

Security



Copyright © 2002, 2003 ESRI. All rights reserved.

Lesson 3 goals

- Understanding security strategies
- Making your Web server more secure
  - Leveraging operating system security
  - Protecting ArcIMS with firewalls
- Restricting services with authentication
- Enabling HTTPS (SSL) Support

Copyright © 2002, 2003 ESRI. All rights reserved.

Understanding security strategies

- Basic security strategies
  - Least privilege
    - Only privileges needed to perform task
  - Defense in depth
    - Use multiple mechanisms that back each other up
  - Choke point
    - Allows monitoring and control
  - Weakest link
    - Eliminate weak links, monitor those you can’t eliminate
  - Fail safe stance
    - Failure of a defense should deny access
  - Universal participation
    - No one can opt out of security measures

Copyright © 2002, 2003 ESRI. All rights reserved.

Making ArcIMS secure

- **Steps that ArcIMS administrators can take to lock down their systems:**
  - **Set up a firewall**
  - **Install ArcIMS on a standalone system**
  - **Install only the OS, Web server, and JRE components**
  - **Disable all non-required services**
  - **Decrease the number of privileged programs**
  - **Set IUSR_computername or daemon user privileges**
  - **Set file permissions on directory structures**
  - **Delete/Move all sample Web sites**
  - **Deploy intrusion detection**

Copyright © 2002, 2003 ESRI. All rights reserved.

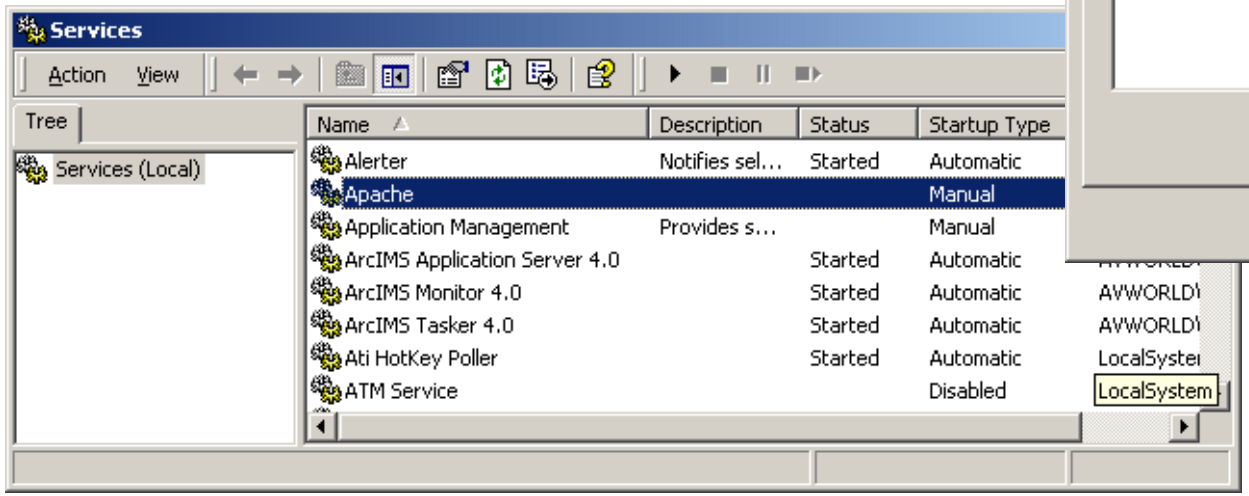
Operating system users and privileges

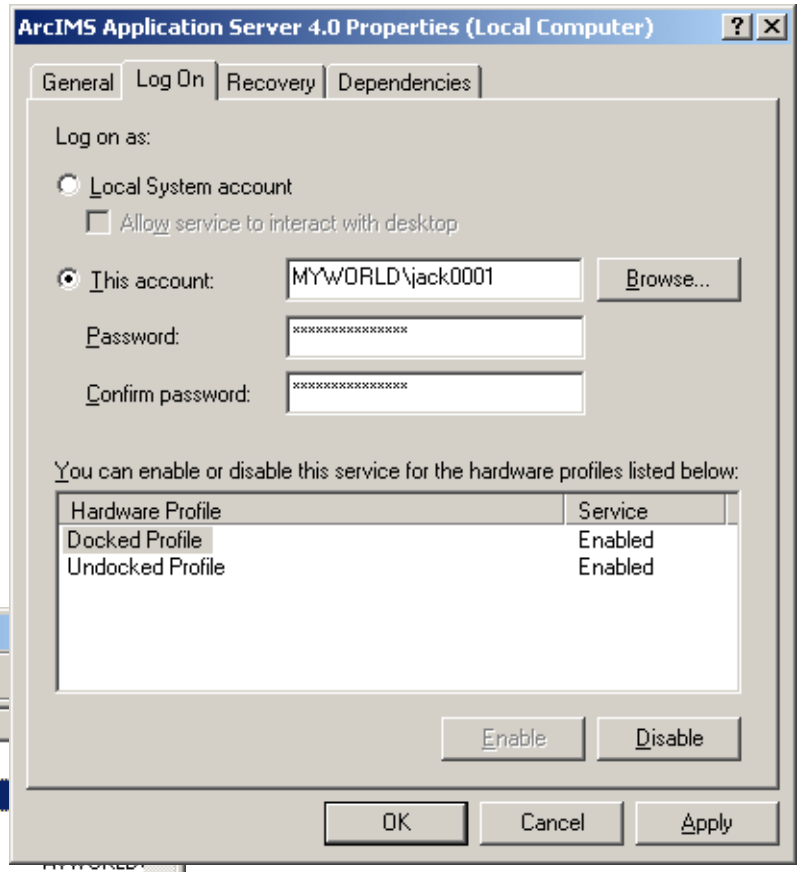
- UNIX hosts are secured with users, groups, and file permissions
  - Root is the most powerful user on the system
  - Non-privileged users are limited by file permissions
    - Read, write, execute
- Windows hosts are secured with Access Control Lists or system policies
  - Controls access to resources
    - Workstations, printers, disk space, applications
  - Use the Microsoft Management Console (MMC)
    - Create and/or edit security configuration files
    - Apply a security configuration to a system

Copyright © 2002, 2003 ESRI. All rights reserved.

Microsoft Windows 2000 services

- Logon account determines the security identity of the service at run time
- Determines the service's ability to access local and network resources

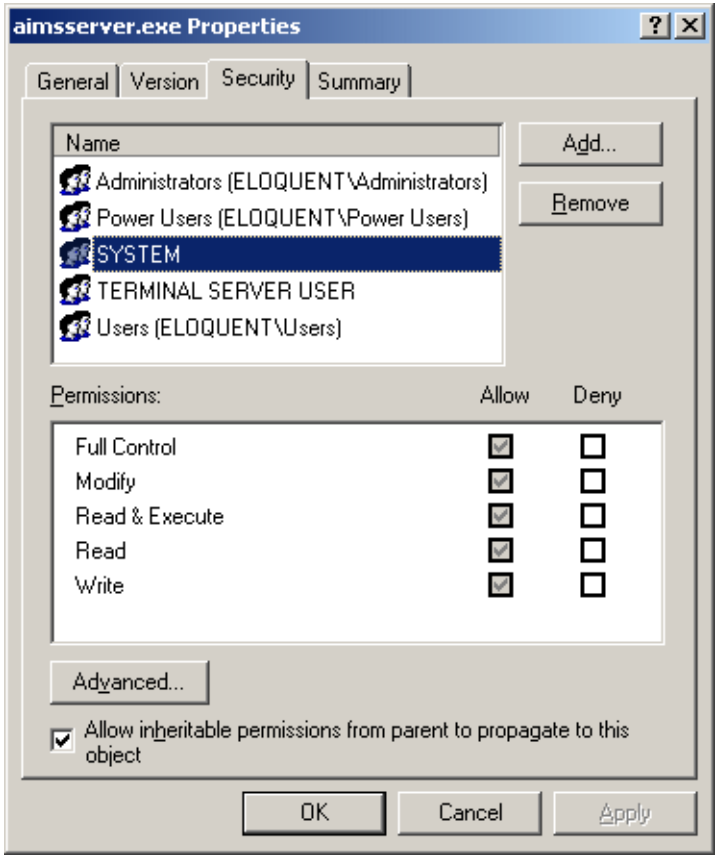




Copyright © 2002, 2003 ESRI. All rights reserved.

NTFS file permissions

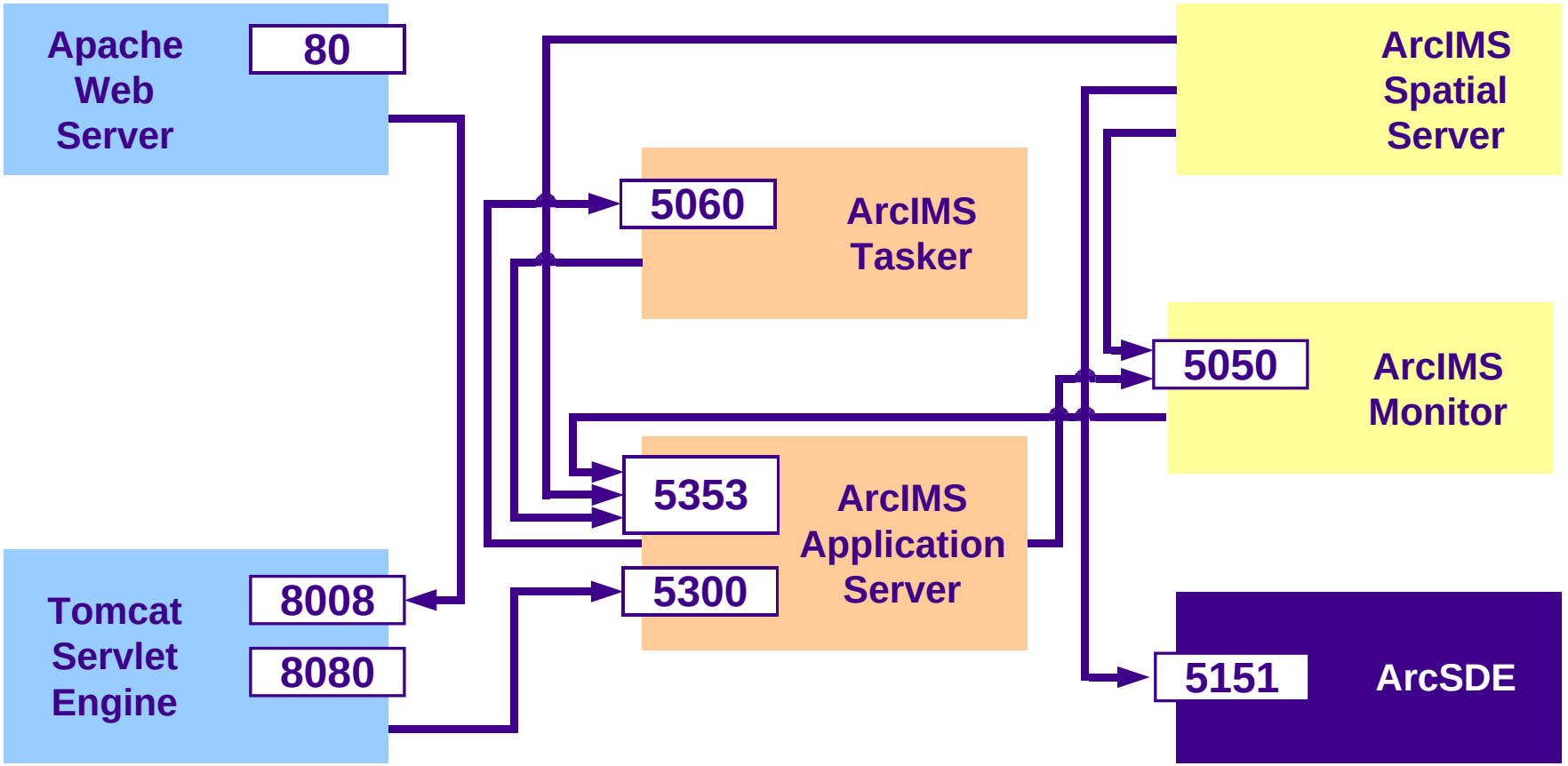
- Different than file *attributes*
- Used by Microsoft Windows NT 4.0 and Microsoft Windows 2000
- Default for most folders:
  - Administrators—Full Control
  - Creator/Owner—Full Control
  - Server Operators—Change
  - Authenticated Users—Read
  - System—Full Control
- Need to be changed to make a server secure



Copyright © 2002, 2003 ESRI. All rights reserved.

ArcIMS host listener ports

- ArcIMS communicates on many open ports
- Clients only need to talk to port 80

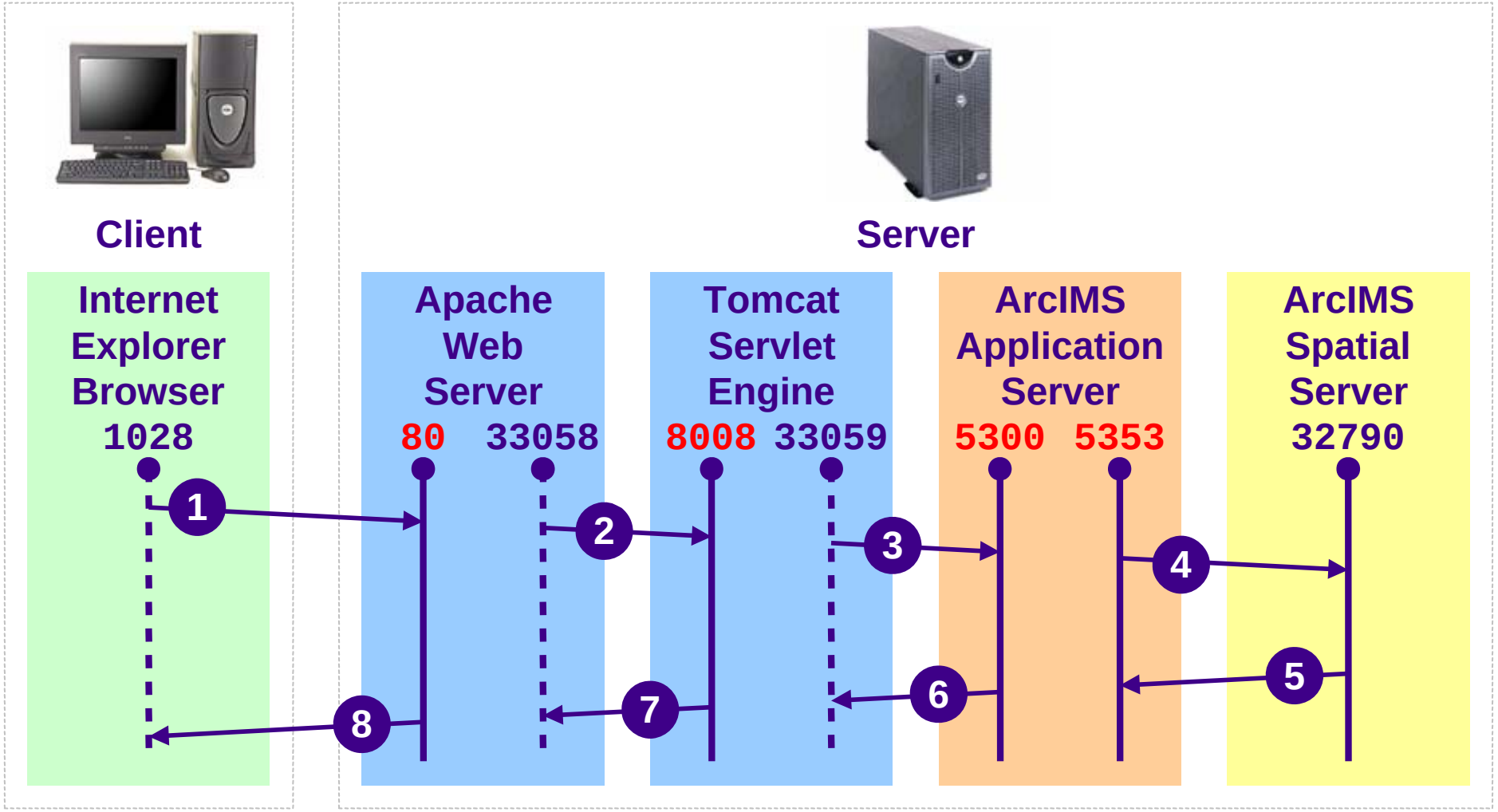


*Example assumes use of Apache, Tomcat, and ArcSDE

Copyright © 2002, 2003 ESRI. All rights reserved.

Life cycle of a request

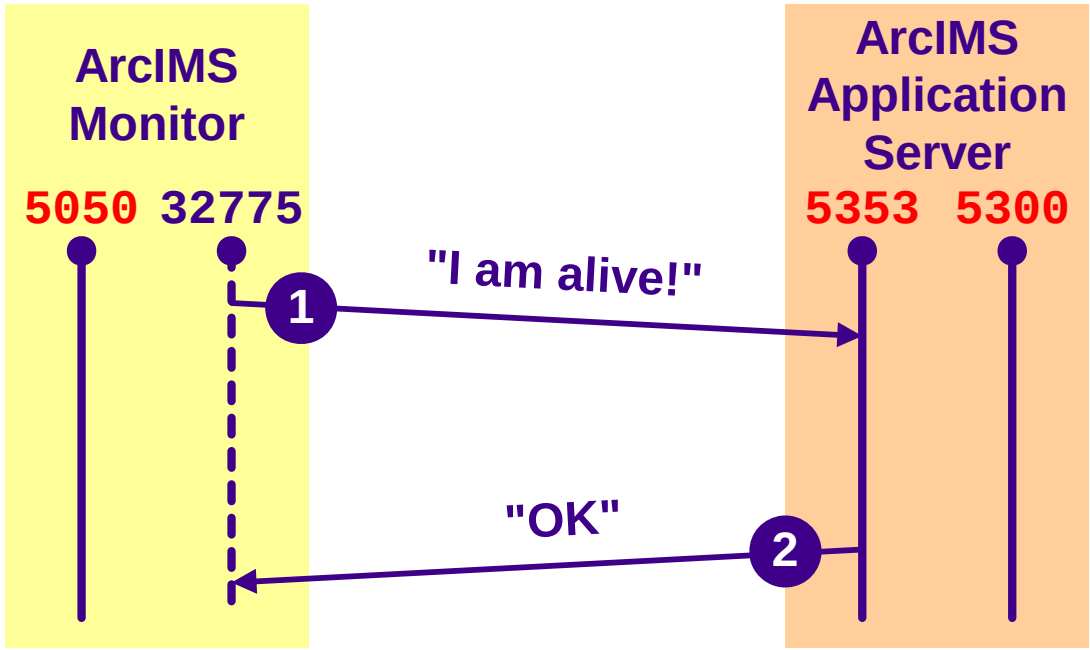
- Example: typical installation with Apache and Tomcat



Copyright © 2002, 2003 ESRI. All rights reserved.

Starting the ArcIMS Monitor service

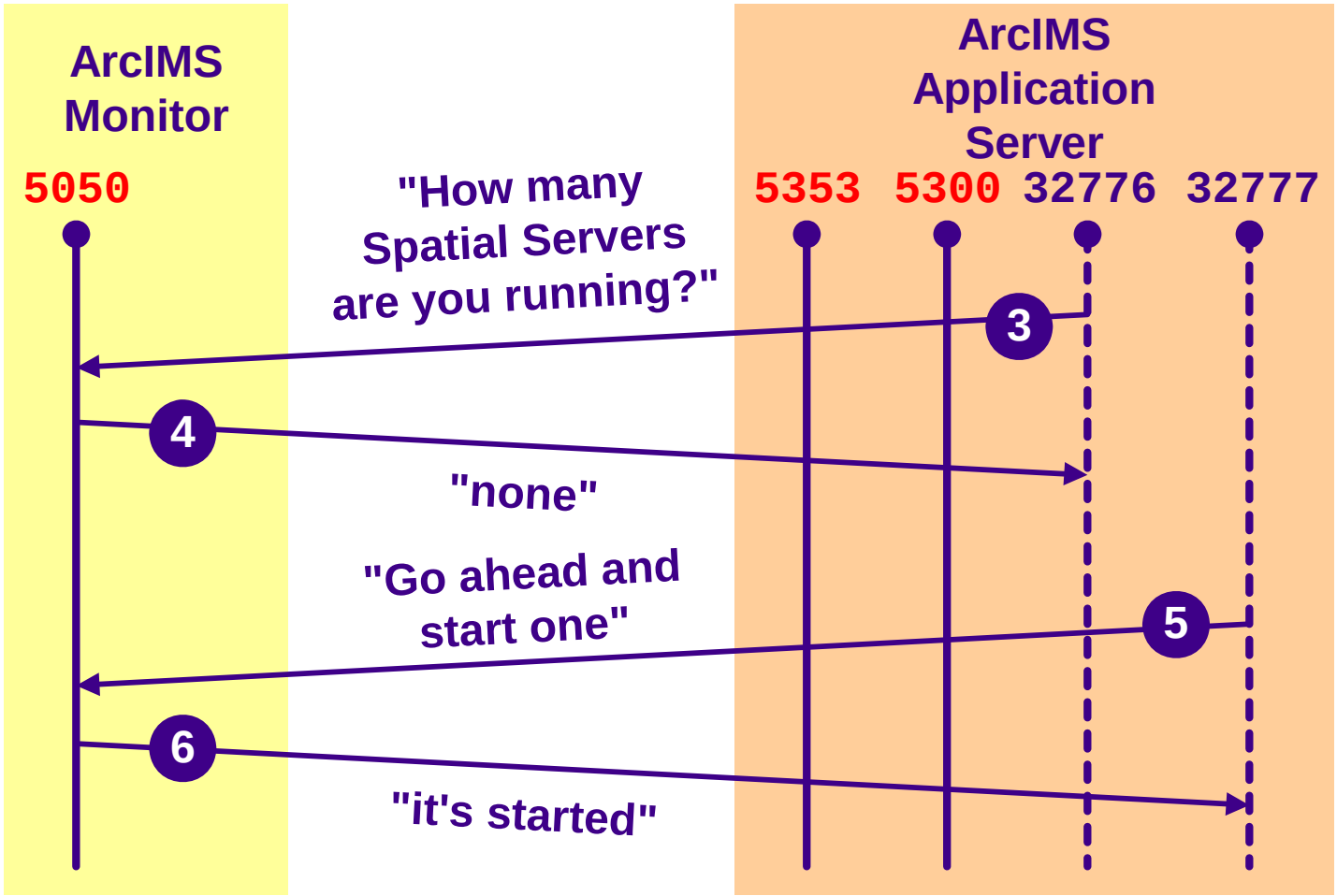
- When ArcIMS Monitor starts, it first registers with the ArcIMS Application Server on port 5353



Copyright © 2002, 2003 ESRI. All rights reserved.

Starting the ArcIMS Monitor service

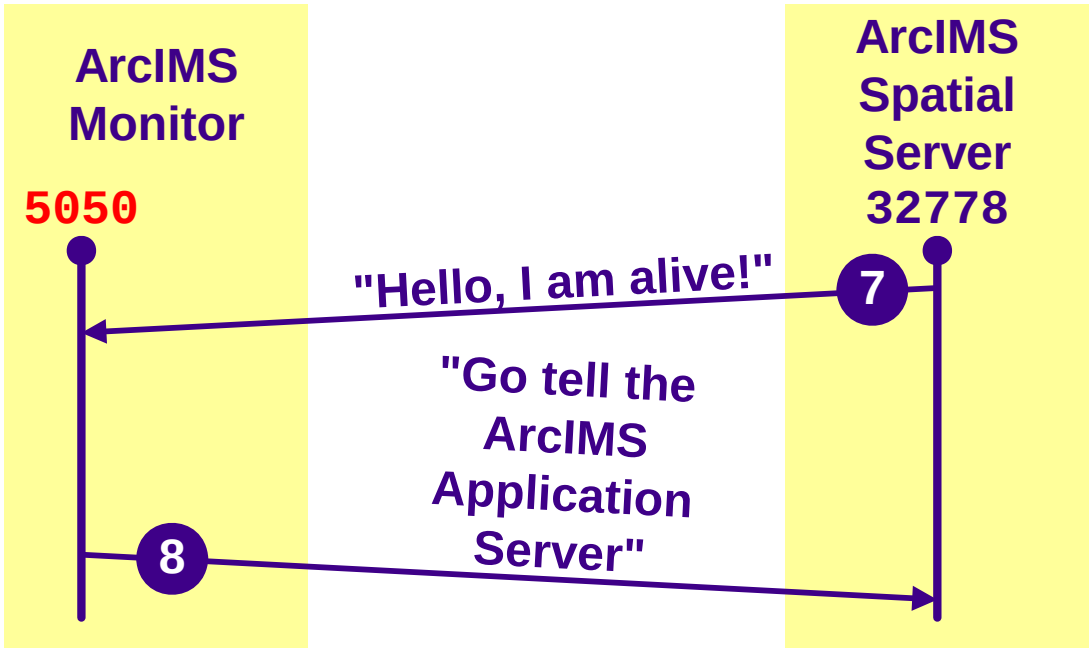
- ArcIMS Application Server tells ArcIMS Monitor to start an ArcIMS Spatial Server



Copyright © 2002, 2003 ESRI. All rights reserved.

Starting the ArcIMS Monitor service

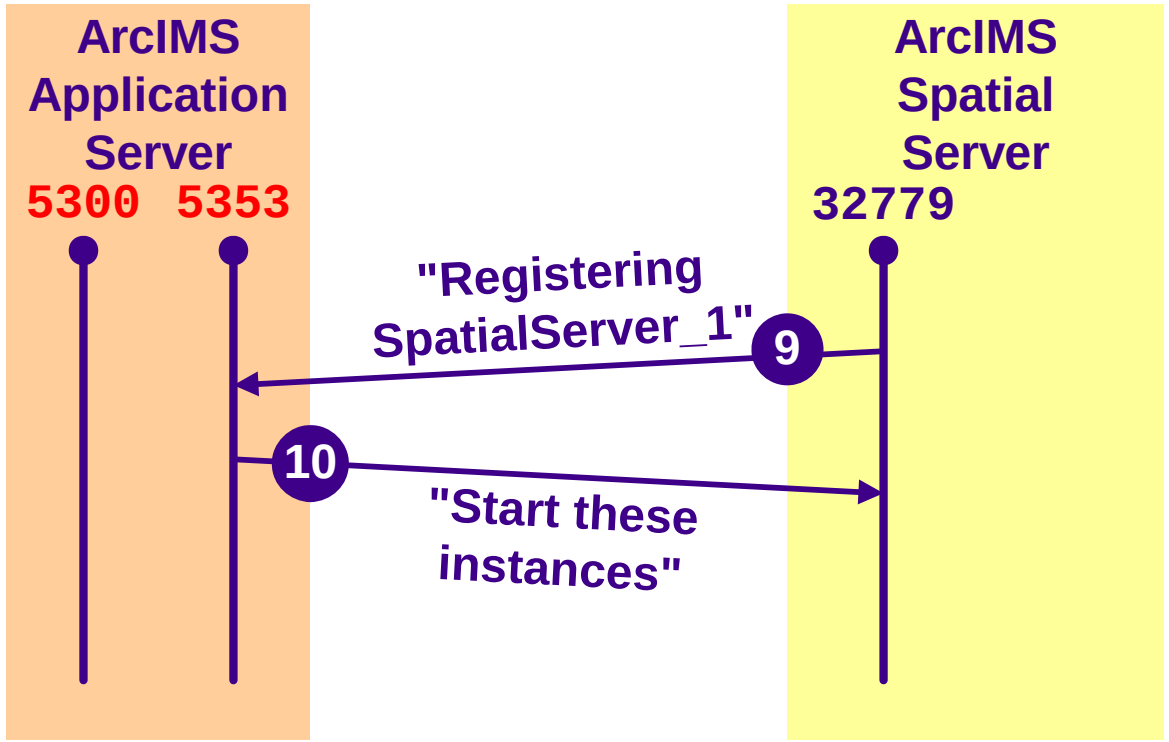
- ArcIMS Spatial Server process is now running
- Registers with ArcIMS Monitor on port 5050



Copyright © 2002, 2003 ESRI. All rights reserved.

Starting the ArcIMS Monitor service

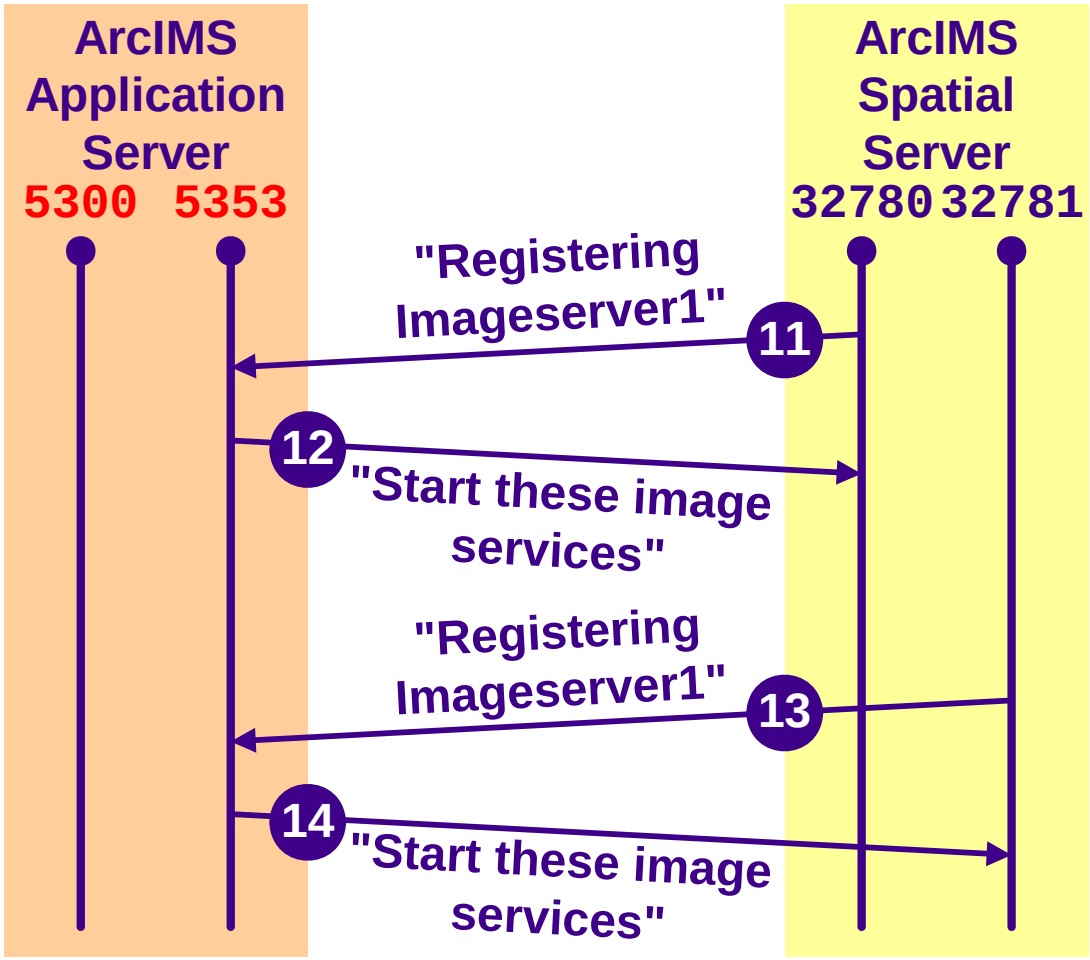
- The ArcIMS Spatial Server contacts the ArcIMS Application Server on port 5353



Copyright © 2002, 2003 ESRI. All rights reserved.

Starting the ArcIMS Monitor service

- Each Virtual Server instance registers with the ArcIMS Application Server



Copyright © 2002, 2003 ESRI. All rights reserved.

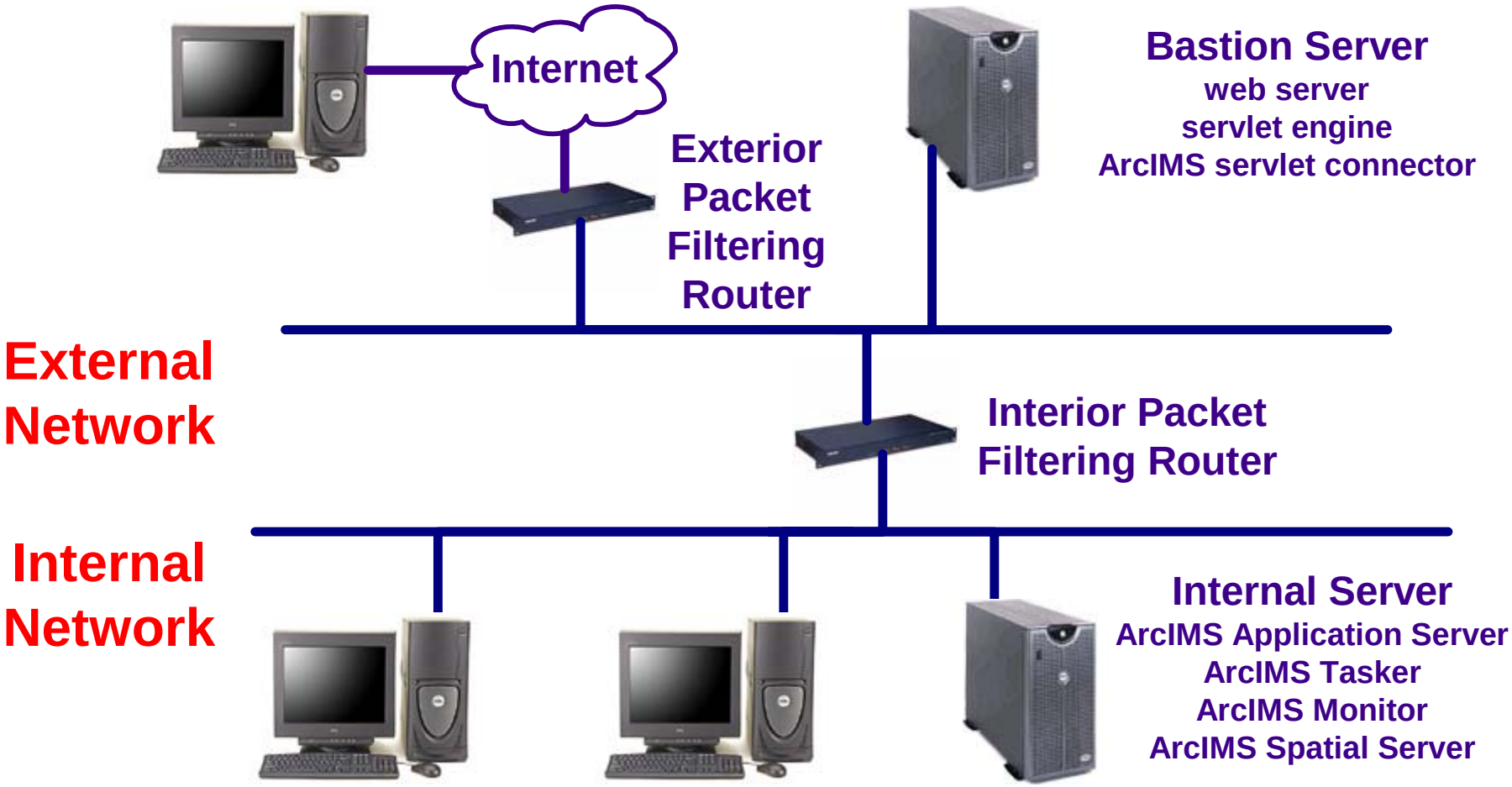
Locating ArcIMS hosts

- The location of the Web server and ArcIMS host has security implications
  - Both Web server and ArcIMS host on a perimeter network
    - Do not store confidential data here
    - Need to move and synchronize data
  - Both Web server and ArcIMS host on an internal network 
    - Implicit trust in Web server security
    - Consider using a proxy instead of a packet filter
  - Web server on a perimeter network and ArcIMS host on an internal network
    - Need to create packet filtering rules for ArcIMS host

Copyright © 2002, 2003 ESRI. All rights reserved.

Example firewall architecture

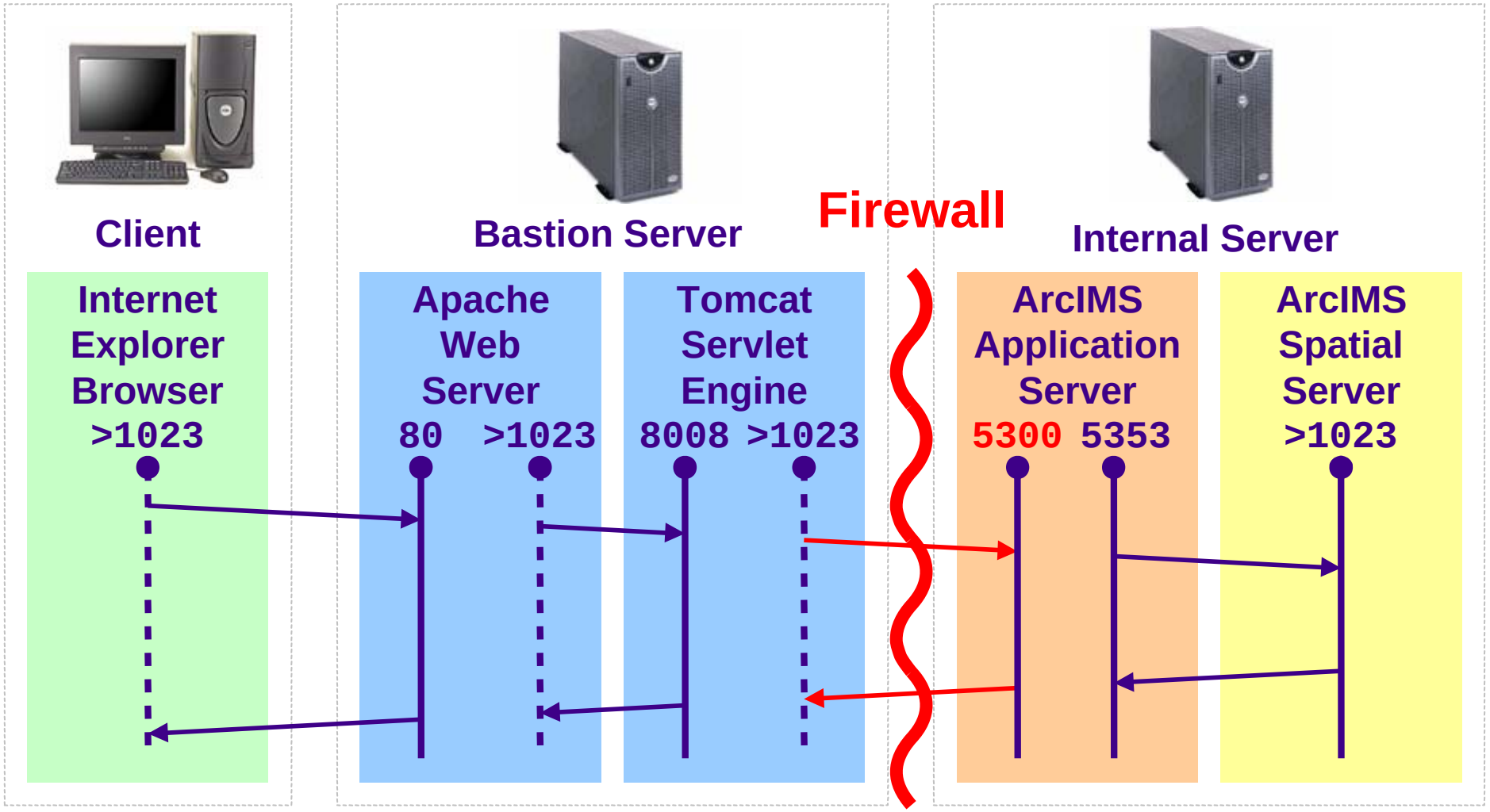
- Web server on a perimeter network and ArcIMS host on an internal network



Copyright © 2002, 2003 ESRI. All rights reserved.

Locating a Web server on an external network

- Need to allow servlet to connect to application server



Copyright © 2002, 2003 ESRI. All rights reserved.

Choosing packet filtering criteria

- Permit or deny packets by examining headers
  - IP source address
  - IP destination address
  - Protocol (TCP, UDP, or ICMP)
  - TCP or UDP source port
  - TCP or UDP destination port
  - ICMP message type
  - Ack Set
- Permit or deny packets by routing direction
  - NIC packet arrives on
  - NIC packet leaves on

Copyright © 2002, 2003 ESRI. All rights reserved.

Creating packet filter rules for ArcIMS

- Example: Web server on an external network
  - Rules needed to permit the external ArcIMS Servlet Connector to connect to the internal ArcIMS Application Server
  - Rules are for packets, not TCP connections

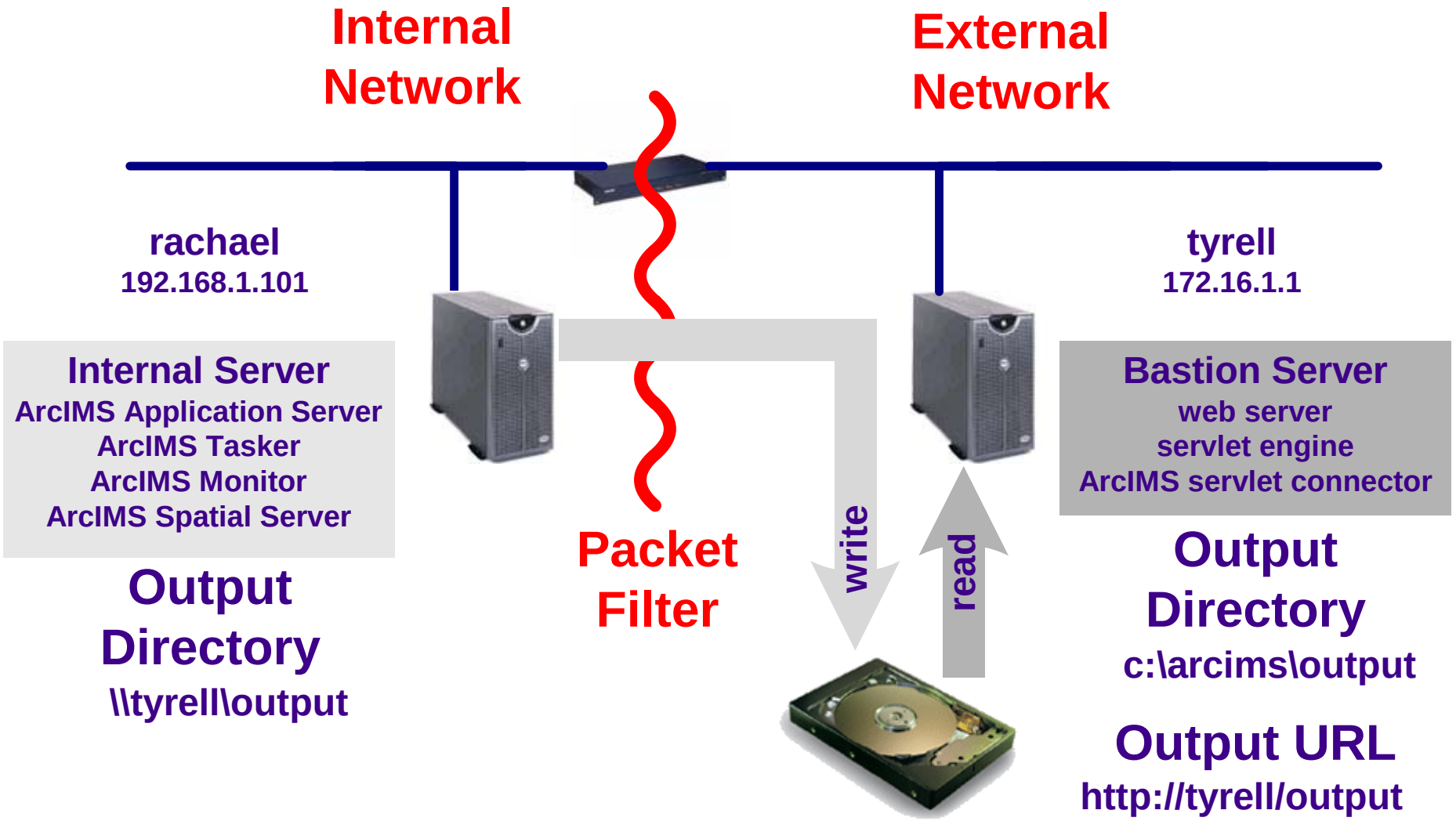
Packet Direction	Source Addr.	Dest Addr.	Prototcol	Source Port	Dest Port	Ack Set	Notes
In	Ext	Int	TCP	>1023	5300	[a]	Incoming connection, Servlet to Application Server
Out	Int	Ext	TCP	5300	>1023	Yes	Incoming connection, Application Server to Servlet

[a] ACK is not set on the first packet when establishing a connection

Copyright © 2002, 2003 ESRI. All rights reserved.

Output directory file I/O

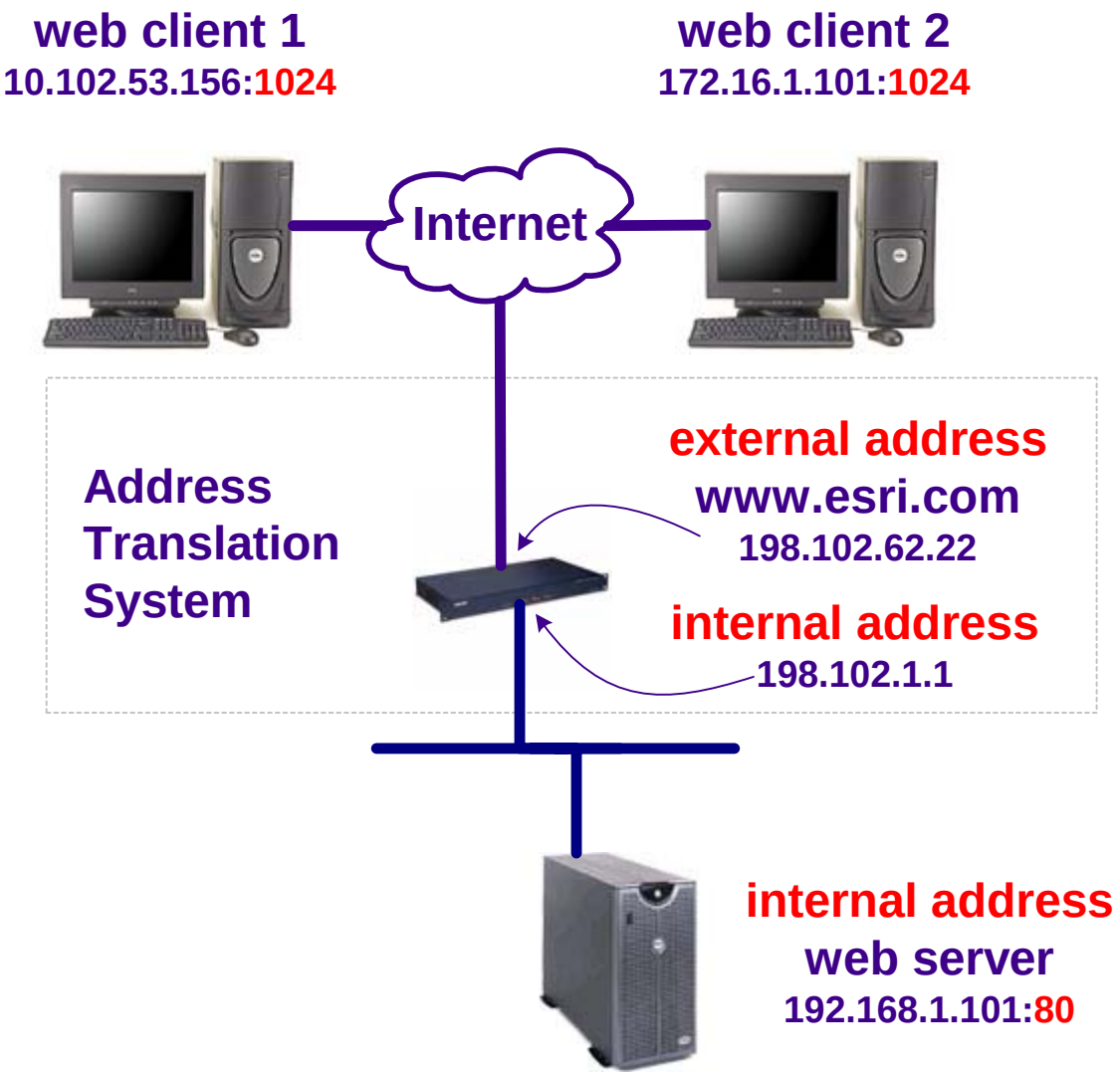
- File sharing through firewall has high risks



Copyright © 2002, 2003 ESRI. All rights reserved.

ArcIMS and Network Address Translation (NAT)

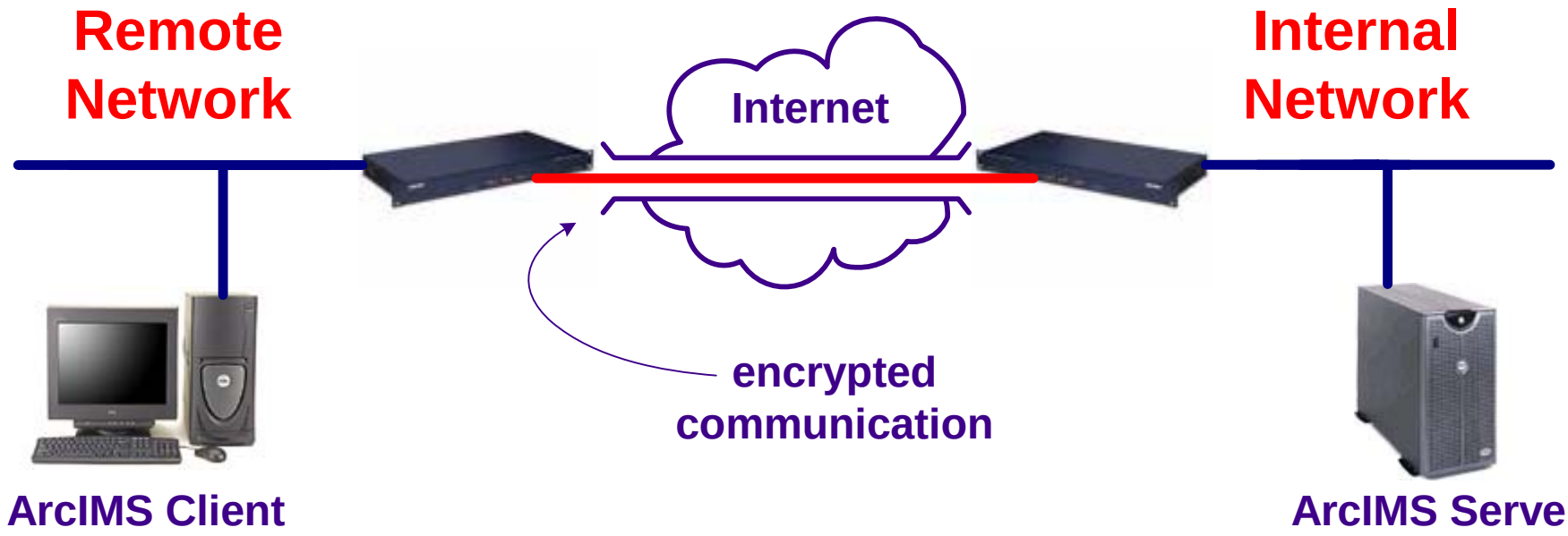
- Modifies packet headers
  - Clients will not see internal addresses
- Complements packet filtering
  - Use private addresses that cannot be routed



Copyright © 2002, 2003 ESRI. All rights reserved.

Virtual Private Network (VPN)

- Uses a public network as a private network
  - All traffic is encrypted, integrity protected, and encapsulated
- Remote network becomes part of internal network
  - Extends network you need to protect

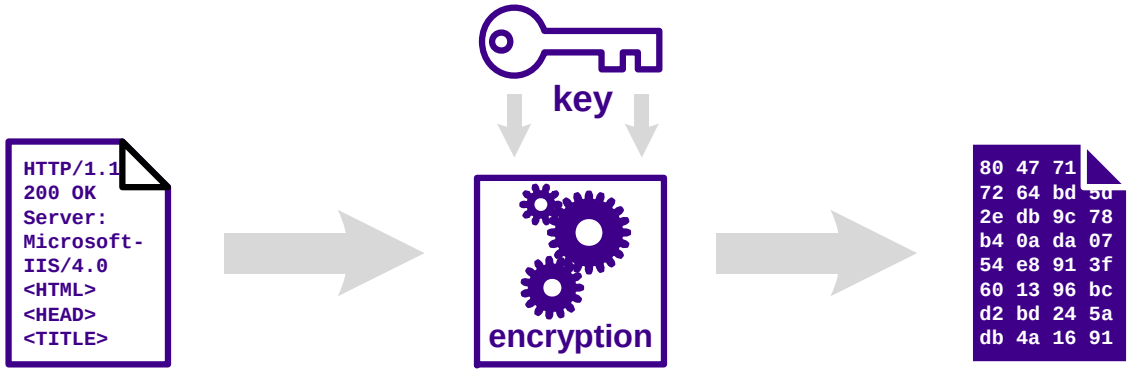


Copyright © 2002, 2003 ESRI. All rights reserved.

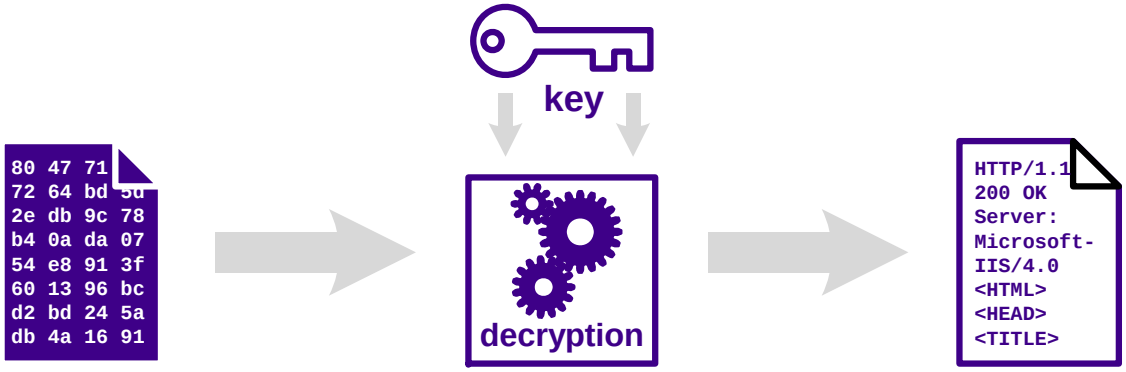
Cryptography basics

◆ Symmetric Key Algorithms

Sender encrypts message using a secret key



Recipient decrypts message using the same key

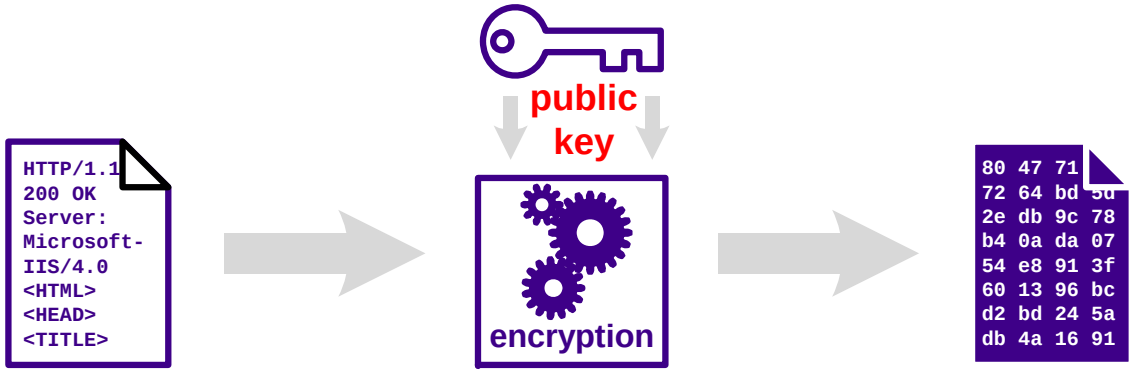


Copyright © 2002, 2003 ESRI. All rights reserved.

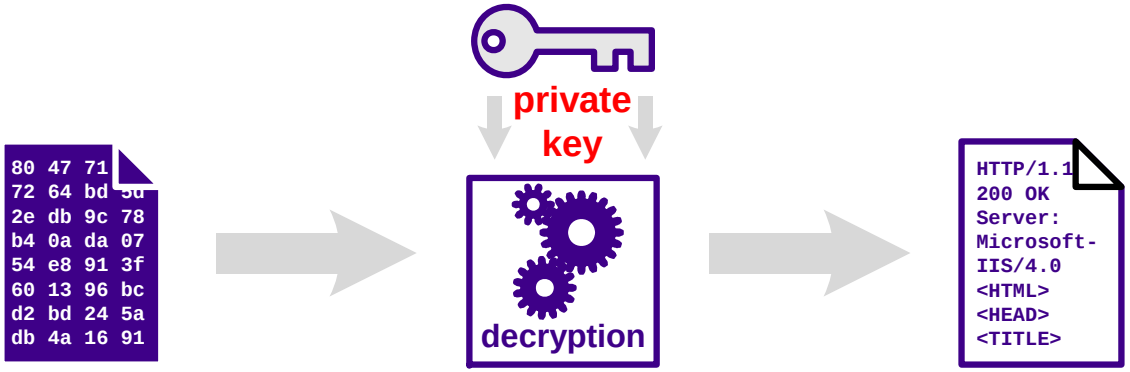
Cryptography basics

◆ Public Key Algorithms

Sender encrypts message using a public key



Recipient decrypts message using the private key



Copyright © 2002, 2003 ESRI. All rights reserved.

Understanding SSL

- Secure Sockets Layer (SSL) is used for sending encrypted information over the Internet
- SSL can be used for many different applications
  - E-mail (POP, SMTP, IMAP)
  - Web (HTTP becomes HTTPS)



- SSL performs the following steps to connect:
  1. Authenticate the server to the client.
  2. Allow the client and server to select the cryptographic algorithms, or ciphers, that they both support.
  3. Use public key encryption techniques to generate shared secrets.
  4. Establish an encrypted SSL connection.



Copyright © 2002, 2003 ESRI. All rights reserved.

Deploying SSL server certificates

- Needed to activate your Web server's SSL security
  - Obtain and install a valid server certificate
  - Certificates are issued by Certification Authorities (CA)

Warning when connecting to a secure server with Internet Explorer

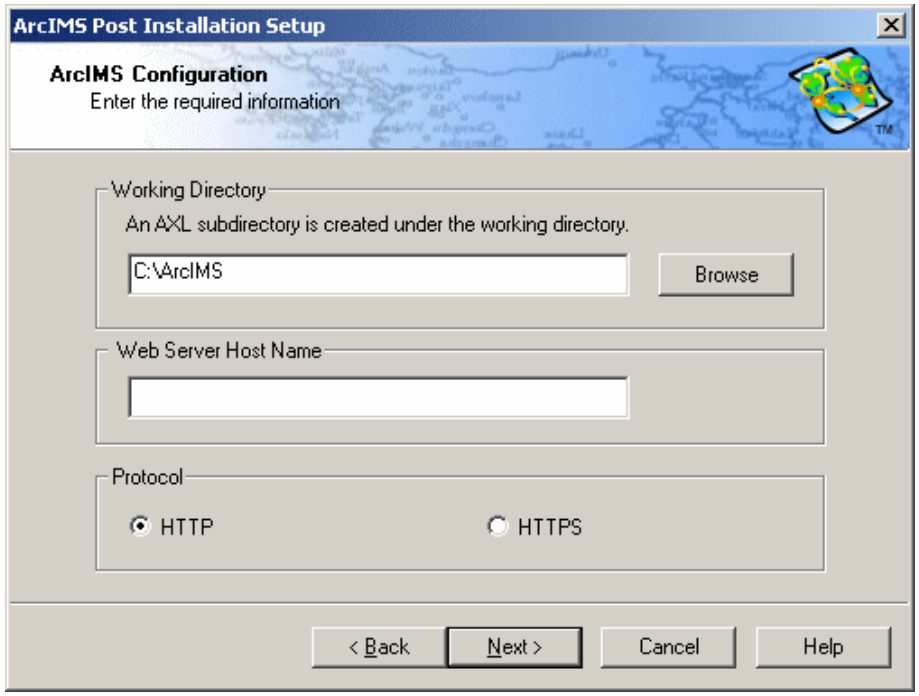


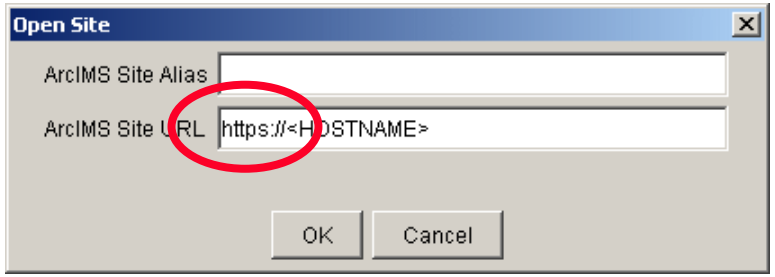


Copyright © 2002, 2003 ESRI. All rights reserved.

SSL and ArcIMS Administrator

- ArcIMS Administrator connects to port 80 by default
  - Specify https to connect using SSL instead
- May need to import the root CA certificate into cacerts





Copyright © 2002, 2003 ESRI. All rights reserved.

Restricting ArcIMS services

- Access to ArcIMS services can be restricted
  - Only people with proper credentials can access ArcIMS services
  - Process is called authentication
- Authentication works with clients using the Servlet Connector and Java Connector
  - Not used with ActiveX, ColdFusion, or AppServerLink

Copyright © 2002, 2003 ESRI. All rights reserved.

Limiting access

- By username and password
- By IP address
- By setting an expiration date
- By limiting the number of times a user can access the MapService
- By limiting certain “GET” elements

Copyright © 2002, 2003 ESRI. All rights reserved.

Access Control List (ACL)

- Text file-based
  - XML based using ArcXML elements
  - File is loaded in memory
  - Cumbersome to manage with many users
  - Must restart servlet engine after every change
- JDBC-based
  - Store permissions in a relational database accessed through a JDBC driver
  - Easier to manage large number of users
  - Changes can be made without restarting the servlet engine
- Services are not accessible unless listed in the ACL

Copyright © 2002, 2003 ESRI. All rights reserved.

Exercise 3 overview

- Update the esrimap_prop file
- Create a text-based ACL file
- Configure IIS 5.0 for Windows 2000
- Test authentication
- Add additional restrictions to ArcIMS services
- Create an SSL certificate request
- Request an SSL certificate
- Configure SSL for IIS
- Make an ArcIMS Web site with SSL

Copyright © 2002, 2003 ESRI. All rights reserved.