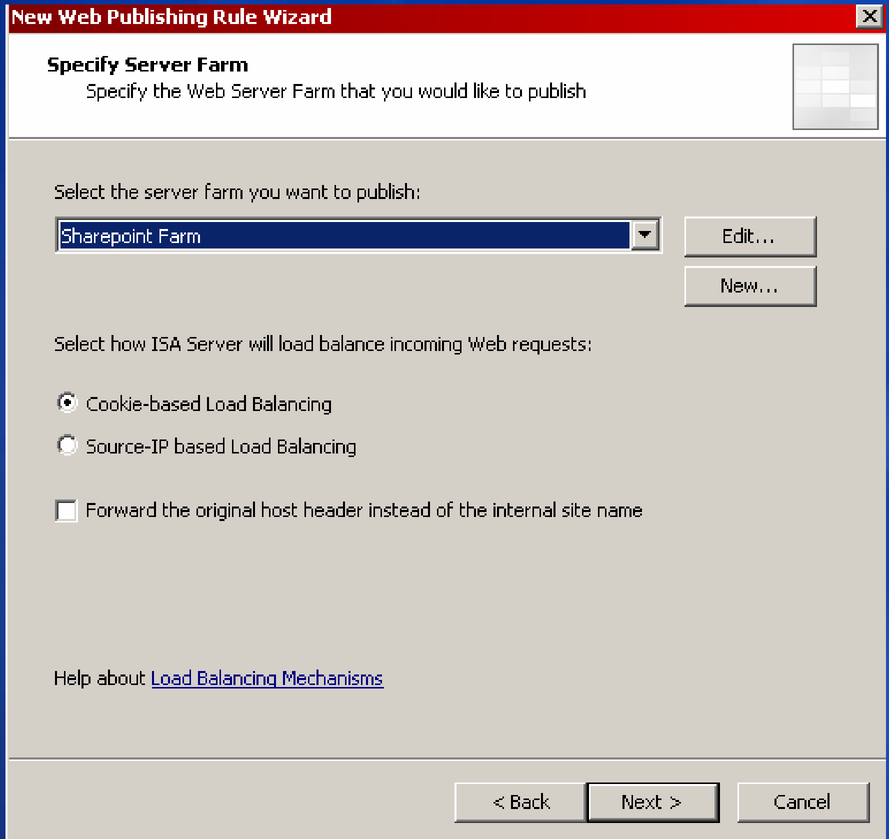
服务器场



- 定义连接验证选项
  - HTTP/S “GET”
  - ping
  - 到某个端口的 TCP 连接



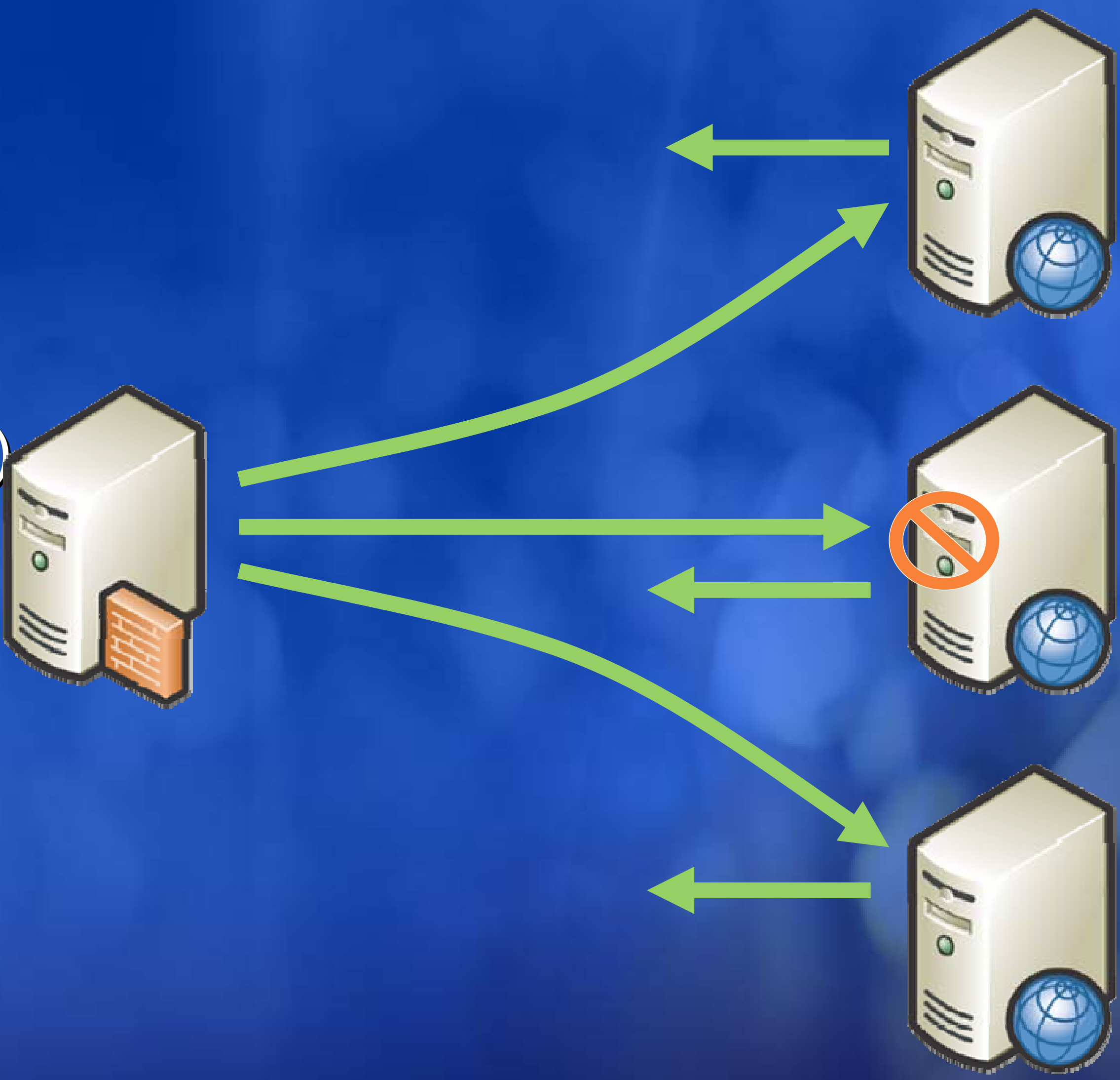
Web 发布负载平衡



- 使用 Web 服务器场
- 保留应用程序上下文
  - 只有单一关联性
- 不需要在已发布的服务器上使用 NLB
  - 消除 NAT 问题和路由错误
  - 不依赖 ISA IP 地址确保了同等地使用所有已发布的服务器
- 能够选择平衡类型
  - Cookie（OWA 默认）
  - 源 IP（RPC/HTTP 默认）

跟踪服务器状态

- 活动
- 排空 (Draining)
- 已删除
- 停用

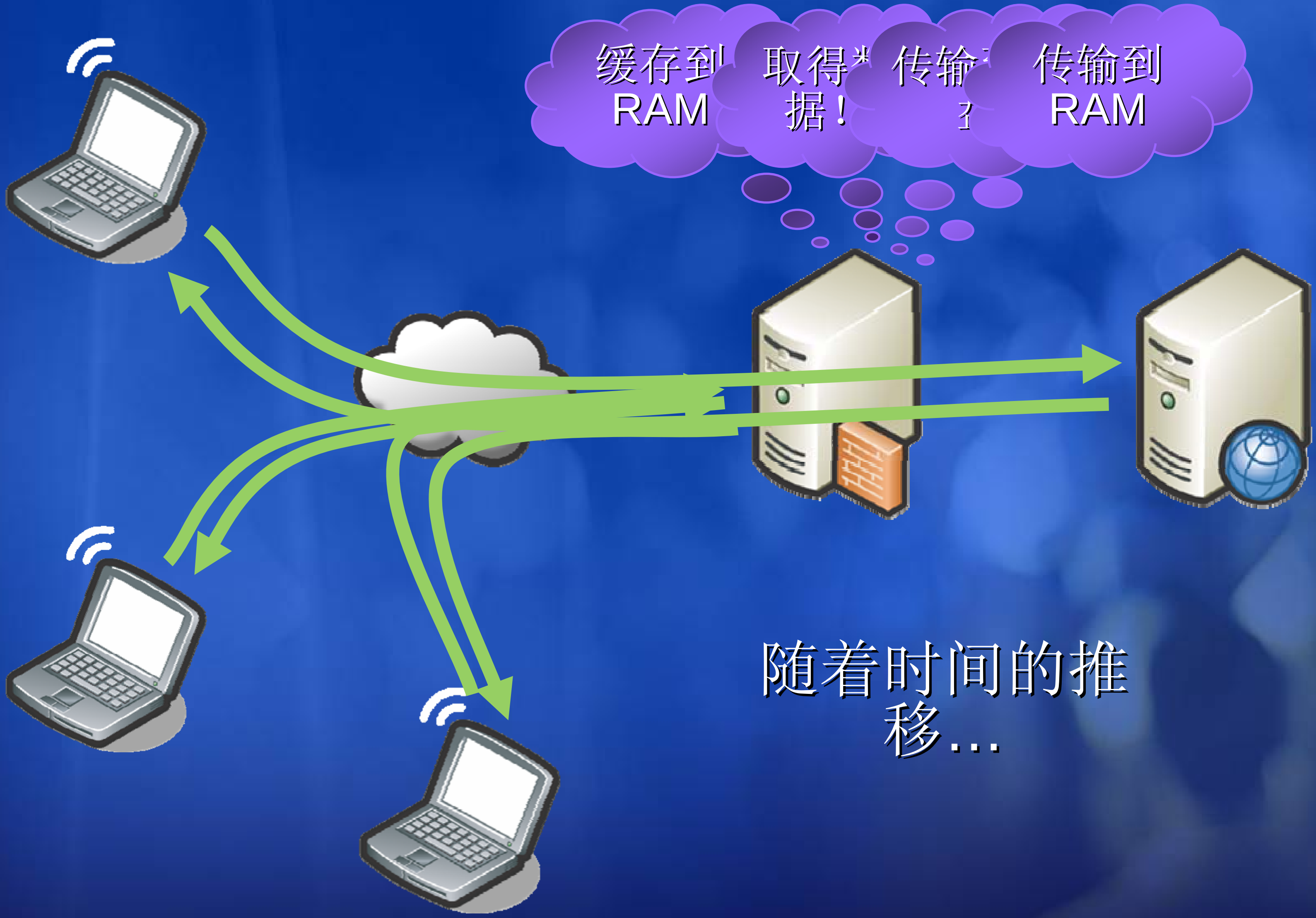


跟踪服务器状态

活动	服务器在添加时的正常状态；将接受传入请求
排空	完成进行中的请求；将接受任何新请求
停用	ISA Server 检测到服务器未响应时的自动安置
已删除	从阵列和从 UI 中删除；不接受任何请求

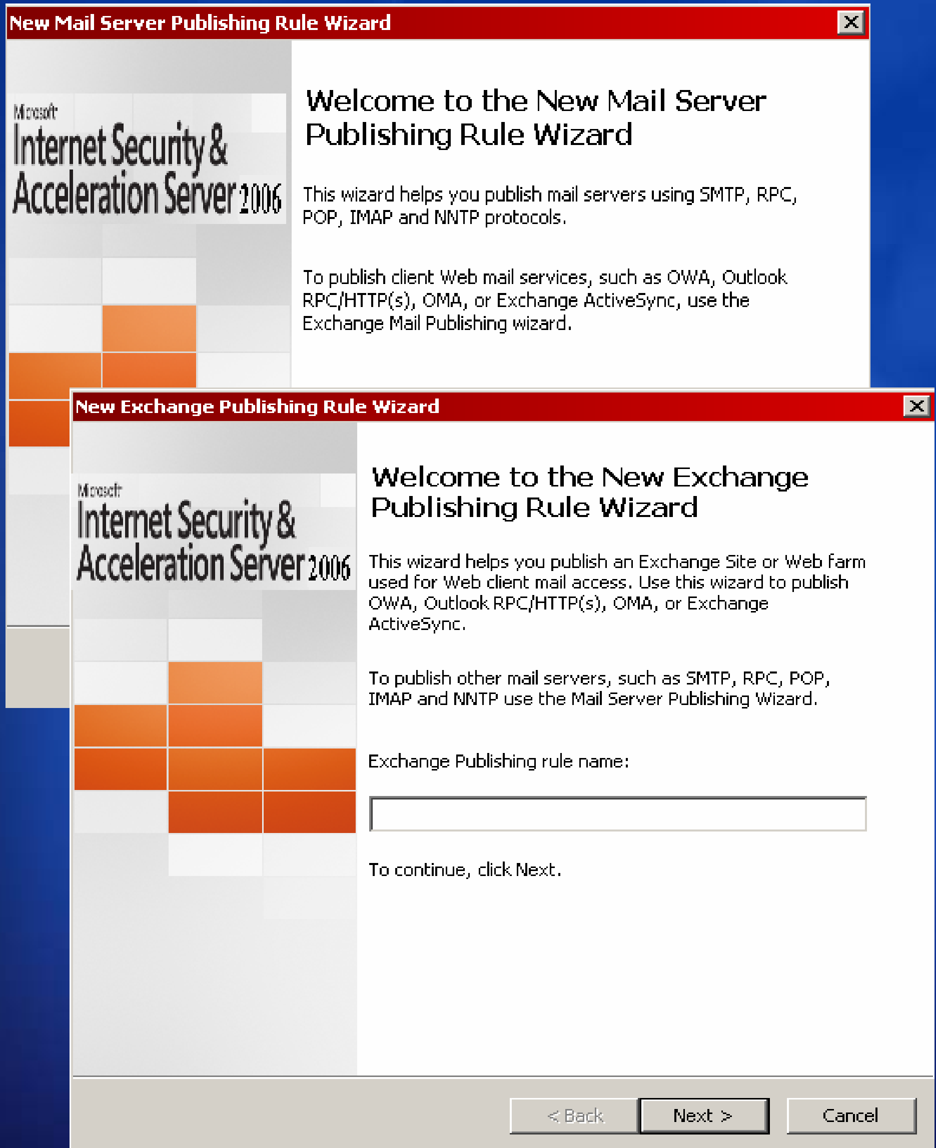
- 当故障服务器恢复时，它将接受新请求；先前的请求将保留在接管服务器上

逆向缓存



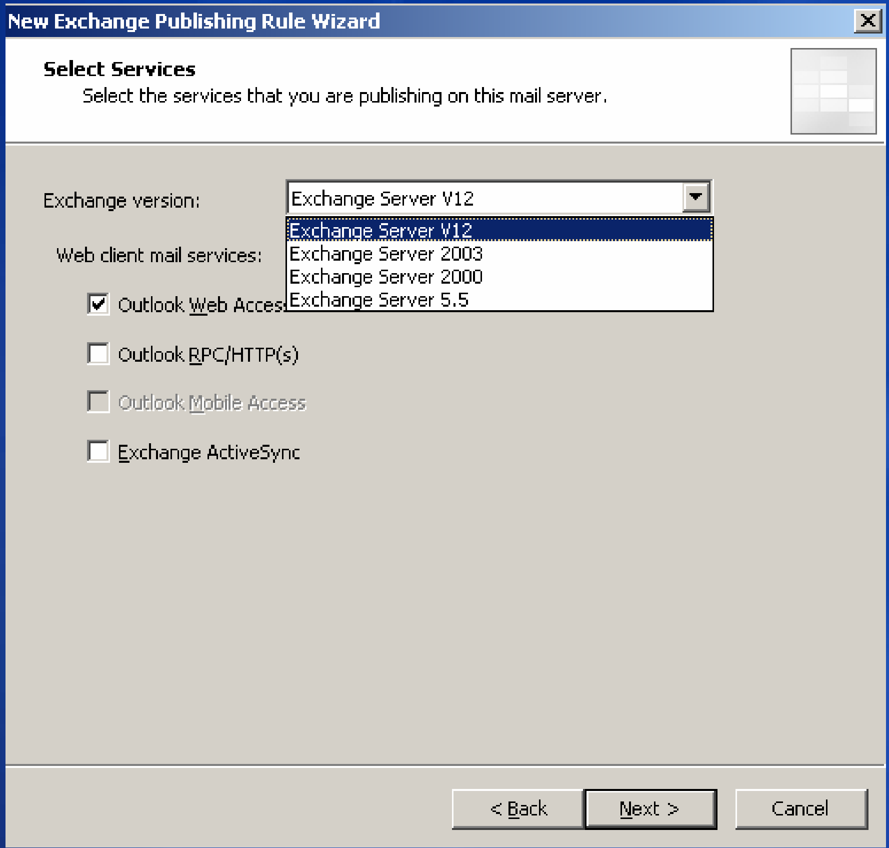
随着时间的推移…

发布邮件服务器



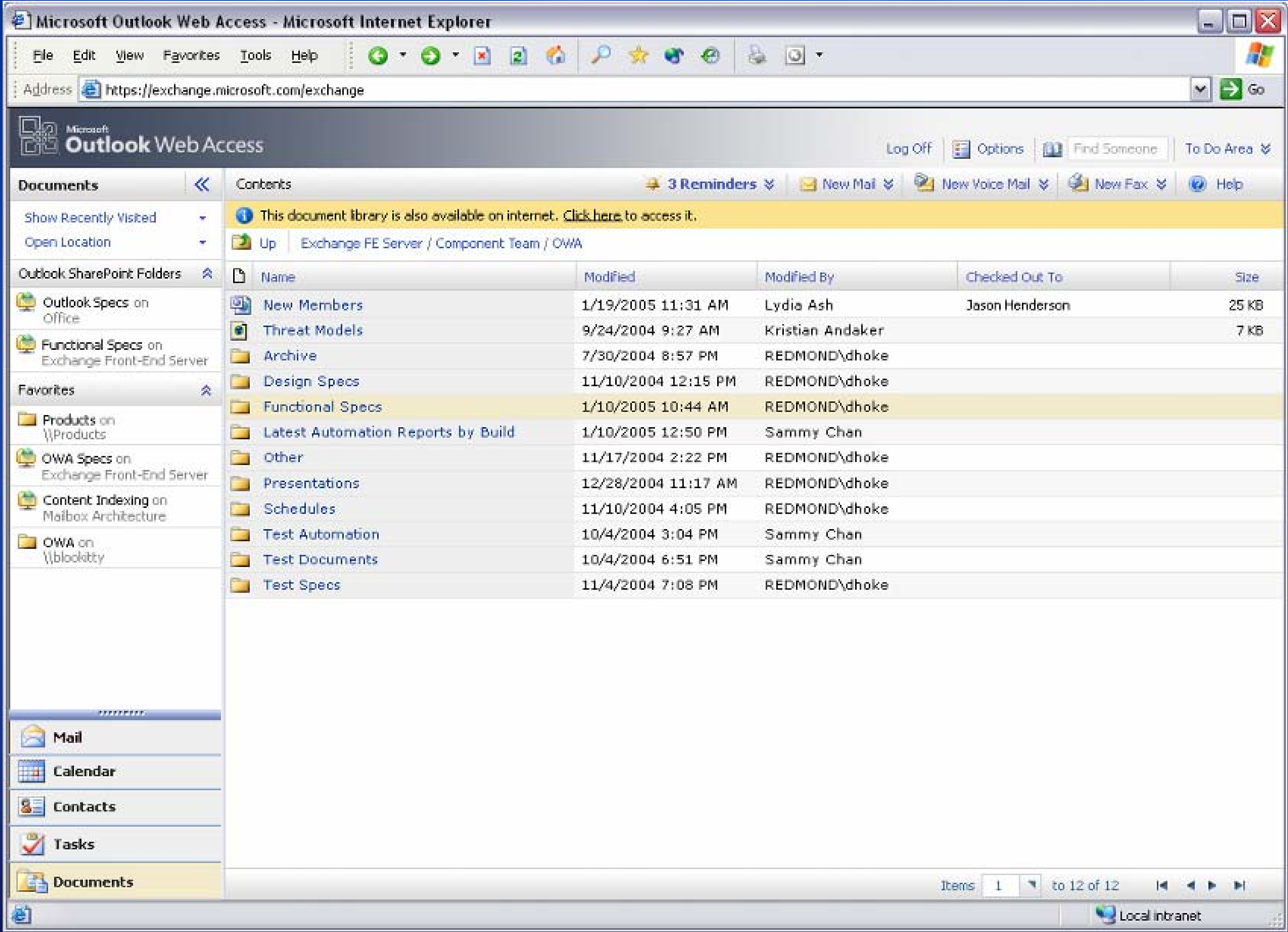
- 非 Web 访问
  - SMTP
  - RPC
  - POP-3
  - IMAP-4
  - NNTP
- Web 访问
  - OWA
  - RPC/HTTPS
  - OMA
  - EAS

Exchange 集成



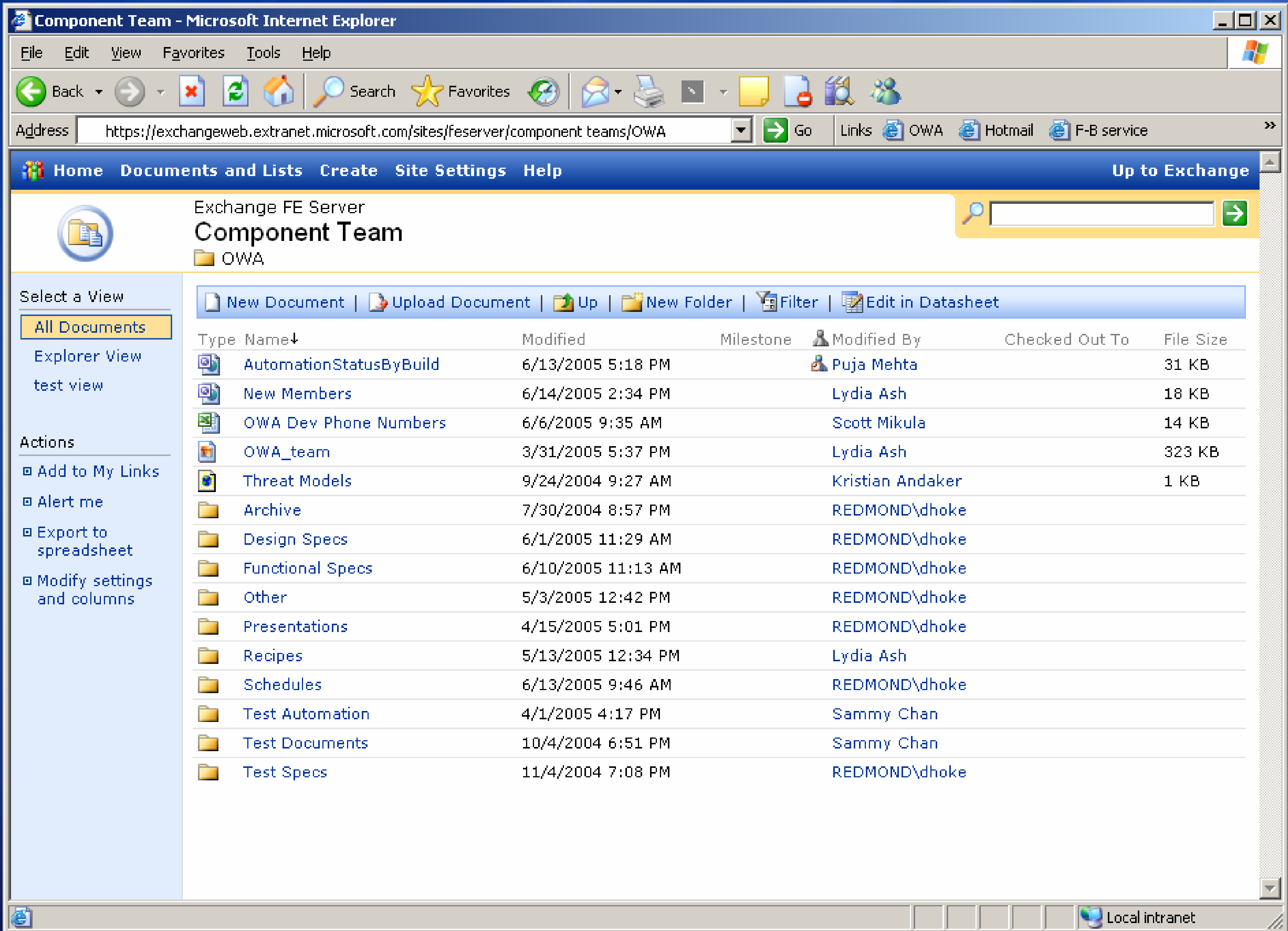
- 选择您正在使用的 Exchange 版本
  - 也适用于服务器场
- 选择方法
- 添加到 Exchange 12 时，ISA 2006 提供对以下资源的*完全*（而不只是*读取*）访问权限—
  - SharePoint 库
  - 网络共享
- 使用专用 OWA UI
  - 非 OWA 12 的“文档”选项卡

OWA 12



Microsoft Outlook Web Access - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://exchange.microsoft.com/exchange
Go
Outlook Web Access
Log Off
Options
Find Someone
To Do Area
Documents
Contents
3 Reminders
New Mail
New Voice Mail
New Fax
Help
Show Recently Visited
Open Location
This document library is also available on internet. Click here to access it.
Up
Exchange FE Server / Component Team / OWA
Outlook SharePoint Folders
Outlook Specs on Office
Functional Specs on Exchange Front-End Server
Favorites
Products on \\Products
OWA Specs on Exchange Front-End Server
Content Indexing on Mailbox Architecture
OWA on \\blookitty
Name
Modified
Modified By
Checked Out To
Size
New Members 1/19/2005 11:31 AM Lydia Ash Jason Henderson 25 KB
Threat Models 9/24/2004 9:27 AM Kristian Andaker 7 KB
Archive 7/30/2004 8:57 PM REDMOND\dhoke
Design Specs 11/10/2004 12:15 PM REDMOND\dhoke
Functional Specs 1/10/2005 10:44 AM REDMOND\dhoke
Latest Automation Reports by Build 1/10/2005 12:50 PM Sammy Chan
Other 11/17/2004 2:22 PM REDMOND\dhoke
Presentations 12/28/2004 11:17 AM REDMOND\dhoke
Schedules 11/10/2004 4:05 PM REDMOND\dhoke
Test Automation 10/4/2004 3:04 PM Sammy Chan
Test Documents 10/4/2004 6:51 PM Sammy Chan
Test Specs 11/4/2004 7:08 PM REDMOND\dhoke
Mail
Calendar
Contacts
Tasks
Documents
Items 1 to 12 of 12
Local intranet

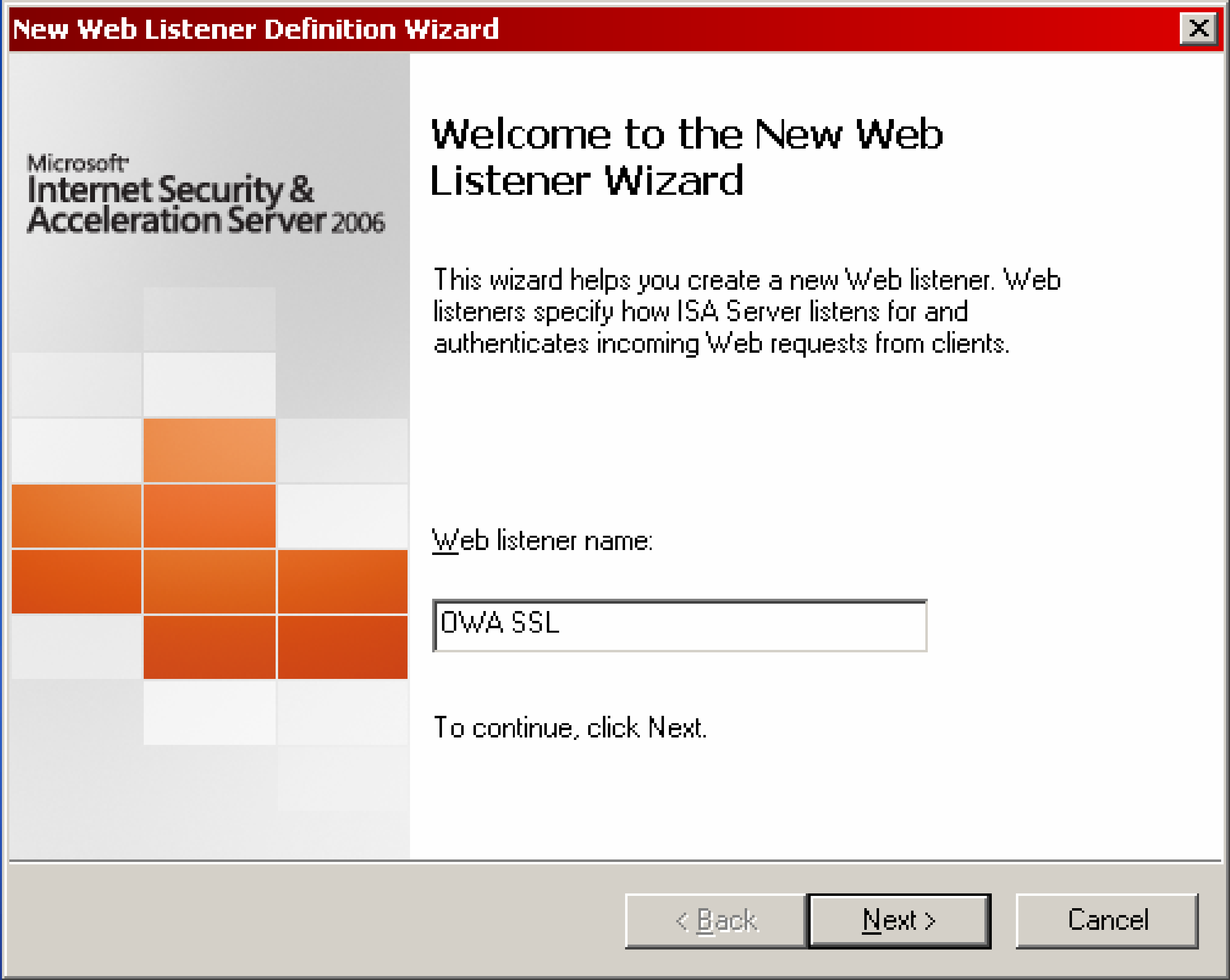
通过 ISA 2006 看到的 OWA 12



发布示例

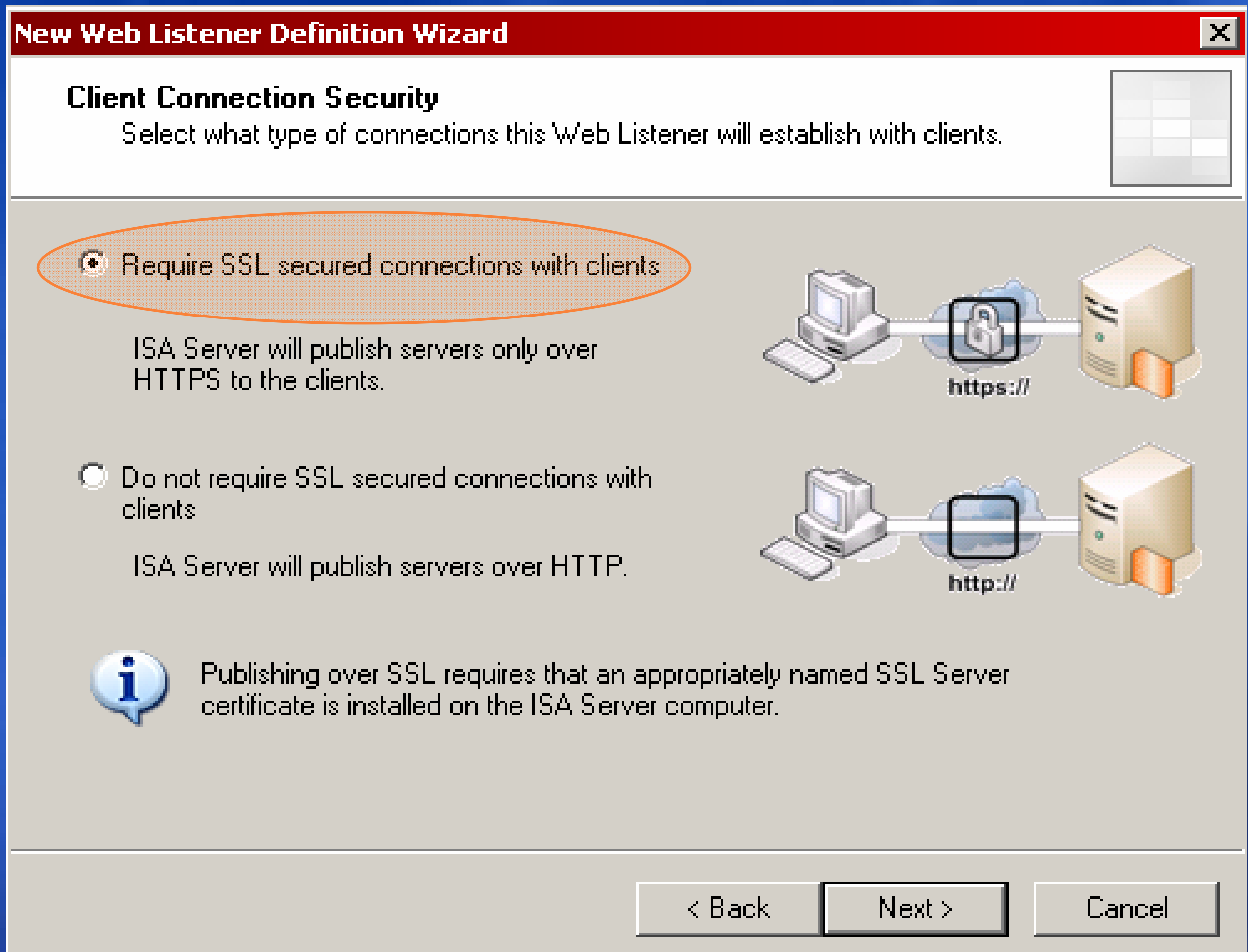
> 构建 HTTPS 侦听器

1



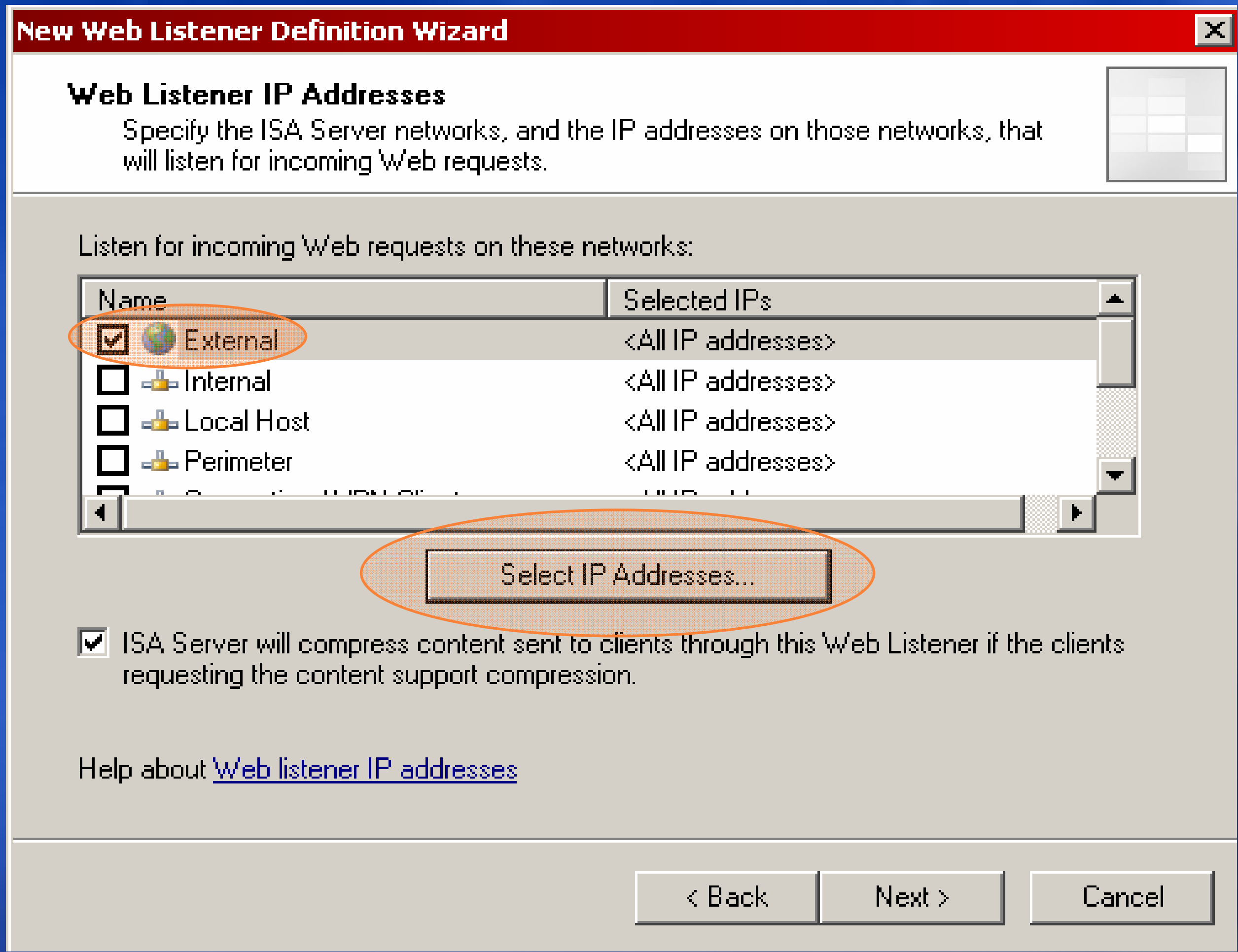
> 构建 HTTPS 侦听器

2



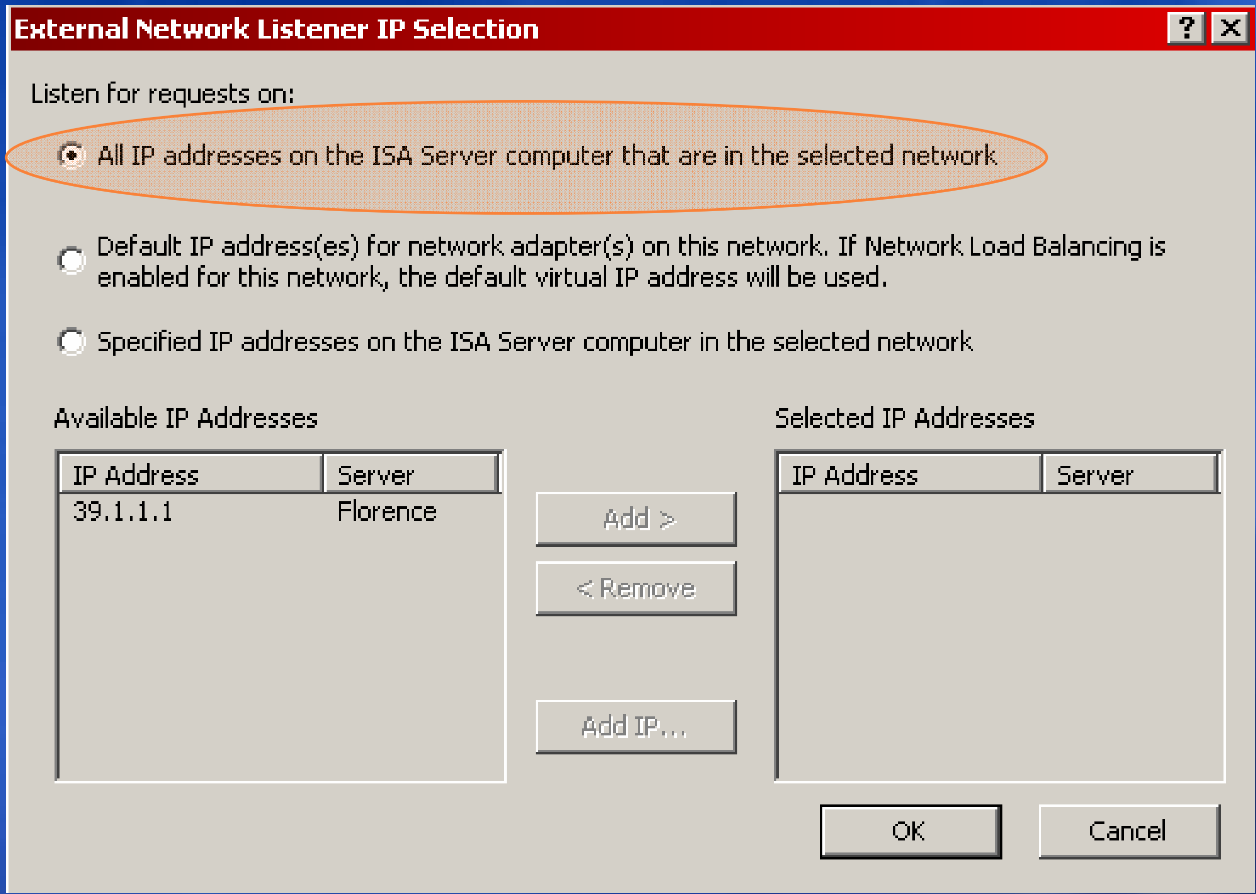
> 构建 HTTPS 侦听器

3

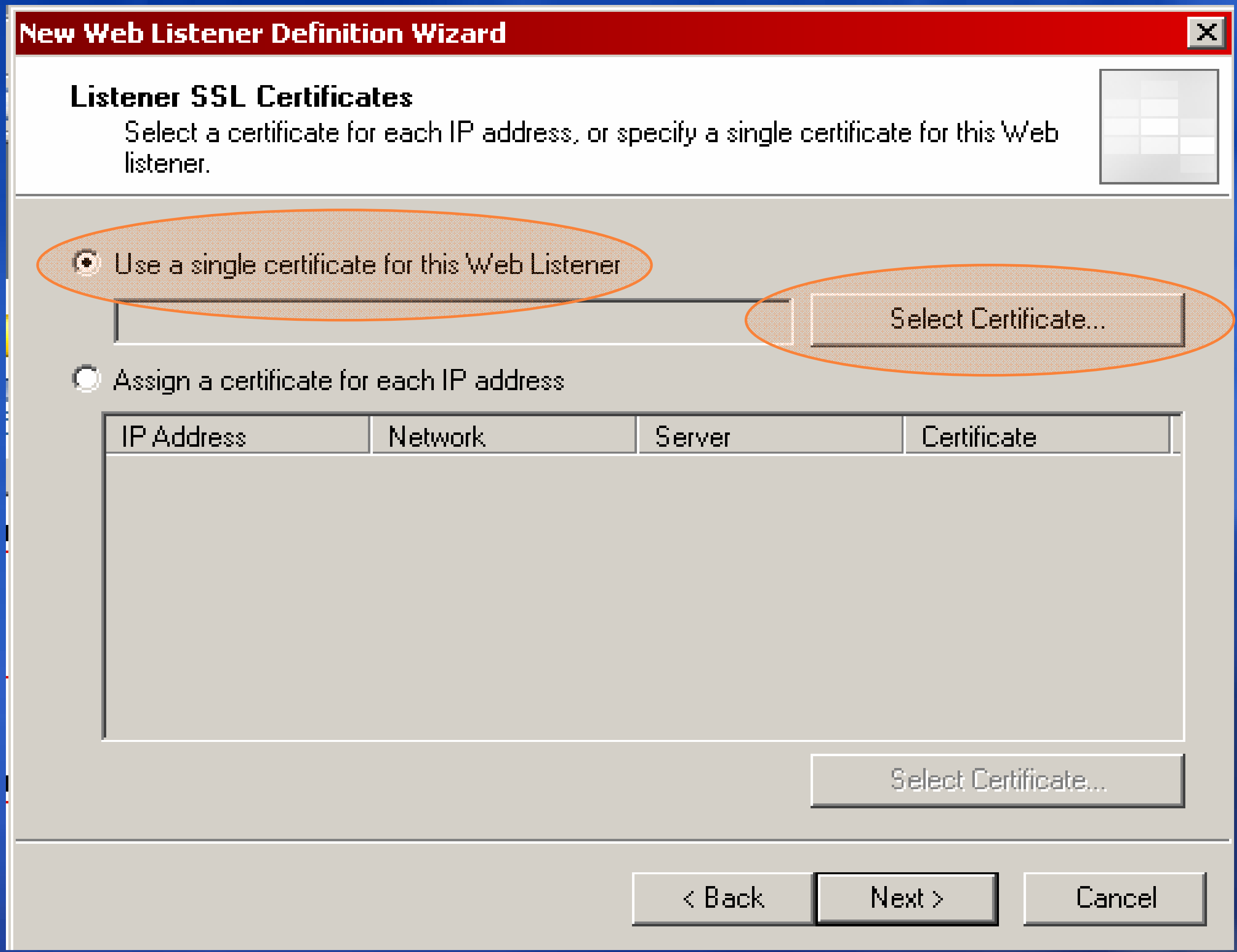


>构建 HTTPS 侦听器

4

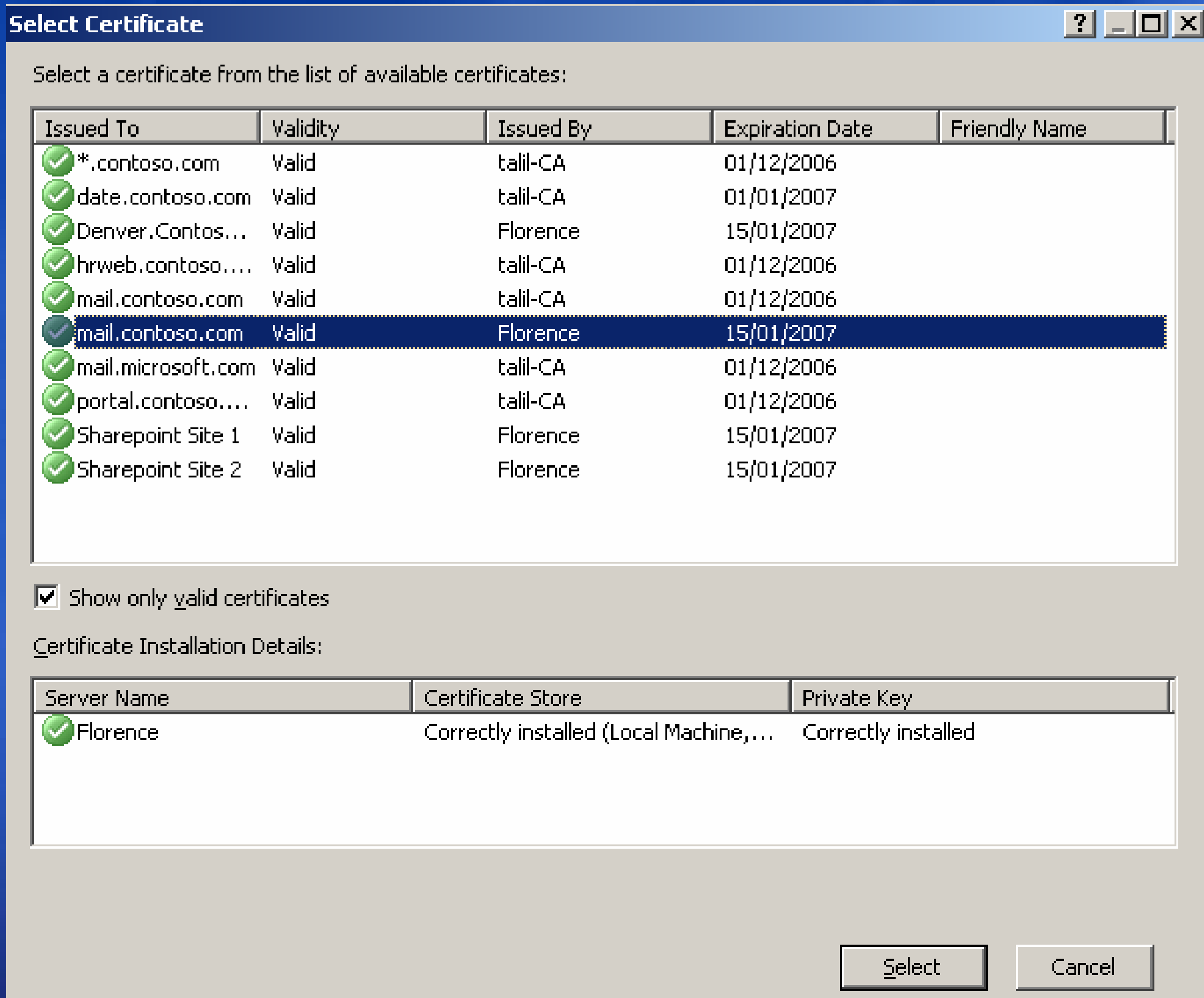


>构建 HTTPS 侦听器


New Web Listener Definition Wizard
Listener SSL Certificates
Select a certificate for each IP address, or specify a single certificate for this Web listener.
Use a single certificate for this Web Listener
Select Certificate...
Assign a certificate for each IP address
IP Address
Network
Server
Certificate
Select Certificate...
< Back
Next >
Cancel

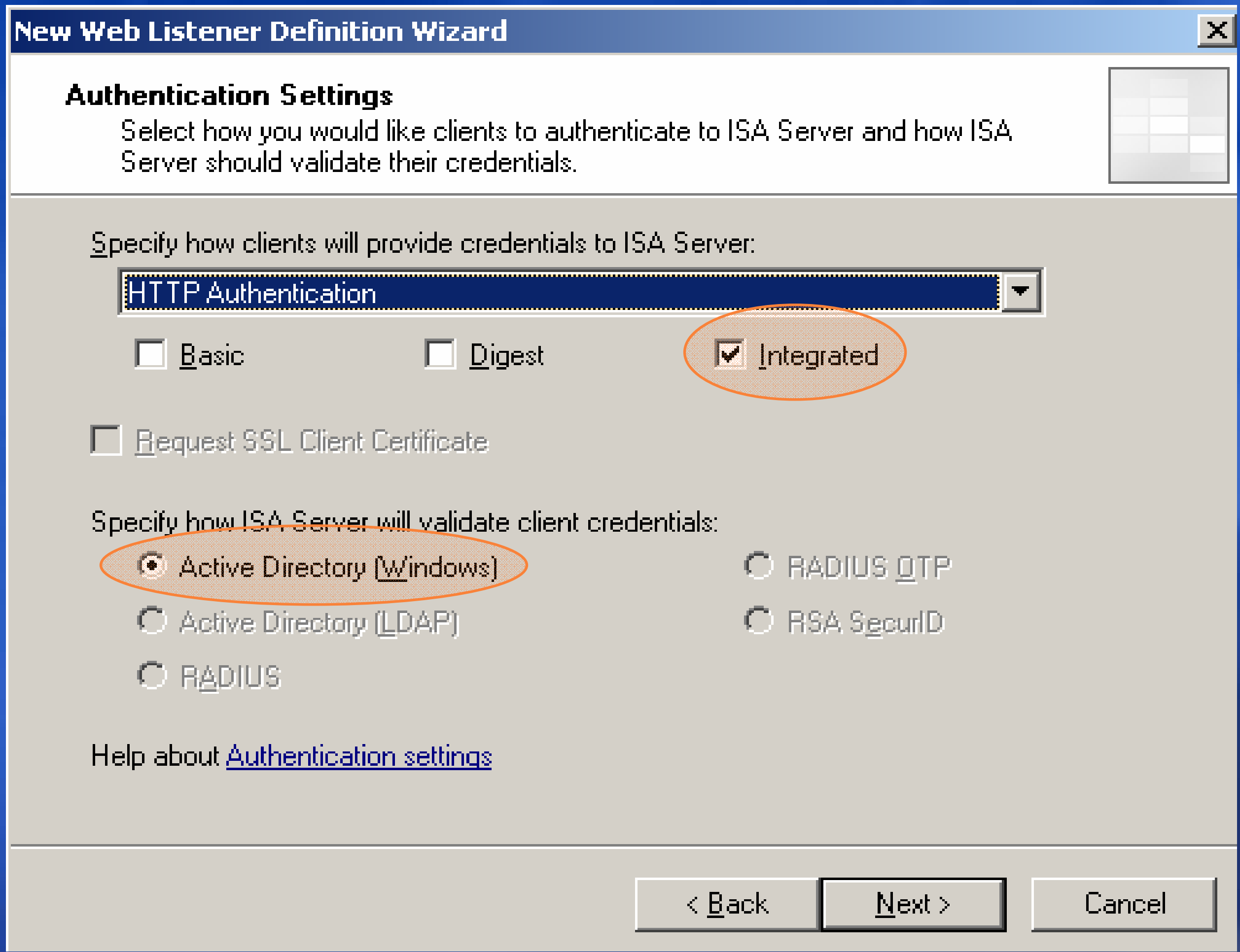
>构建 HTTPS 侦听器

6



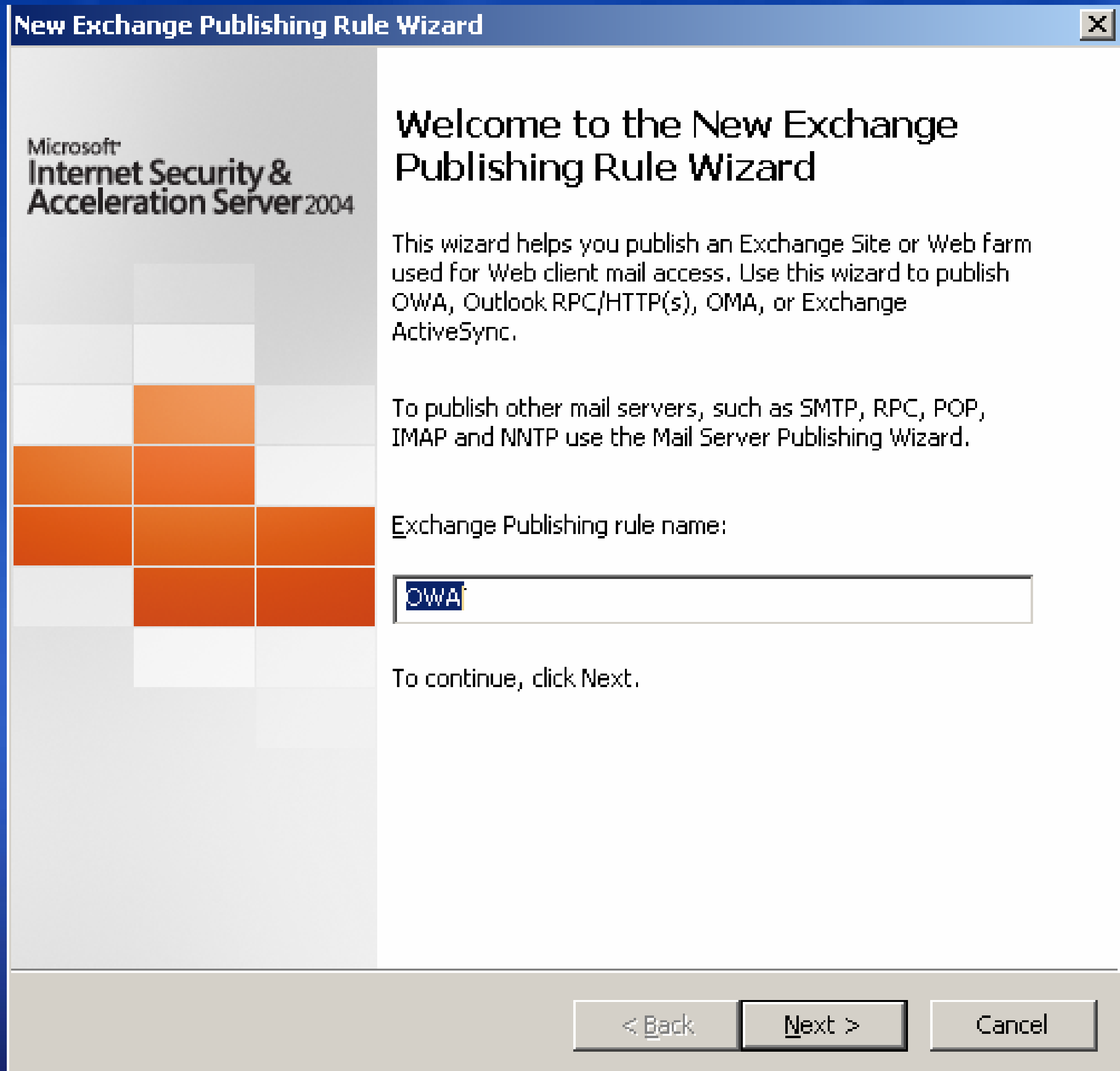
>构建 HTTPS 侦听器

完成



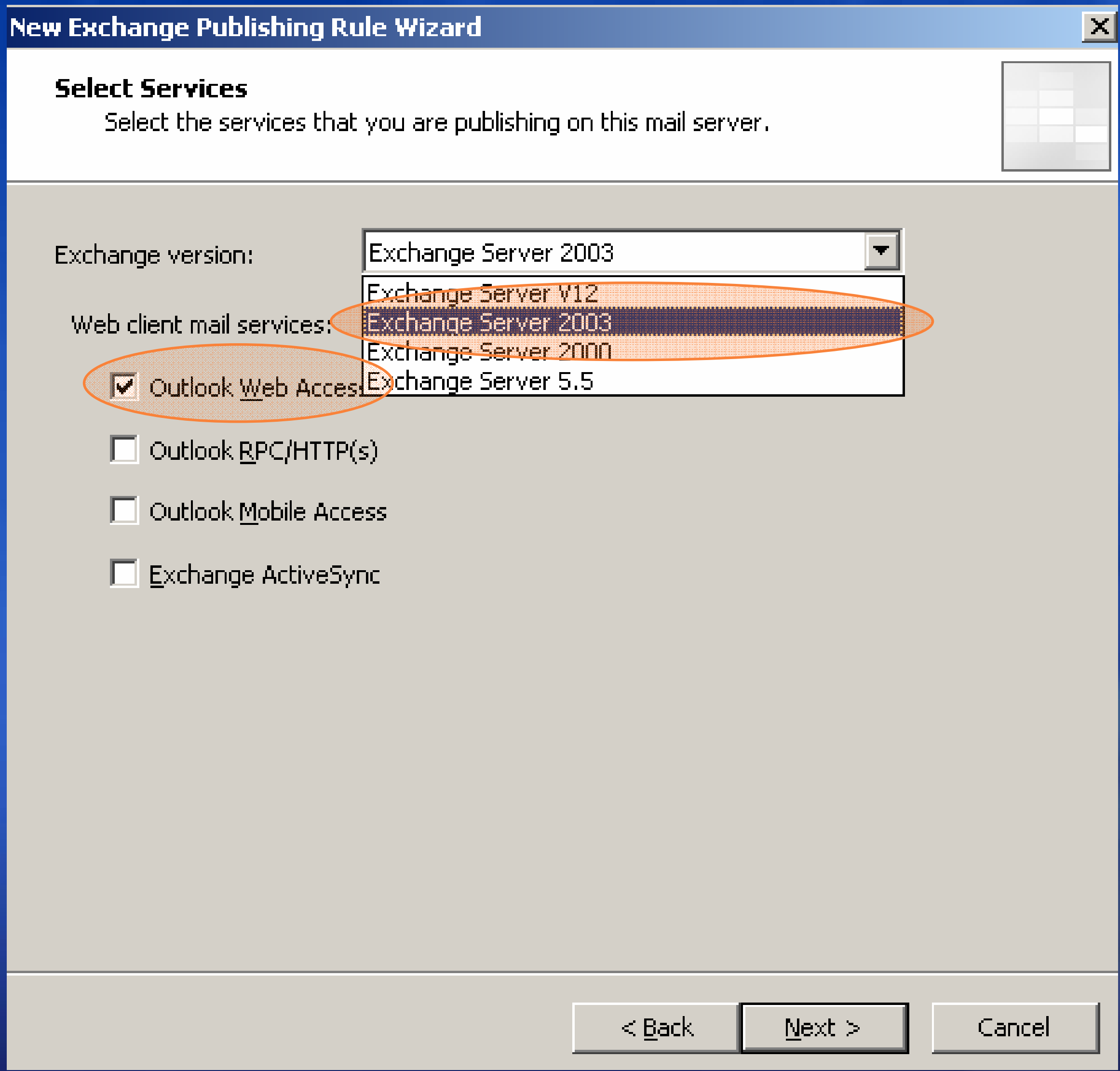
> 发布 Exchange web

1



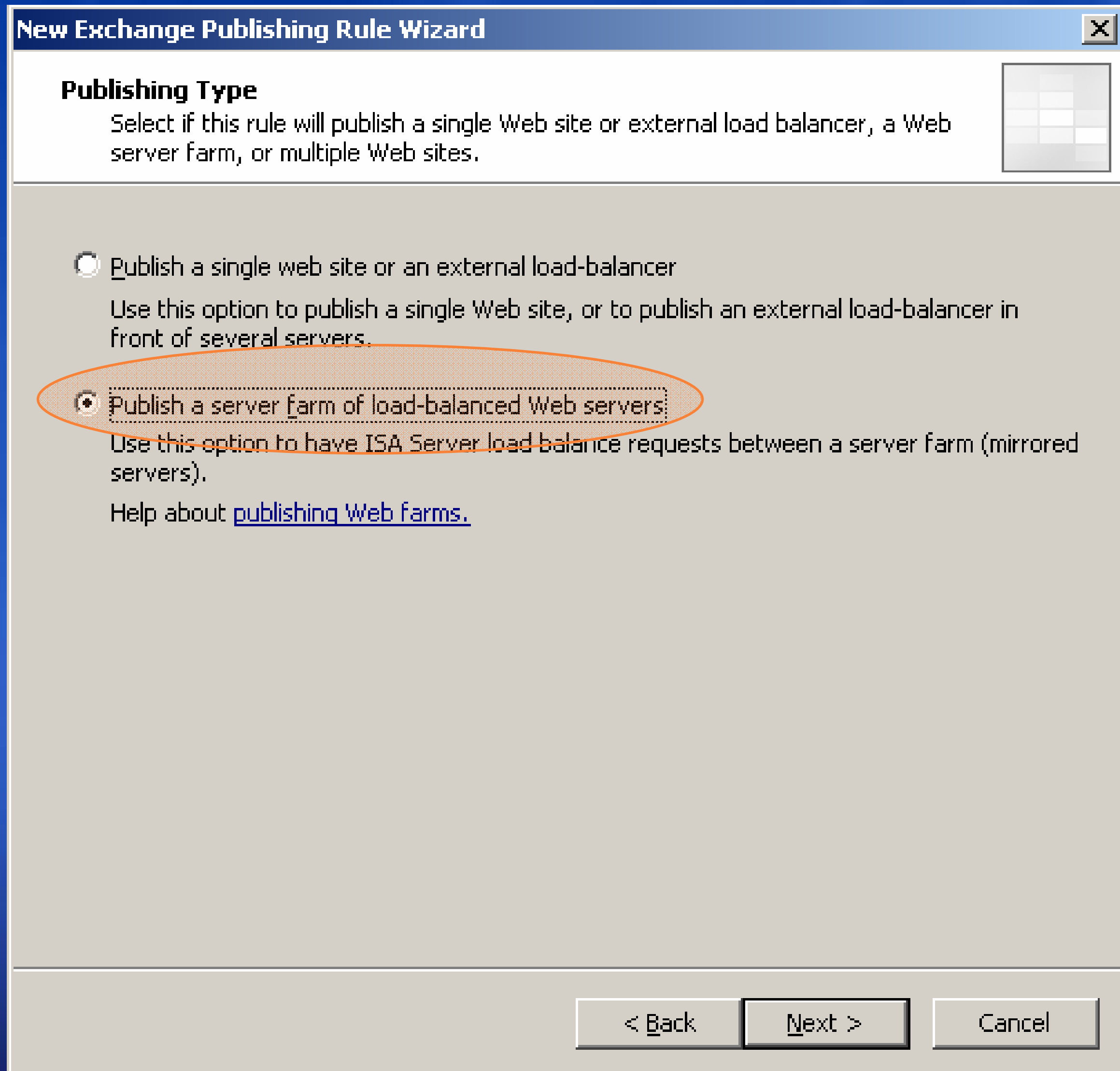
> 发布 Exchange web

2



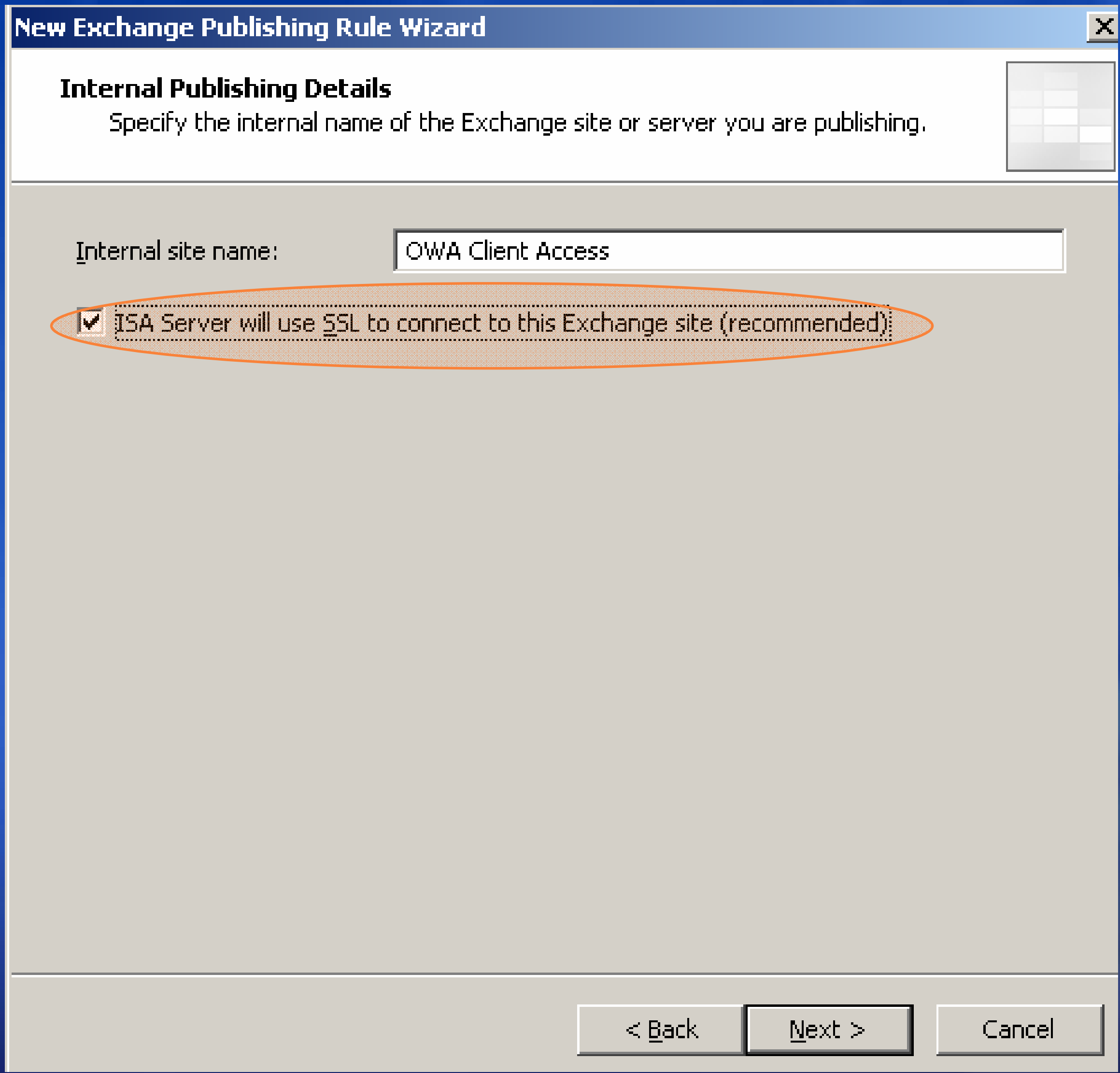
> 发布 Exchange web

3



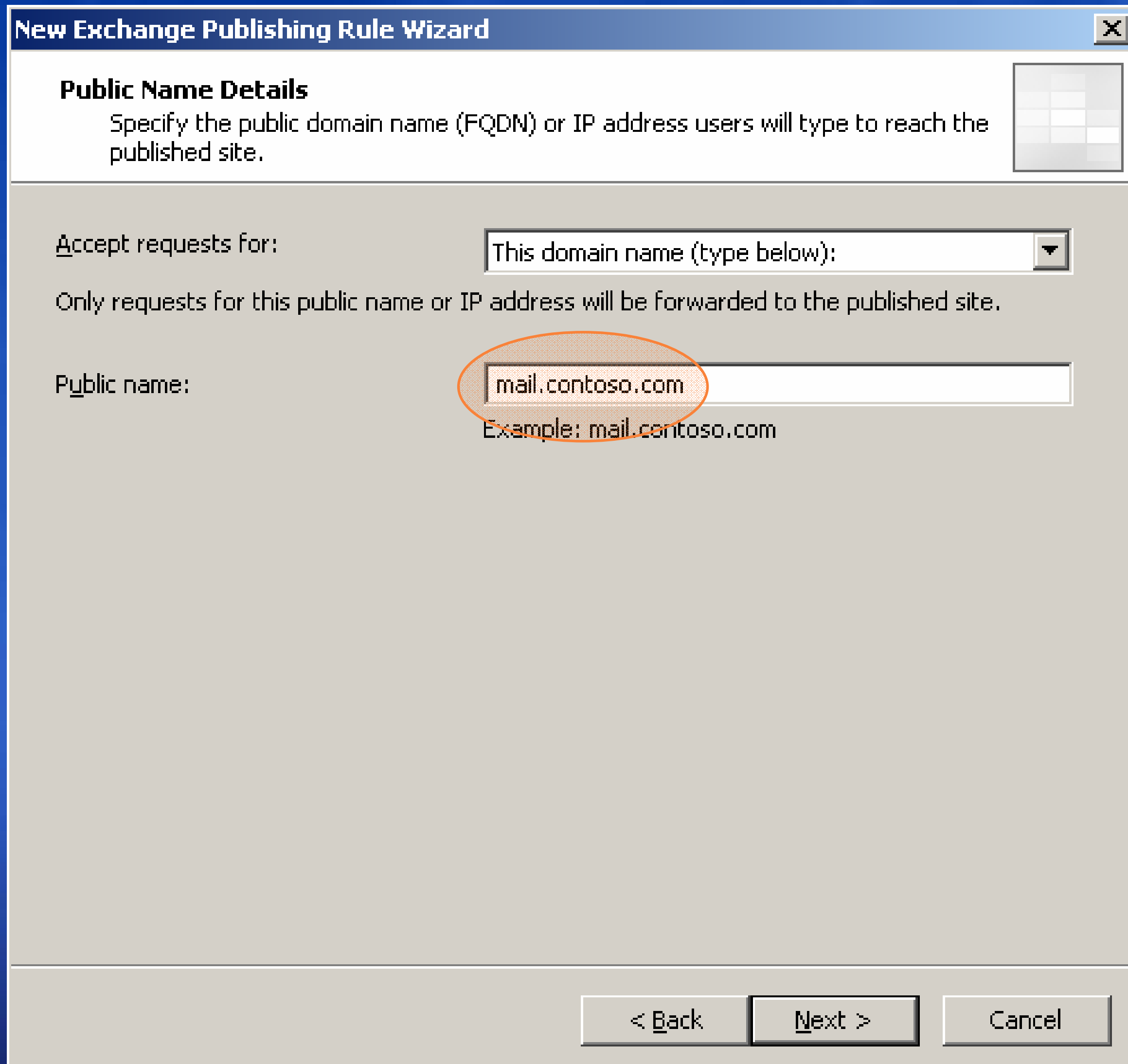
> 发布 Exchange web

4



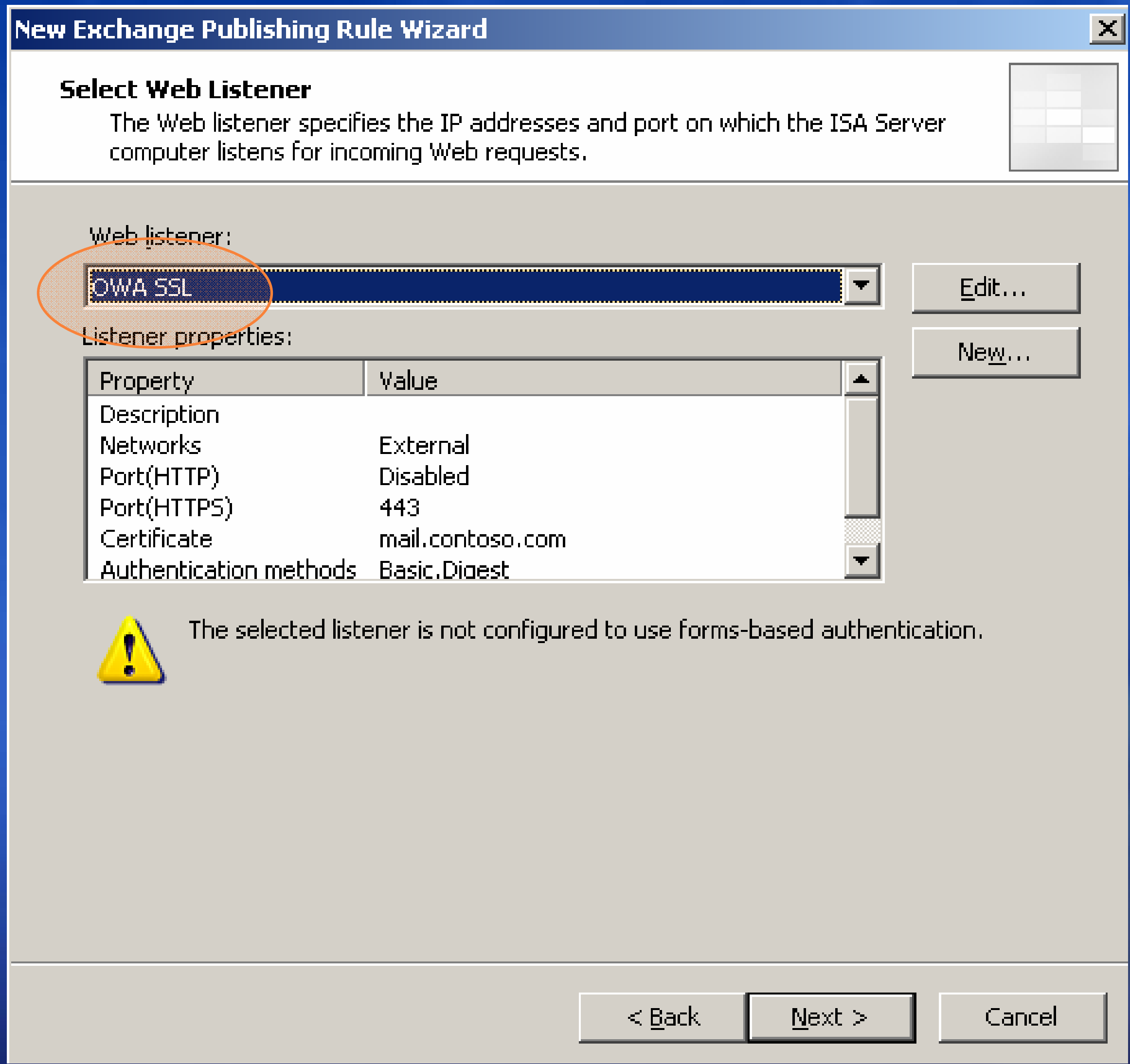
> 发布 Exchange web

5

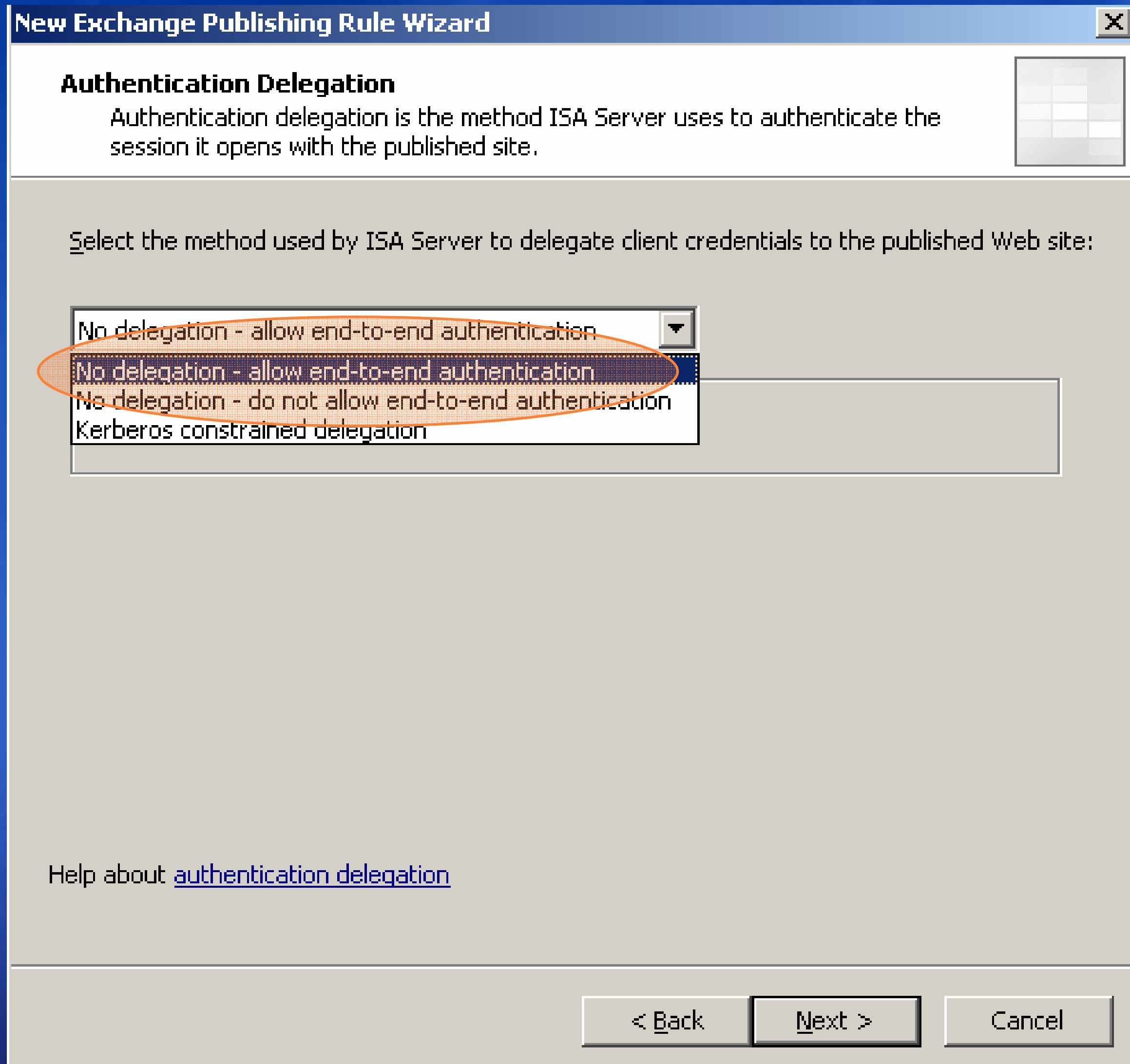


> 发布 Exchange web

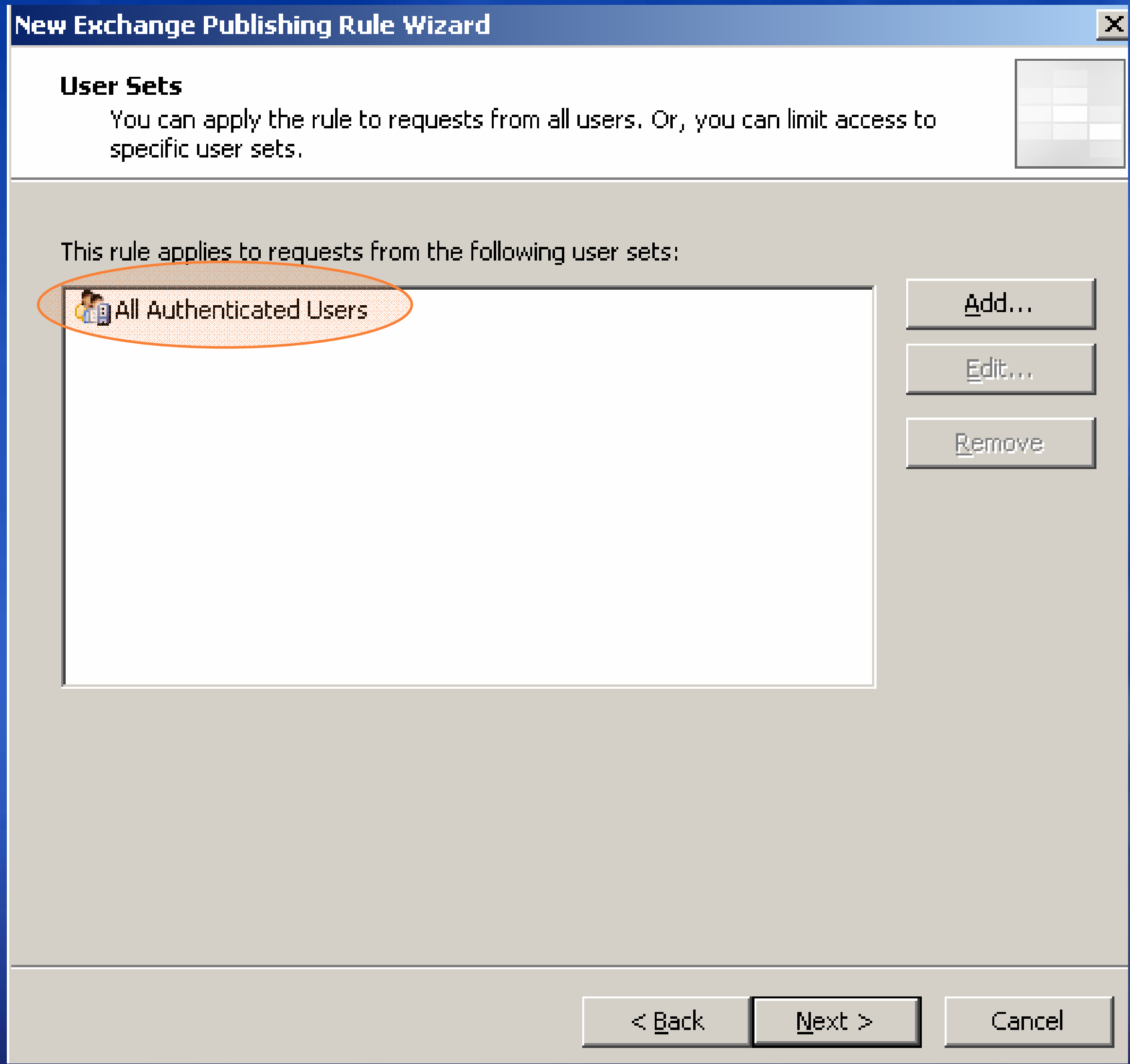
6



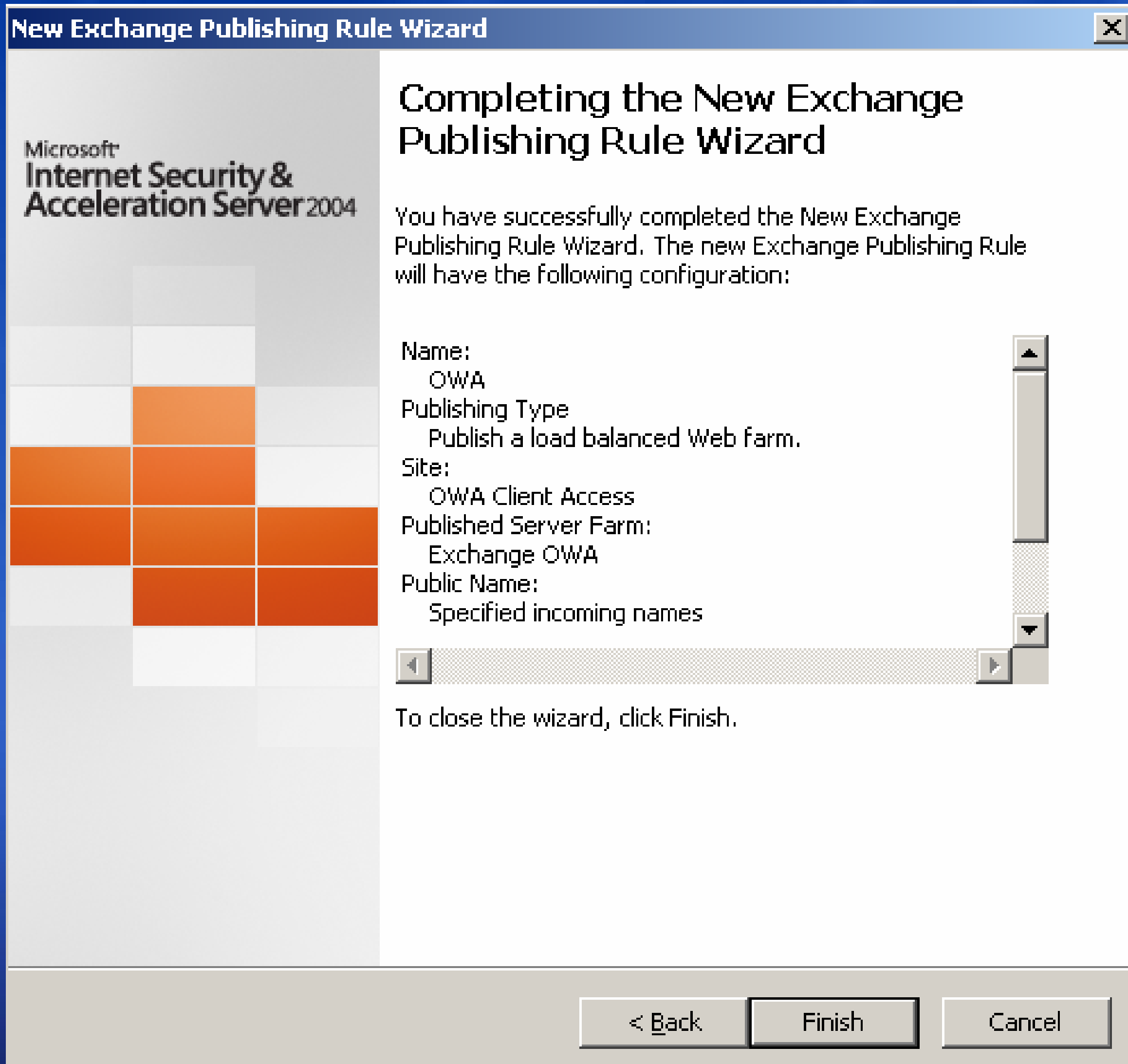
> 发布 Exchange web



> 发布 Exchange web

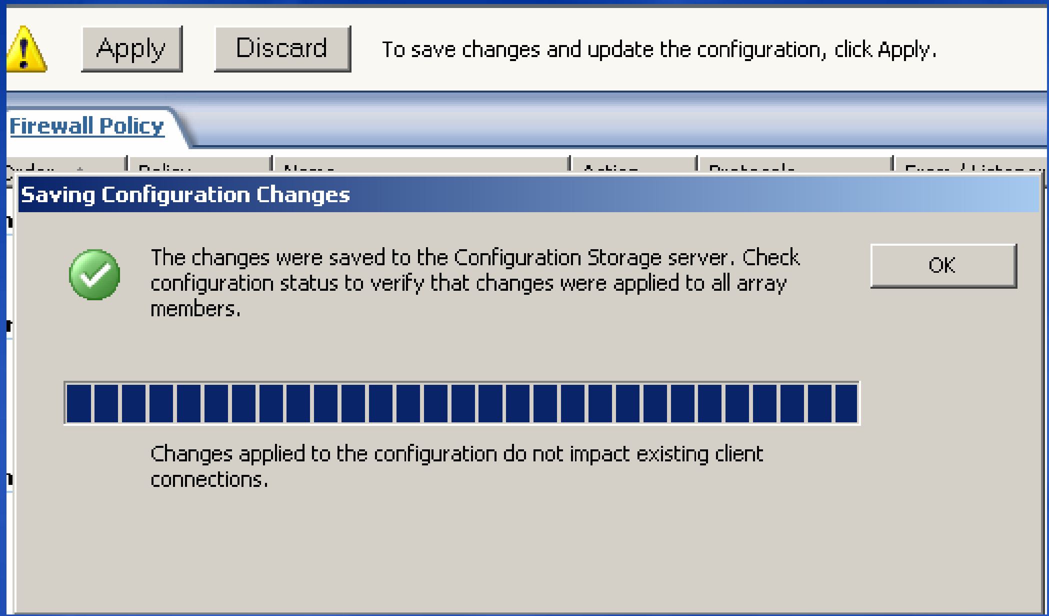


> 发布 Exchange web



> 发布 Exchange web

完成



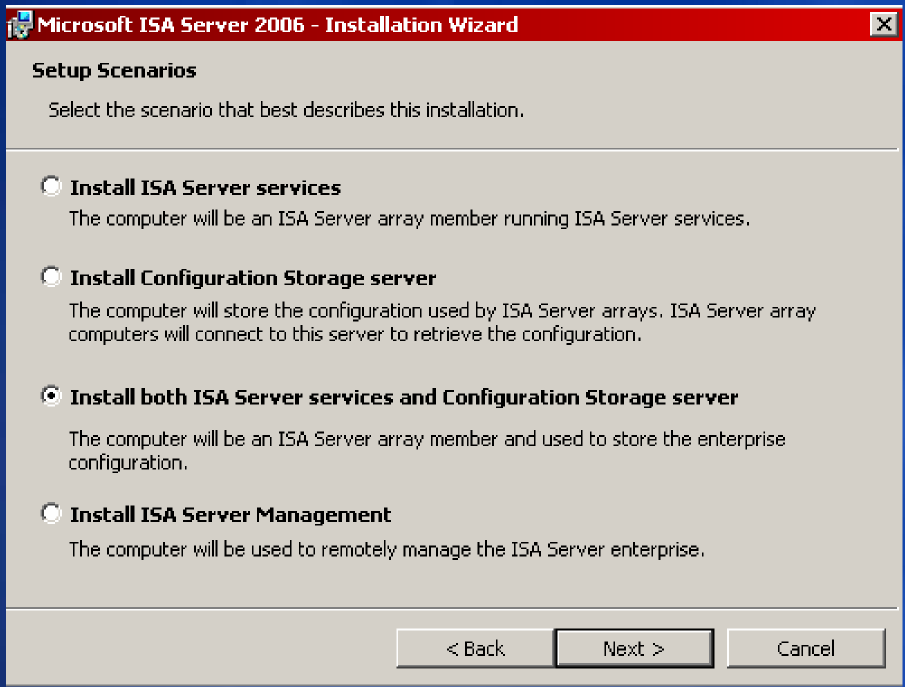
分支机构网关

按数量

30%	拥有远程分支机构的企业
33%	它们消耗的 IT 预算额度
$25,000,000,000	员工超过 1000 人的企业的 WAN 开支
55%	分支机构员工超过 1000 人的企业
0	分支机构 IT 团队的典型规模

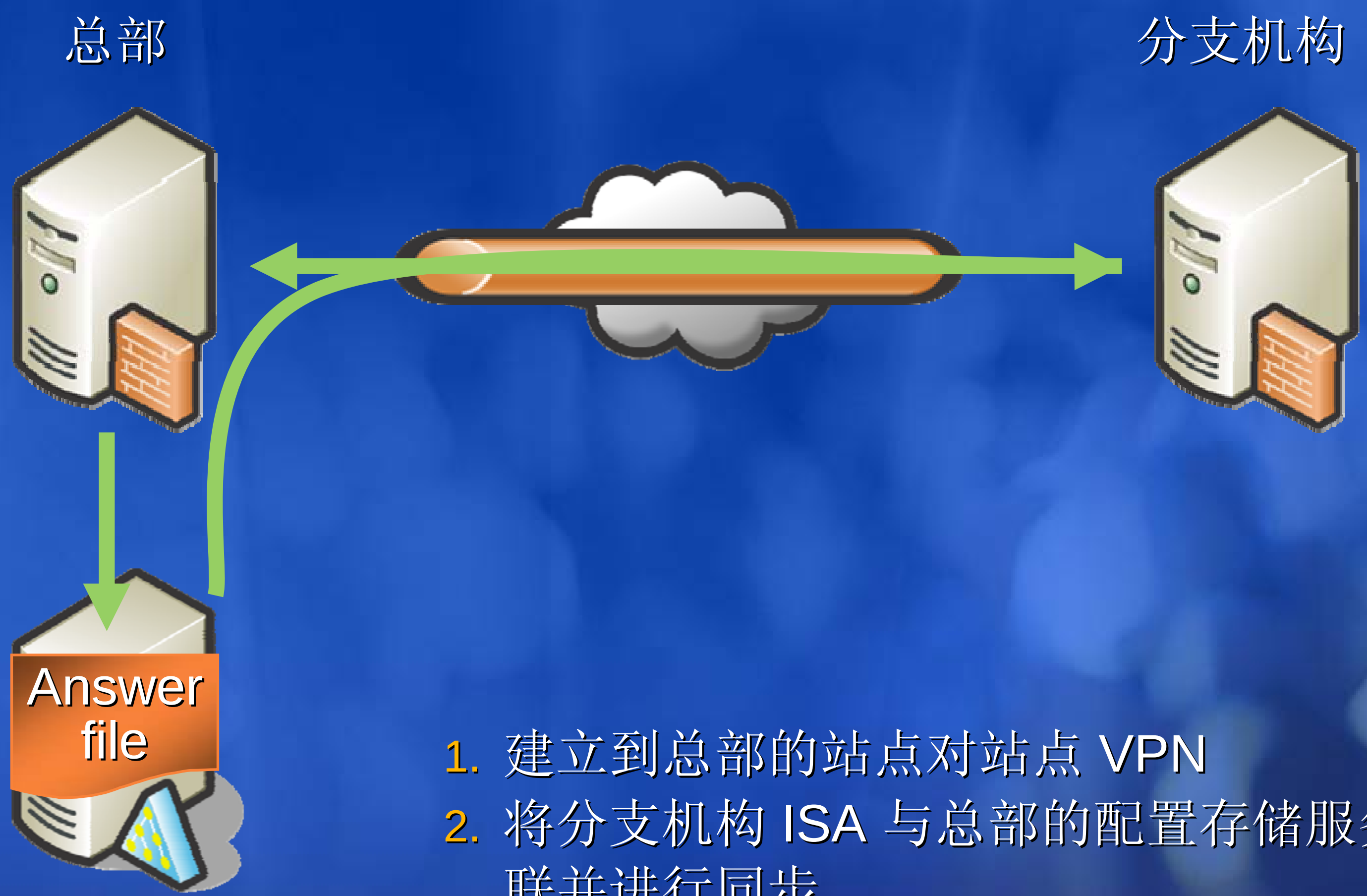
Harte-Hanks 2004; AMI Partners 2003

配置存储服务器



- ADAM 的实例
  - 通过 LDAP 协议访问的目录
  - 无 DNS，无 Windows 域
- 安装详细信息
  - 在 ISA、域或工作组计算机上
  - 必须是域成员才能进行多主复制
  - 任何数量的阵列
  - 可以在多个服务器之间分布
- 由 ISA 管理单元管理
  - AD 和 LDAP 工具也适用
- 大块的配置读取
  - 传播单个更改的时间少于 1 分钟
  - 完全复制时间为 20-30 分钟

分支机构向导



1. 建立到总部的站点对站点 VPN
2. 将分支机构 ISA 与总部的配置存储服务器关联并进行同步
3. 将分支机构 ISA 加入指定的阵列

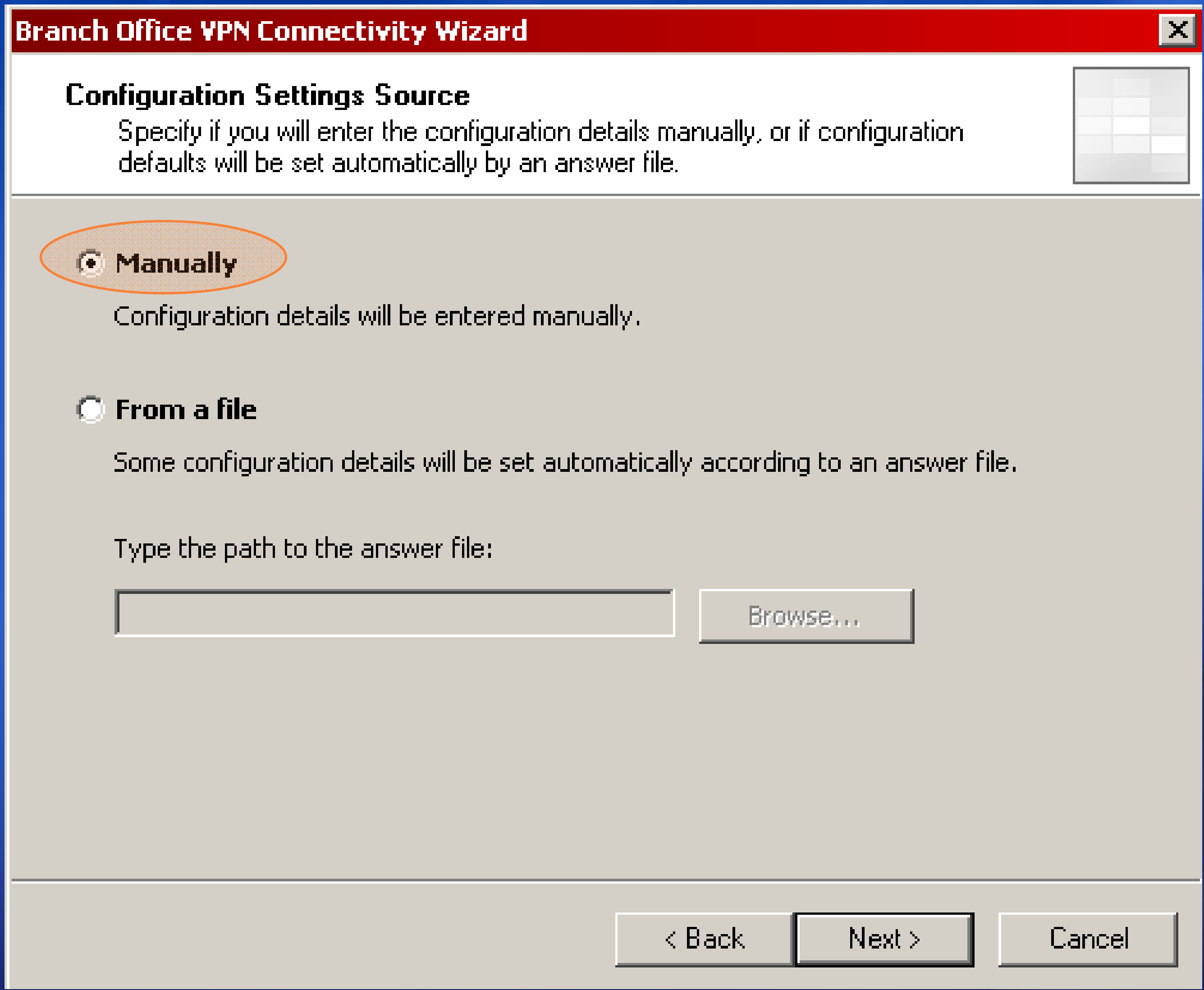
运行该向导

1

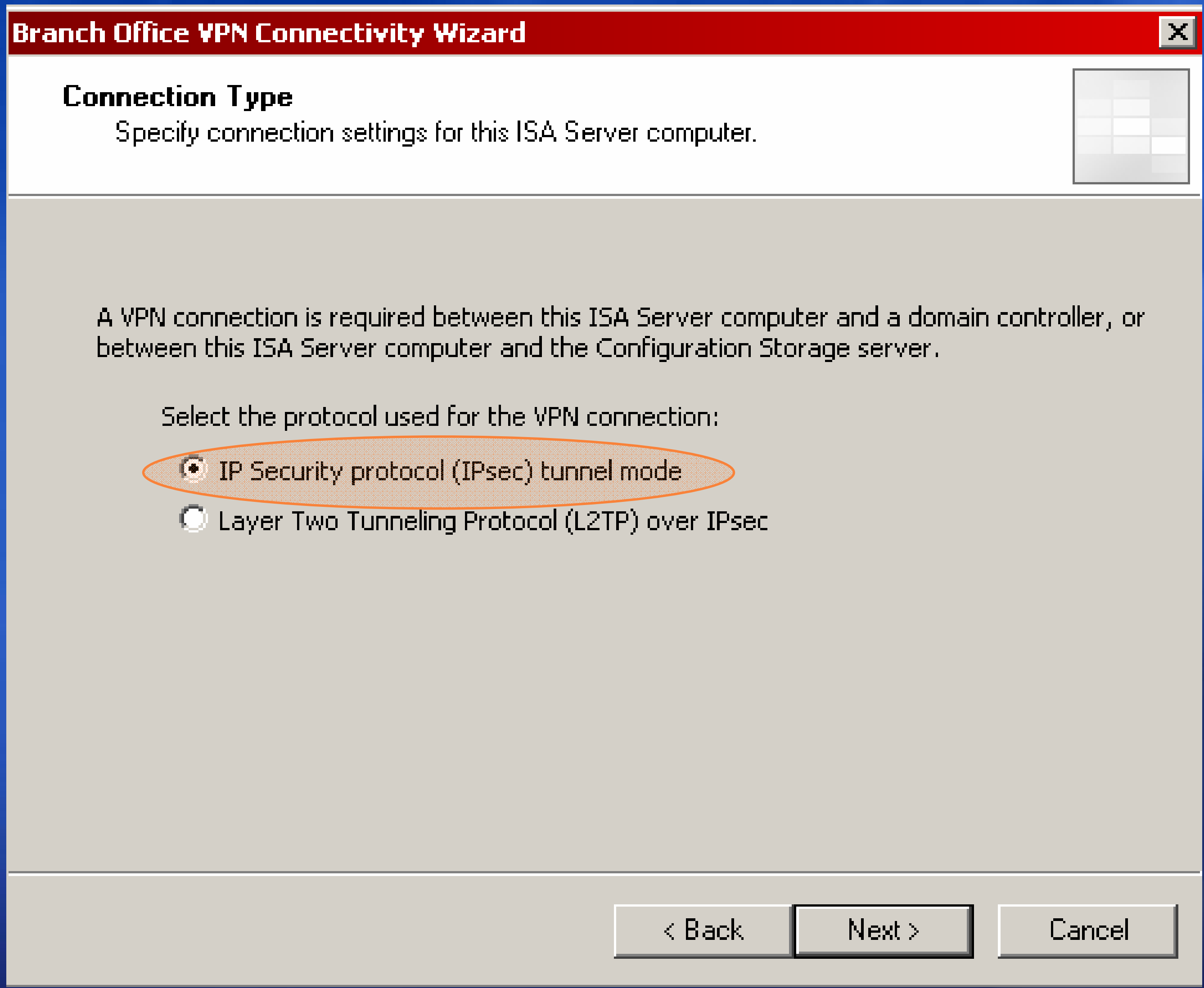

Branch Office VPN Connectivity Wizard
Microsoft
Internet Security & Acceleration Server 2004
Welcome to the ISA Server Branch Office VPN Connectivity Wizard
This wizard helps you configure a VPN connection between this branch office and a remote VPN site. Complete this wizard to create the VPN connection, and configure this computer as an ISA Server array member connected to an ISA Server Configuration Storage server.
To continue, click Next.
< Back
Next >
Cancel

>运行该向导

2

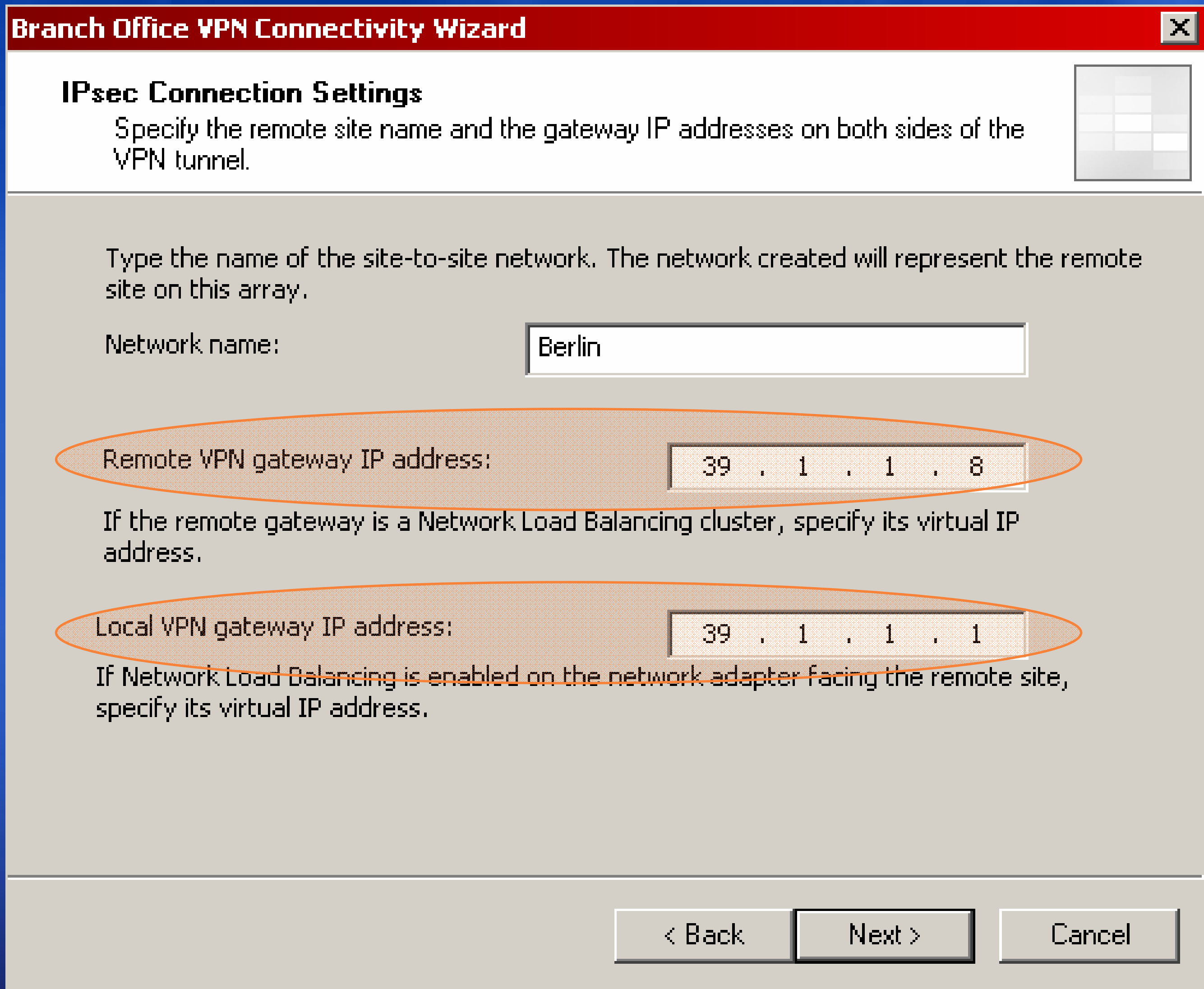

Branch Office VPN Connectivity Wizard
Configuration Settings Source
Specify if you will enter the configuration details manually, or if configuration defaults will be set automatically by an answer file.
Manually
Configuration details will be entered manually.
From a file
Some configuration details will be set automatically according to an answer file.
Type the path to the answer file:
Browse...
< Back
Next >
Cancel

>运行该向导


Branch Office VPN Connectivity Wizard
Connection Type
Specify connection settings for this ISA Server computer.
A VPN connection is required between this ISA Server computer and a domain controller, or between this ISA Server computer and the Configuration Storage server.
Select the protocol used for the VPN connection:
IP Security protocol (IPsec) tunnel mode
Layer Two Tunneling Protocol (L2TP) over IPsec
< Back
Next >
Cancel

>运行该向导

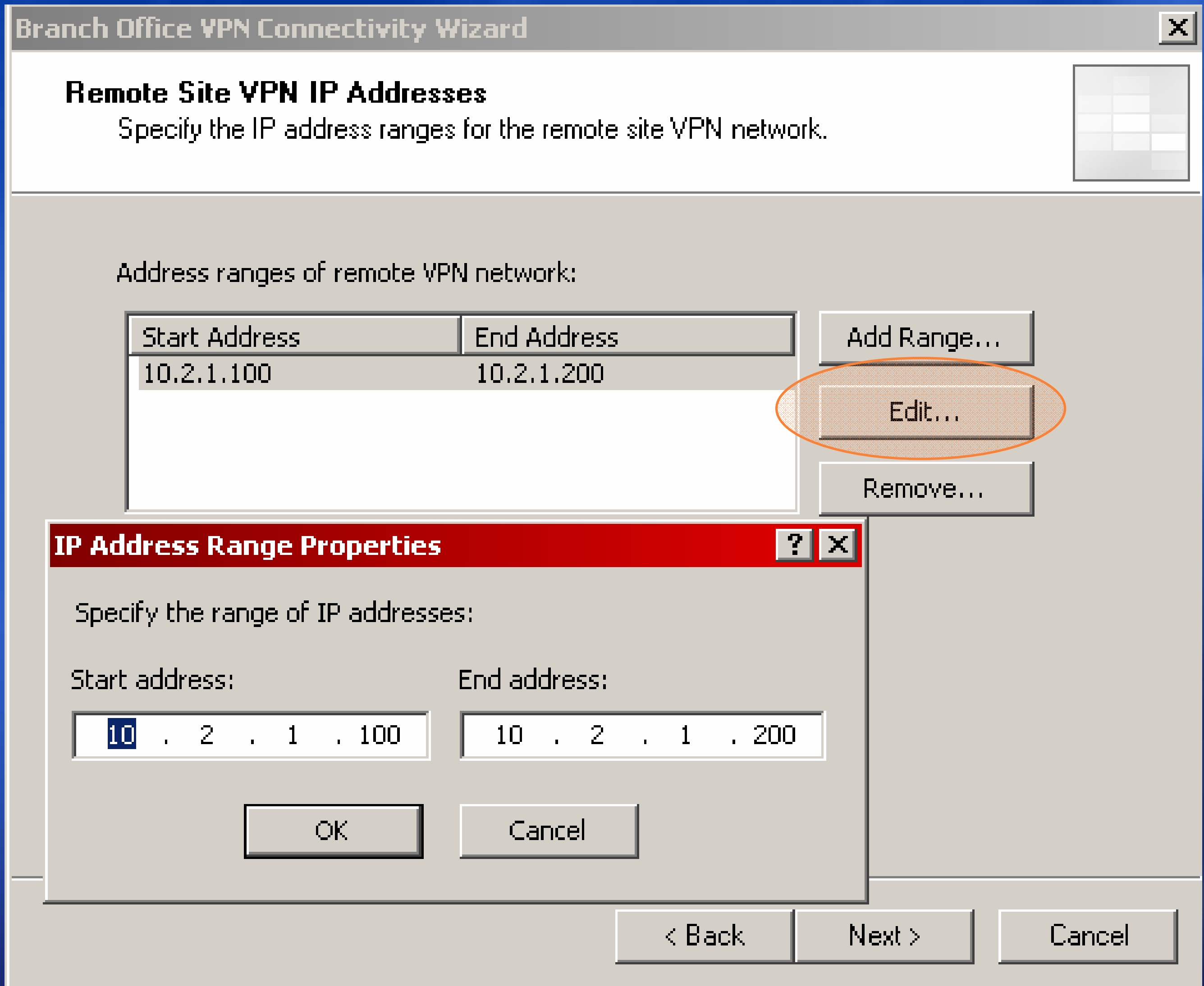
4



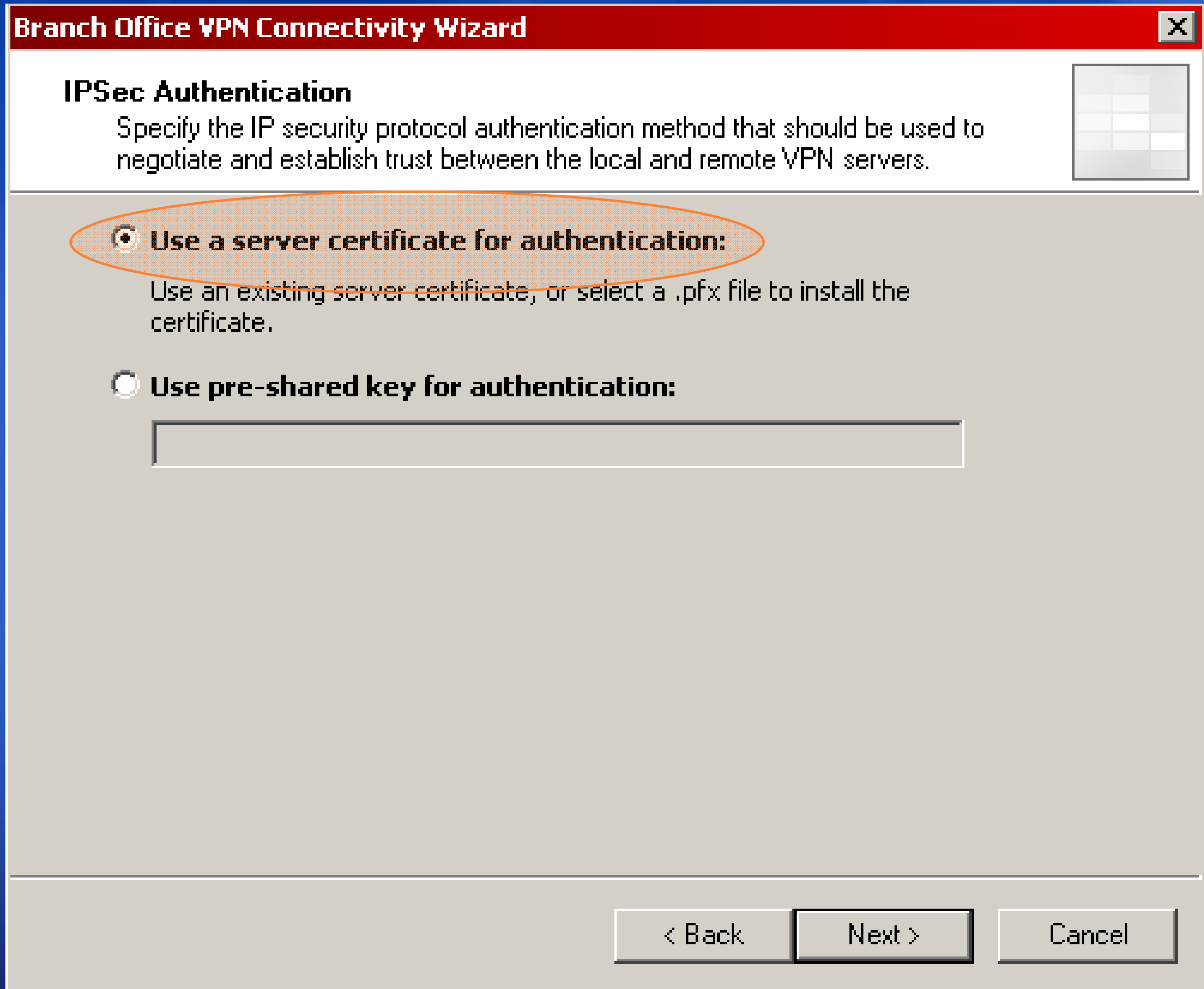
Branch Office VPN Connectivity Wizard
IPsec Connection Settings
Specify the remote site name and the gateway IP addresses on both sides of the VPN tunnel.
Type the name of the site-to-site network. The network created will represent the remote site on this array.
Network name:
Berlin
Remote VPN gateway IP address:
39 . 1 . 1 . 8
If the remote gateway is a Network Load Balancing cluster, specify its virtual IP address.
Local VPN gateway IP address:
39 . 1 . 1 . 1
If Network Load Balancing is enabled on the network adapter facing the remote site, specify its virtual IP address.
< Back
Next >
Cancel

>运行该向导

5

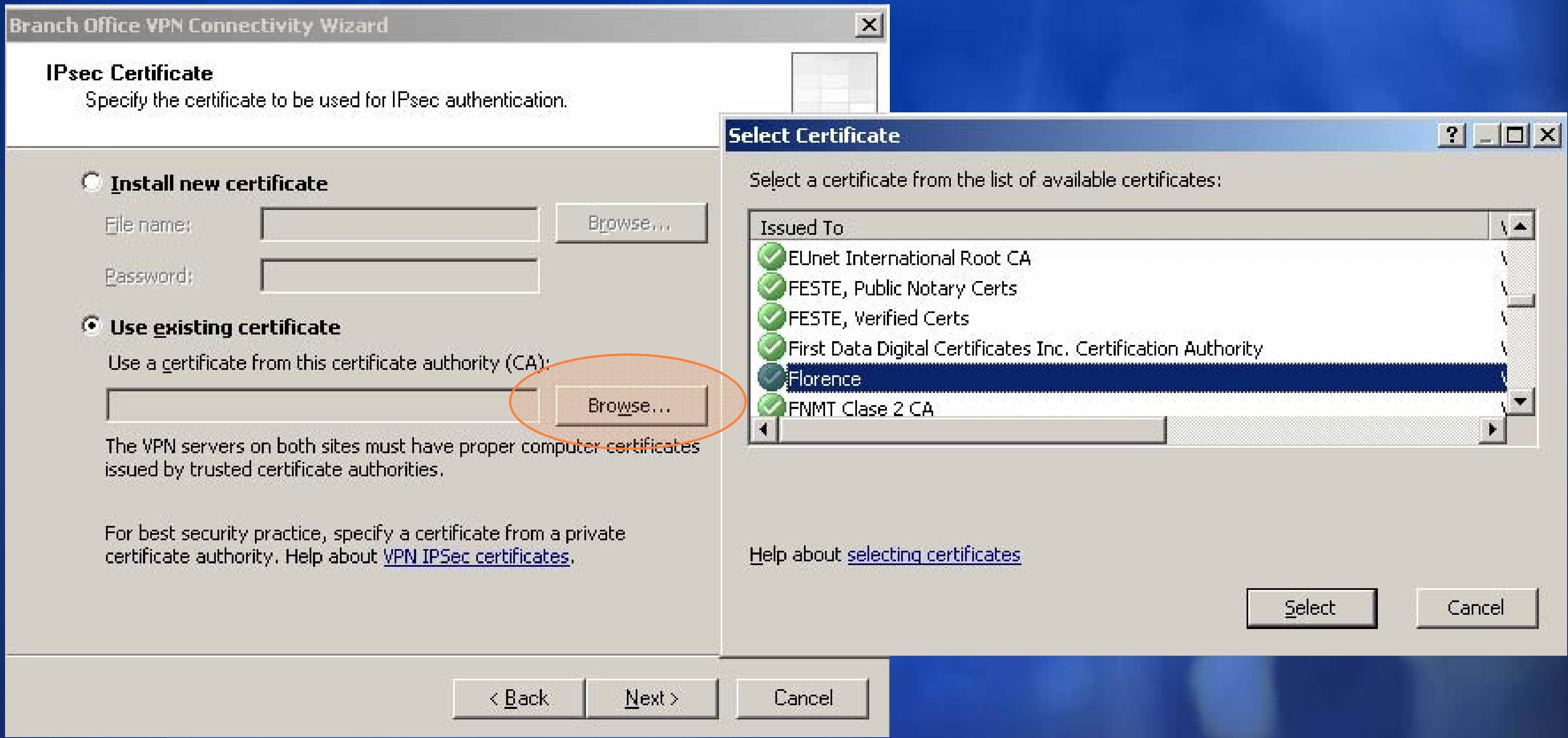

Branch Office VPN Connectivity Wizard
Remote Site VPN IP Addresses
Specify the IP address ranges for the remote site VPN network.
Address ranges of remote VPN network:
Start Address
End Address
10.2.1.100
10.2.1.200
Add Range...
Edit...
Remove...
IP Address Range Properties
Specify the range of IP addresses:
Start address:
End address:
10 . 2 . 1 . 100
10 . 2 . 1 . 200
OK
Cancel
< Back
Next >
Cancel

>运行该向导


Branch Office VPN Connectivity Wizard
IPSec Authentication
Specify the IP security protocol authentication method that should be used to negotiate and establish trust between the local and remote VPN servers.
Use a server certificate for authentication:
Use an existing server certificate, or select a .pfx file to install the certificate.
Use pre-shared key for authentication:
< Back
Next >
Cancel

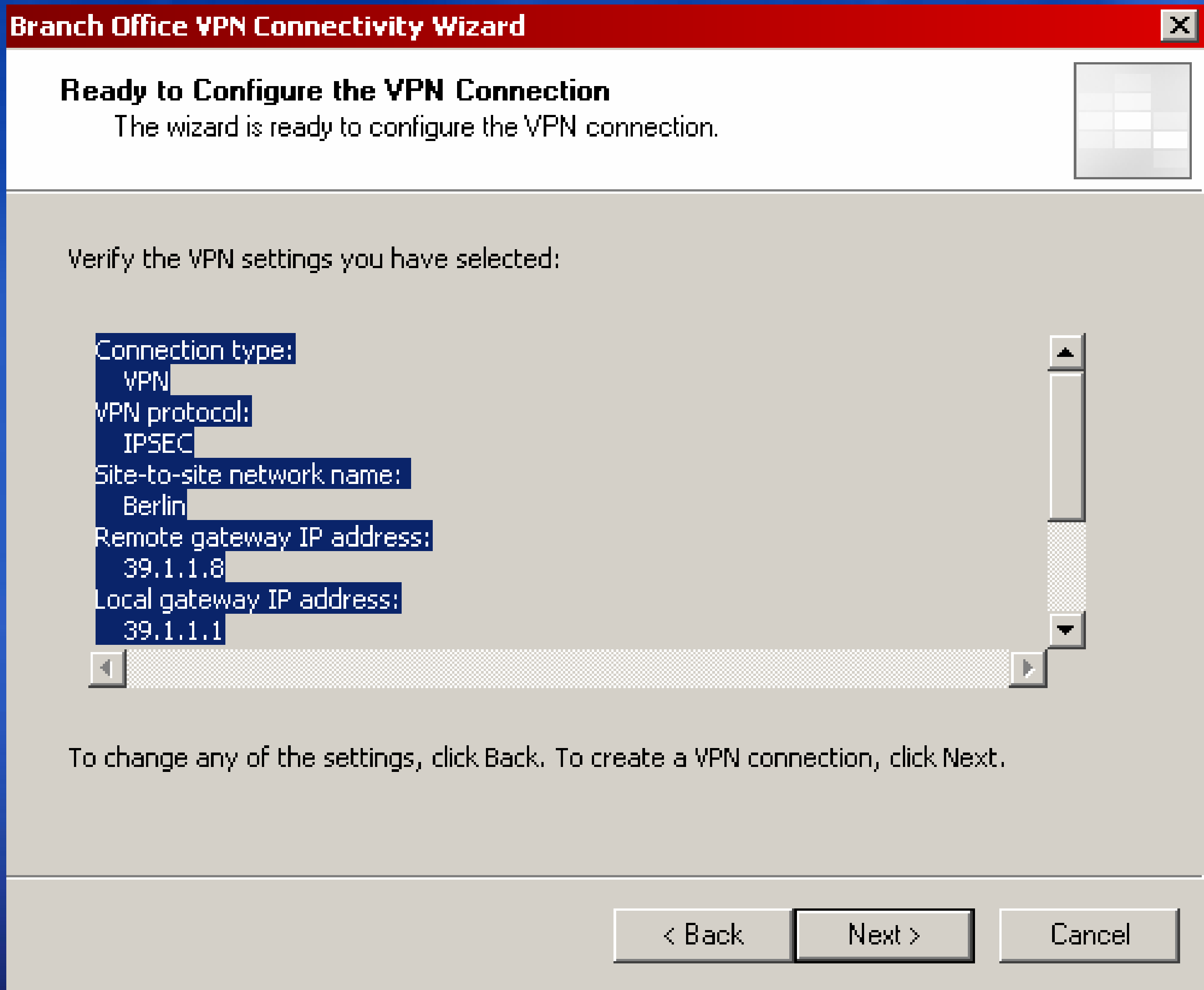
>运行该向导

7



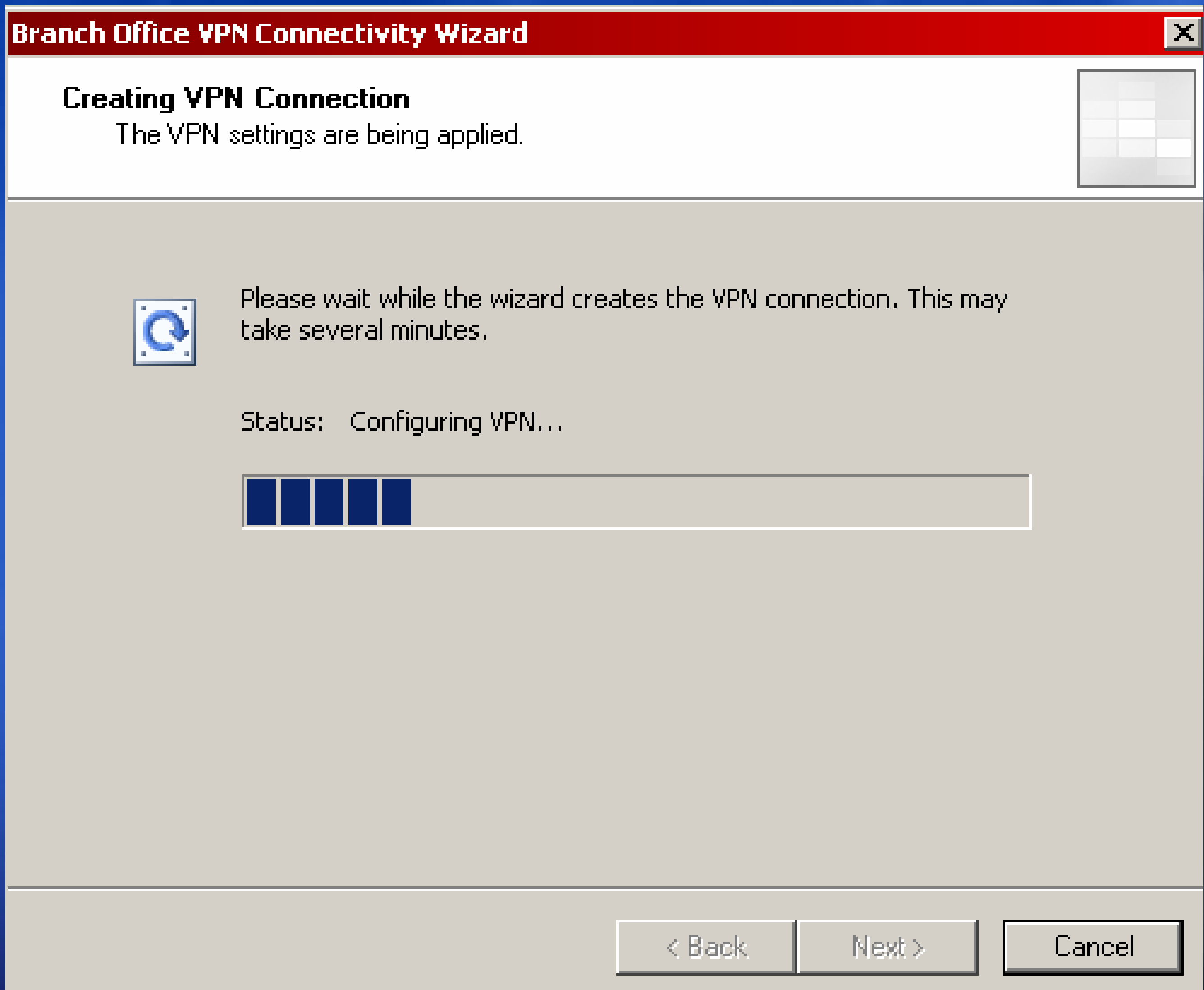
Branch Office VPN Connectivity Wizard
IPsec Certificate
Specify the certificate to be used for IPsec authentication.
Install new certificate
File name:
Browse...
Password:
Use existing certificate
Use a certificate from this certificate authority (CA):
Browse...
The VPN servers on both sites must have proper computer certificates issued by trusted certificate authorities.
For best security practice, specify a certificate from a private certificate authority. Help about VPN IPSec certificates.
< Back
Next >
Cancel
Select Certificate
Select a certificate from the list of available certificates:
Issued To
EUnet International Root CA
FESTE, Public Notary Certs
FESTE, Verified Certs
First Data Digital Certificates Inc. Certification Authority
Florence
FNMT Clase 2 CA
Help about selecting certificates
Select
Cancel

>运行该向导

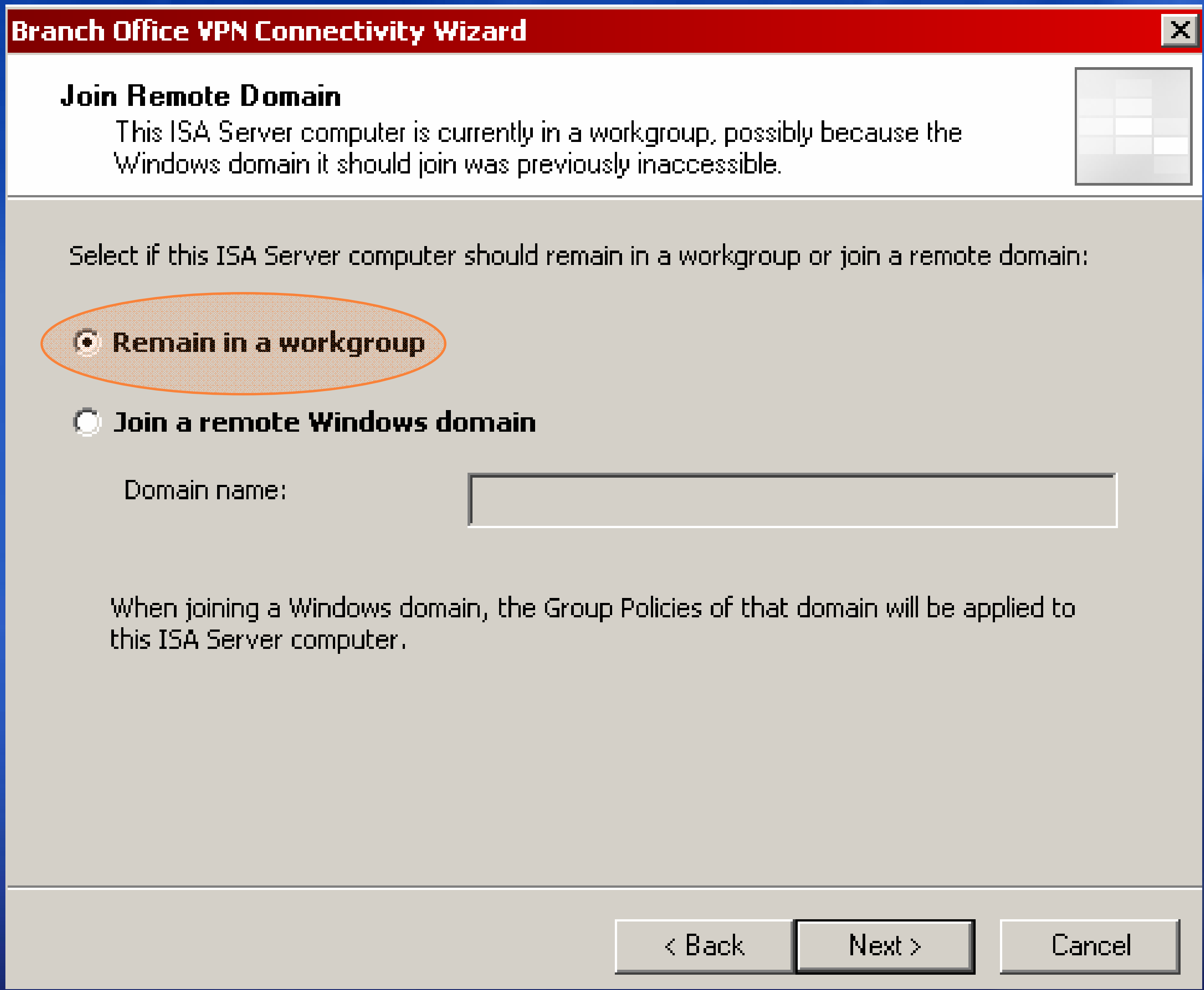

Branch Office VPN Connectivity Wizard
Ready to Configure the VPN Connection
The wizard is ready to configure the VPN connection.
Verify the VPN settings you have selected:
Connection type:
VPN
VPN protocol:
IPSEC
Site-to-site network name:
Berlin
Remote gateway IP address:
39.1.1.8
Local gateway IP address:
39.1.1.1
To change any of the settings, click Back. To create a VPN connection, click Next.
< Back
Next >
Cancel

>运行该向导

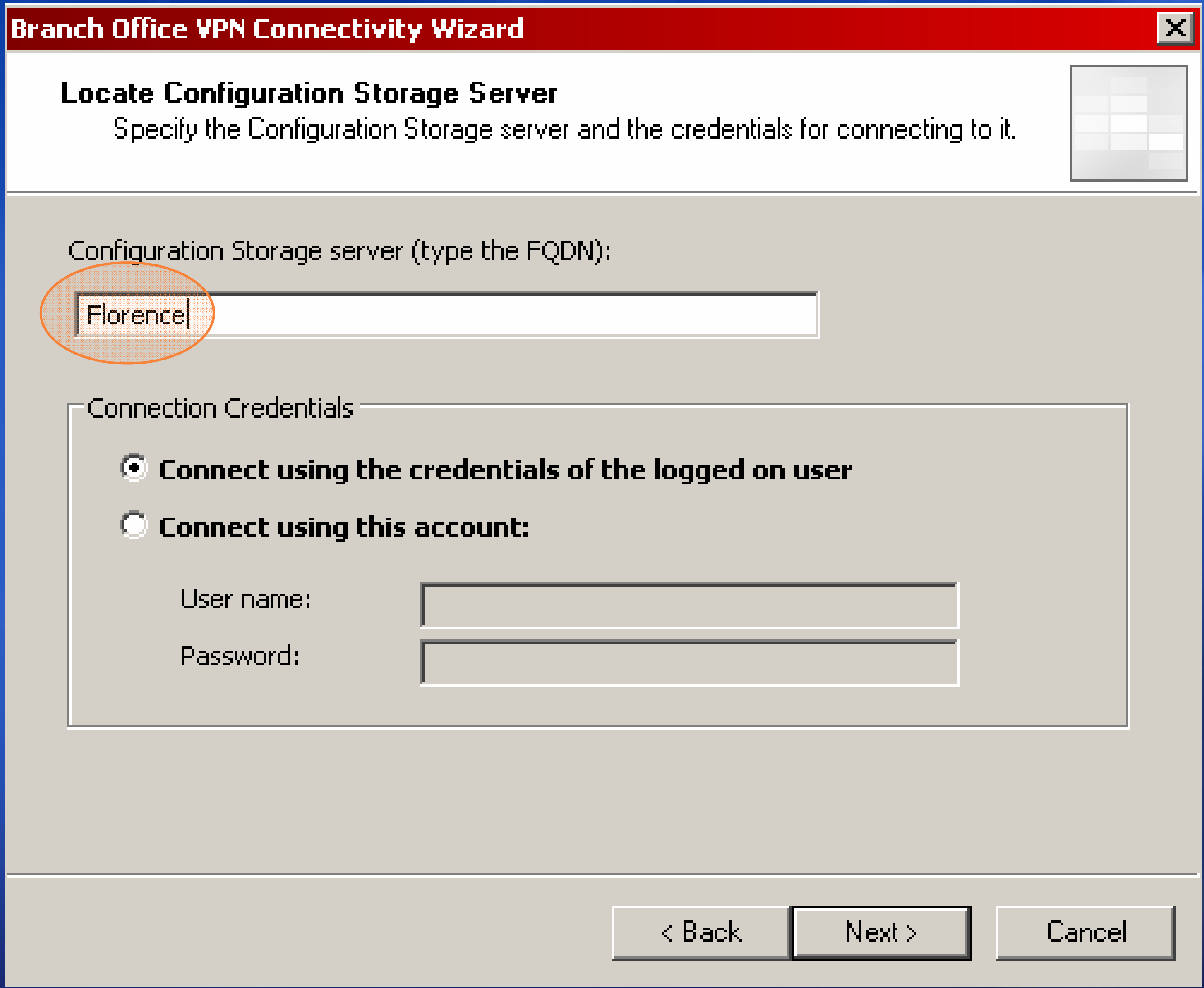
9


Branch Office VPN Connectivity Wizard
Creating VPN Connection
The VPN settings are being applied.
Please wait while the wizard creates the VPN connection. This may take several minutes.
Status: Configuring VPN...
< Back
Next >
Cancel

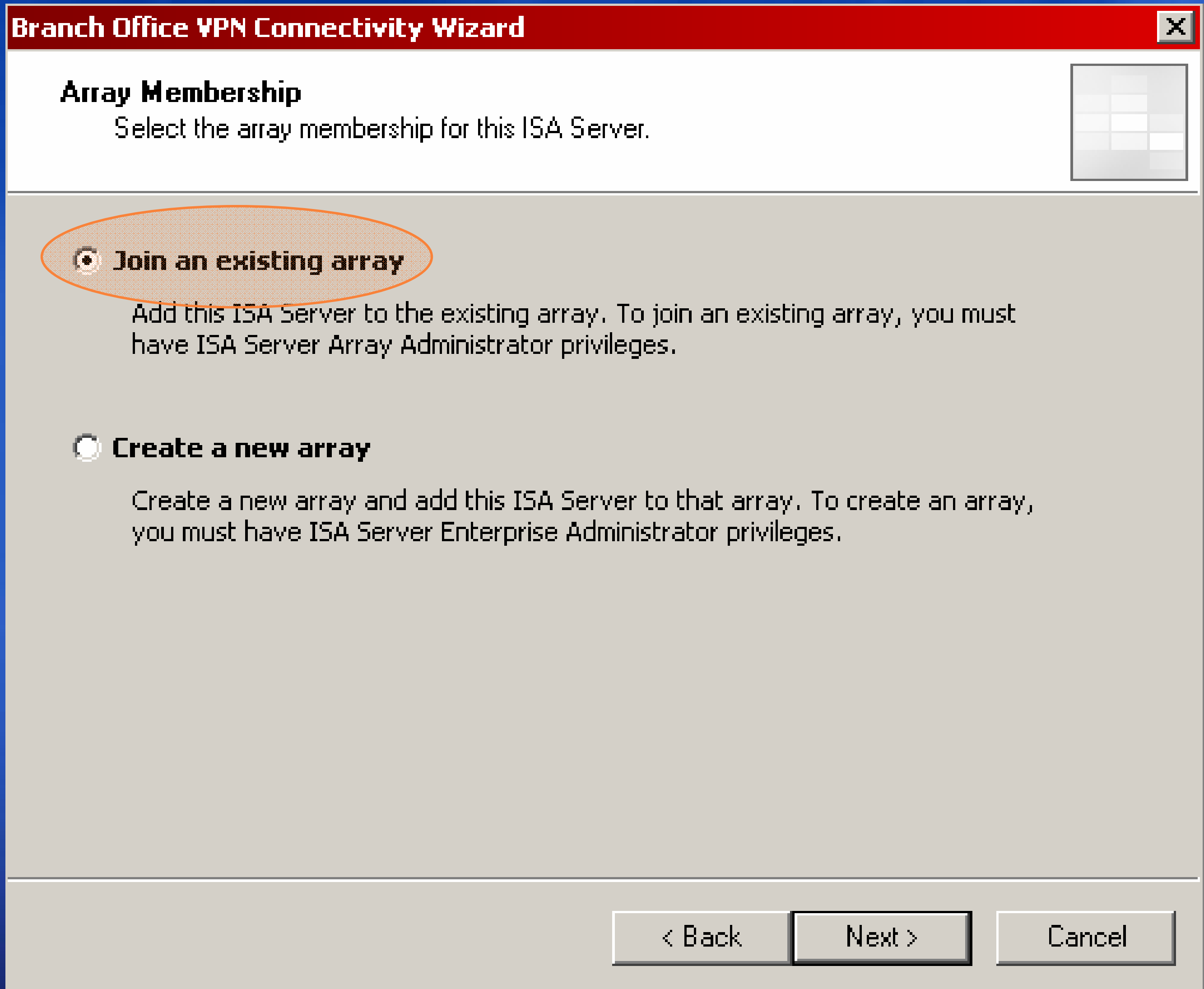
>运行该向导


Branch Office VPN Connectivity Wizard
Join Remote Domain
This ISA Server computer is currently in a workgroup, possibly because the Windows domain it should join was previously inaccessible.
Select if this ISA Server computer should remain in a workgroup or join a remote domain:
Remain in a workgroup
Join a remote Windows domain
Domain name:
When joining a Windows domain, the Group Policies of that domain will be applied to this ISA Server computer.
< Back
Next >
Cancel

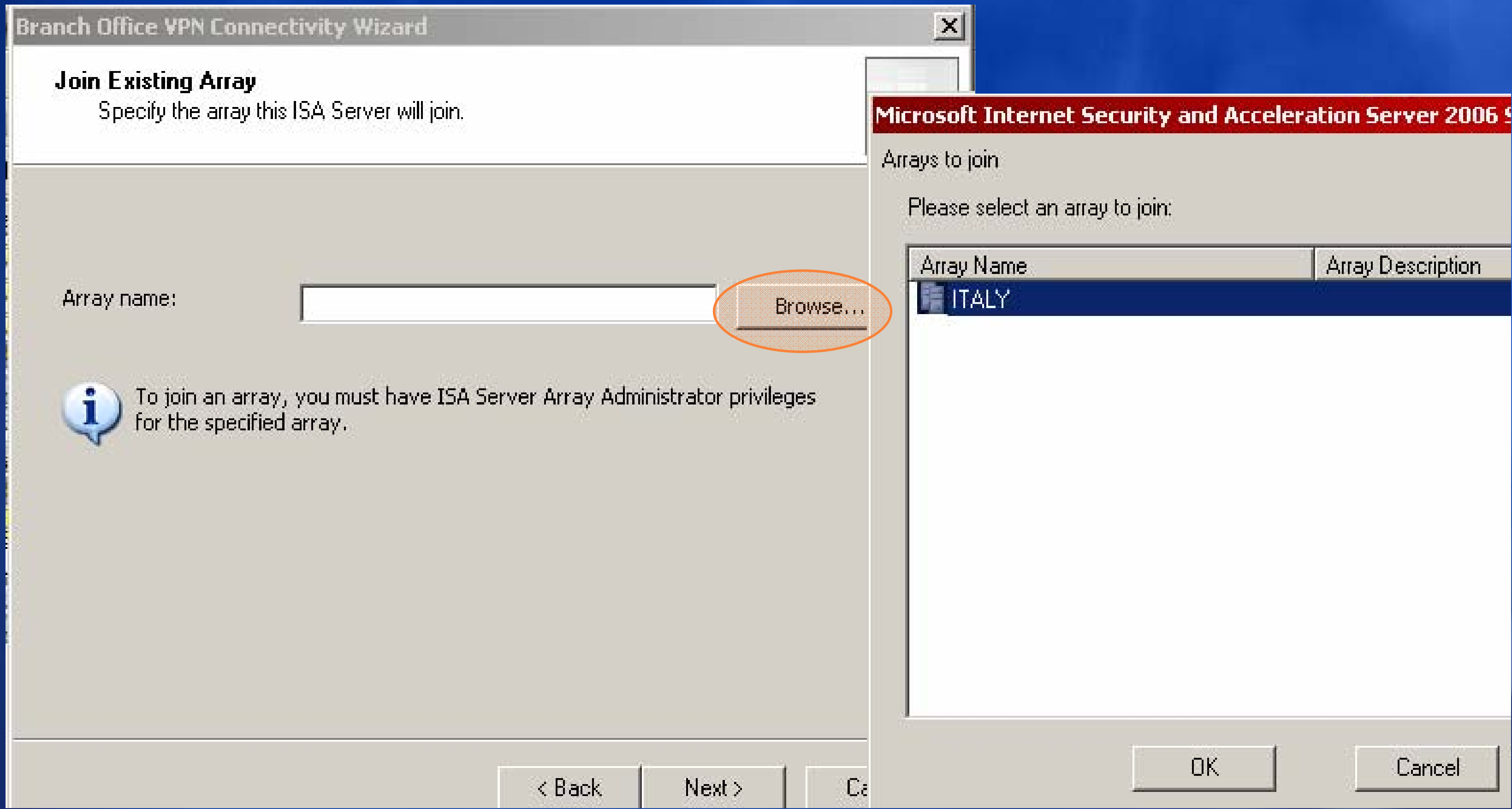
>运行该向导


Branch Office VPN Connectivity Wizard
Locate Configuration Storage Server
Specify the Configuration Storage server and the credentials for connecting to it.
Configuration Storage server (type the FQDN):
Florence
Connection Credentials
Connect using the credentials of the logged on user
Connect using this account:
User name:
Password:
< Back
Next >
Cancel

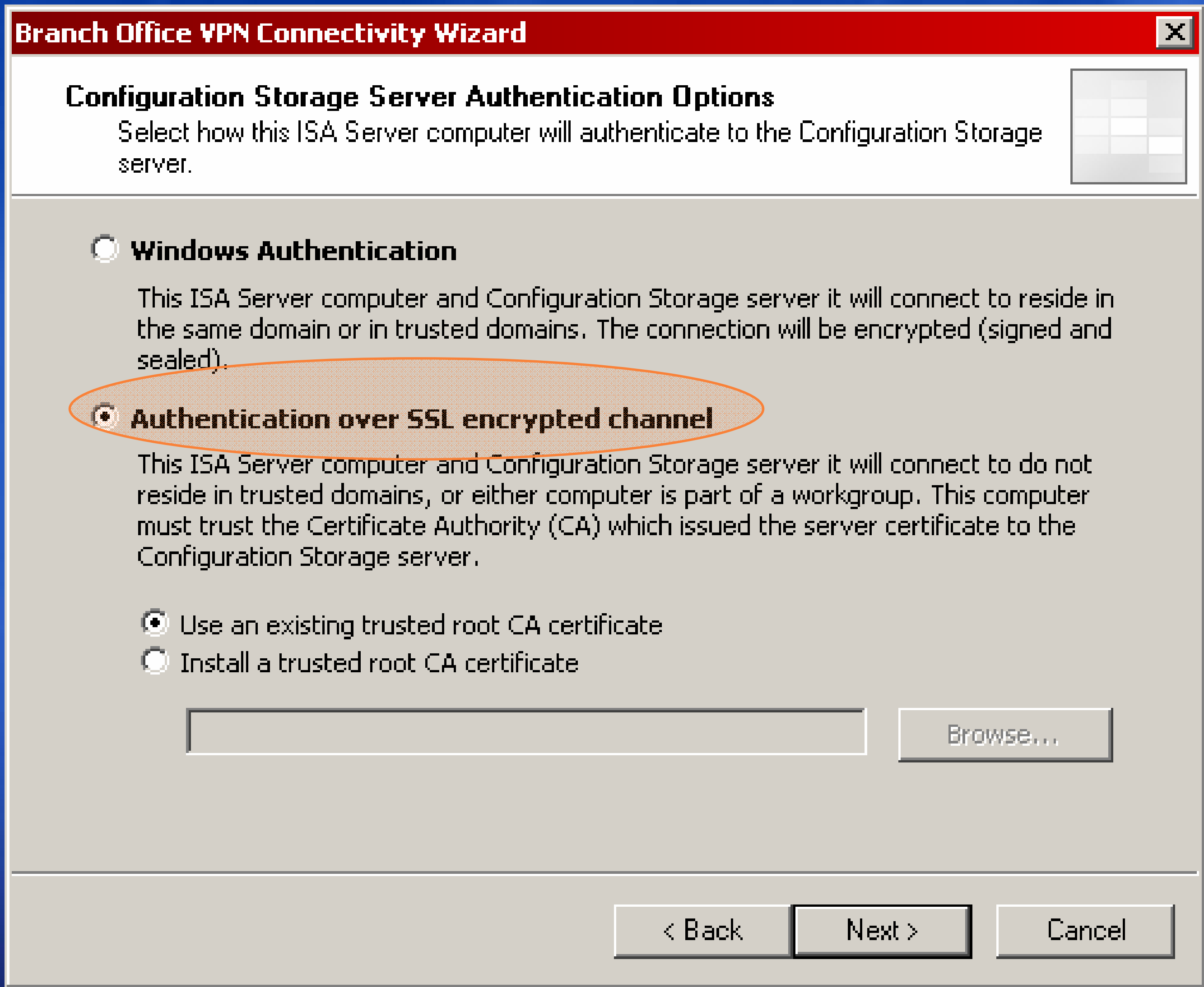
>运行该向导


Branch Office VPN Connectivity Wizard
Array Membership
Select the array membership for this ISA Server.
Join an existing array
Add this ISA Server to the existing array. To join an existing array, you must have ISA Server Array Administrator privileges.
Create a new array
Create a new array and add this ISA Server to that array. To create an array, you must have ISA Server Enterprise Administrator privileges.
< Back
Next >
Cancel

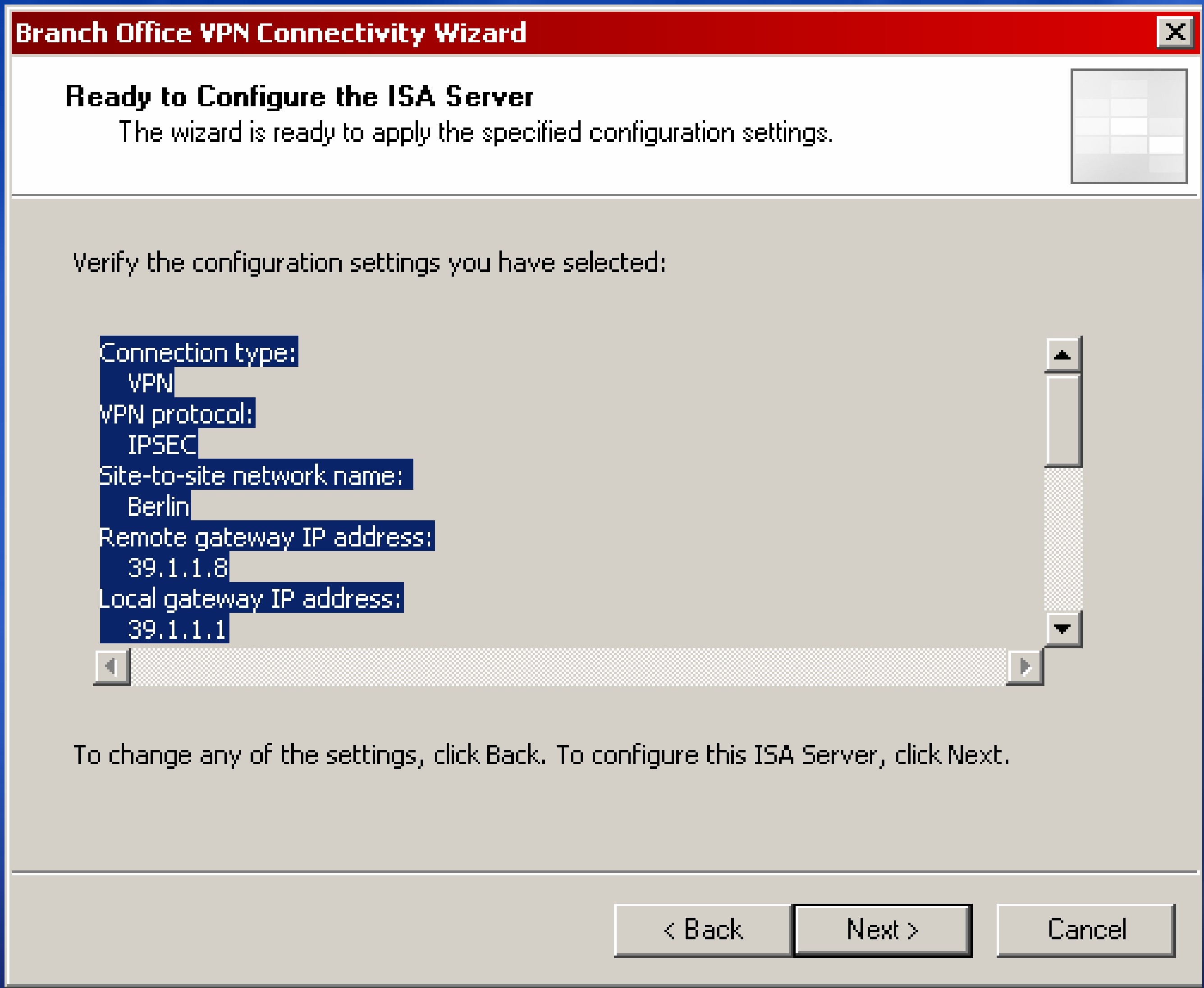
>运行该向导


Branch Office VPN Connectivity Wizard
Join Existing Array
Specify the array this ISA Server will join.
Array name:
Browse...
To join an array, you must have ISA Server Array Administrator privileges for the specified array.
< Back
Next >
Microsoft Internet Security and Acceleration Server 2006
Arrays to join
Please select an array to join:
Array Name
Array Description
ITALY
OK
Cancel

>运行该向导

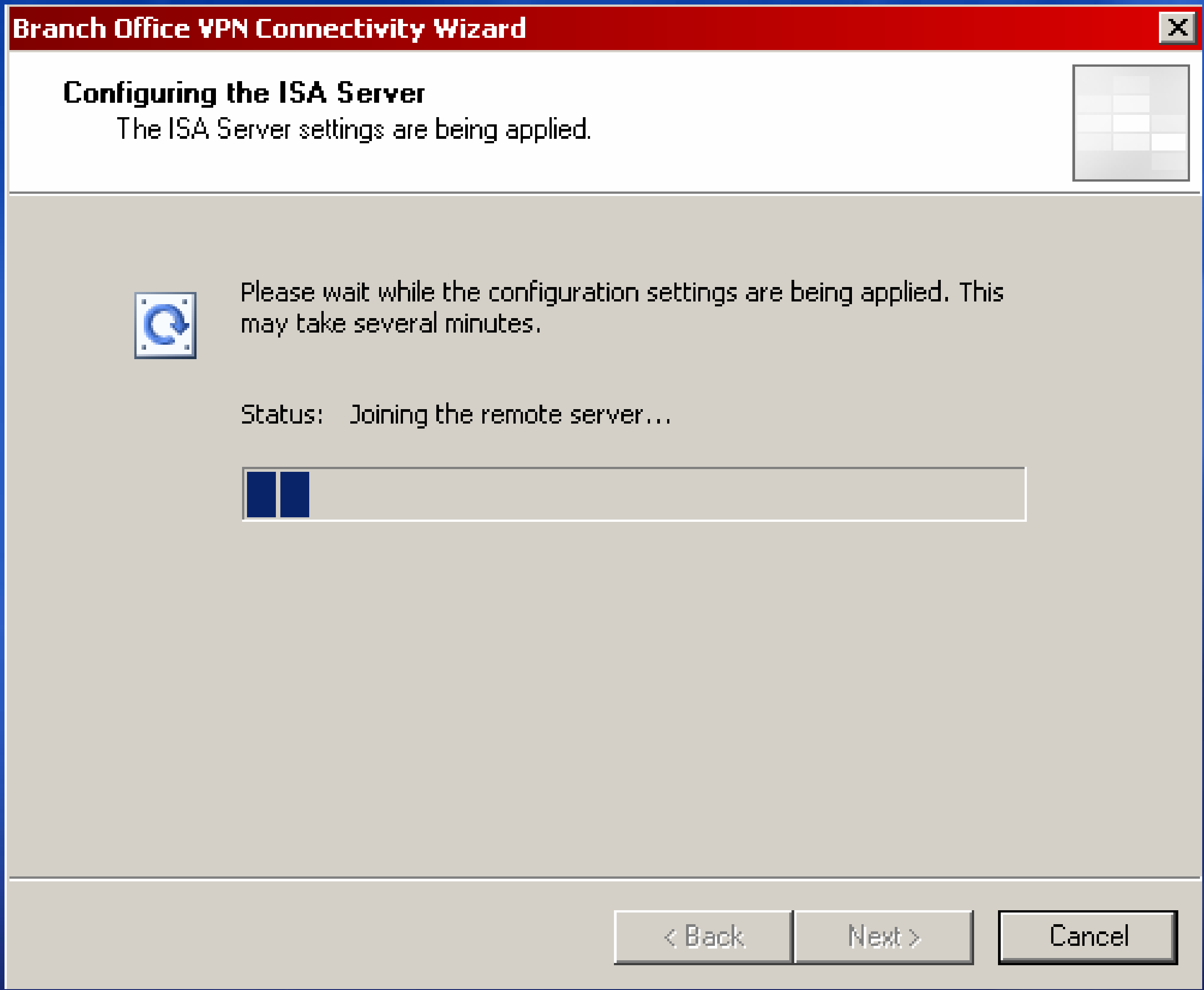

Branch Office VPN Connectivity Wizard
Configuration Storage Server Authentication Options
Select how this ISA Server computer will authenticate to the Configuration Storage server.
Windows Authentication
This ISA Server computer and Configuration Storage server it will connect to reside in the same domain or in trusted domains. The connection will be encrypted (signed and sealed).
Authentication over SSL encrypted channel
This ISA Server computer and Configuration Storage server it will connect to do not reside in trusted domains, or either computer is part of a workgroup. This computer must trust the Certificate Authority (CA) which issued the server certificate to the Configuration Storage server.
Use an existing trusted root CA certificate
Install a trusted root CA certificate
Browse...
< Back
Next >
Cancel

>运行该向导


Branch Office VPN Connectivity Wizard
Ready to Configure the ISA Server
The wizard is ready to apply the specified configuration settings.
Verify the configuration settings you have selected:
Connection type:
VPN
VPN protocol:
IPSEC
Site-to-site network name:
Berlin
Remote gateway IP address:
39.1.1.8
Local gateway IP address:
39.1.1.1
To change any of the settings, click Back. To configure this ISA Server, click Next.
< Back
Next >
Cancel

>运行该向导

完成

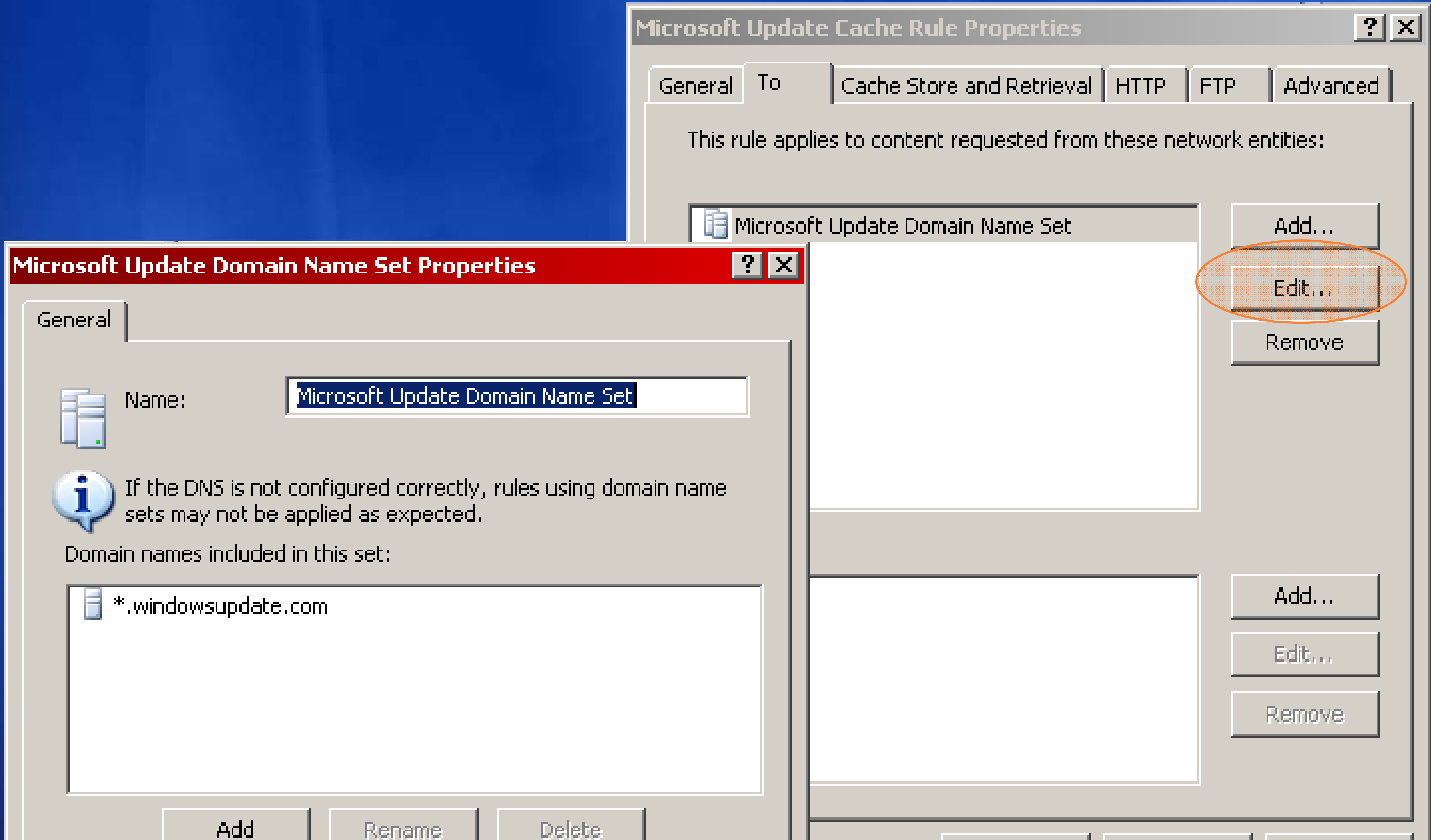


Branch Office VPN Connectivity Wizard
Configuring the ISA Server
The ISA Server settings are being applied.
Please wait while the configuration settings are being applied. This may take several minutes.
Status: Joining the remote server...
< Back
Next >
Cancel

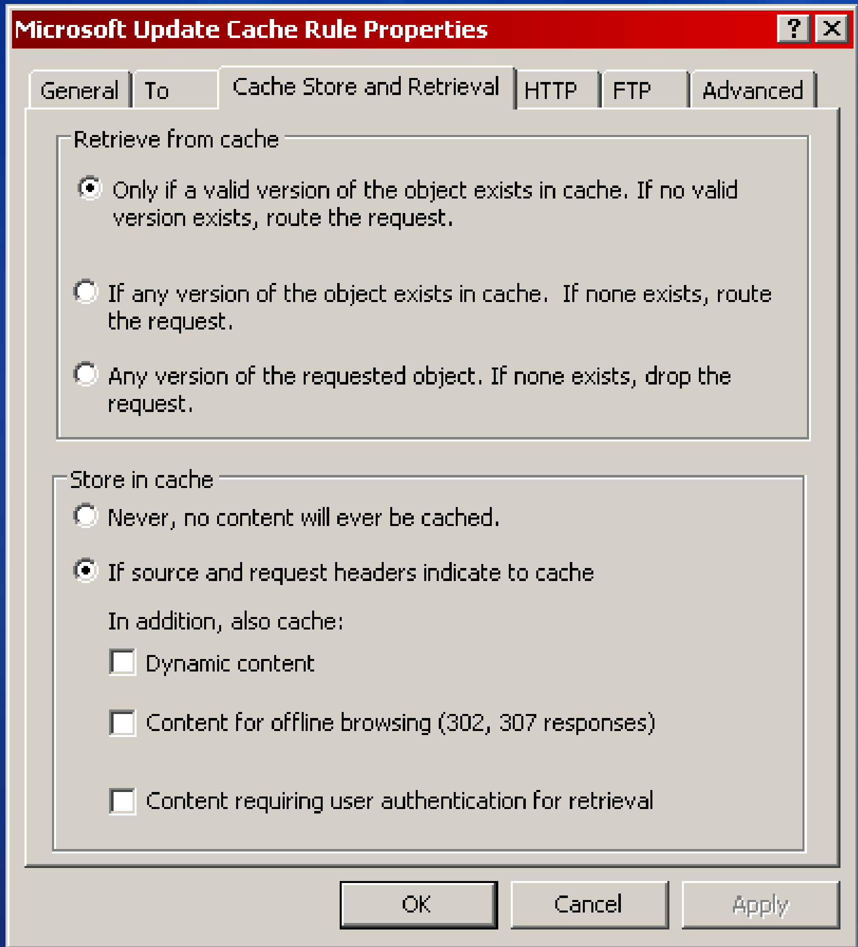
更新的 BITS 缓存

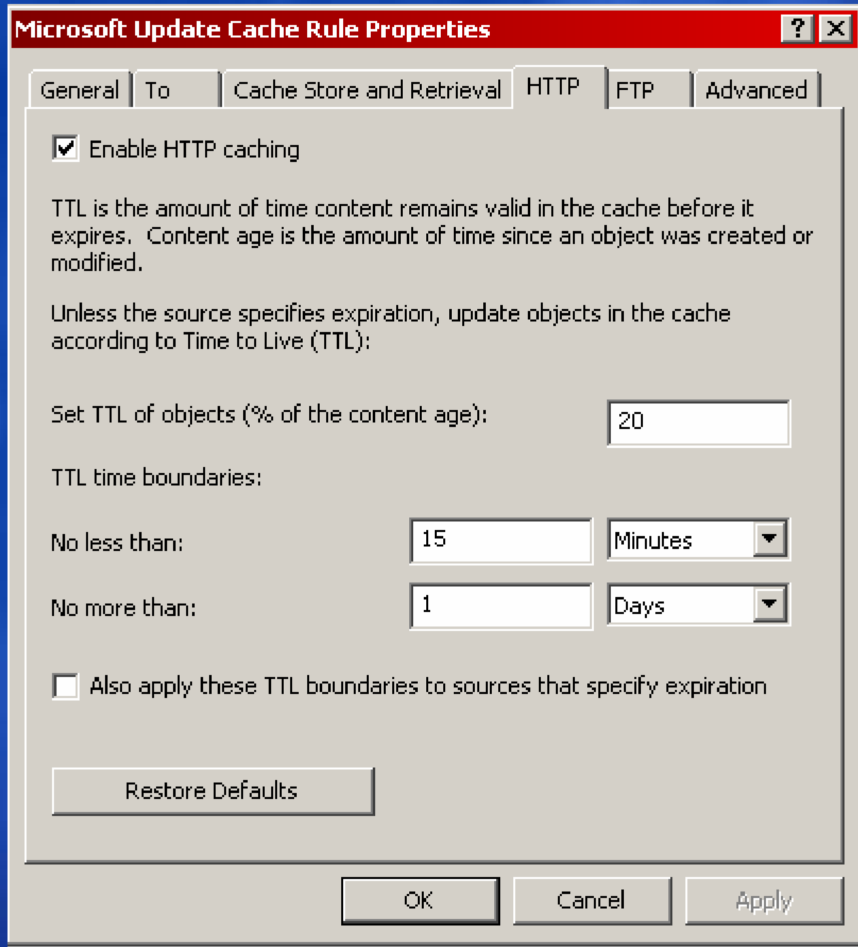
- 用于缓存从 Microsoft Update 网站下载的内容的内置规则（和元素）
- 客户端从缓存提取更新
- 考虑来自客户端的范围请求
  - ISA 仅缓存正在使用的任何客户端操作系统的更新
  - 节省带宽使用和存储空间
- *任何* web 发布规则均可用 BITS 来缓存…

> 配置更新缓存


Microsoft Update Cache Rule Properties
General
To
Cache Store and Retrieval
HTTP
FTP
Advanced
This rule applies to content requested from these network entities:
Microsoft Update Domain Name Set
Add...
Edit...
Remove
Add...
Edit...
Remove
Microsoft Update Domain Name Set Properties
General
Name:
Microsoft Update Domain Name Set
If the DNS is not configured correctly, rules using domain name sets may not be applied as expected.
Domain names included in this set:
*.windowsupdate.com
Add
Rename
Delete

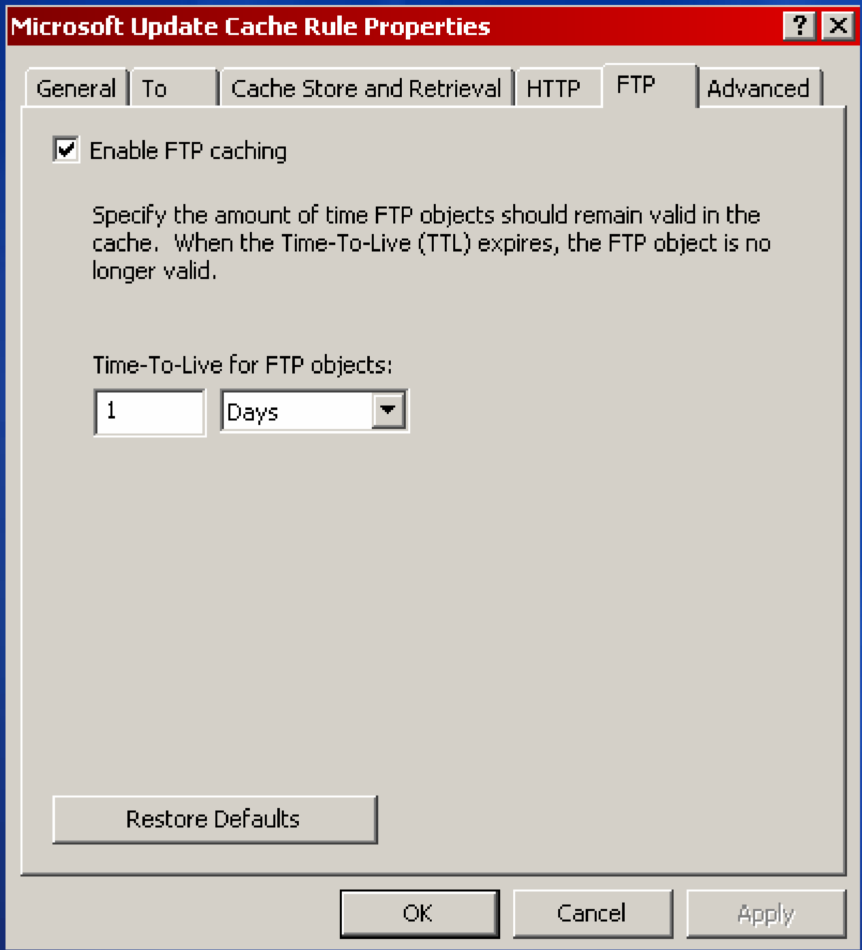
> 配置更新缓存

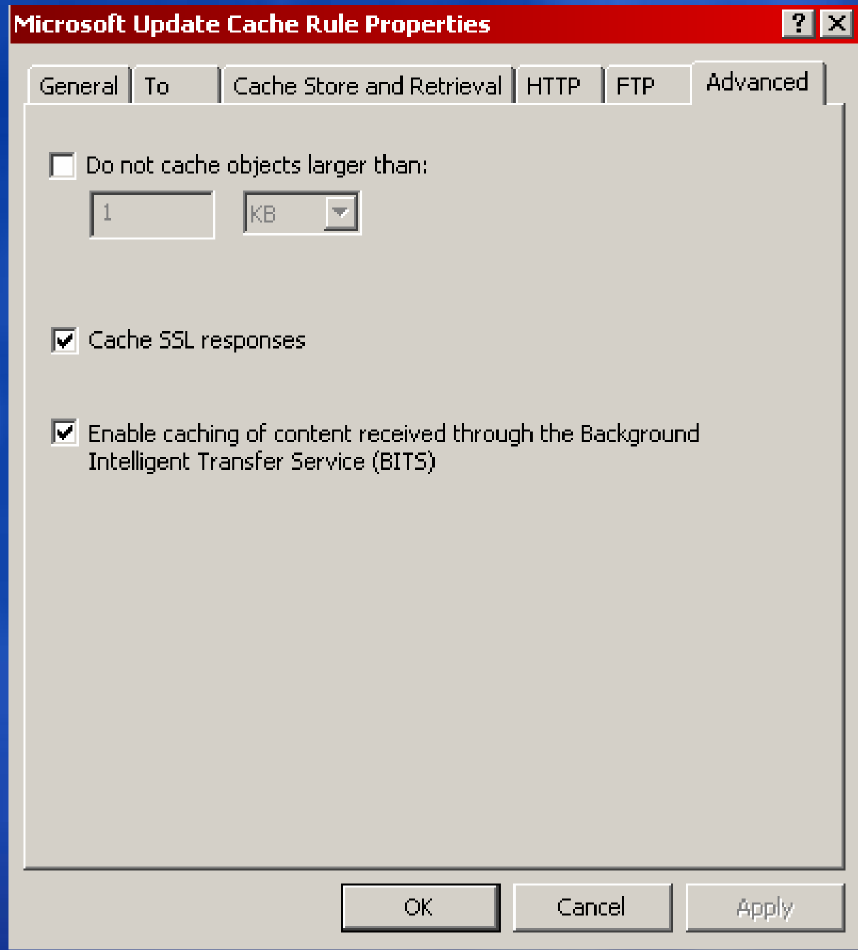

Microsoft Update Cache Rule Properties
General
To
Cache Store and Retrieval
HTTP
FTP
Advanced
Retrieve from cache
Only if a valid version of the object exists in cache. If no valid version exists, route the request.
If any version of the object exists in cache. If none exists, route the request.
Any version of the requested object. If none exists, drop the request.
Store in cache
Never, no content will ever be cached.
If source and request headers indicate to cache
In addition, also cache:
Dynamic content
Content for offline browsing (302, 307 responses)
Content requiring user authentication for retrieval
OK
Cancel
Apply


Microsoft Update Cache Rule Properties
General
To
Cache Store and Retrieval
HTTP
FTP
Advanced
Enable HTTP caching
TTL is the amount of time content remains valid in the cache before it expires. Content age is the amount of time since an object was created or modified.
Unless the source specifies expiration, update objects in the cache according to Time to Live (TTL):
Set TTL of objects (% of the content age):
20
TTL time boundaries:
No less than:
15
Minutes
No more than:
1
Days
Also apply these TTL boundaries to sources that specify expiration
Restore Defaults
OK
Cancel
Apply

> 配置更新缓存

完成


Microsoft Update Cache Rule Properties
General
To
Cache Store and Retrieval
HTTP
FTP
Advanced
Enable FTP caching
Specify the amount of time FTP objects should remain valid in the cache. When the Time-To-Live (TTL) expires, the FTP object is no longer valid.
Time-To-Live for FTP objects:
1
Days
Restore Defaults
OK
Cancel
Apply


Microsoft Update Cache Rule Properties
General
To
Cache Store and Retrieval
HTTP
FTP
Advanced
Do not cache objects larger than:
1
KB
Cache SSL responses
Enable caching of content received through the Background Intelligent Transfer Service (BITS)
OK
Cancel
Apply

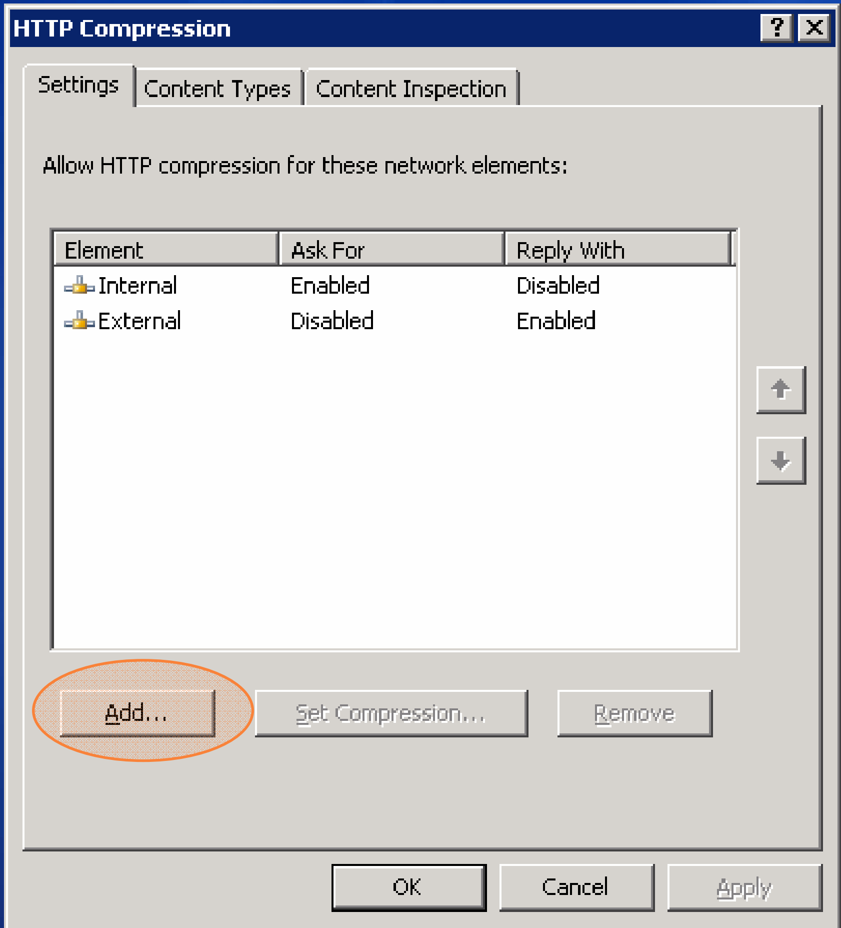
HTTP 压缩

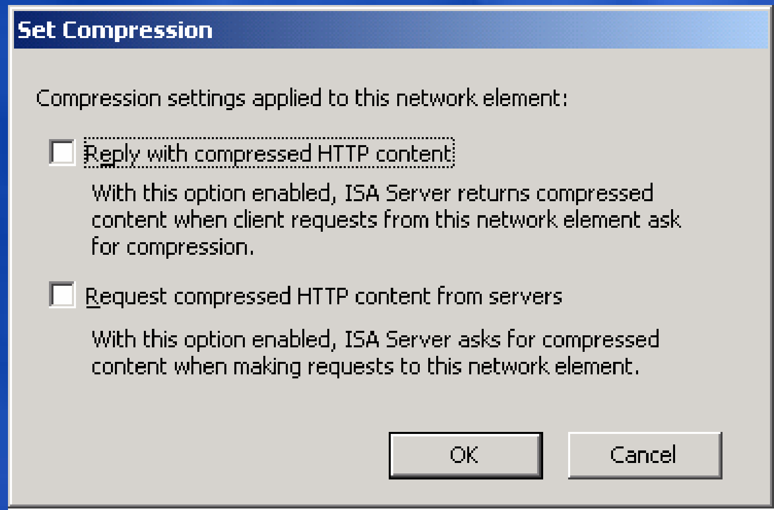
☐ Enable HTTP compression for this Web Listener

ISA Server will compress content sent to clients through this Web Listener if the clients requesting the content support compression.

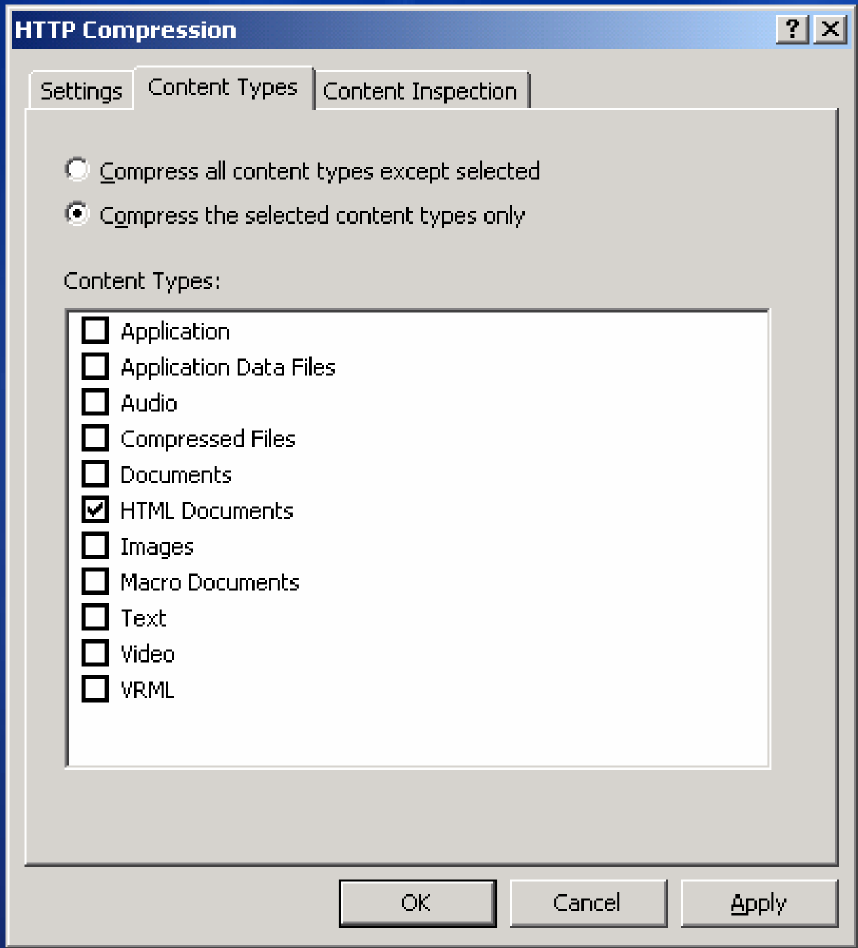
- GZip 和 Deflate；需要 HTTP 1.1
- 范围：按侦听器（ISA 2006 中的新增功能）或全局
  - 无法按每个规则进行设置
- 实现为 Web 筛选器
  - 在筛选器顺序中处于高位；高优先级
  - 必须解压缩，然后 ISA 才能检查
- 若客户端请求，缓存的材料将以压缩形式传递
  - 即使存储的数据未压缩
  - 将影响性能；在此情况下应清空缓存
    - 禁用缓存功能
    - 删除每个驱动器上的 `Urlcache` 文件夹中的缓存文件
- HTTPS 从不压缩

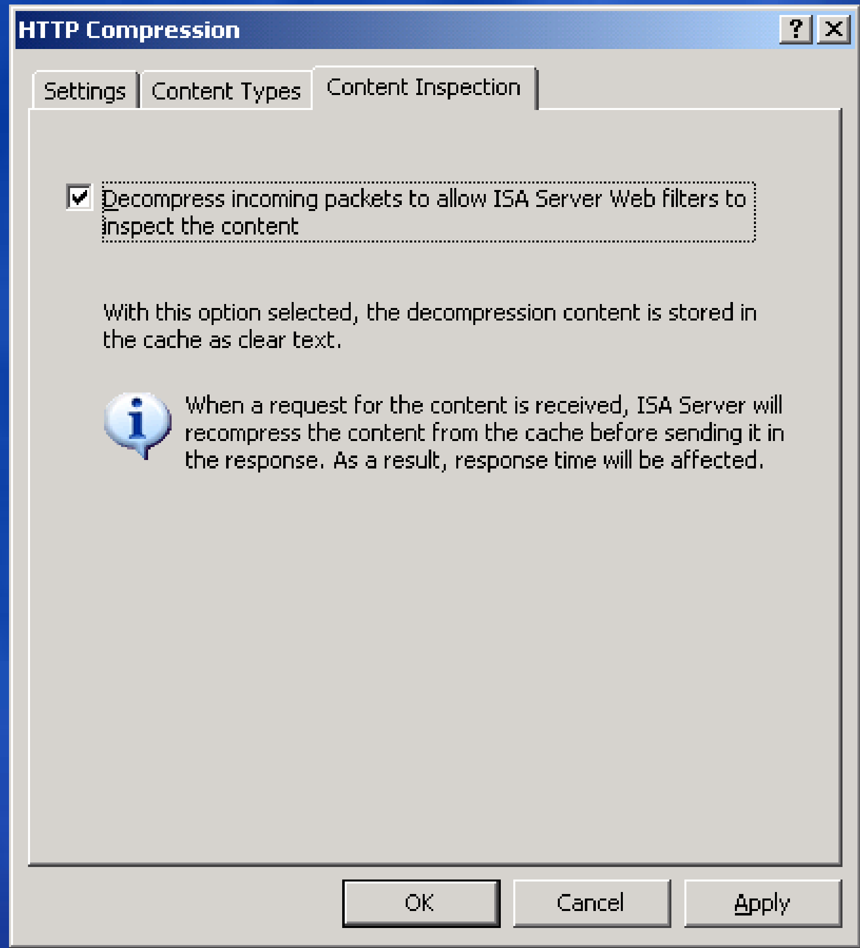
全局压缩设置


HTTP Compression
Settings
Content Types
Content Inspection
Allow HTTP compression for these network elements:
Element
Ask For
Reply With
Internal
Enabled
Disabled
External
Disabled
Enabled
Add...
Set Compression...
Remove
OK
Cancel
Apply

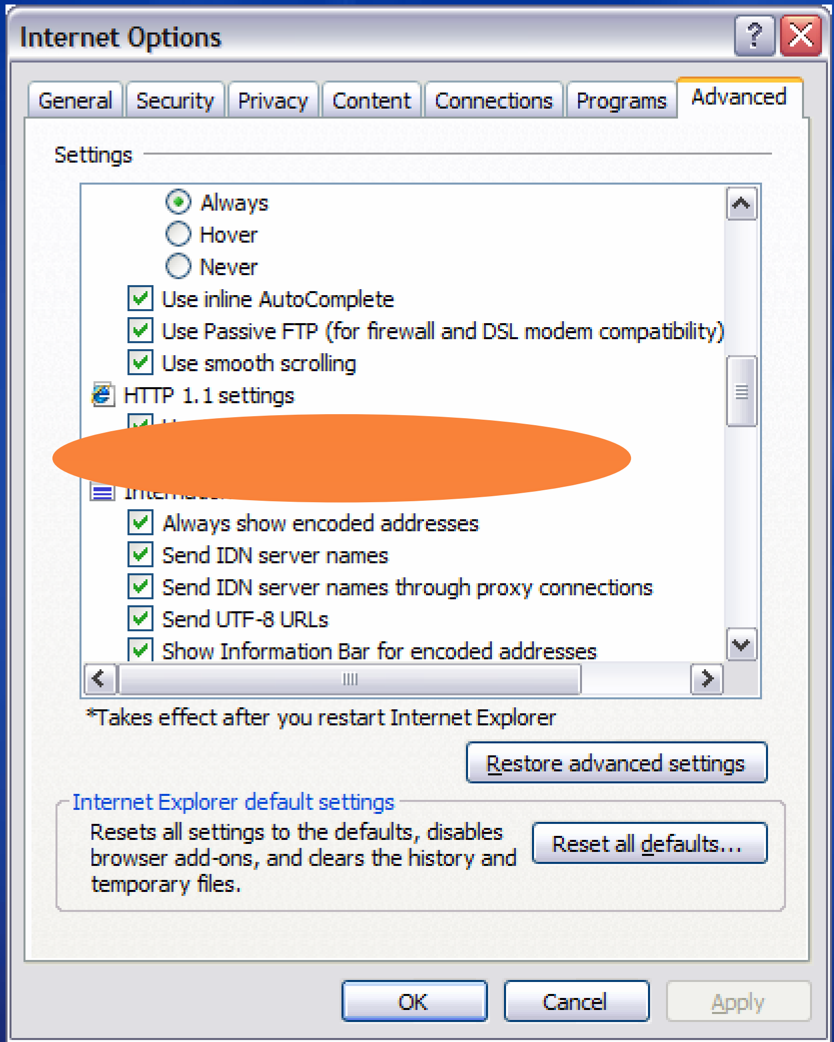

Set Compression
Compression settings applied to this network element:
Reply with compressed HTTP content
With this option enabled, ISA Server returns compressed content when client requests from this network element ask for compression.
Request compressed HTTP content from servers
With this option enabled, ISA Server asks for compressed content when making requests to this network element.
OK
Cancel

全局压缩设置


HTTP Compression
Settings
Content Types
Content Inspection
Compress all content types except selected
Compress the selected content types only
Content Types:
Application
Application Data Files
Audio
Compressed Files
Documents
HTML Documents
Images
Macro Documents
Text
Video
VRML
OK
Cancel
Apply


HTTP Compression
Settings
Content Types
Content Inspection
Decompress incoming packets to allow ISA Server Web filters to inspect the content
With this option selected, the decompression content is stored in the cache as clear text.
When a request for the content is received, ISA Server will recompress the content from the cache before sending it in the response. As a result, response time will be affected.
OK
Cancel
Apply

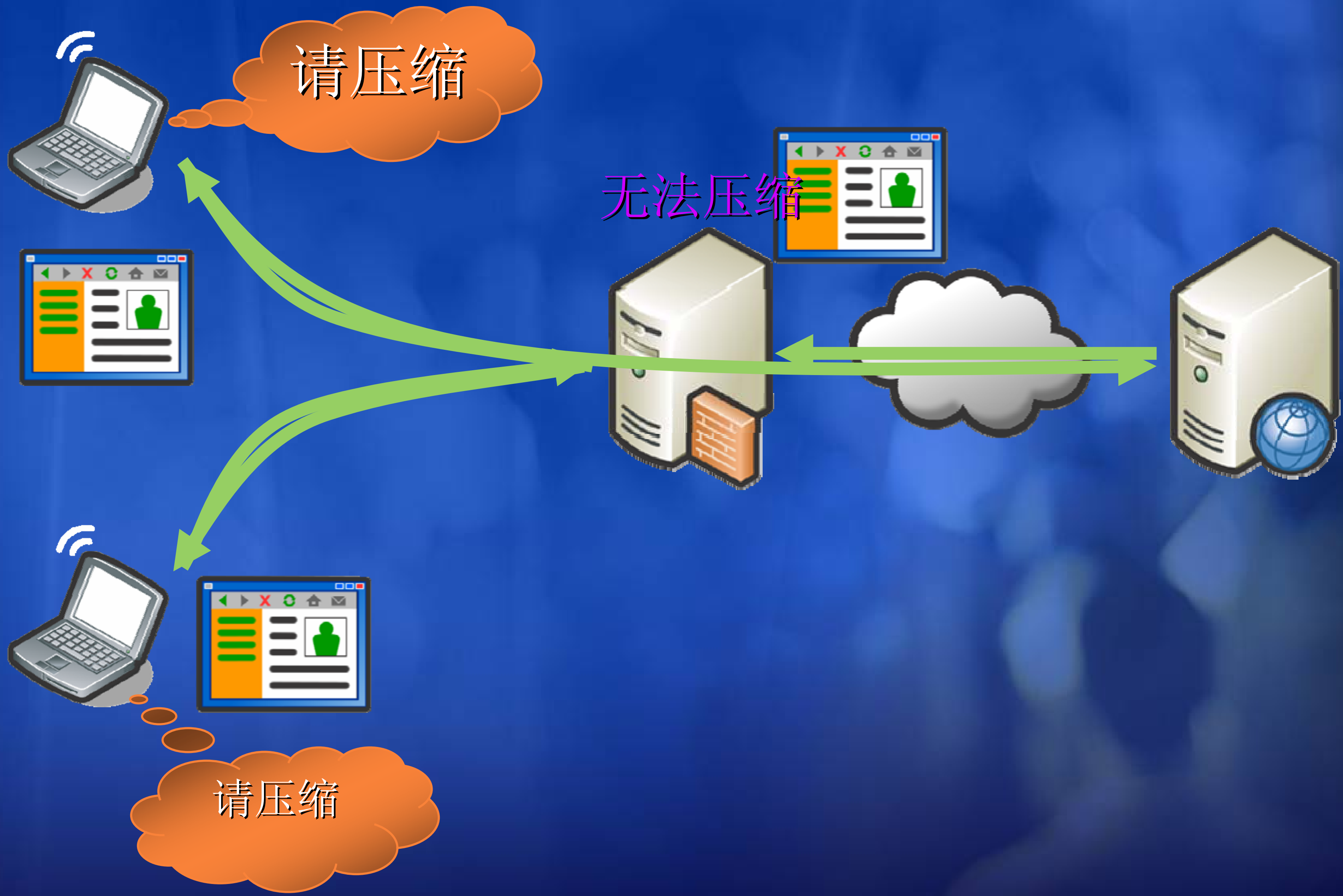
客户端上的 HTTP 压缩



- HTTP 1.1 客户端自动请求压缩
- 必须启用浏览器设置

缓存和压缩

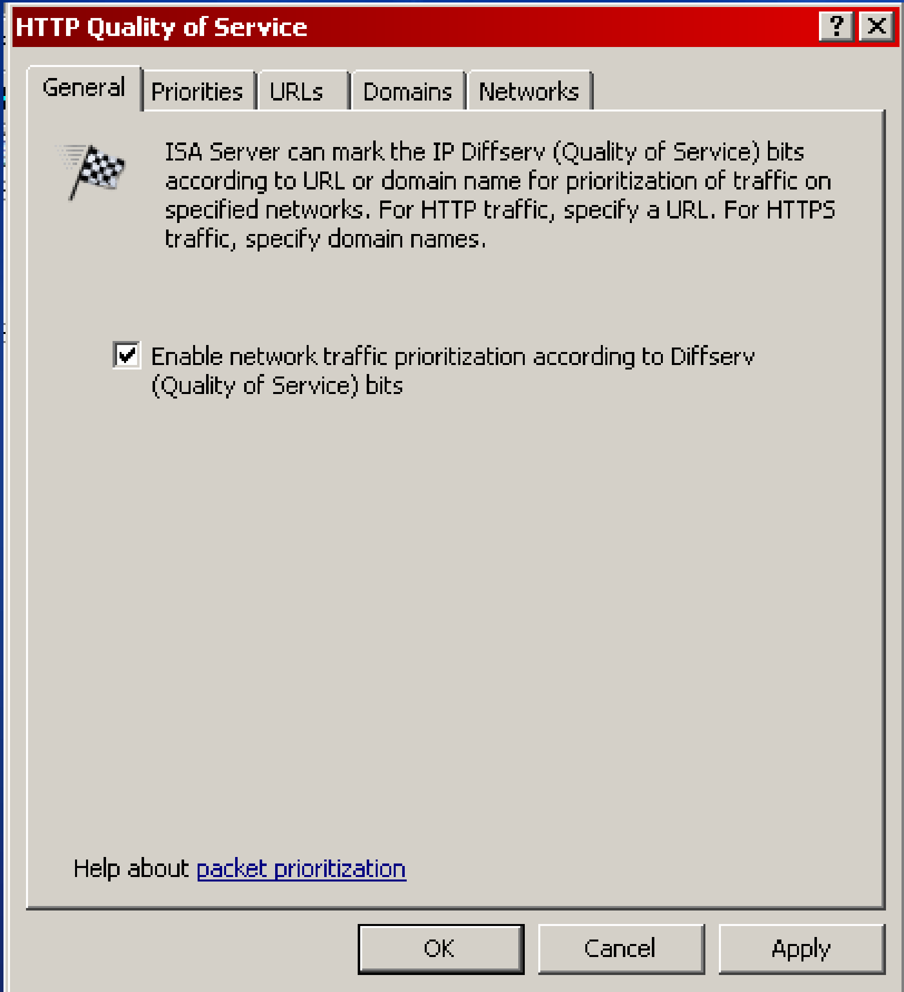
缓存和压缩



缓存、压缩、检查

为缓解性能问题，关闭检查时请清除缓存

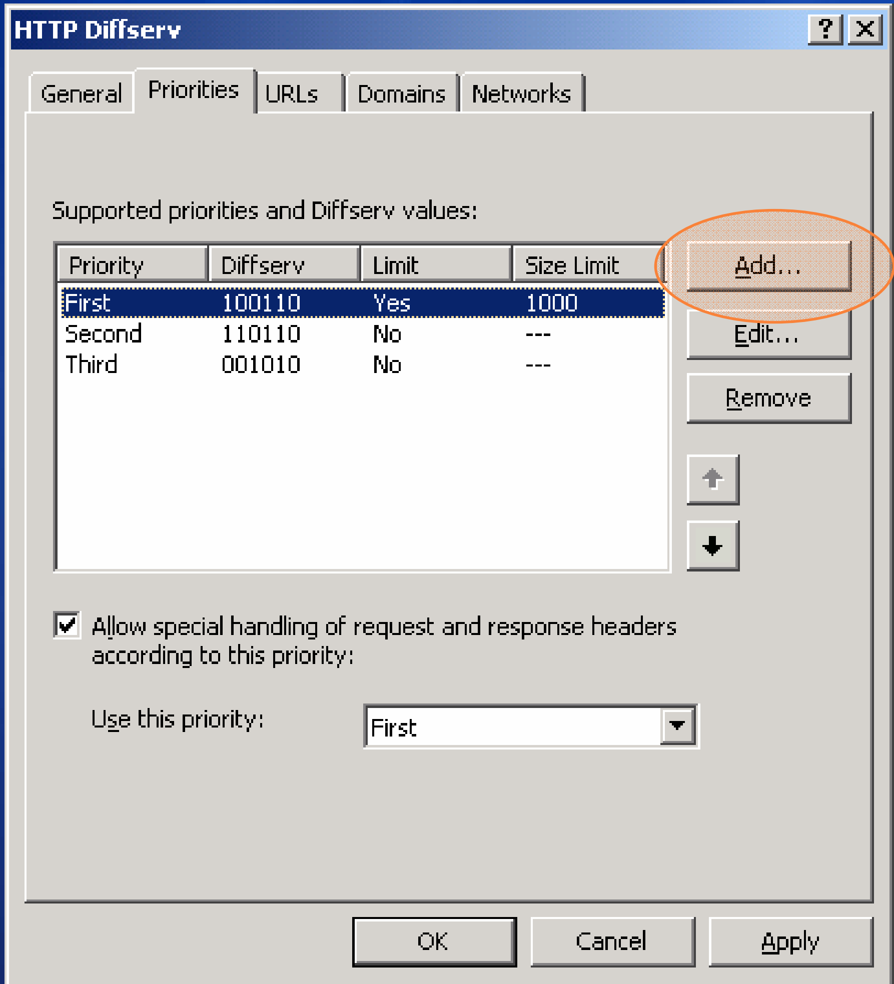
DiffServ 优先化

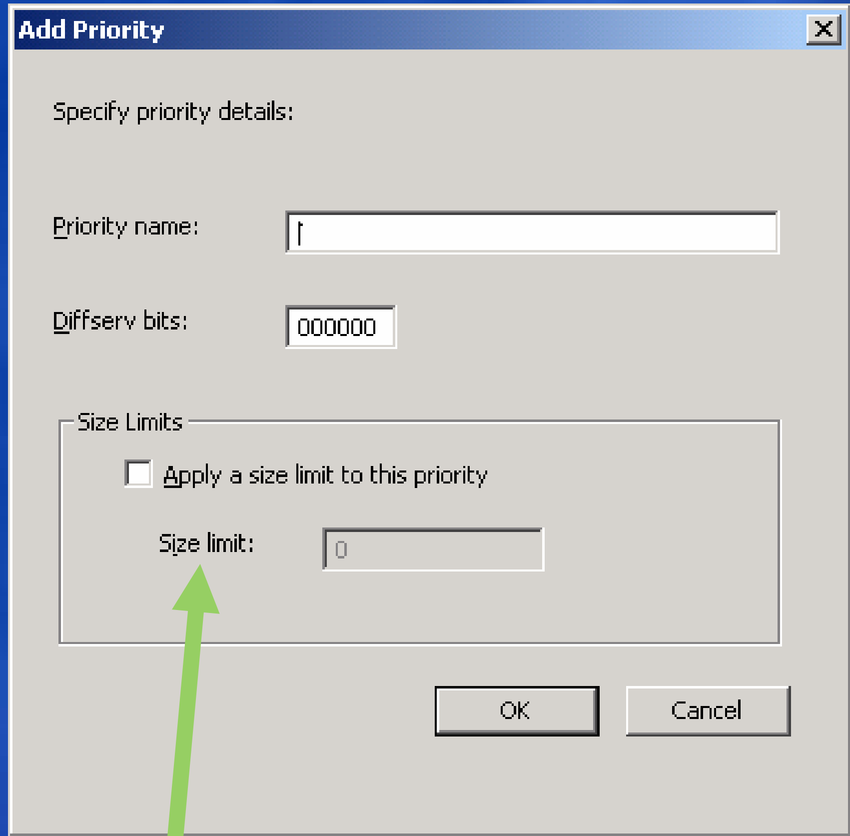


- 全局 HTTP 策略
- 扫描 URL 或域；分配流量优先级
- 将配置与路由器中的 DiffServ 设置进行匹配
- 仅适用于 HTTP 和 HTTPS
  - 不要将 DiffServ 位添加到其它协议
  - 可以从非 HTTP 非 HTTPS 中删除 DiffServ

> 应用优先化

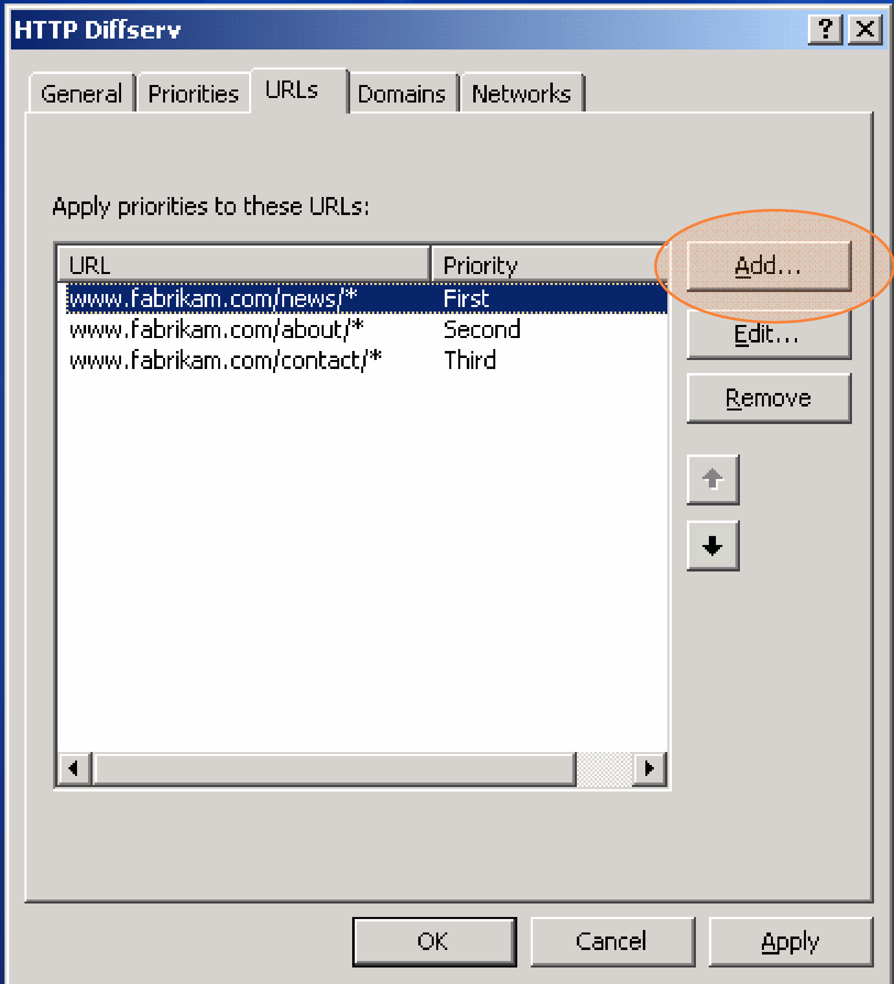
1

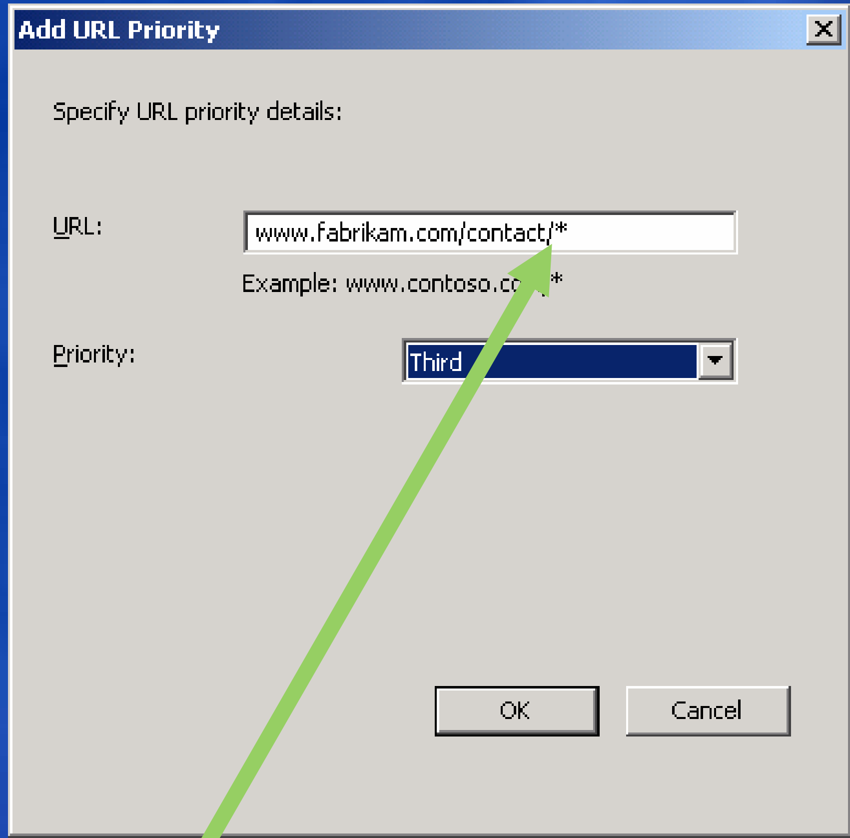




超过此限制的请求或响
应将收到下一个优先级

> 应用优先化



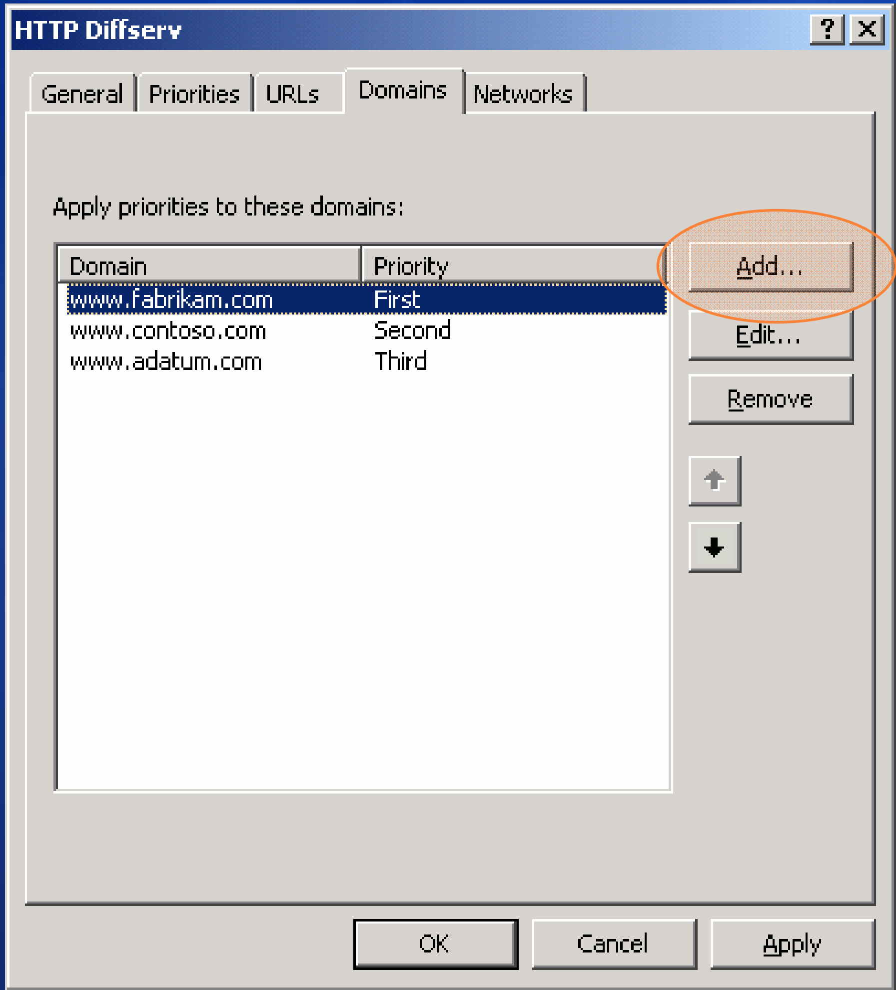


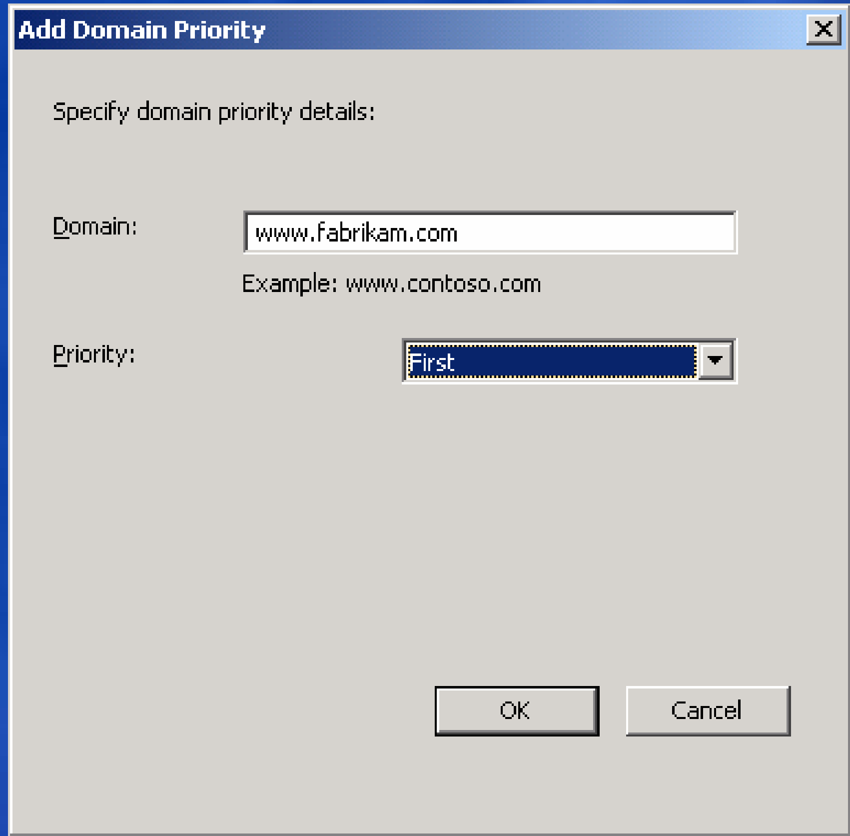
* 用于整个分支机构，但是记住要考虑顺序！

- 不适用于 HTTPS（无法知道 URL）

> 应用优先化

3

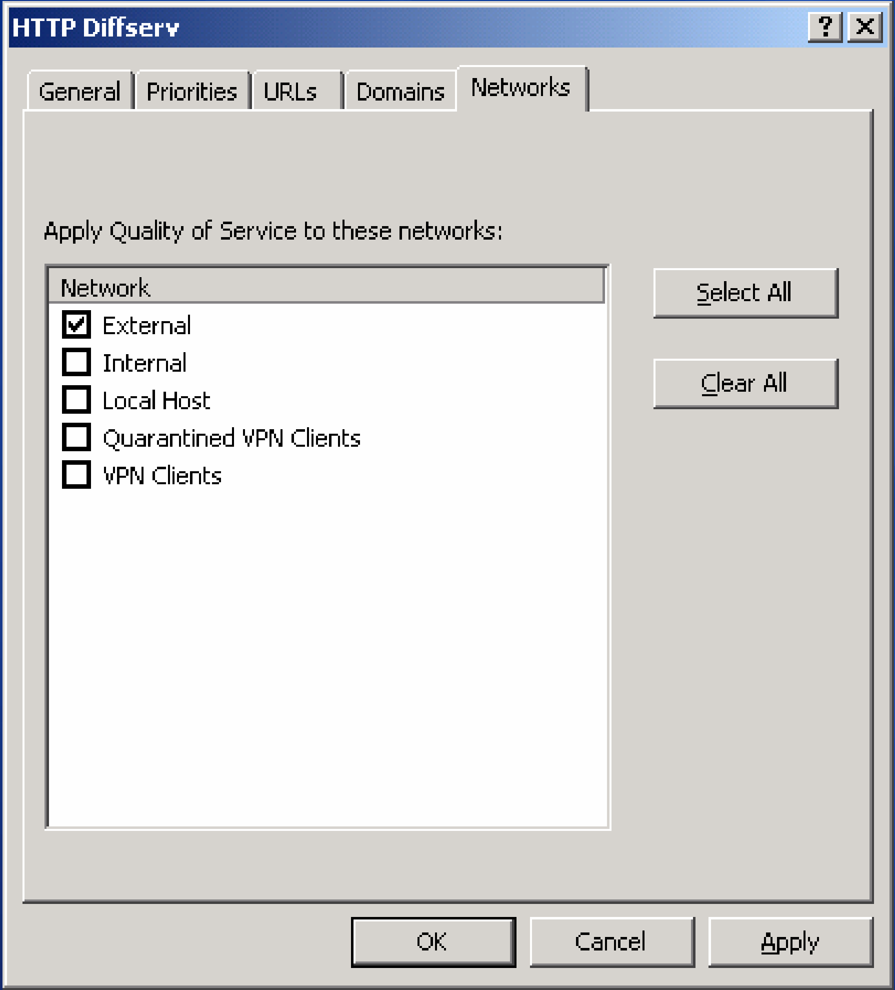




- 这是用于 HTTPS 站点的配置

> 应用优先化

完成


HTTP Diffserv
General
Priorities
URLs
Domains
Networks
Apply Quality of Service to these networks:
Network
External
Internal
Local Host
Quarantined VPN Clients
VPN Clients
Select All
Clear All
OK
Cancel
Apply

Internet 访问保护

按数量

70%	发生在应用程序层的攻击
95%	配置漏洞导致的攻击
炫耀	最少见的攻击动机
利益	最常见的攻击动机

各种研究

防洪抑制

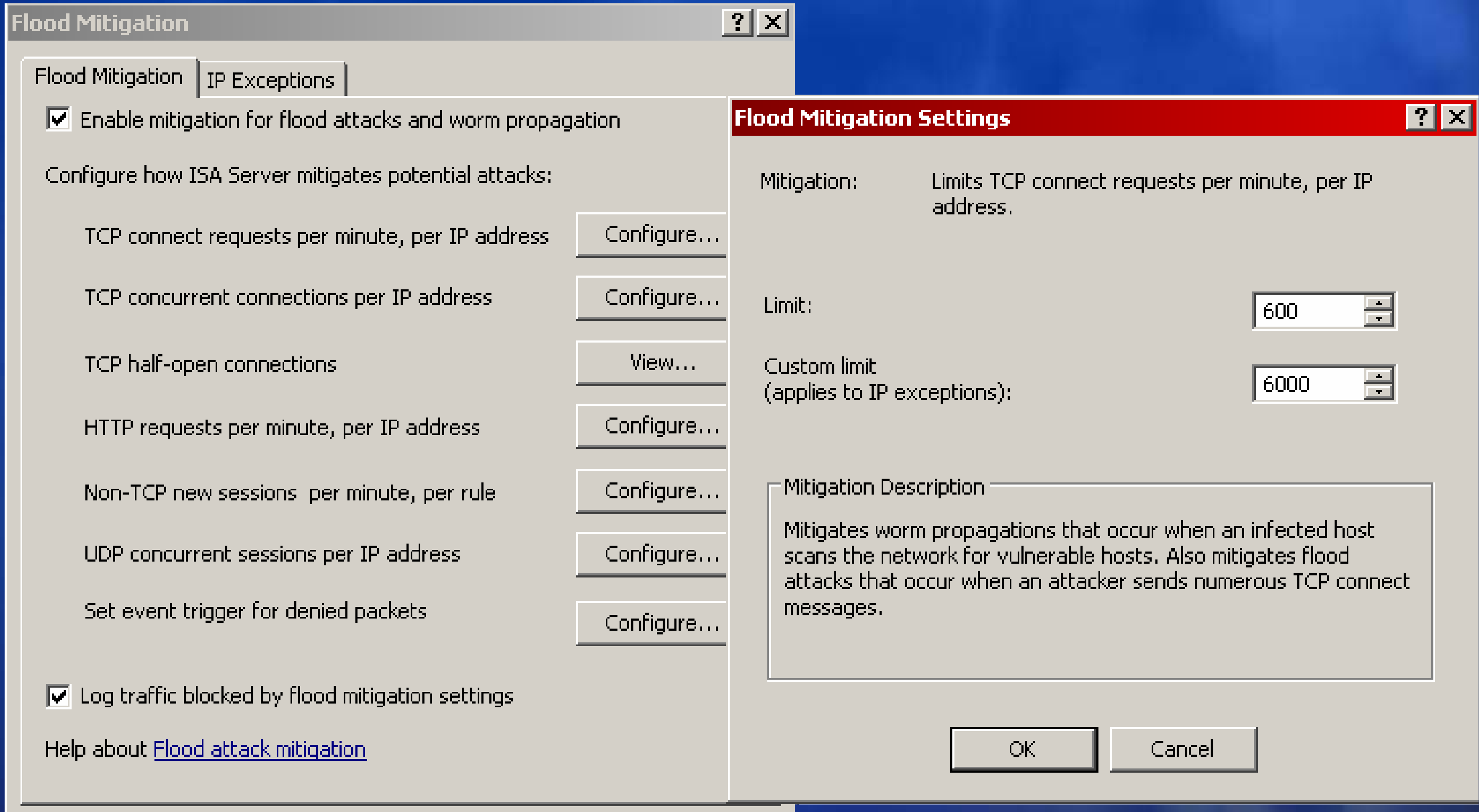
- 保护 ISA Server 避免—
  - 蠕虫传播
  - Syn 泛洪
  - 拒绝服务
  - 分布式 DoS
  - HTTP 轰炸
- 在某些情况下，ISA 后面的计算机也受到保护，但这不是该功能的主要目标

缓解缺省设置

缓解	缺省值	例外
每个源 IP 允许的并发 TCP 连接数量 *在恶意主机保持与 ISA 或 ISA 后面的受害计算机的无数 TCP 连接时，缓解 TCP 泛洪攻击*	100	400
每个源 IP 每分钟创建的 HTTP 请求数量 *在恶意主机向受害网站发送无数的 HTTP 请求时，缓解 HTTP DoS 攻击*	600	6000
每个源 IP 允许的并发非 TCP 连接数 *在恶意主机向 ISA 后面的受害计算机发送无数的 UDP 或 ICMP 消息时，缓解非 TCP 泛洪攻击*	100	400
每个规则每分钟的非 TCP 会话数量 *在许多傀儡 主机参与攻击或用无数非 TCP 数据包堵塞网络时，缓解非 TCP DDoS*	1000	
在每个 IP 每分钟被拒绝的数据包超过限制时触发事件 *向 ISA 管理员发出有关恶意 IP 的警报通知*	100	

> 应用防洪缓解

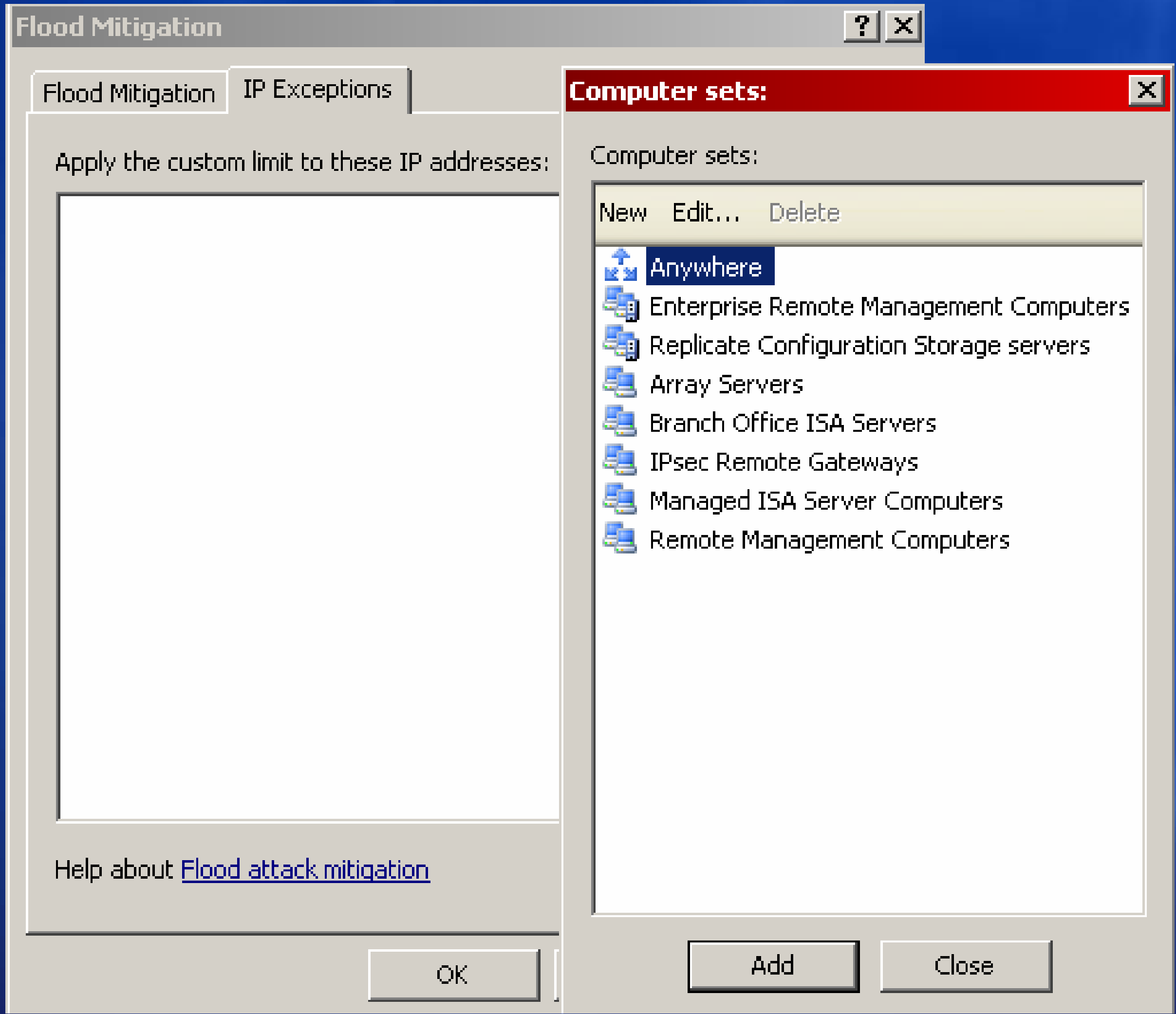
1



Flood Mitigation
Flood Mitigation
IP Exceptions
Enable mitigation for flood attacks and worm propagation
Configure how ISA Server mitigates potential attacks:
TCP connect requests per minute, per IP address
Configure...
TCP concurrent connections per IP address
Configure...
TCP half-open connections
View...
HTTP requests per minute, per IP address
Configure...
Non-TCP new sessions per minute, per rule
Configure...
UDP concurrent sessions per IP address
Configure...
Set event trigger for denied packets
Configure...
Log traffic blocked by flood mitigation settings
Help about Flood attack mitigation
Flood Mitigation Settings
Mitigation:
Limits TCP connect requests per minute, per IP address.
Limit:
600
Custom limit (applies to IP exceptions):
6000
Mitigation Description
Mitigates worm propagations that occur when an infected host scans the network for vulnerable hosts. Also mitigates flood attacks that occur when an attacker sends numerous TCP connect messages.
OK
Cancel

> 应用防洪缓解

完成



Flood Mitigation
Flood Mitigation
IP Exceptions
Apply the custom limit to these IP addresses:
Help about Flood attack mitigation
OK
Computer sets:
Computer sets:
New
Edit...
Delete
Anywhere
Enterprise Remote Management Computers
Replicate Configuration Storage servers
Array Servers
Branch Office ISA Servers
IPsec Remote Gateways
Managed ISA Server Computers
Remote Management Computers
Add
Close

资源控制

日志调节	达到某个阈值后停止登记被拒绝的记录
内存消耗	如果消耗的 NPP 达到总数的 90%，则拒绝新连接 • 继续为现有连接提供服务 • 完全自动化；不大可能触发
DNS 查询	使用的线程达到 80% 后限制挂起的 DNS 查询数量 • FW 客户端请求 ISA 解析主机 • ISA 作为规则的一部分解析 DNS 名称

攻击缓解方案

蠕虫传播

- 内部感染主机向全都在同一端口上的随机 IP 发送无数的 TCP 请求
- 检查连接阈值
- 检查源 IP 未被欺骗
- 阻止该 IP 直至获得行政允许
- 最常见的泛洪攻击形式
- ISA 2004 并不能完全抵御它

攻击缓解方案

ISA 连接表滥用

- 攻击者使用许多非欺骗的 IP 对 ISA 的 TCP 连接进行 DoS 攻击
- 不会触发每个源的限制
- 检查非分页内存池数量；在 NPP 达到 90% 后停止接受新连接
- 清空空闲连接的连接表

- 不常见的攻击
- 可能导致针对 ISA 2004 的永久 DoS
- 市场上很少有防火墙能抵挡这种攻击

攻击缓解方案

挂起的 DNS 滥用

- ISA 被配置为拒绝到不希望的域的连接（或仅允许到特定域的连接）
- 感染主机向随机 IP 发送许多 TCP 连接；ISA 执行逆向 DNS 查找
- 在可用线程已使用 80% 以后阻止新请求
- 继续为不需要逆向 DNS 或答案在缓存中的请求服务
- 最常见原因：蠕虫传播
- 可能导致针对 ISA 2004 的临时 DoS

攻击缓解方案

连续 TCP 连接泛洪

- 攻击者连续打开并关闭许多 TCP 连接
- 使用同样的蠕虫传播缓解措施：检测来自相同 IP 的高数量连接
- 阻止该 IP

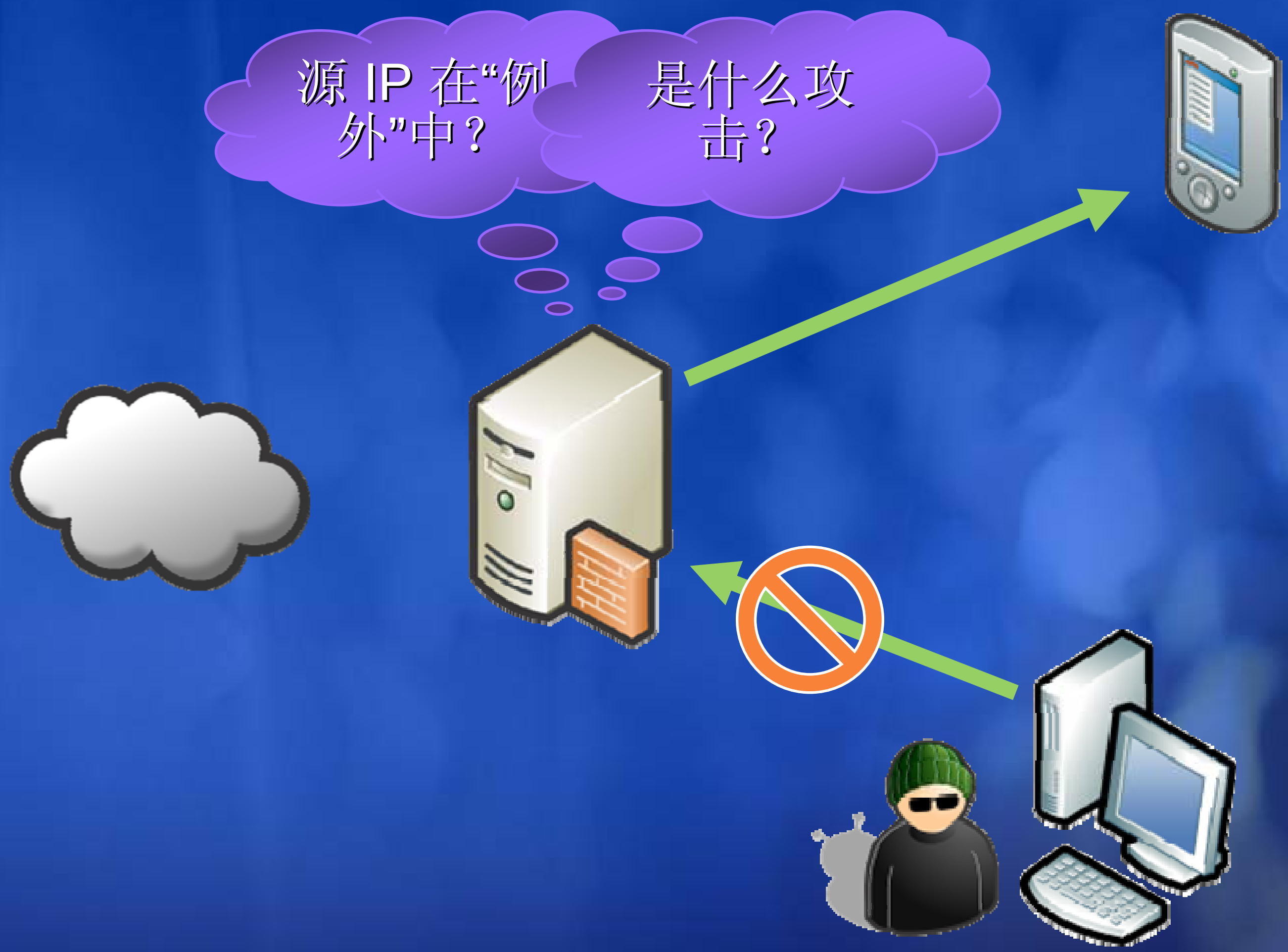
- 不常见
- 可能导致针对 ISA 2004 的临时 DoS

攻击缓解方案

通过现有连接的 HTTP DoS

- 攻击者建立到 Web 服务器的 TCP 连接
- 发送无数 HTTP 请求，超过阈值
- ISA 检测并限制客户端的请求速度
- 正在逐渐流行
- 可能导致针对 ISA 2004 的临时 DoS

警报触发器



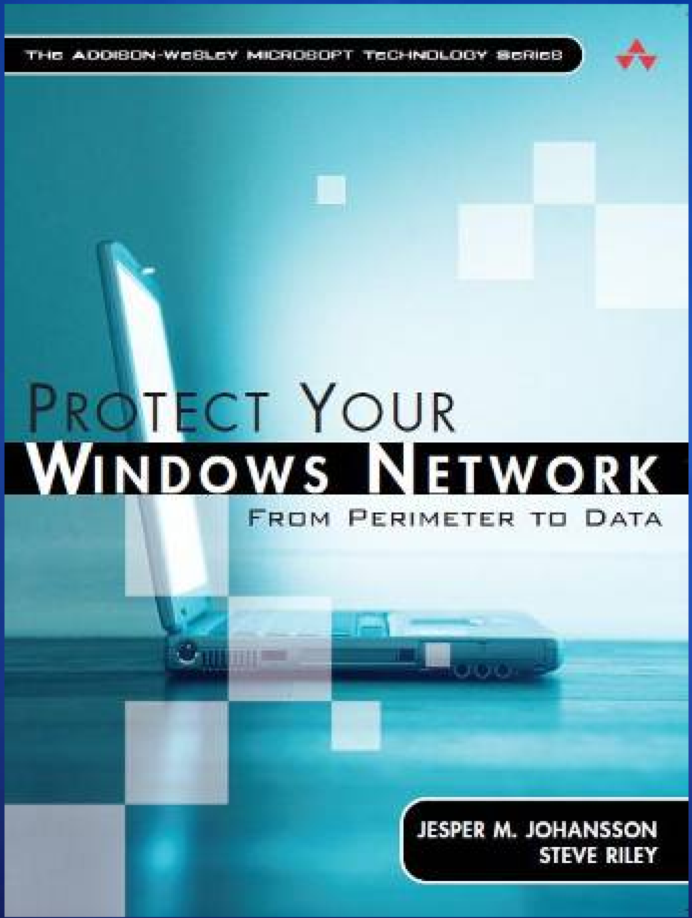
还有什么其它功能?

工具

- Windows Server 2003 的硬化版本
- 一些附加组件
  - 协议加速器
  - 反病毒网关
  - 内容筛选软件（URL、Web）
  - 反垃圾邮件筛选器
  - 高可用性加载项
- Standard 和 Enterprise 版本
- 工具场
  - NLB、CARP
  - 多服务器监视控制台
  - 专用配置存储
- 无人看管的部署
  - USB 驱动器
  - 分支机构向导

Steve Riley

steve.riley@microsoft.com
http://blogs.technet.com/steriley



www.protectyourwindowsnetwork.com

非常感谢！

Microsoft®

Your potential. Our passion.™