Implementing Network and Perimeter Security

Presenter Name

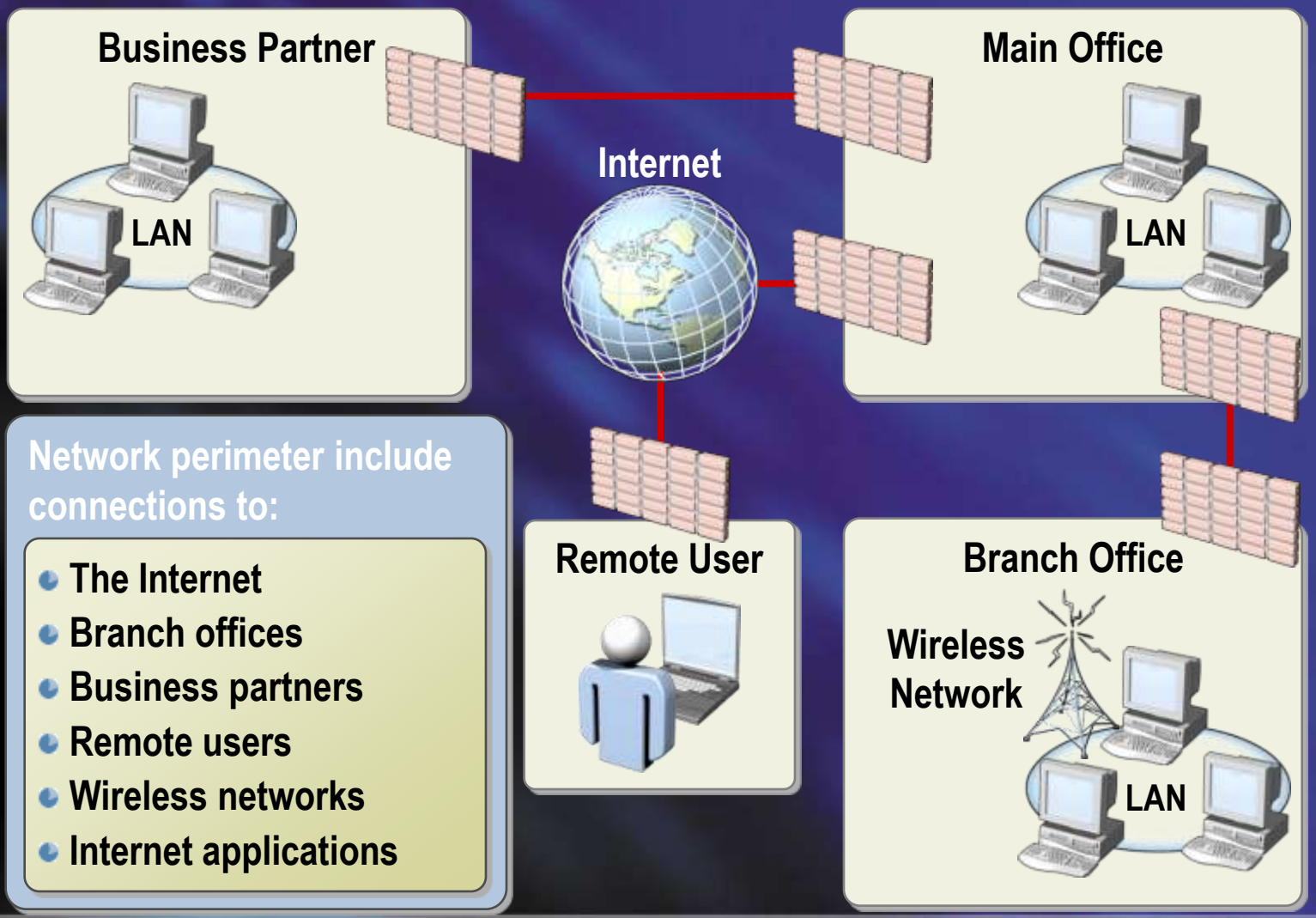
Job Title

Company

Goals of Network Security

	Perimeter Defense	Client Defense	Intrusion Detection	Network Access Control	Confi-dentiality	Secure Remote Access
ISA Server	✓		✓	✓		✓
Windows Firewall		✓				
IPSec		✓			✓	✓
Network Access Quarantine				✓		✓

Perimeter Connections Overview



Network perimeter include connections to:

- The Internet
- Branch offices
- Business partners
- Remote users
- Wireless networks
- Internet applications

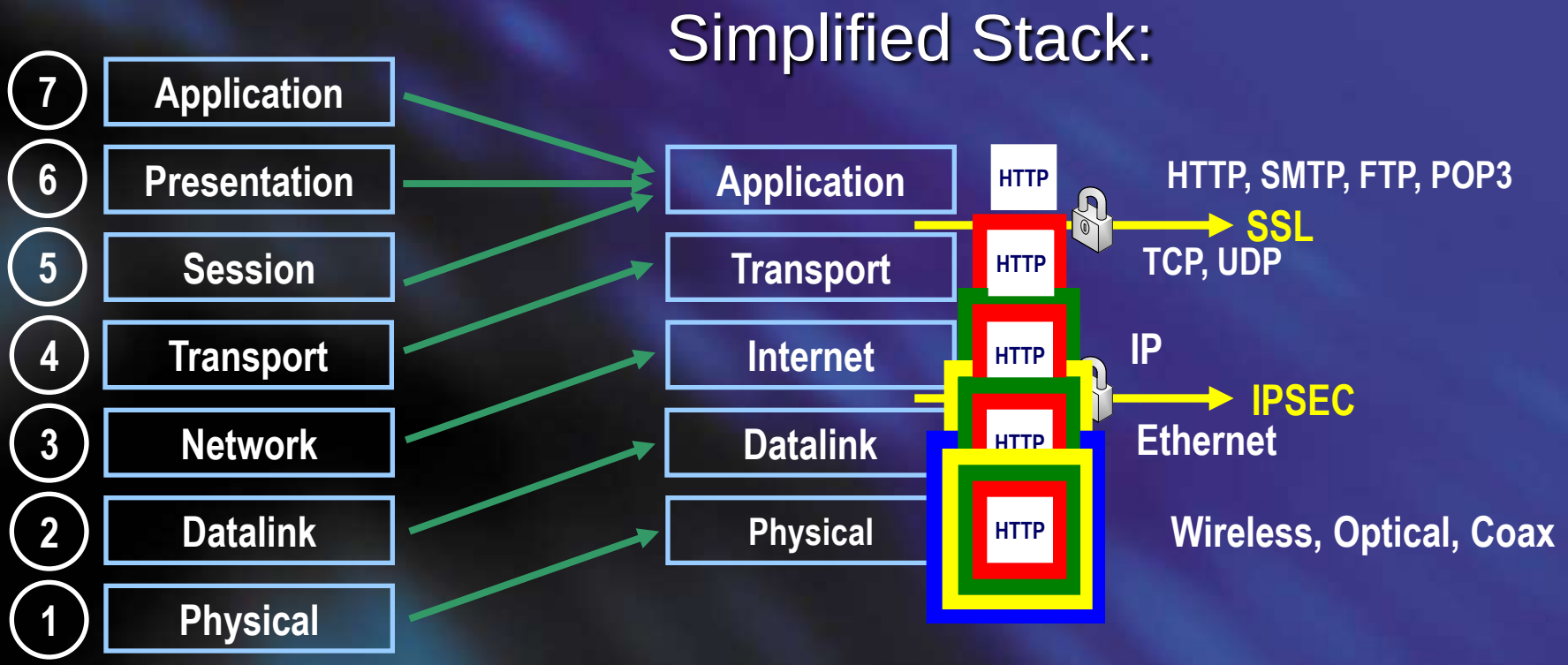
What Firewalls Do Not Protect Against

A firewall does not protect against all types of attacks:

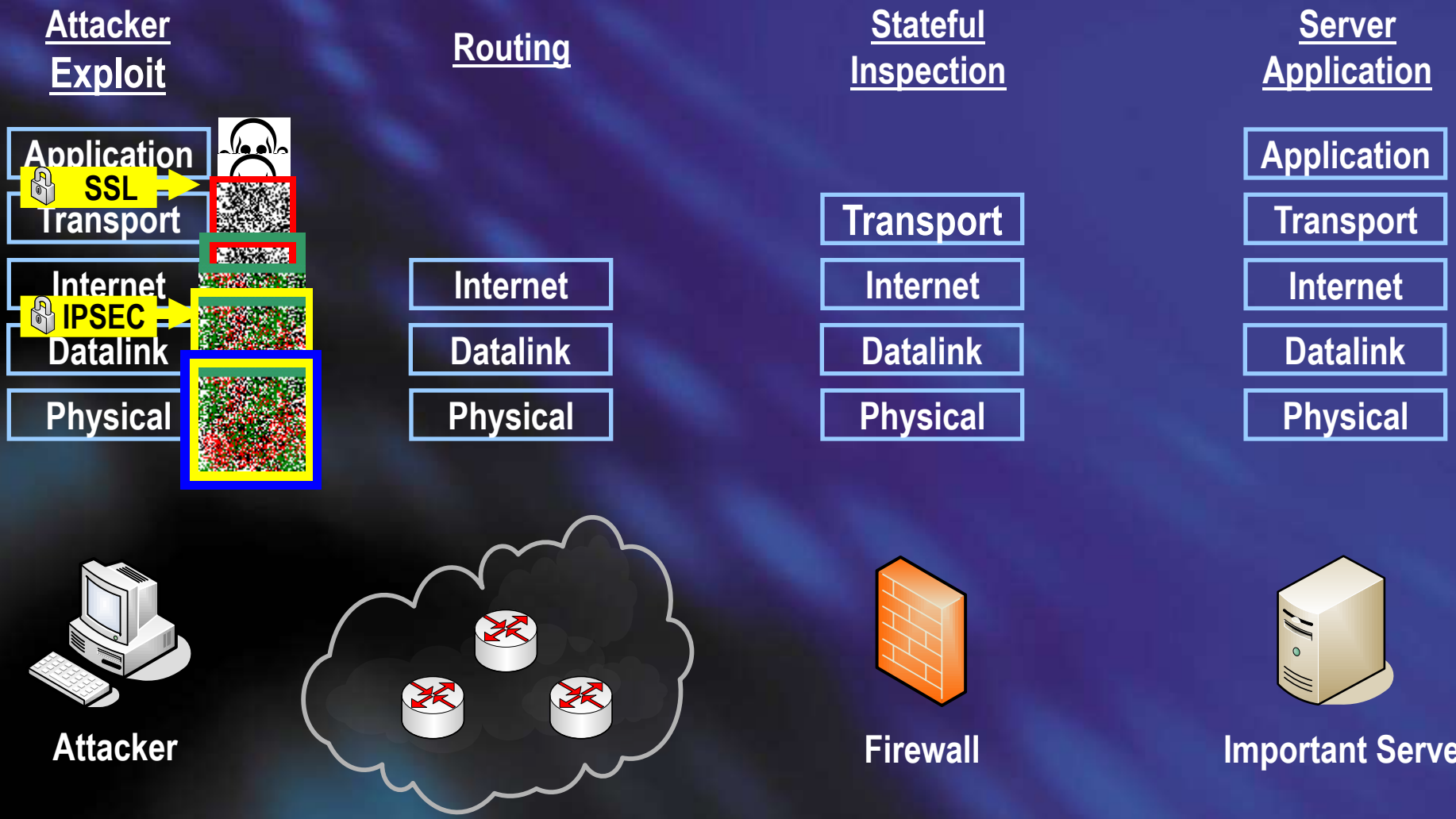
- Malicious traffic that is passed on open ports and not inspected at the application layer by the firewall
- Any traffic that passes through an encrypted tunnel or session
- Attacks after a network has been penetrated
- Traffic that appears legitimate
- Users and administrators who intentionally or accidentally infect environments with viruses
- Administrators and users who use weak passwords

Does your Firewall protect
"the Application Layer"?

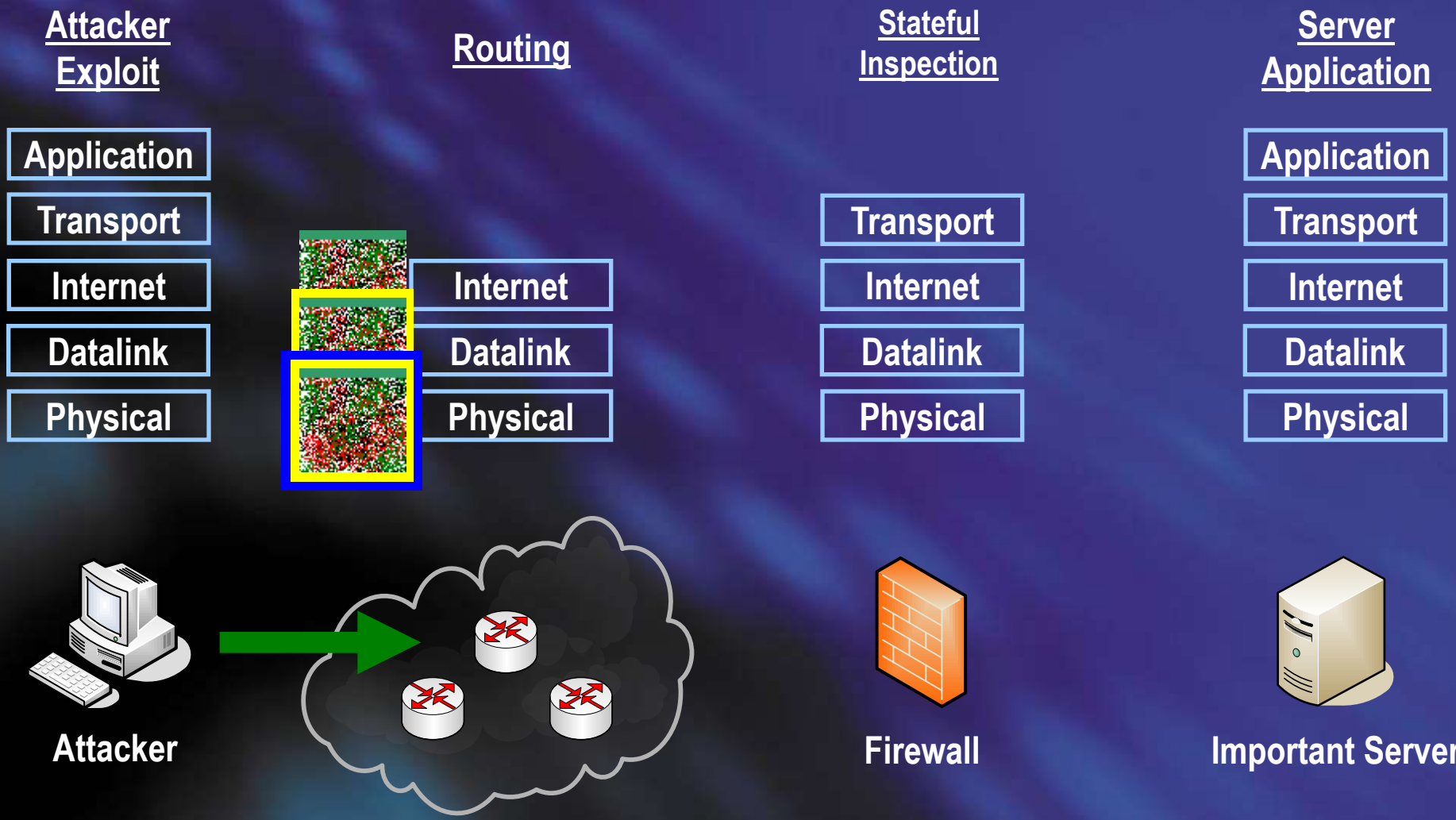
Networking Stack:



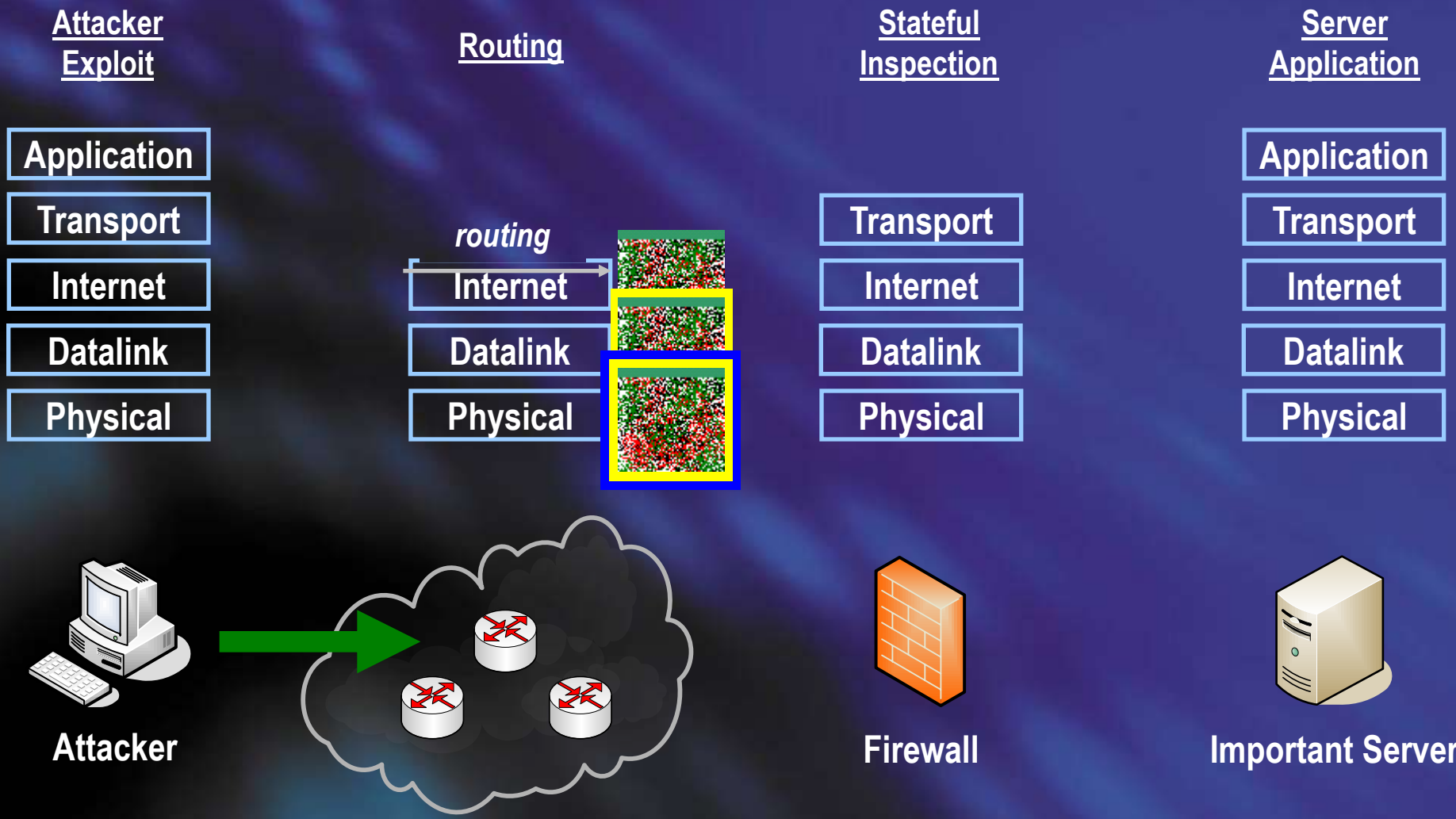
Example: Application Layer Attack



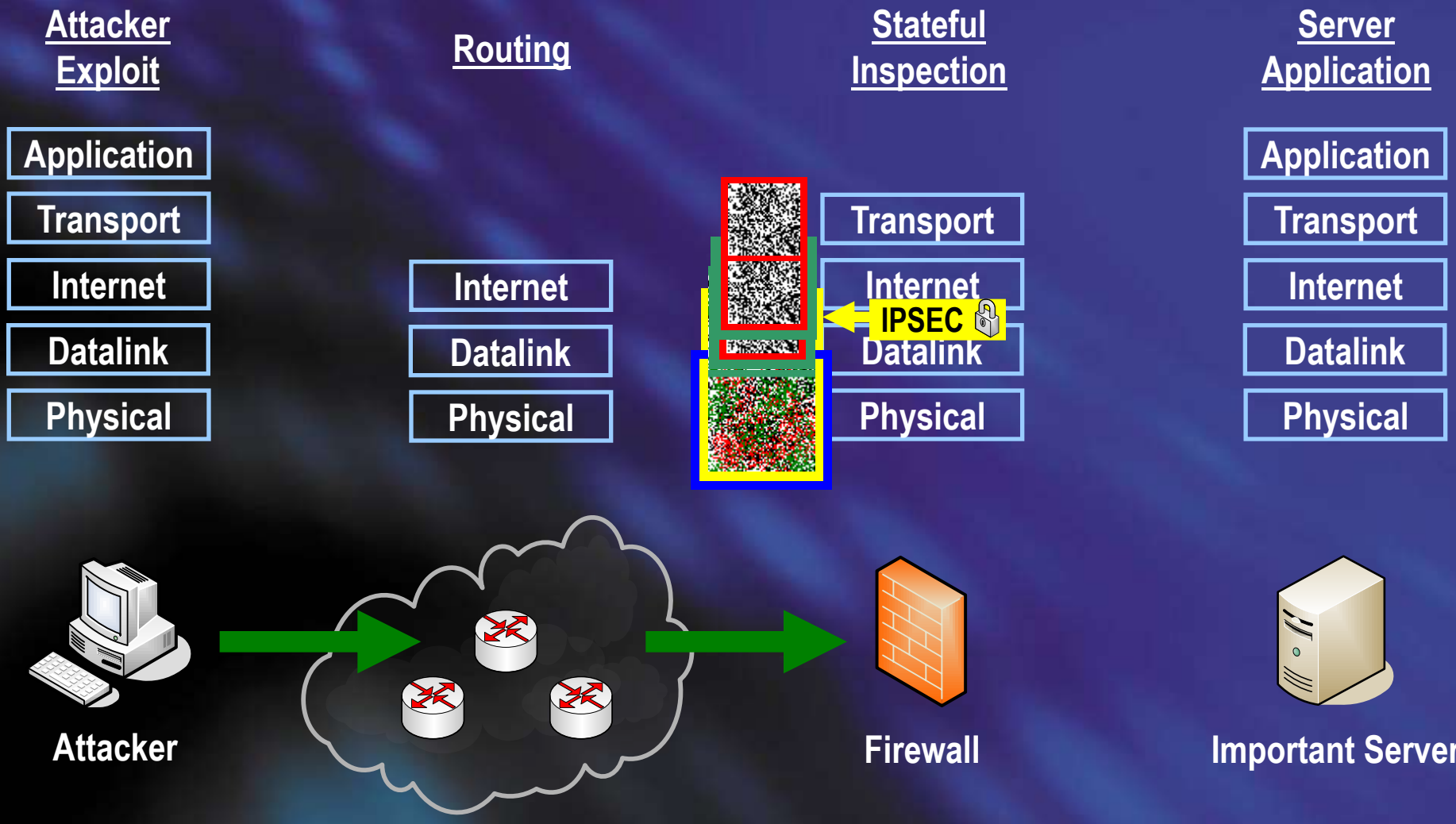
Example: Application Layer Attack



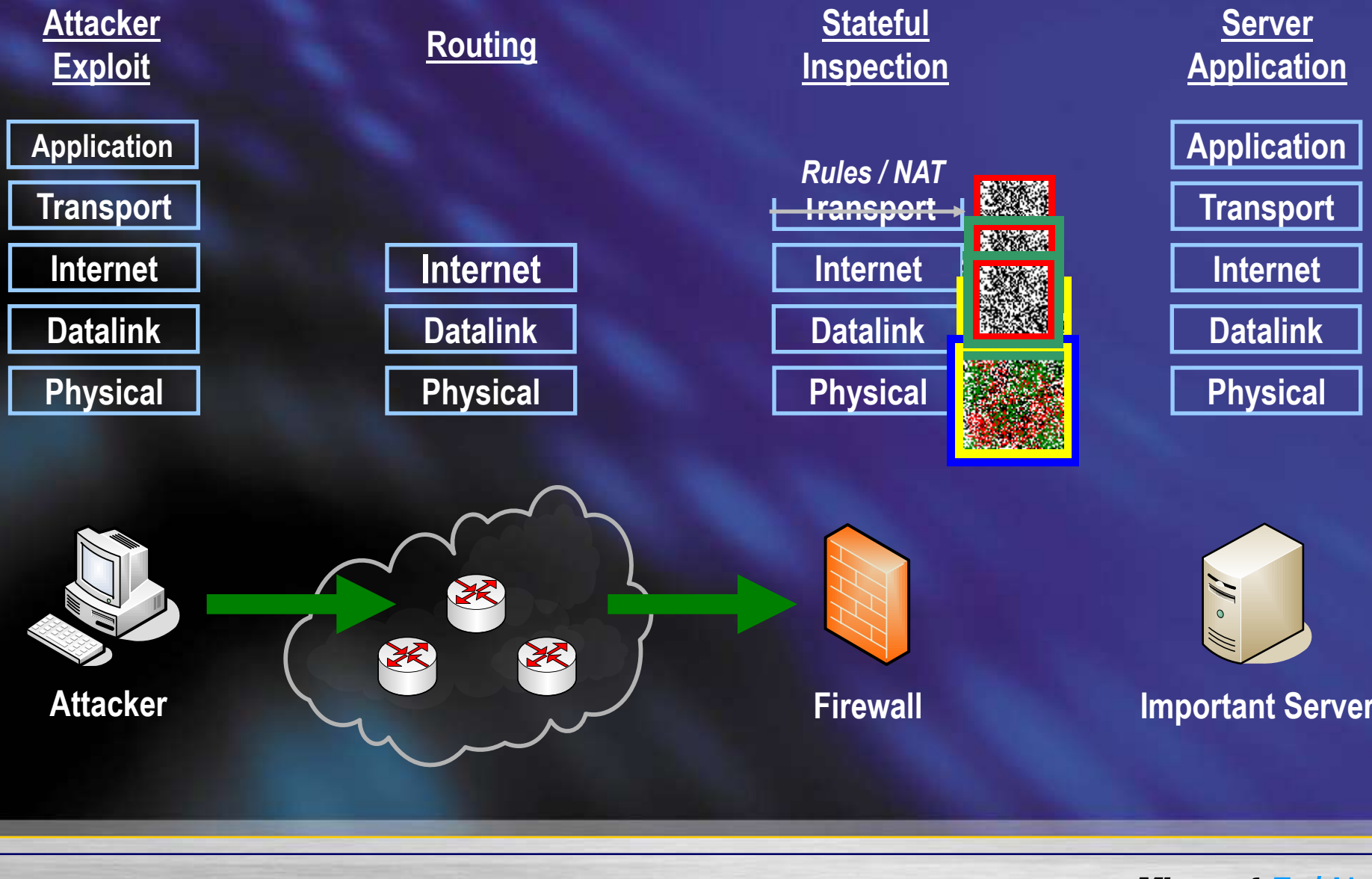
Example: Application Layer Attack



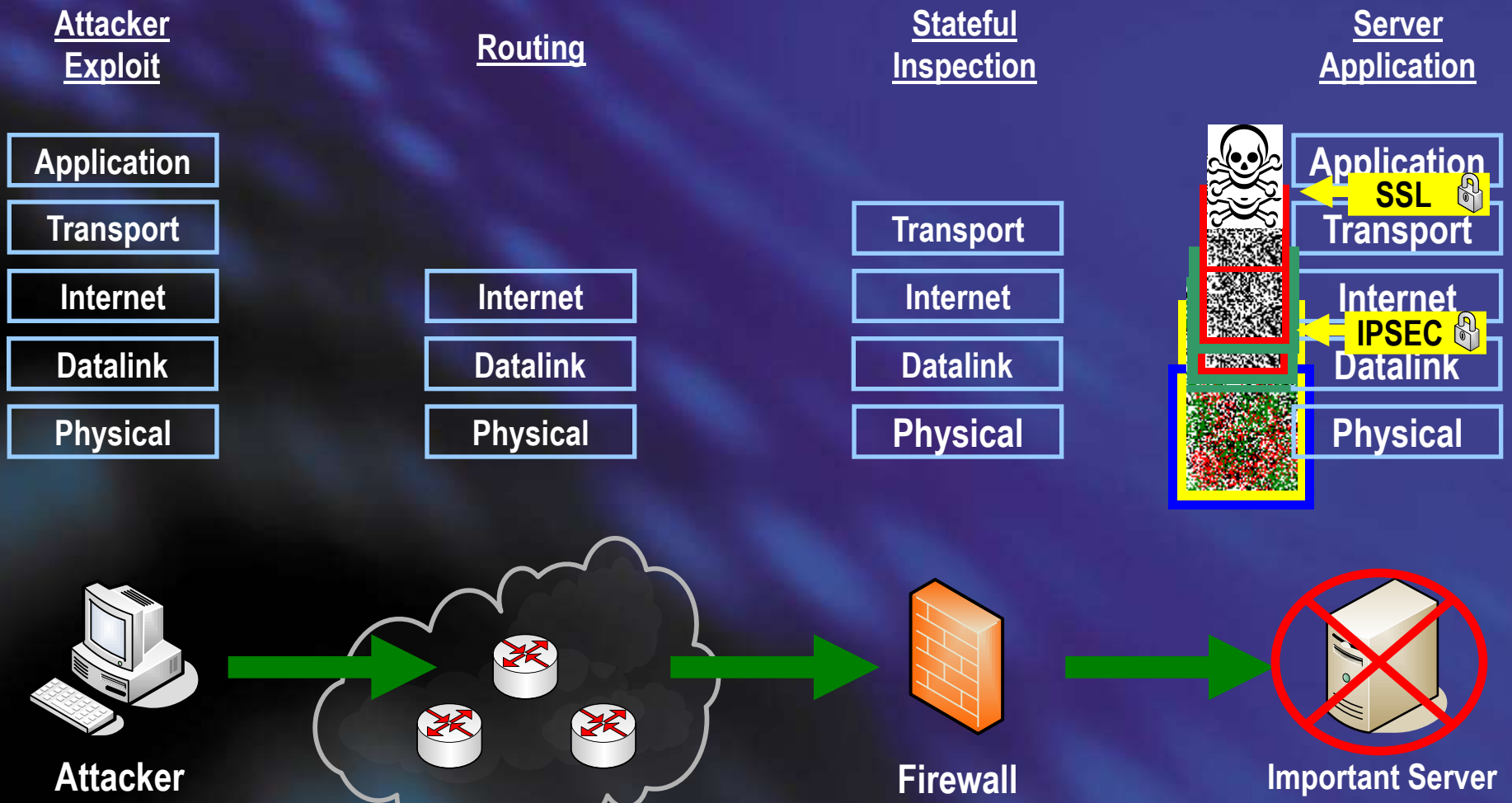
Example: Application Layer Attack



Example: Application Layer Attack



Example: Application Layer Attack



Using ISA Server to Protect Perimeters

- Introduction to Perimeter Defenses
- Using ISA Server to Protect Perimeters
- Using IPSec to Protect Communications
- Protecting Remote Access Using Network Access Quarantine

Protecting Clients

Method	Description
Proxy Functions	Processes all requests for clients and never allows direct connections
Client Support	Support for all clients without special software. Installation of ISA Firewall software on Windows clients enables additional functionality
Rules	Web access rules can restrict access to the Internet based on user name, client computer IP address, destination server or URL, and schedules
Add-ons	Add-ons enable companies to customize and extend firewall functionality with additional security and management features using non-Microsoft solutions

Protecting Web Servers

- Web Publishing Rules
  - Protect Web servers behind the firewall from external attacks by inspecting HTTP traffic and ensuring that it is properly formatted and complies with standards
- Inspection of Secure Socket Layer (SSL) traffic
  - Decrypts and inspects incoming encrypted Web requests for proper formatting and standards compliance
  - Will optionally re-encrypt the traffic before sending it to your Web server

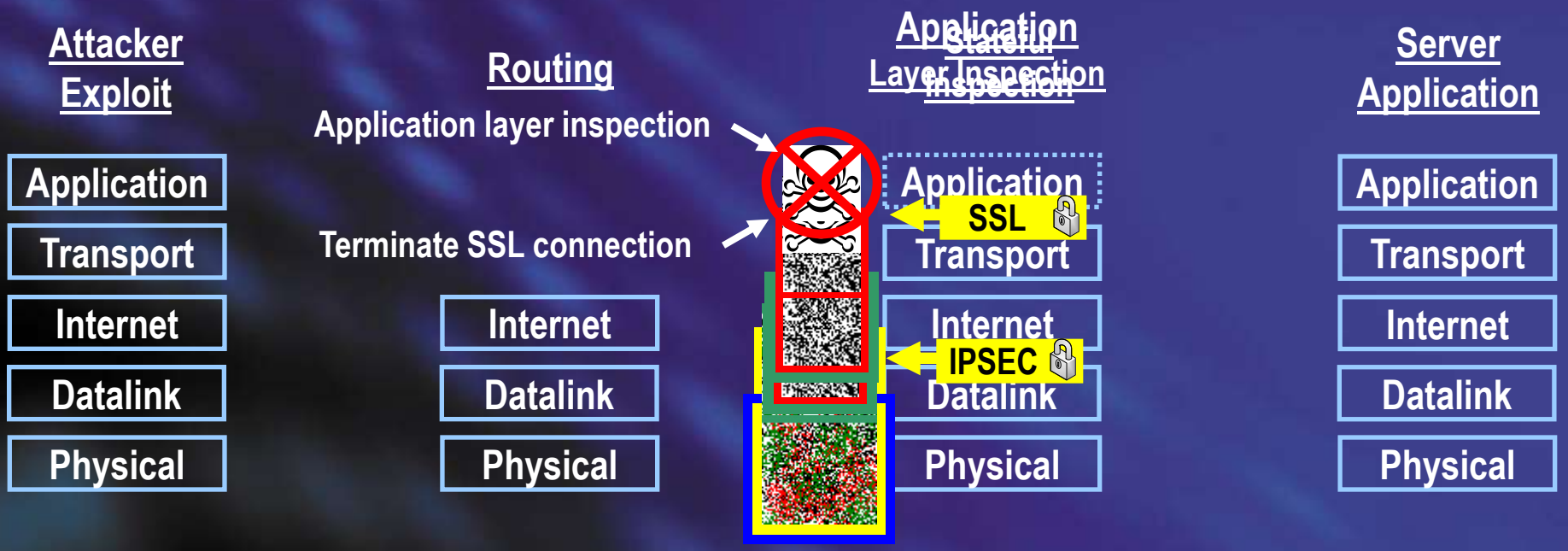
HTTP Filtering

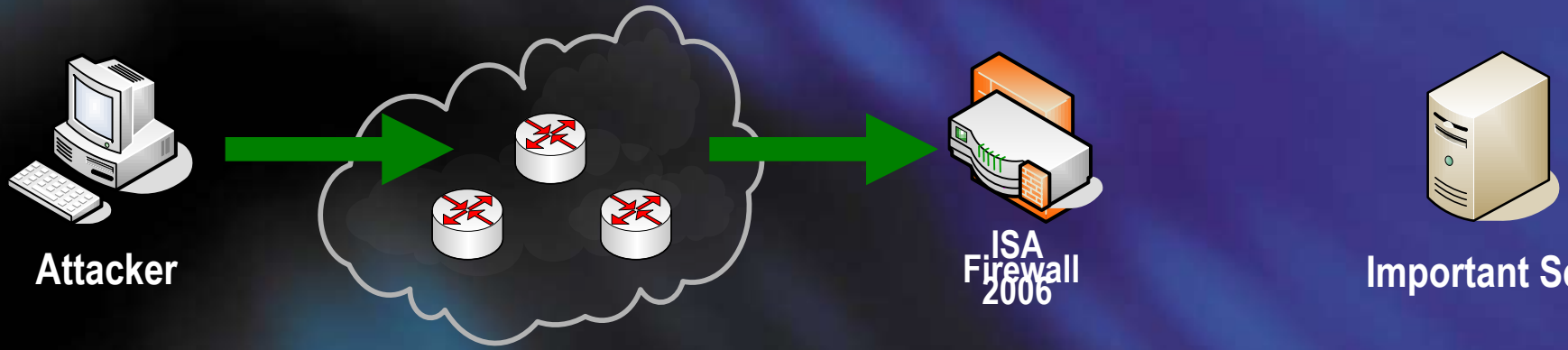
- Internet applications use HTTP to tunnel application traffic
- ISA Server 2006 includes an HTTP filter that:
  - Provides granular control over the HTTP traffic
  - Provides URLScan functionality at the perimeter of your network
  - Can be used in conjunction with URLScan on internal Web servers to meet complex requirements
- The HTTP filter can filter traffic:
  - By examining HTTP requests, responses, headers, and body contents
  - Based on file extensions, methods, and signatures

Traffic That Bypasses Firewall Inspection

- There are several types of traffic that are potentially not inspected by a firewall including:
  - SSL tunnels through traditional firewalls because the traffic is encrypted
  - VPN traffic is encrypted and cannot be inspected
  - Instant Messenger (IM) traffic often is not inspected and might be used to transfer files
- Determine the protocol entry points into your network and evaluate if the risk of allowing those protocols to enter the network without inspection is acceptable
- Use intrusion detection and other mechanisms to inspect VPN traffic after it has been decrypted
  - Remember: Defense in depth

Example: Application Layer Attack





Using ISA Server to Inspect Encrypted Traffic

- ISA Server can operate as the end-point for an SSL connection so it can decrypt and inspect SSL traffic
- ISA Server can also operate as a VPN remote-access and VPN gateway server and filter all VPN traffic
- ISA Server is compatible with many add-on products that improve the inspection capabilities

Best Practices

- Use access rules that only allow requests that are specifically allowed
- Use ISA Server's authentication capabilities to restrict access and log Internet access
- Configure Web publishing rules only for specific URLs
- Use SSL inspection to inspect encrypted data that is entering your network

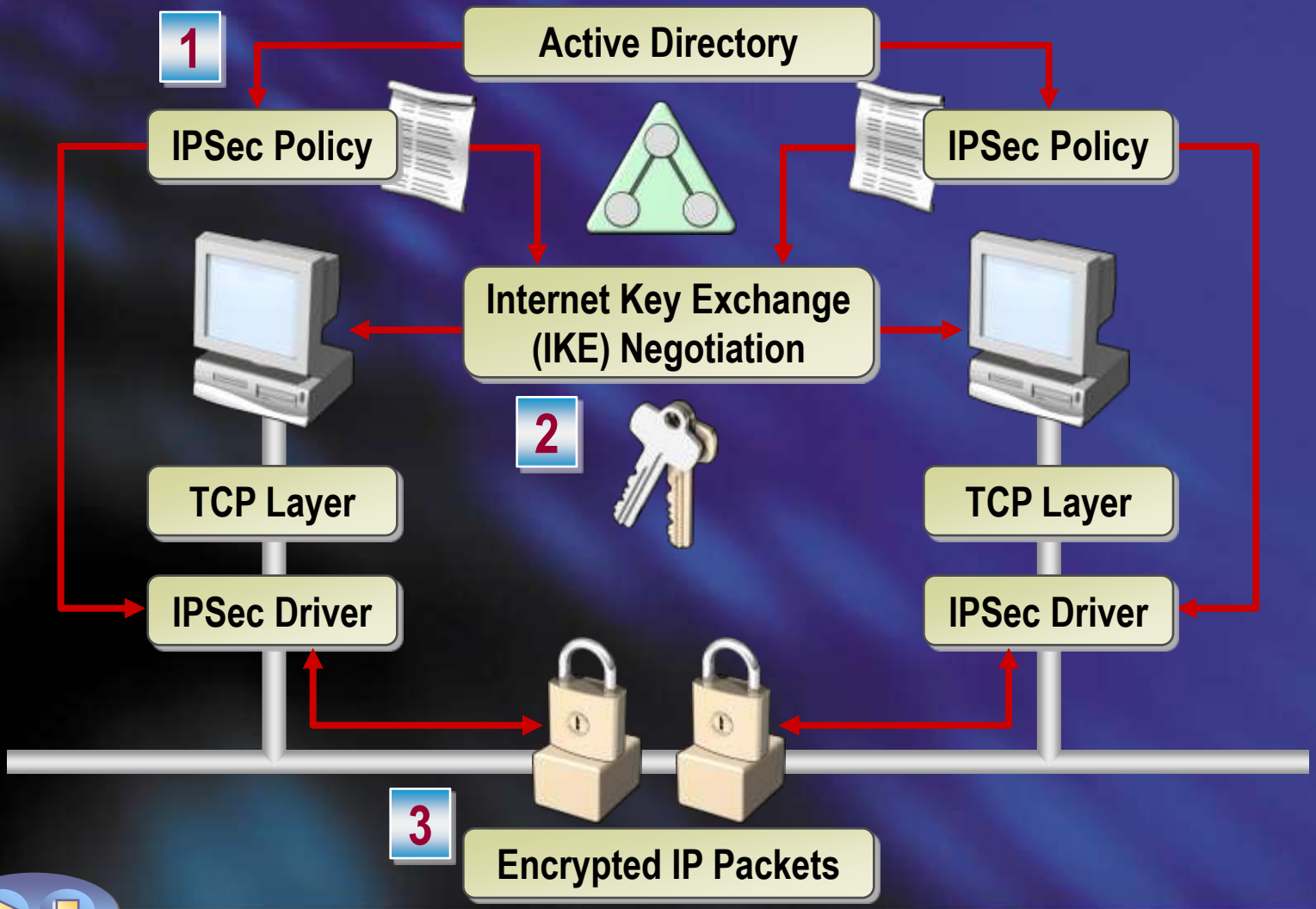
Using IPSec to Protect Communications

- Introduction to Perimeter Defenses
- Using ISA Server to Protect Perimeters
- Using IPSec to Protect Communications

Overview of IPSec

- IPSec is a method to secure IP traffic built on a framework of open standards
- IPSec goals are:
  - To ensure encrypted and authenticated communications at the IP layer
  - To provide a defense against network attacks through packet filtering and enforce trusted communication
- IPSec is based on an end-to-end security model
- IPSec is transparent to applications

How Does IPSec Secure Traffic?

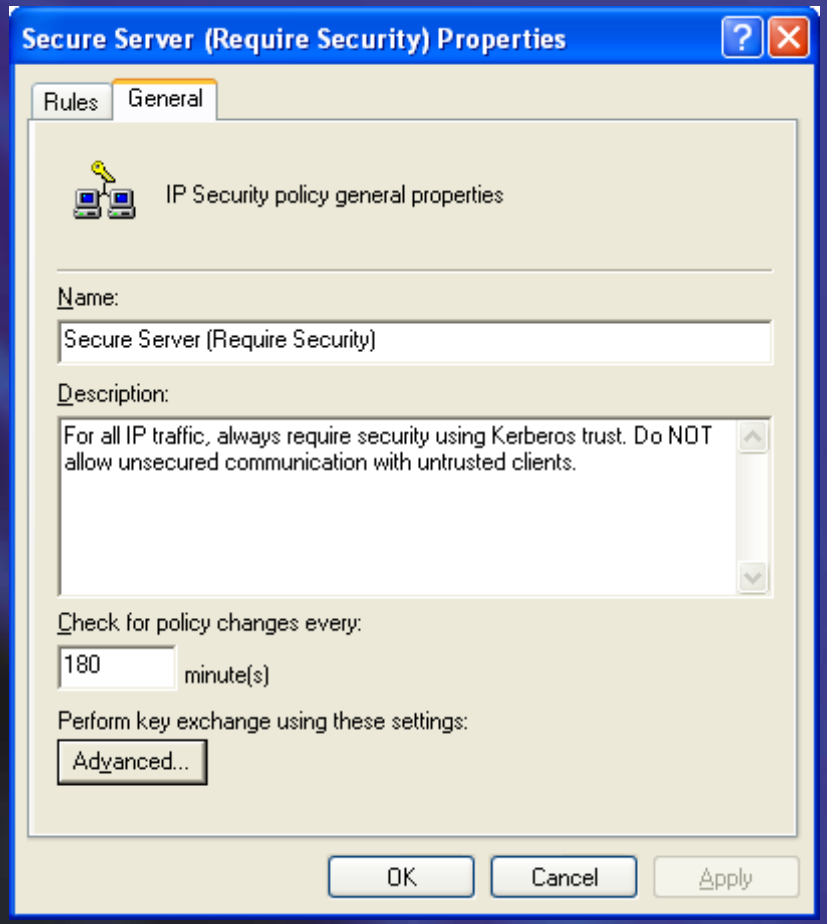


IPSec Protocols

- Use Authentication Header (AH) to ensure packet integrity
  - AH provides packet integrity
  - AH does not encrypt, allowing for network intrusion detection
- Use Encapsulation Security Payload (ESP) to encrypt sensitive traffic
  - ESP provides packet integrity and confidentiality
  - Encryption prevents packet inspection

IPSec Scenarios

- Basic permit/block packet filtering
- Secure internal LAN communications
- VPN across untrusted media



Using IPSec to Secure Internal Communications

- Default IPSec Policies
  - Secure Server (Require Security)
  - Server (Request Security)
  - Client (Respond Only)

Use IPSec to provide mutual device authentication

  - Use certificates or Kerberos
  - Preshared key suitable for testing only
- Carefully plan which traffic should be secured

Using IPSec for Virtual Private Networking

- Client VPN
  - Use L2TP/IPSec
- Branch Office VPN
  - Between Windows 2000 or Windows Server 2003 running RRAS: Use L2TP/IPSec tunnel (easy to configure, appears as routable interface)
  - To third-party gateway: Use L2TP/ISec or pure IPSec tunnel mode

Best Practices

- Plan your IPSec implementation carefully
- Choose between AH and ESP
- Use Group Policy to implement IPSec Policies
- Consider the use of IPSec NICs
- Never use pre-shared key authentication outside your test lab
- Choose between certificates and Kerberos authentication
- Use care when requiring IPSec for communications with domain controllers and other infrastructure servers

Questions and Answers