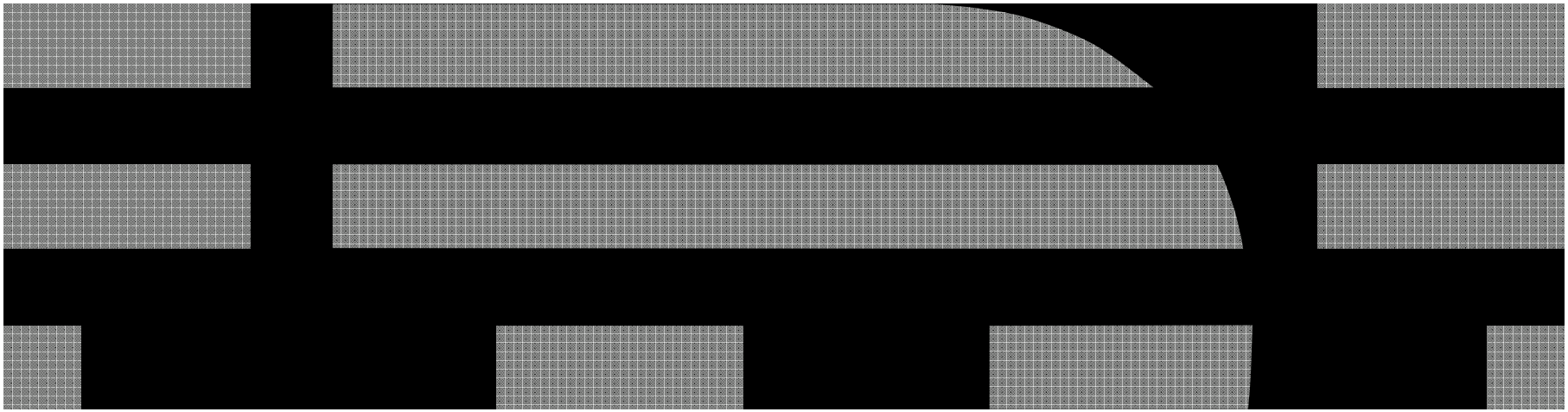
FD6:
Section 2: IP Security Basics



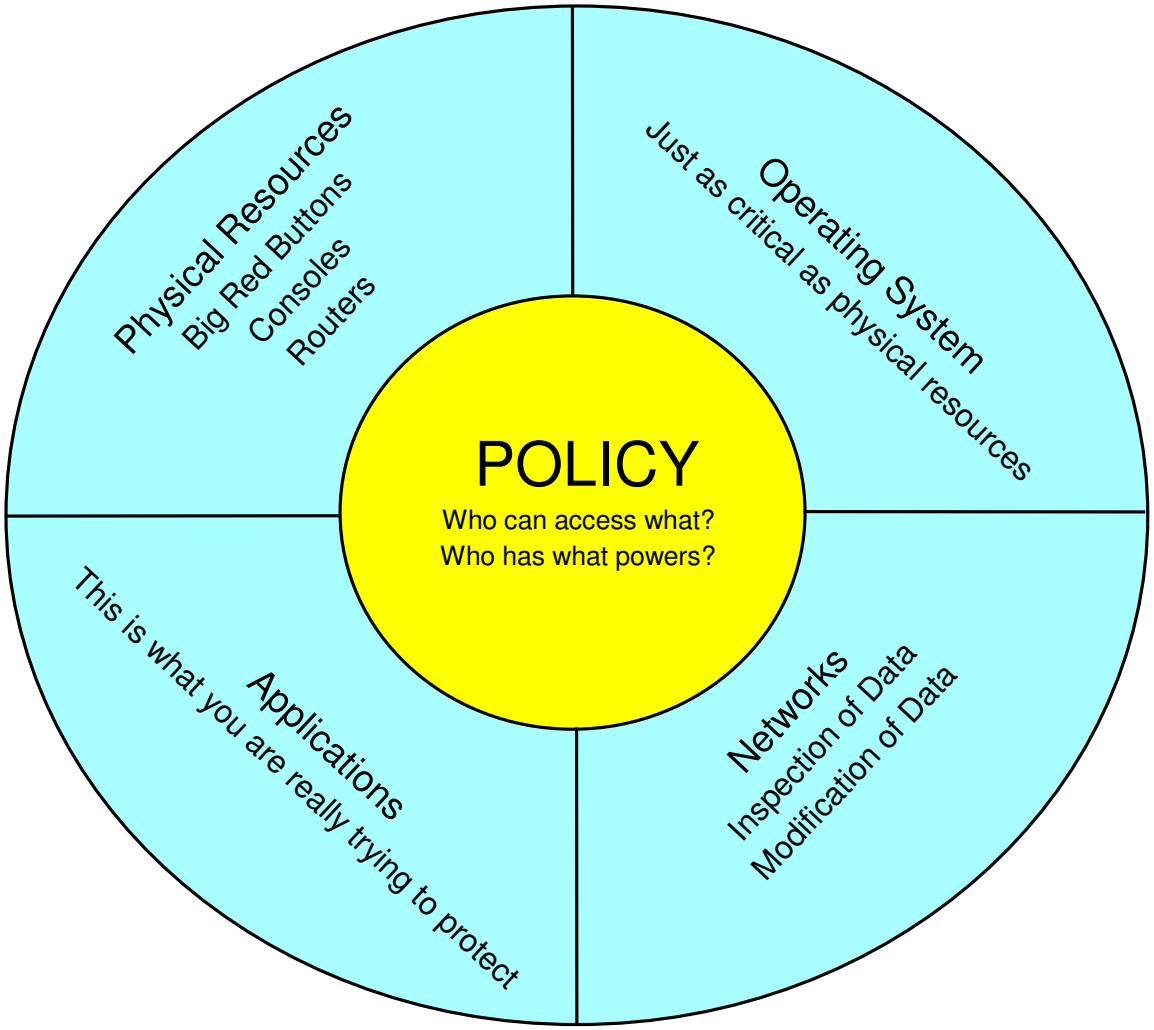
© 2009 IBM Corporation

Security Architecture

- **Authentication:**
  - Is this person or process what you think he/she/it is? How can you be sure?
  - Without strong authentication everything else is useless!
- **Authorization:**
  - Does this person or process have the right to access this resource?
- **Data Integrity:**
  - Has this data been modified since it was created by its rightful owner?
- **Confidentiality:**
  - Has this data been read by those who should not see it?
- **Non-repudiation:**
  - Is there positive proof that the identity of the creator of this message is authentic?

© 2009 IBM Corporation

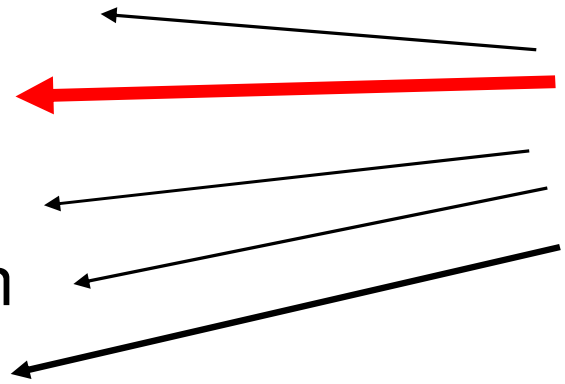
Security Controls



© 2009 IBM Corporation

Principles of Security

1. Paranoia
2. Trust no-one
3. Multiple Layers:
   - Physical
   - Network
   - OS
   - Application
   - Policy



This Class

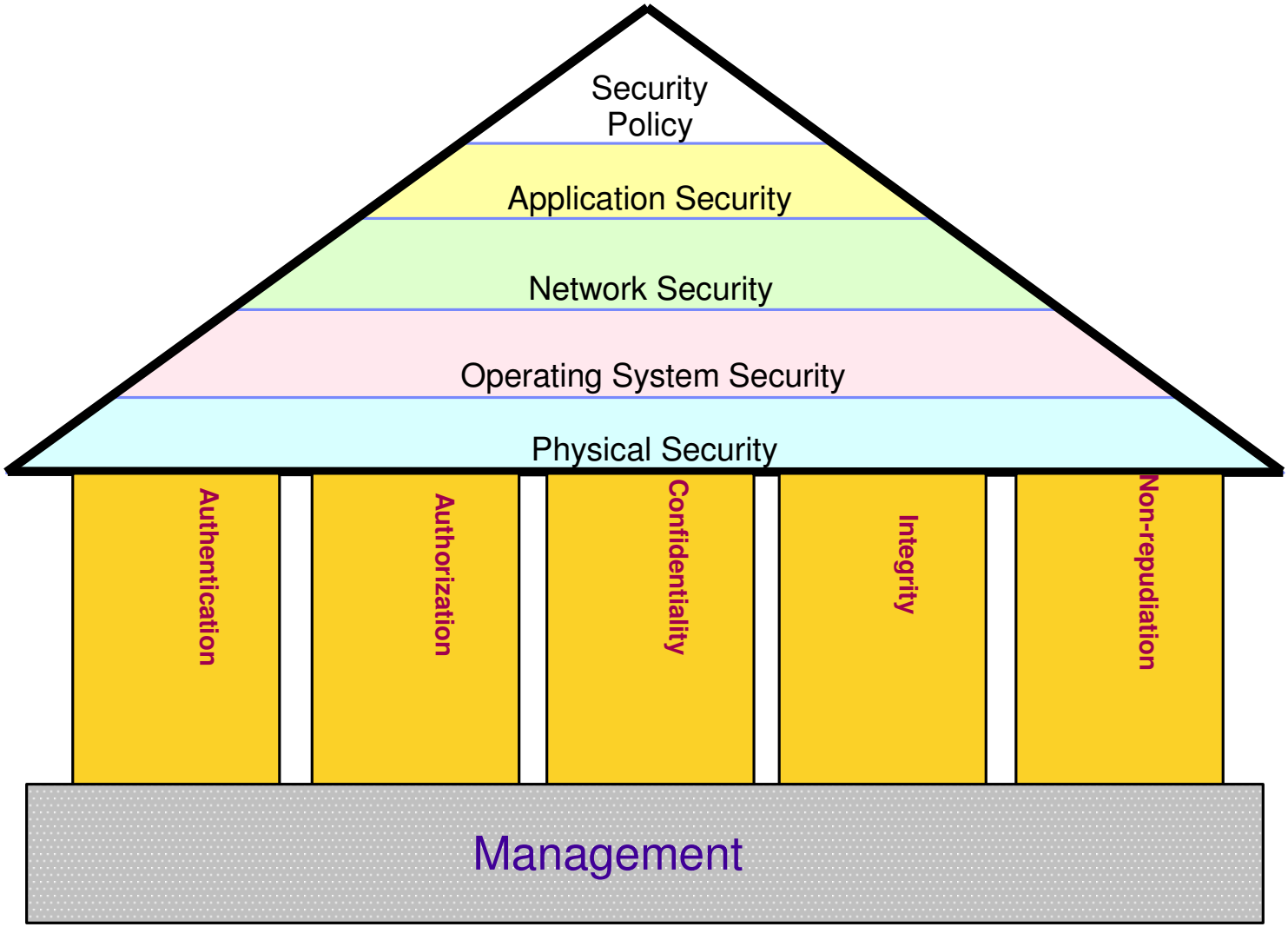
© 2009 IBM Corporation

Know Your Enemy

- Amateurs
  - Was the Largest group of hackers
  - Opportunistic
  - No temptation, no attacks
- Crackers & CyberTerrorists
  - Denial of Service specialists
  - Very expensive
  - Thrive on publicity
  - College Students
  - Disgruntled employees
- Career Criminals
  - Now the Largest Hacker Threat
  - No publicity
  - Careful planning
  - Defined goal
  - Can be just as expensive
  - On the rise and rise

© 2009 IBM Corporation

The Security Edifice



© 2009 IBM Corporation

Implementing Security on Your System

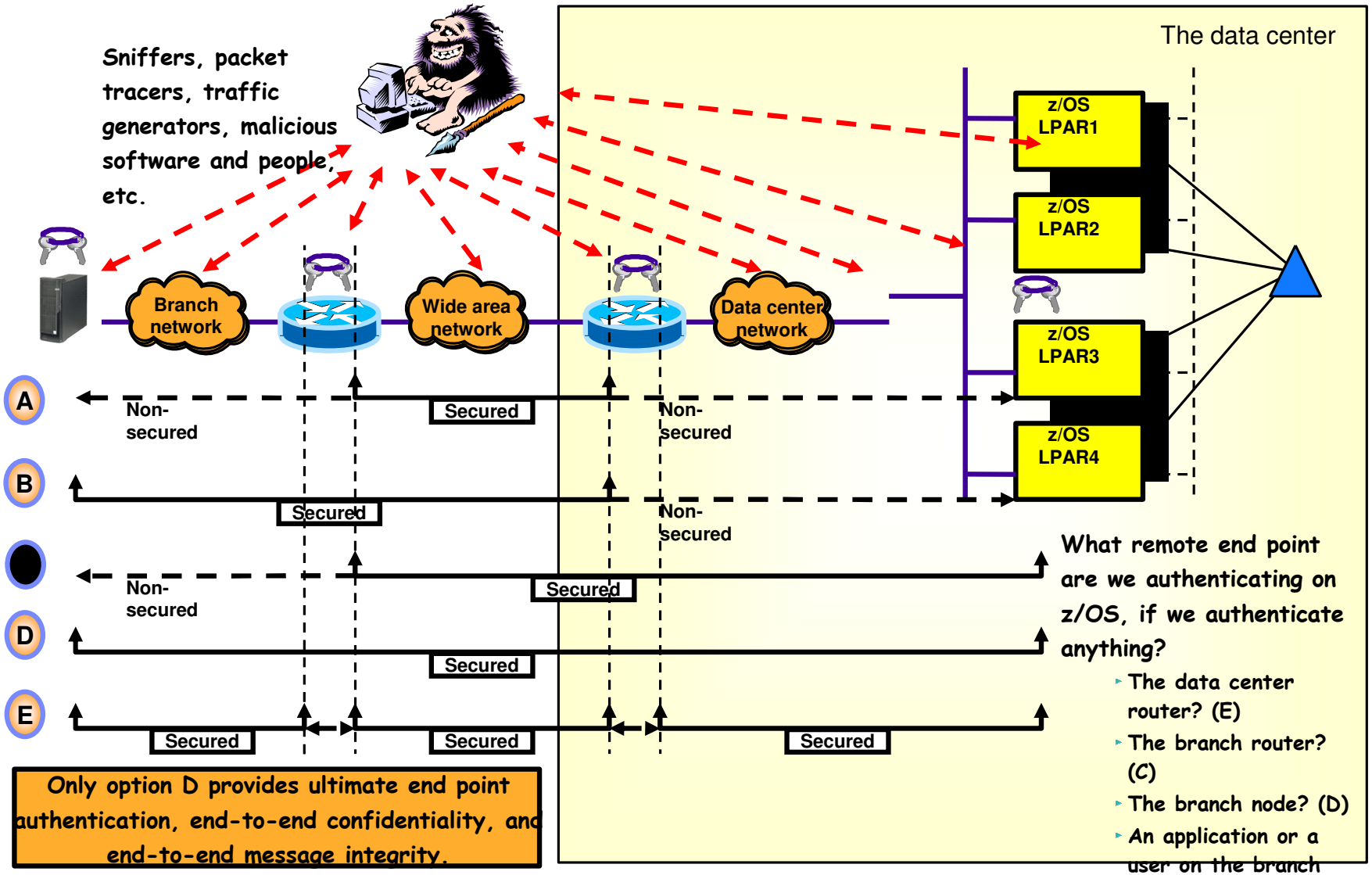
- **What kind of security do you need?**
  - Users
    - Internet, Intranet, Business partners
    - Legitimate Users or Hackers and Thieves?
    - Who can be Trusted, and how far?
  - Data
    - What applications need protecting?
    - How is the data transferred?
    - Do we need just integrity, or confidentiality?
  - Denial of Service Attacks
    - External
    - Internal (Trojans, zombies)

- **Where do you do Security?**
  - Routers?
  - Servers?
  - Applications?
  - Firewalls?
  - All of these?

- **What will it cost?**
  - Risk Analysis

© 2009 IBM Corporation

End to End Security - Where is the End?



© 2009 IBM Corporation

Authenticating the User

This is NOT the same as authenticating the process

- **There are Several Classes of Authentication that you can use for a user**
  - **Something that you know**
  - **Something that you have**
  - **Something that you are**

  - **Two Factor Authentication is when you use two of the above methods to authenticate a person**

© 2009 IBM Corporation

ID and Password

- The basis of security (authentication) for many years
- Often sent in the clear
  - Therefore, need encryption
- Often easily guessed
  - Therefore, need complex rules
- Often written down
  - How many different services do YOU use?
  - How complex are the rules, and how different?

© 2009 IBM Corporation

Digital Certificates

- Not easily guessed!
- Key never sent in the clear
- Must protect the certificate store
  - How complex is the password to YOUR keyring?
  - How does z/OS protect it?

© 2009 IBM Corporation

© 2009 IBM Corporation

Biometrics

- Fingerprint reader
- Retina scan
- But have you read "Angels & Demons"?

The Best Authentication is Three-way

- Something you Know (Password)
- Something you Have (Smart Card)
- Something you Are (Biometrics)

© 2009 IBM Corporation

Protecting TCP/IP system resources and data in the network

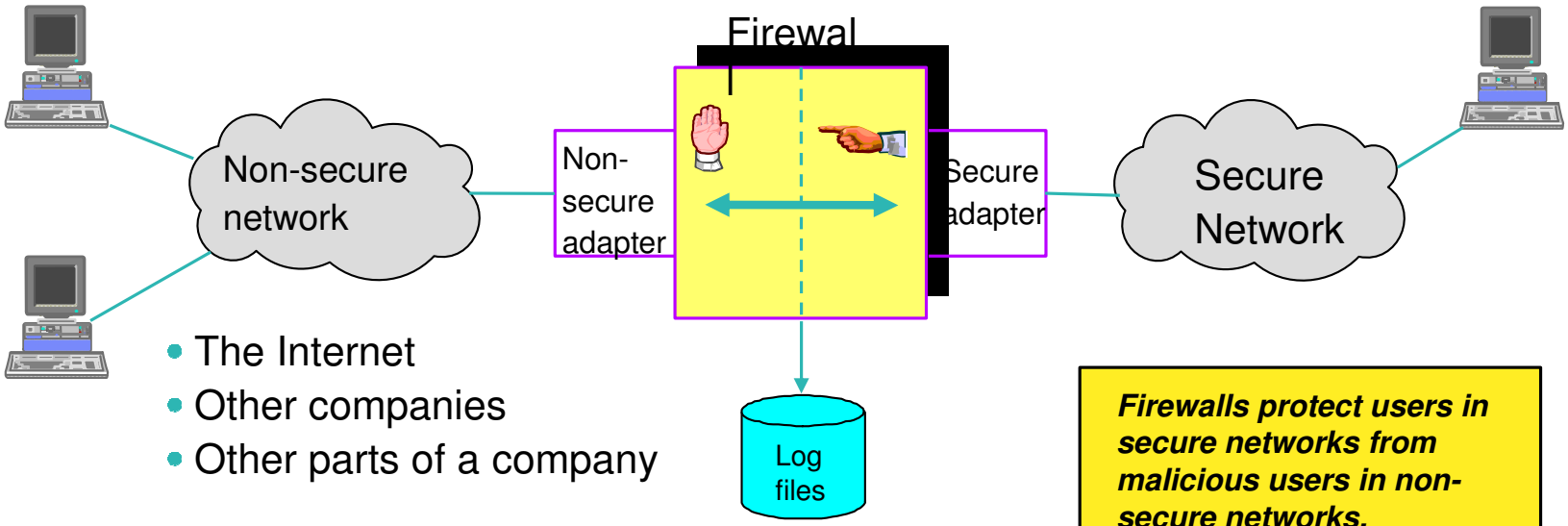
- **Protect against malicious or accidental access attempts**
  - Solution: IP packet filtering
- **Protect against malicious or accidental DoS attacks**
  - Solution: Intrusion detection
- **Protect confidentiality and integrity of data in the network**
  - Solution: Encryption
  - Solution: Virtual Private Networks
- **Build multiple barriers between you and the bad guys**
  - Solution: Gateways (Proxy and SOCKS)
  - Solution: Demilitarized Zone

(not really security but worth a mention)

- Network Address Translation

© 2009 IBM Corporation

What is a Firewall?



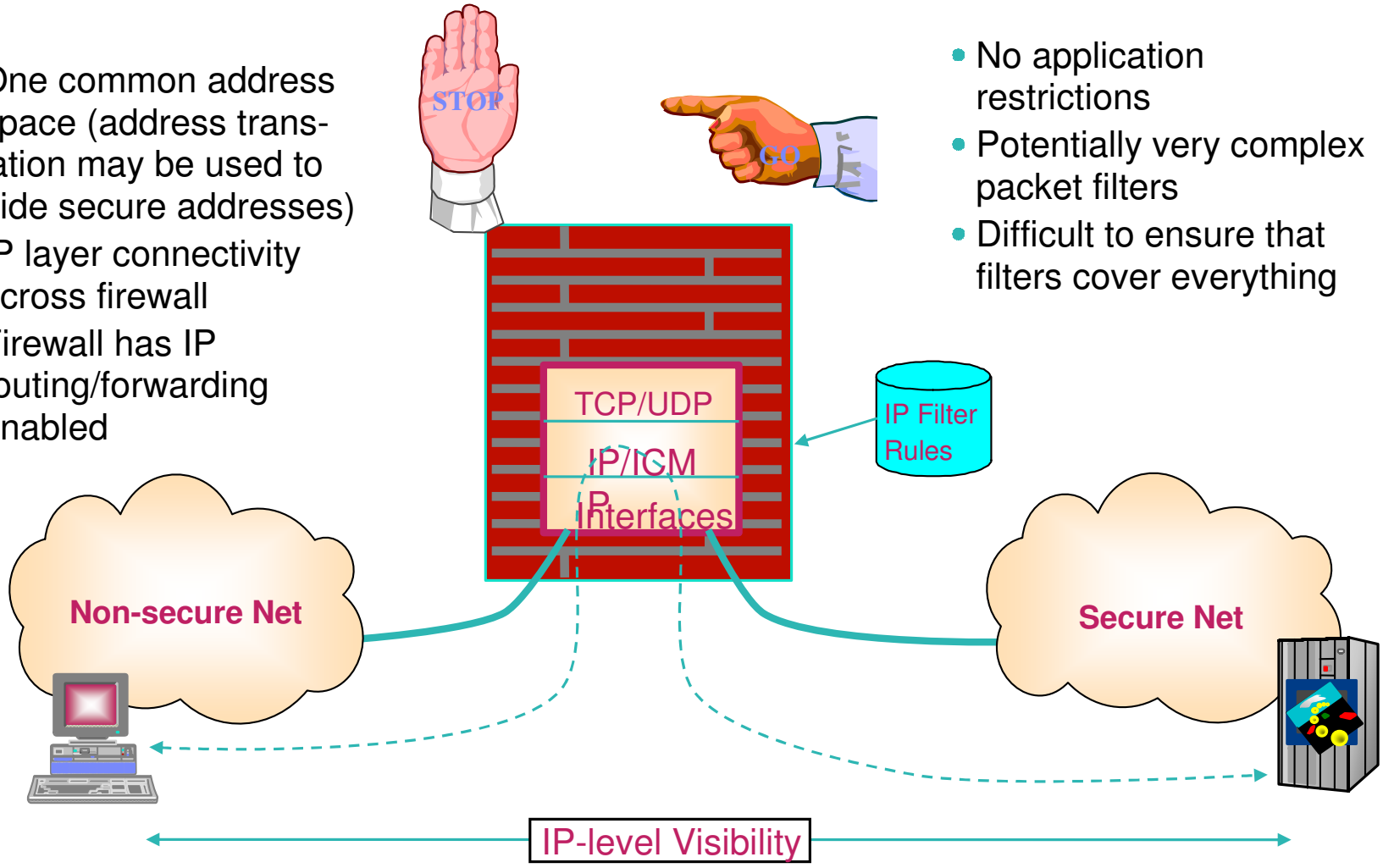
Firewalls protect users in secure networks from malicious users in non-secure networks.
N.B. Don't forget that you might have malicious users inside your intranet too!!!!

1. A Firewall is most often a dedicated machine, but need not be
2. It controls TCP/IP traffic at the IP level and/or at the application level in and out of the secure network
3. A Firewall maintains log files of suspicious access patterns and rejected access attempts.

© 2009 IBM Corporation

Packet Filtering Firewall

- One common address space (address translation may be used to hide secure addresses)
- IP layer connectivity across firewall
- Firewall has IP routing/forwarding enabled

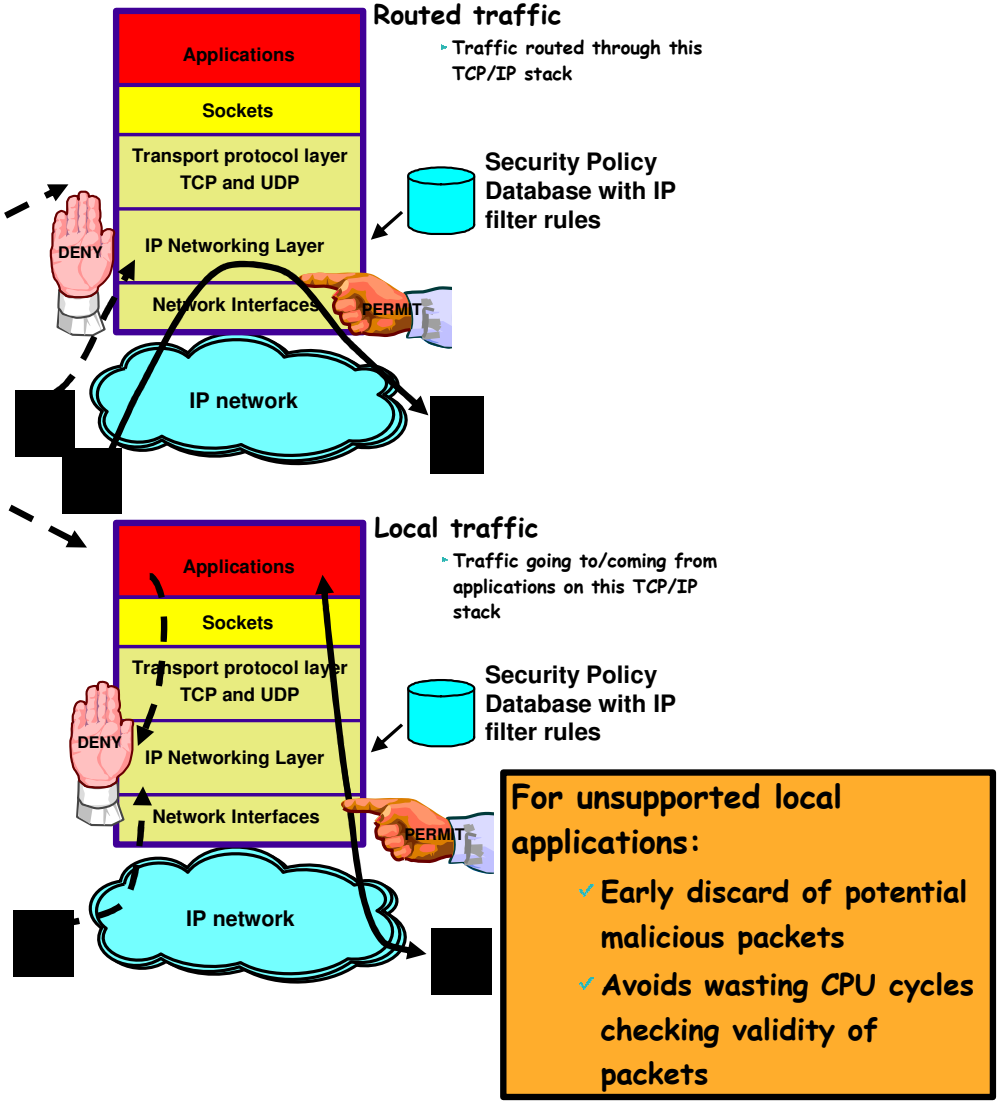


- No application restrictions
- Potentially very complex packet filters
- Difficult to ensure that filters cover everything

© 2009 IBM Corporation

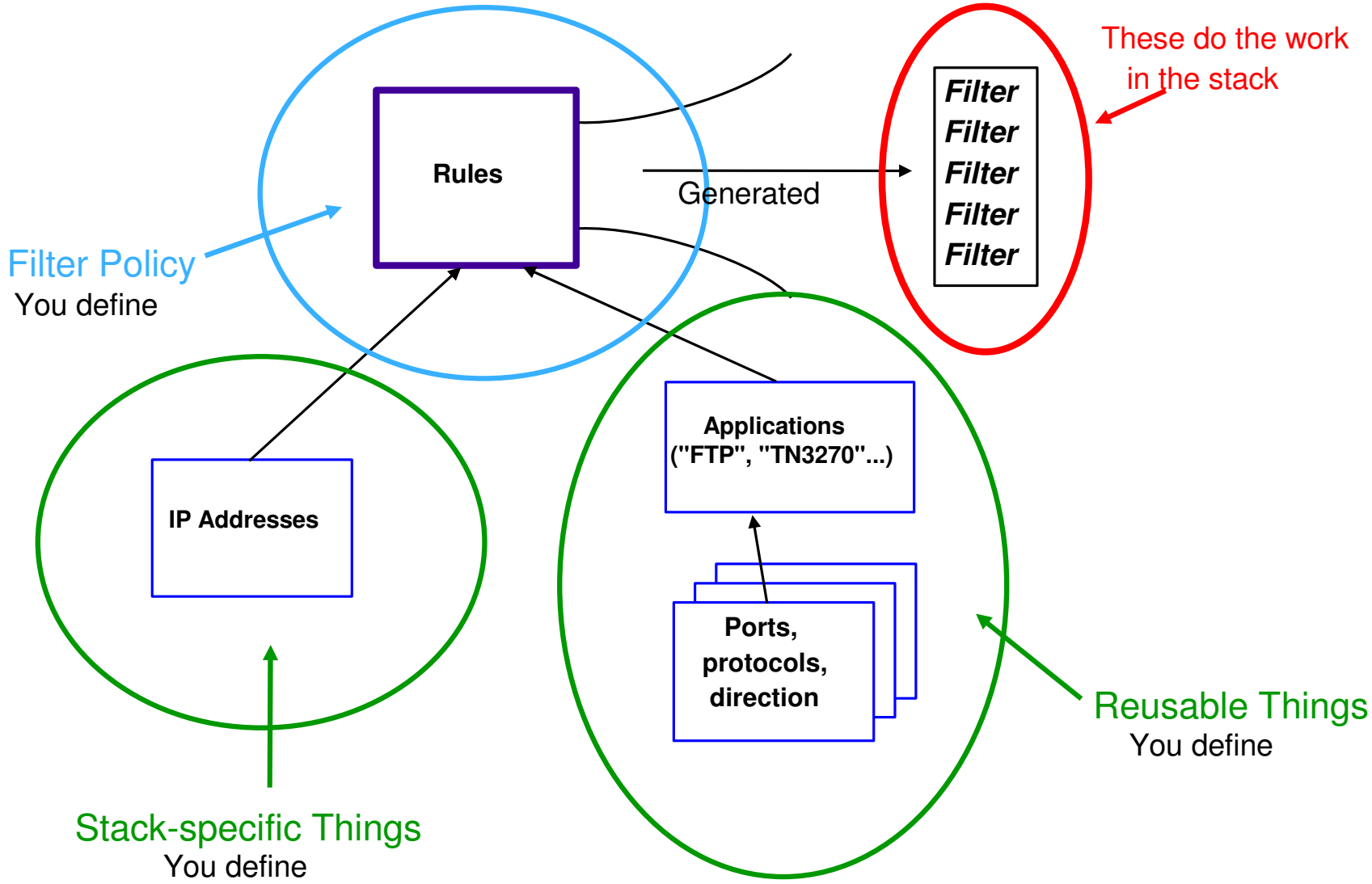
Blocking unnecessary IP traffic through IP filtering

- **IP filtering at the IP Layer**
  - Filter rules defined to deny or permit packets based on:
    - IP source/destination address
    - Protocol (TCP, TCP with ACK, UDP, ICMP, ?)
    - Source/destination Port
    - Direction of flow
    - Local or routed traffic
    - Time
    - Network interface
  - Used to control
    - traffic being routed
    - traiic to this host (local)
  - When IP filtering is active, a default rule (implicit deny all) will lose all packets that are not specifically permitted



© 2009 IBM Corporation

Typical Packet Filter Implementation



© 2009 IBM Corporation

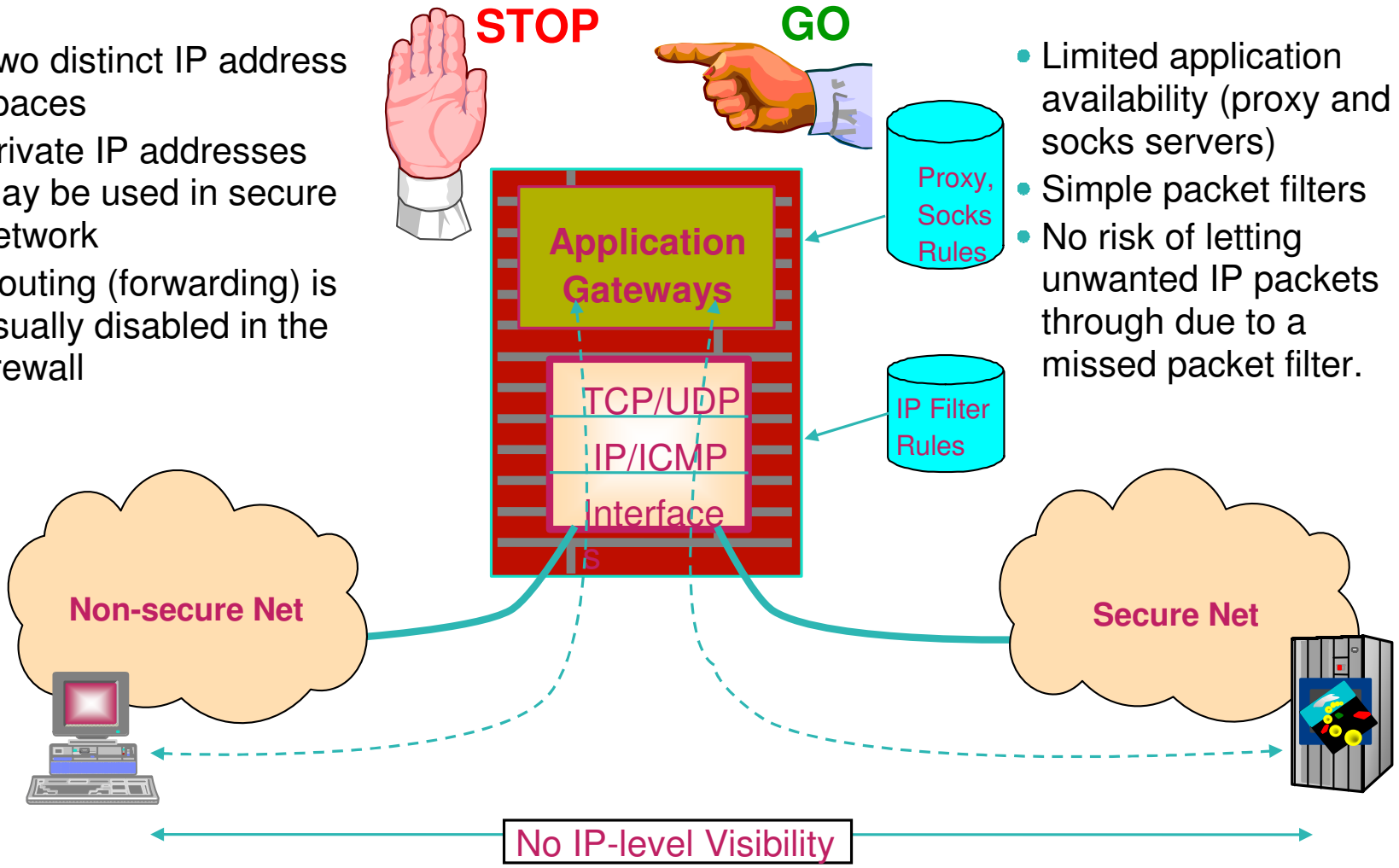
Packet Filter Definitions

permit 9.0.0.0 255.0.0.0 0.0.0.0 0.0.0.0 tcp any 0 eq 20 both both inbound l=no f=yes t=0
permit 9.0.0.0 255.0.0.0 0.0.0.0 0.0.0.0 tcp any 0 eq 21 both both inbound l=no f=yes t=0
permit 9.0.0.0 255.0.0.0 0.0.0.0 0.0.0.0 tcp any 0 eq 23 both both inbound l=no f=yes t=0
permit 9.0.0.0 255.0.0.0 0.0.0.0 0.0.0.0 udp eq 53 any 0 both both inbound l=no f=yes t=0
permit 9.0.0.0 255.0.0.0 0.0.0.0 0.0.0.0 udp any 0 eq 68 both both inbound l=no f=yes t=0
permit 9.0.0.0 255.0.0.0 0.0.0.0 0.0.0.0 tcp eq 515 any 0 both both inbound l=no f=yes t=0
permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 udp eq 53 any 0 both both inbound l=no f=yes t=0
permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tcp/ack eq 80 any 0 both both inbound l=no f=yes t=0
permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tcp/ack eq 443 any 0 both both inbound l=no f=yes t=0
permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tcp eq 20 any 0 both both inbound l=no f=yes t=0
permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tcp/ack eq 21 any 0 both both inbound l=no f=yes t=0
permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tcp/ack eq 23 any 0 both both inbound l=no f=yes t=0
permit 192.168.0.0 255.255.0.0 0.0.0.0 0.0.0.0 tcp any 0 eq 20 both both inbound l=no f=yes t=0
permit 192.168.0.0 255.255.0.0 0.0.0.0 0.0.0.0 tcp any 0 eq 21 both both inbound l=no f=yes t=0
permit 192.168.0.0 255.255.0.0 0.0.0.0 0.0.0.0 tcp any 0 eq 23 both both inbound l=no f=yes t=0
permit 192.168.0.0 255.255.0.0 0.0.0.0 0.0.0.0 udp any 0 eq 68 both both inbound l=no f=yes t=0
deny 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tcp any 0 lt 1024 both both inbound l=yes f=yes t=0
deny 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 udp any 0 lt 1024 both both inbound l=yes f=yes t=0
permit 9.0.0.0 255.0.0.0 0.0.0.0 0.0.0.0 icmp any 0 any 0 both both inbound l=no f=yes t=0
permit 192.168.0.0 255.255.0.0 0.0.0.0 0.0.0.0 icmp any 0 any 0 both both inbound l=no f=yes t=0
deny 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 icmp any 0 any 0 both both inbound l=yes f=yes t=0
permit 9.0.0.0 255.0.0.0 0.0.0.0 0.0.0.0 all any 0 any 0 both both inbound l=no f=yes t=0
permit 192.168.0.0 0.0.0.0 0.0.0.0 0.0.0.0 all any 0 any 0 both both inbound l=no f=yes t=0
permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 all any 0 any 0 both both outbound l=no f=yes t=0

© 2009 IBM Corporation

Application Layer Gateway

- Two distinct IP address spaces
- Private IP addresses may be used in secure network
- Routing (forwarding) is usually disabled in the firewall

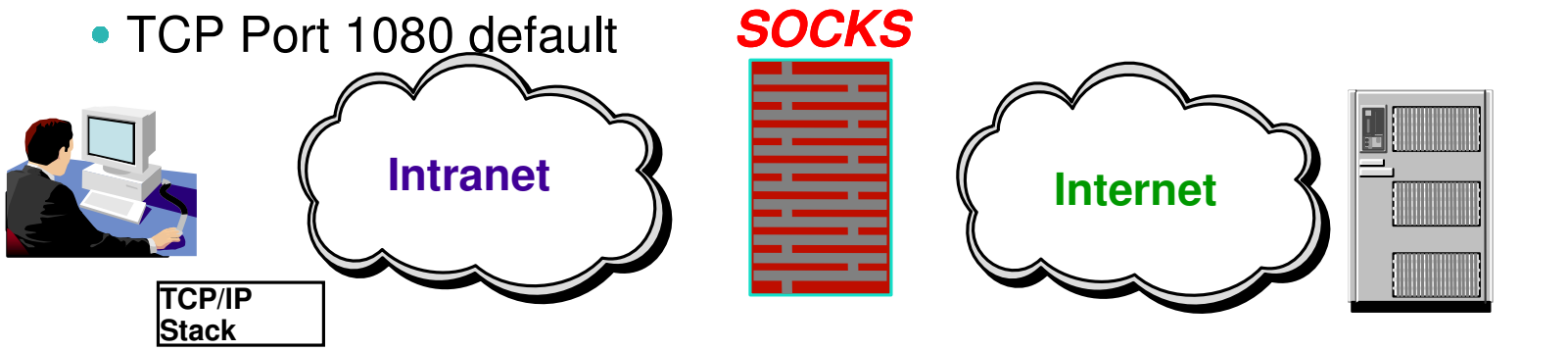


- Limited application availability (proxy and socks servers)
- Simple packet filters
- No risk of letting unwanted IP packets through due to a missed packet filter.

© 2009 IBM Corporation

SOCKS and Proxy

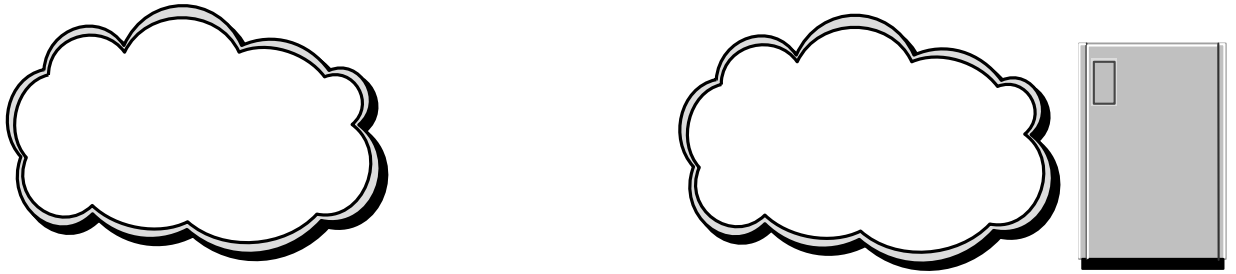
- SOCKS
  - Stack-specific gateway
  - Transparent to client / server
  - Outbound Connections
  - TCP Port 1080 default



© 2009 IBM Corporation

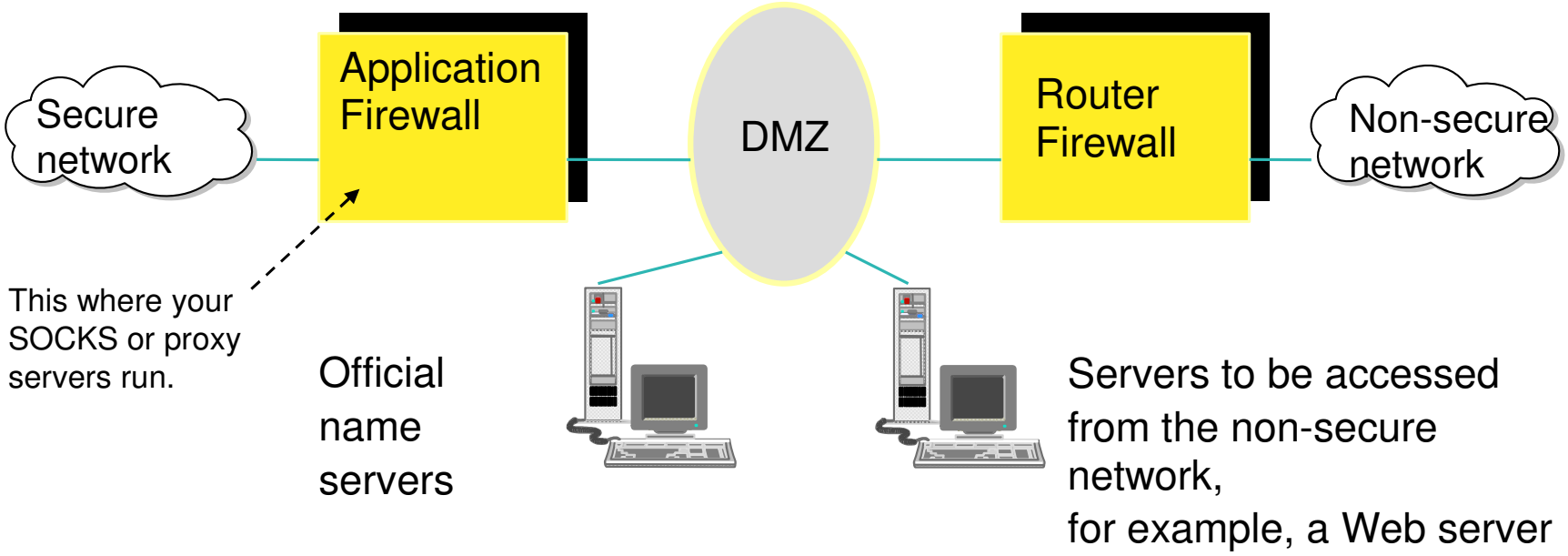
SOCKS and Proxy

- Proxy Server
  - Application-specific gateway
  - Outbound (needs client modification)
  - Inbound (Reverse) needs no modification



© 2009 IBM Corporation

Demilitarized Zone



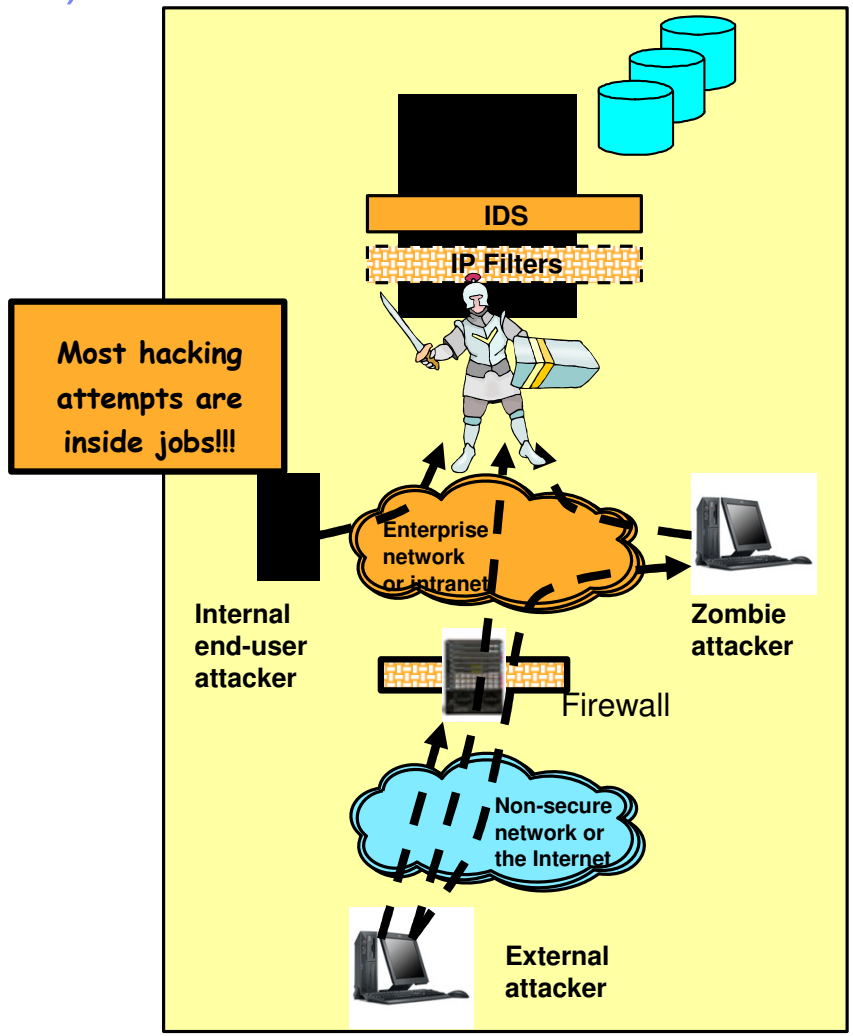
May have multiple DMZs

Parallel or serial

© 2009 IBM Corporation

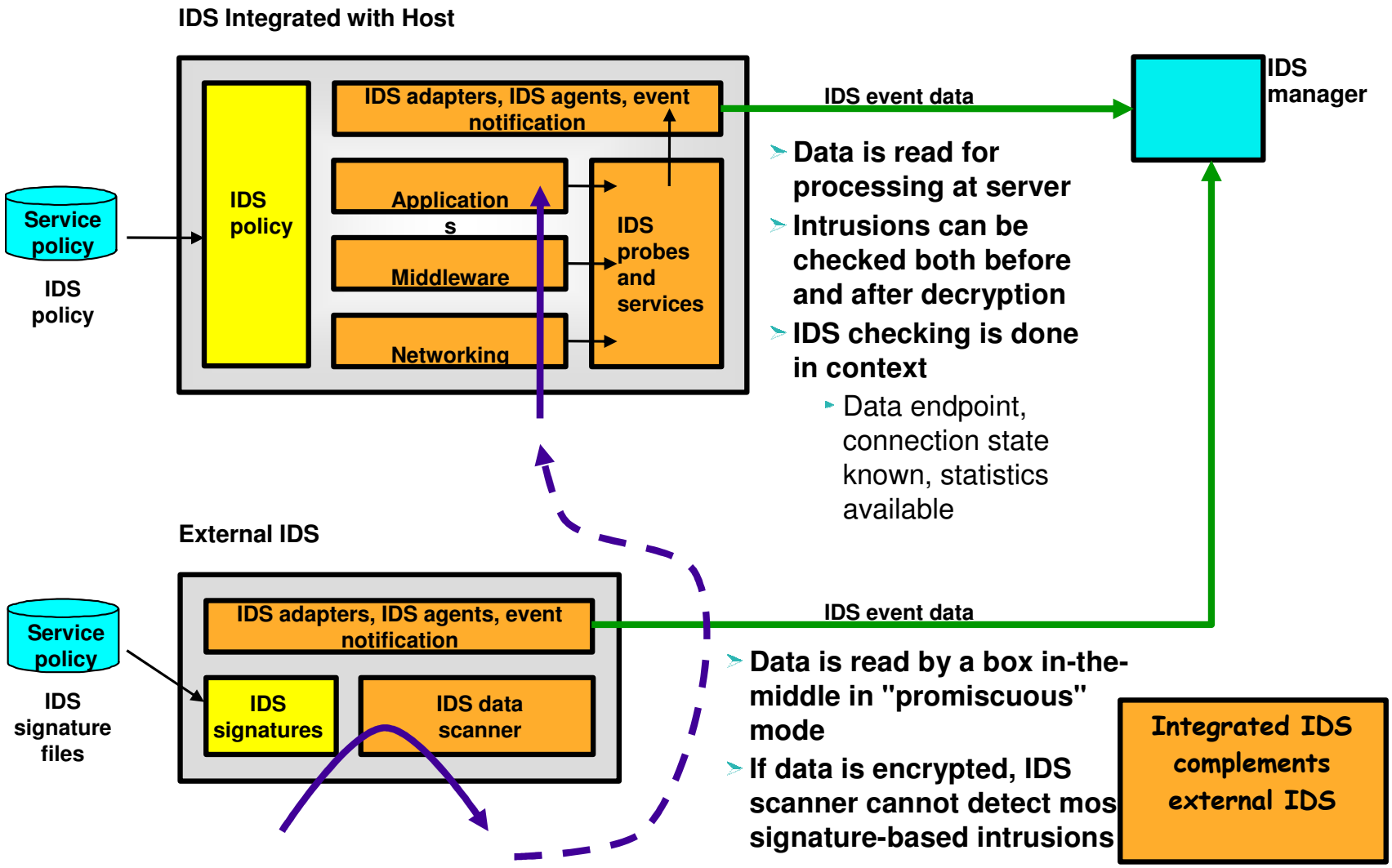
Protecting against malicious or accidental attacks on your system or your legitimate (open) services

- **What is an intrusion?**
  - Information Gathering
    - Network and system topology
    - Data location and contents
  - Denial of Service
    - Single packet attacks - exploits system or application vulnerability
    - Multi-packet attacks - floods systems to exclude useful work
- **Attacks can occur from Internet or intranet**
  - External firewall can provide some level of protection from Internet
  - Perimeter security strategy alone may not be sufficient.
  - Attacks can be deliberate with malicious intent, or they can occur as a result of various forms of errors on nodes in the network
  - Attacks may come from a trojan or zombie installed during a previous hack



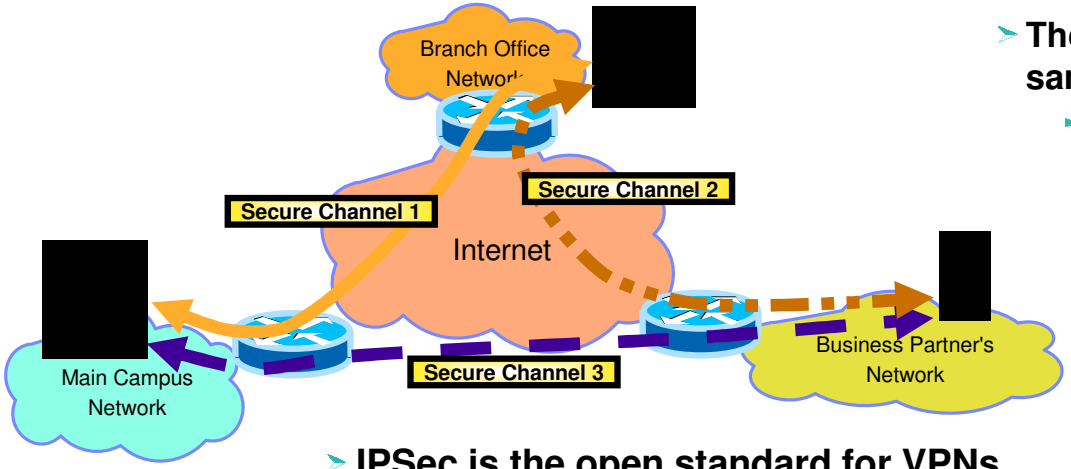
© 2009 IBM Corporation

Integrated versus external Intrusion Detection Services (IDS)



© 2009 IBM Corporation

IPSec Virtual Private Network (VPN) overview

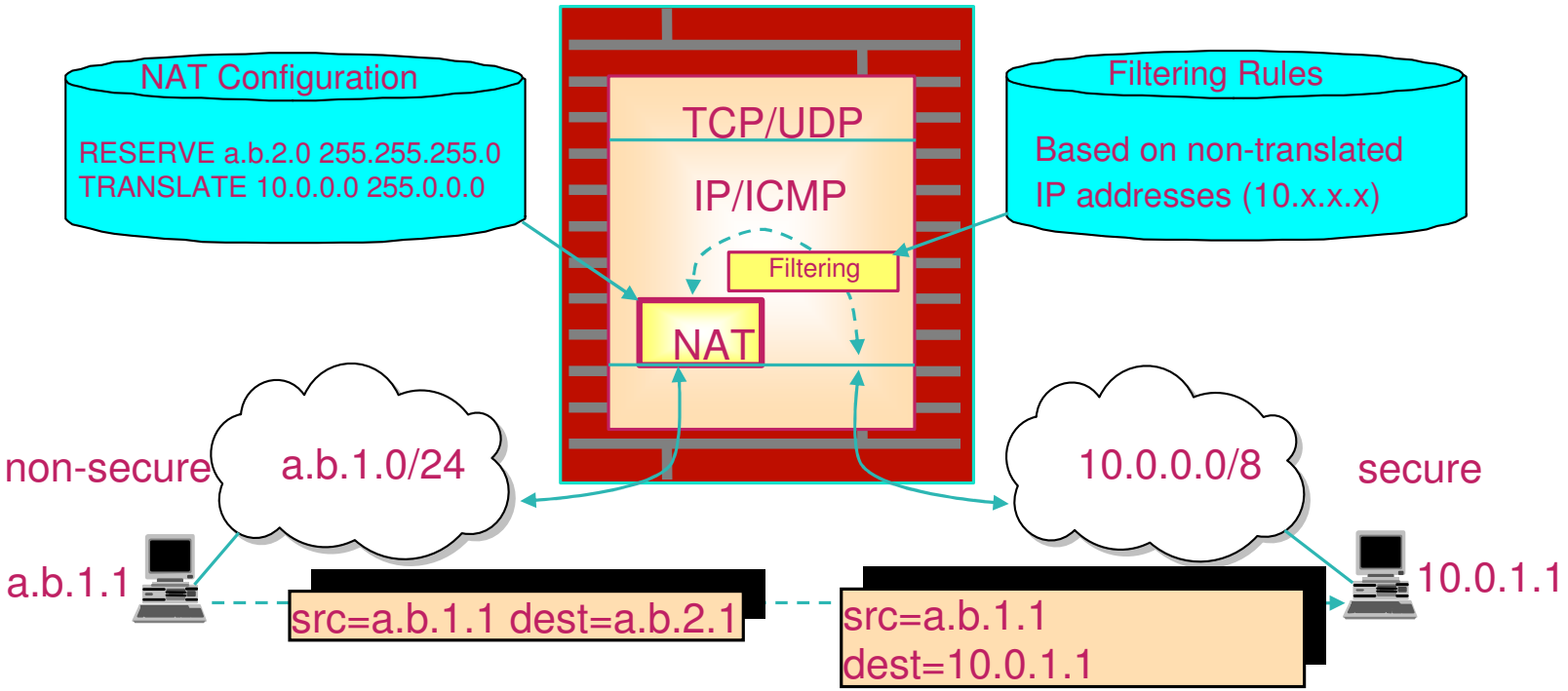


- **The three secure channels in this sample configuration make up a VPN**
  - Each secure channel in itself can be considered a VPN

- **IPSec is the open standard for VPNs**
  - Defined in RFCs
- **Provides authentication,51.48248293(t)8.82055(i)-3.52405(o)5.29649(n)13.8275(,)5.00699(**

© 2009 IBM Corporation

Network Address Translation



- NAT was done to conserve IP addresses
- NAT is "security by obscurity"
- NAPT is also used (port translation)
- NAT and NAPT make crypto-based security more difficult!

© 2009 IBM Corporation

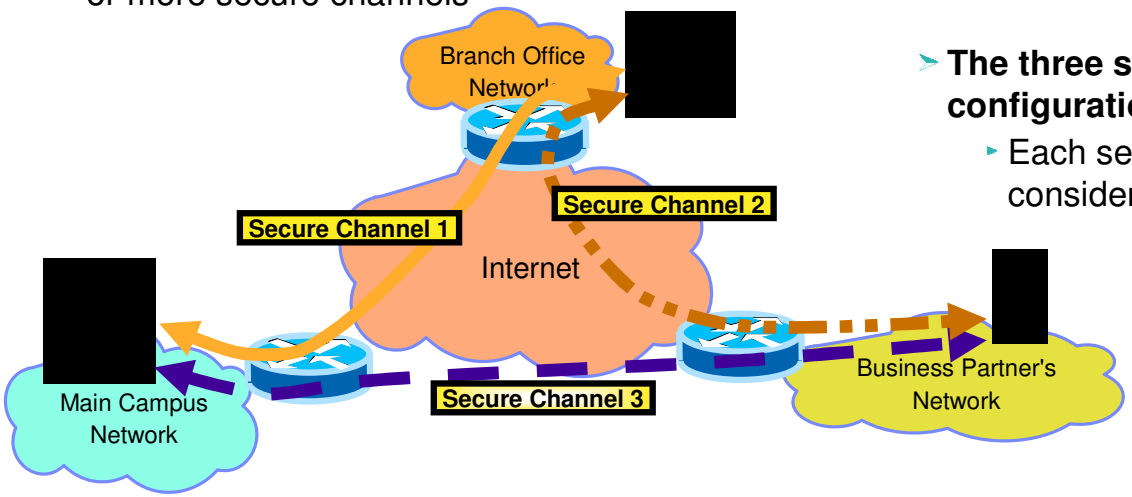
IPSec Architecture

- **Security Association**
- **Authentication Header (AH) Protocol**
- **Encapsulated Security Payload (ESP) protocol**
- **Transport mode and Tunnel mode**
- **ISAKMP/Oakley**
- **Internet Key Exchange (IKE)**
- **IPSec Data Flows**

© 2009 IBM Corporation

IPSec Overview

- **Virtual Private Network**
  - Logical network of connected nodes that communicate over unsecure networks using one or more secure channels



- **The three secure channels in this sample configuration make up a VPN**
  - Each secure channel in itself can be considered a VPN

- **IPSec is a set of standards (RFCs) defining how to do VPNs.**
- **A secure channel is commonly called an IPSec security association (SA).**
  - The term "tunnel" is also sometimes used in this context, but it is ambiguous and can be confusing
- **A secure channel provides point-to-point security: Authentication, Data Integrity and optionally Confidentiality.**
- **There is no "client" or "server" - only "initiator" and "responder".**
- **IPSec utilizes IP security protocols defined by the IPSec working group**
  - Original Ones : RFC 2401 to RFC 2412
  - New Ones : RFC 4301 to RFC 4308

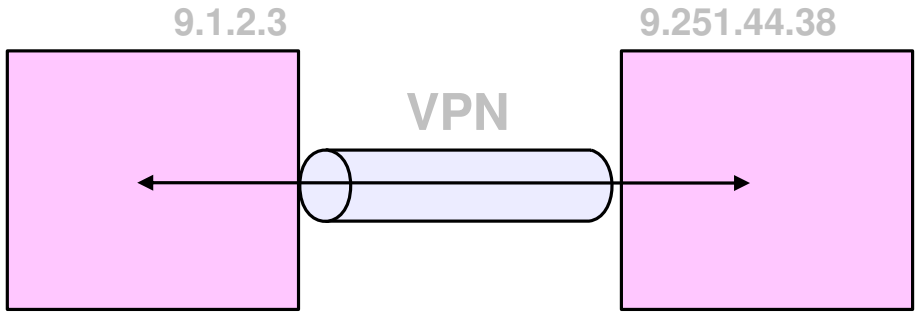
© 2009 IBM Corporation

IPSec - How to encapsulate?

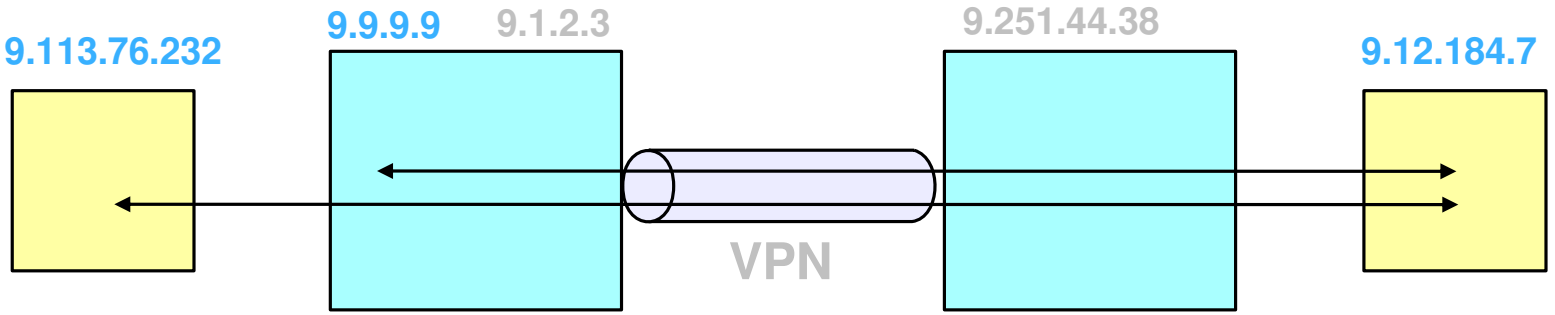
- **Two modes**
  - Transport mode
    - Inserts IPSec headers between original IP header and protected data
  - Tunnel mode
    - Creates a new IP header with an IPSec header
    - IPSec header followed by original IP header and protected data
- **If one or both security endpoints are acting as a gateway**
  - Tunnel mode must be selected
  - The endpoints are ADDRESSES not HOSTS (z/OS usually has many addresses)
- **If neither security endpoint is acting as a gateway**
  - Tunnel or transport may be selected
  - Usually transport mode is used in this case
    - No need for extra cost of adding a new IP header in this case
- **The counterpart to encapsulation is decapsulation**

© 2009 IBM Corporation

Transport & Tunnel mode with z/OS



Transport Mode



Tunnel Mode

© 2009 IBM Corporation

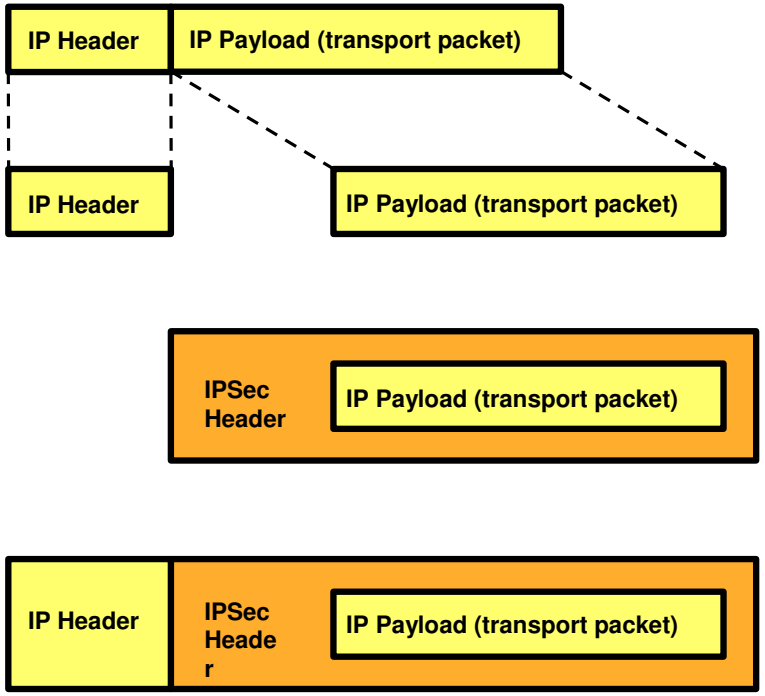
IPSec Packet Using Transport Mode

Original IP packet

Separate IP header and transport packet

Create IPSec packet

Attach and modify original IP header to IPSec packet



Transport mode is typically used between two hosts that establish an IPSec VPN end-to-end between them.

© 2009 IBM Corporation

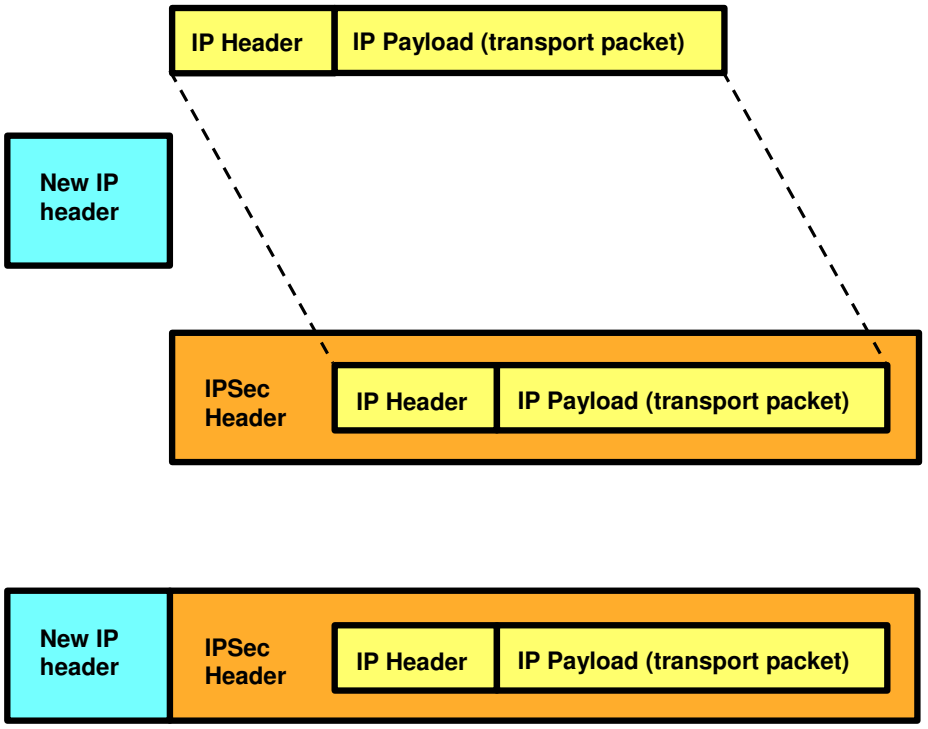
IPSec Packet Using Tunnel Mode

Original IP packet

Create new IP header

Create IPSec packet

Update and attach new IP header to IPSec packet

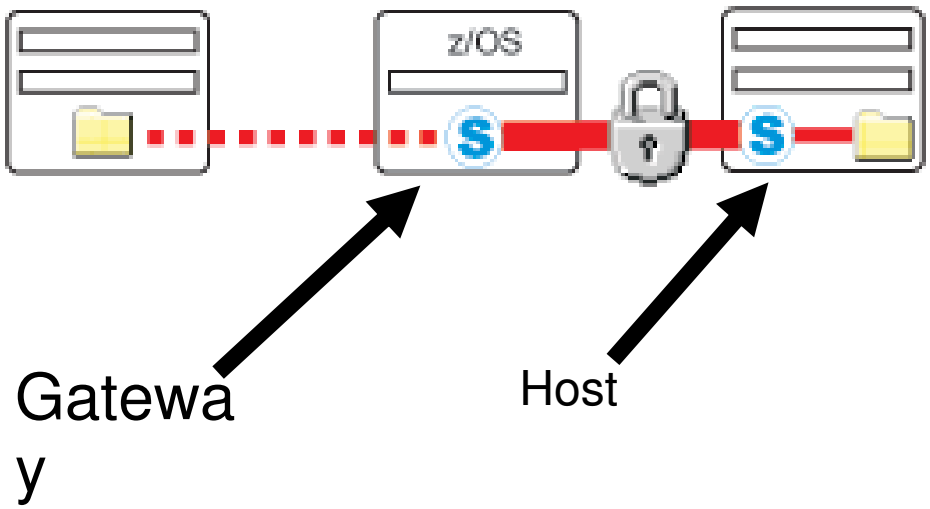


Tunnel mode is used if at least one of the two IPSec VPN endpoints is a gateway.

© 2009 IBM Corporation

Security Endpoints

- **The endpoints of an IPSec secure channel**
  - Where IPSec protection is applied
- **Endpoint roles**
  - Host
    - Local data endpoint and secure channel endpoint are the same IP address
  - Gateway (or Security Gateway)
    - Local data endpoint and secure channel endpoint are different IP addresses



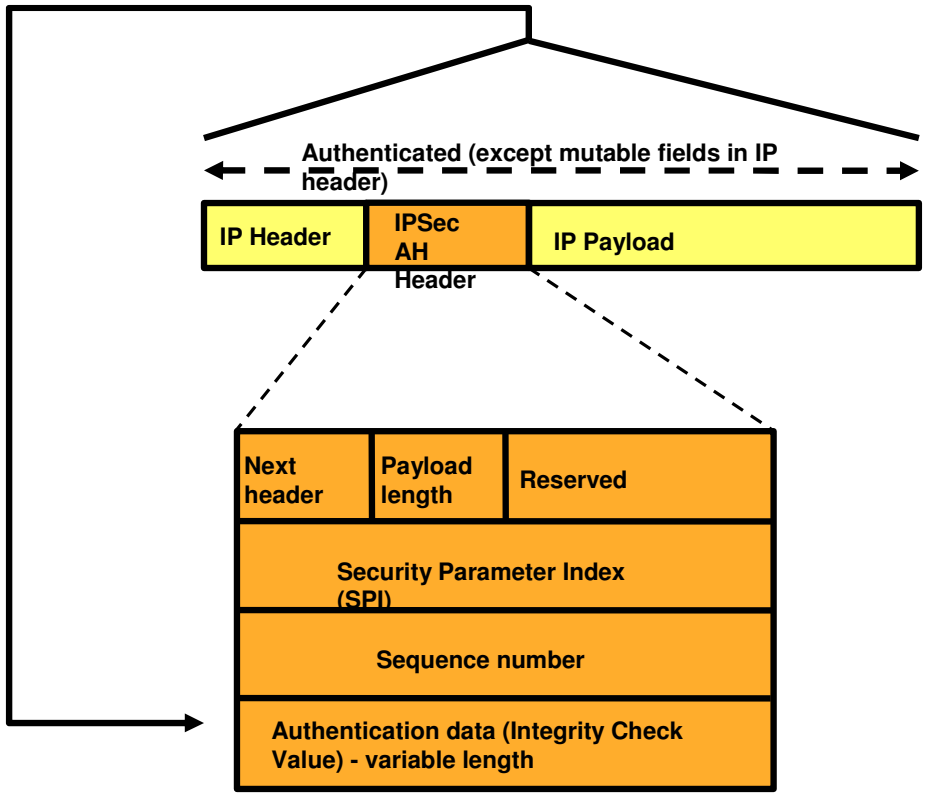
© 2009 IBM Corporation

© 2009 IBM Corporation

Authentication Header Protocol

IP Protocol number 51

- **Authentication algorithms**
  - HMAC-SHA
  - HMAC-MD5



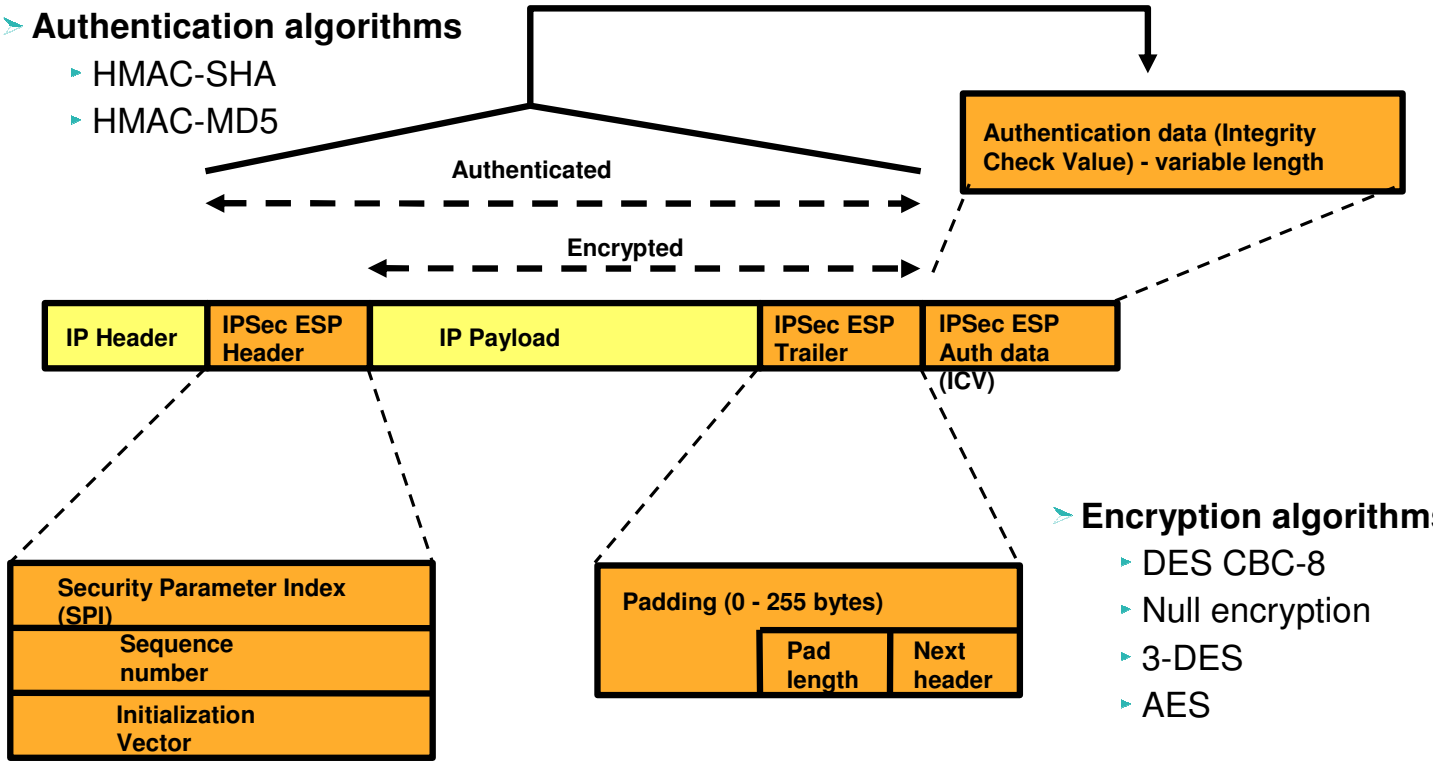
- **If transport mode, then "Payload" contains the original transport header and original data**
- **If tunnel mode, then "Payload" contains the original IP header, original transport header, and original data**

© 2009 IBM Corporation

Encapsulating Security Payload

IP Protocol number 50

- **Authentication algorithms**
  - HMAC-SHA
  - HMAC-MD5



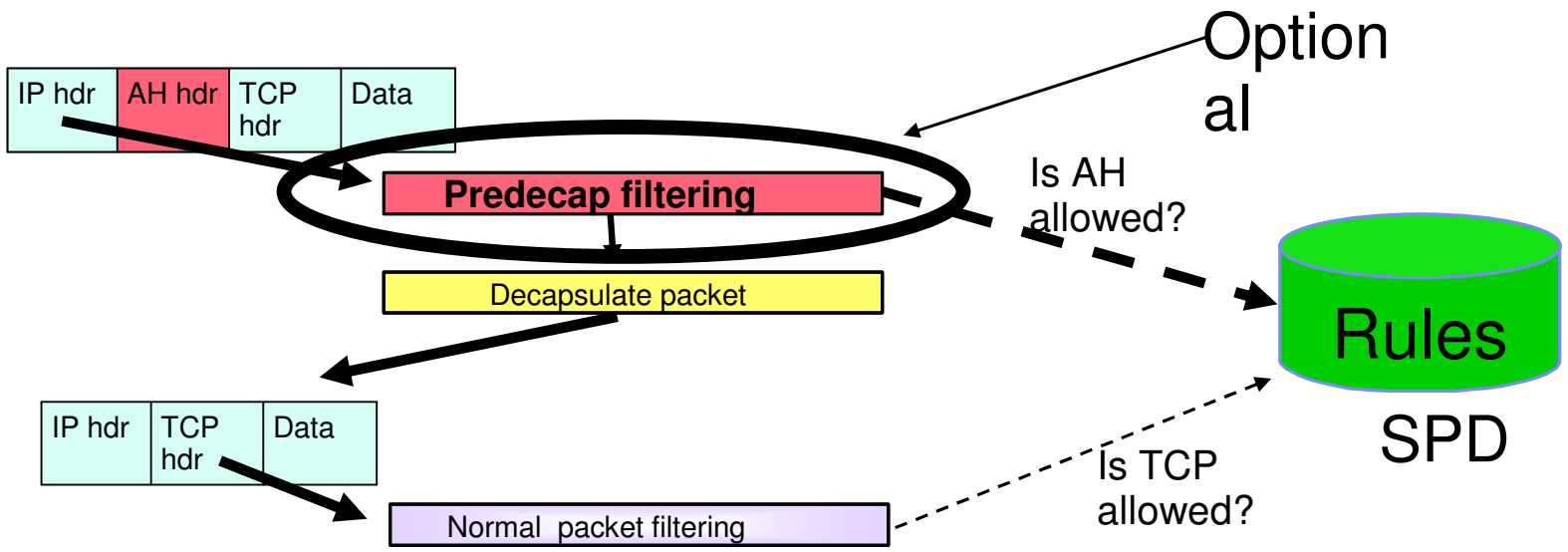
- **Encryption algorithms**
  - DES CBC-8
  - Null encryption
  - 3-DES
  - AES

- **If transport mode, then "Payload" contains the original transport header and original data (possibly encrypted)**
- **If tunnel mode, then "Payload" contains original IP header, original transport header, and original data**
  - "Payload" can be encrypted

© 2009 IBM Corporation

Predecap Filtering

- IPSec protected traffic arrives as an AH or ESP packet (UDP-encapsulated ESP packets are interpreted as ESP packets; see charts on UDP-encapsulation)
- The stack can optionally perform filtering on AH/ESP packets before decapsulation
  - Known as predecap filtering
  - Prevents decapsulation of AH/ESP traffic from unacceptable sources
- The AH/ESP packet is then decapsulated revealing the original packet
  - Filtering is always performed on the decapsulated packet



© 2009 IBM Corporation

Security Associations

- **IPSec secure channel endpoints must agree on how to protect traffic**
  - Security protocol
    - AH
    - ESP
  - Algorithms to be used by the security protocols
    - Encryption Algorithm
      - DES or Triple DES or AES
    - Authentication Algorithm
      - HMAC_MD5 or HMAC_SHA
  - Cryptographic keys
  - Encapsulation mode
    - Tunnel
    - Transport
  - Lifetime/lifesize (for dynamic SAs)
- **This agreement is known as a "security association" - or for short, an SA**

© 2009 IBM Corporation

Security Associations

- **Used to protect IP traffic**

- **Unidirectional**
  - Need one for inbound and another for outbound - each IPSec secure channel endpoint consists of two SAs
    - Generally symmetrical with regards to algorithms used
    - Cryptographic keys will be different
  - A pair of matching SAs are, on z/OS, referred to as a "Tunnel ID" - in a sense identifying the secure channel

- **An SA is identified by:**
  - A Security Parameter Index (SPI)
    - The SPI is a 32-bit value
    - SPI numbers in themselves may not be unique on a given IPSec node
    - The SPI is carried in the IPSec headers
  - IPSec protocol
  - Destination IP address information

- **Manually defined SAs**
  - Statically defined in the Security Policy Database (SPD - Pagent IPSec config file)

- **Dynamically defined SAs**
  - Negotiated using the Internet Key Exchange protocol
  - Acceptable values (policy) defined in the SPD (Pagent IPSec config file)

- **Security Association Database (SAD)**
  - The collection of all SAs known to the stack

© 2009 IBM Corporation

SA

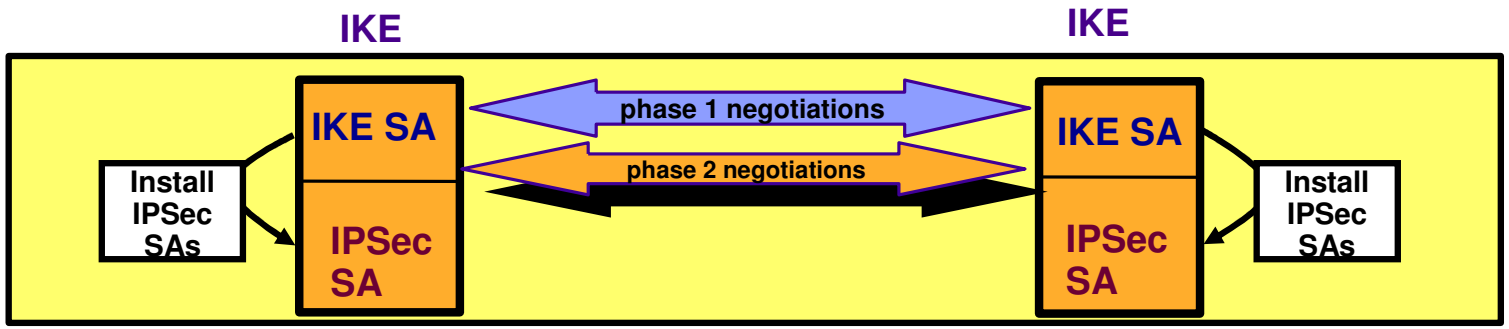
Manual or Dynamic SAs

- Manual SA
  - Not often used - less secure
  - Symmetric keys defined at each end
  - Authentication is done via possession of key
  - Keys need to be updated regularly
- Dynamic SA
  - Symmetric keys generated securely
  - Authentication may be done by certificates, or shared keys
  - Keys are automatically refreshed at intervals
  - Standards used are
    - IKE (Internet Key Exchange) and
    - ISAKMP (Internet Security Association Key Management Protocol, a.k.a. Oakley)
    - Done using UDP port 500

© 2009 IBM Corporation

Two Phases of Key Negotiation for a Dynamic Tunnel

- **Phase 1 negotiation**
  - Creates a secure channel with a remote security endpoint
    - Negotiates an IKE SA
      - Generates cryptographic keys that will be used to protect Phase 2 negotiations and Informational exchanges
      - Authenticates the identity of the parties involved
      - Bidirectional, and not identified via SPIs
  - Requires processor-intensive cryptographic operations
  - Done infrequently
- **Phase 2 negotiation**
  - Negotiates a pair of IPSec SAs with a remote security endpoint
    - Generates cryptographic keys that are used to protect data
      - Authentication keys for use with AH
      - Authentication and/or encryption keys for use with ESP
  - Performed under the protection of an IKE SA
  - Done more frequently than phase 1



© 2009 IBM Corporation

ISAKMP Security Associations

- **Used to protect Phase 2 negotiations**
- **Bidirectional**
- **Endpoints must agree on**
  - Encryption algorithm
    - DES/Triple DES/AES...
  - Hash Algorithm
    - MD5/SHA1...
  - Authentication Method
    - Preshared Key
    - RSA Signature
  - Diffie-Hellman Group
  - Lifetime/Lifesize
- **Policy definition is based on identities exchanged during phase 1**
  - Key Exchange Policy
    - A set of filter rules for IKE

© 2009 IBM Corporation

IKE/ISAKMP Details

- There are two different phase 1 exchange modes. Both exchange the same information, but one utilizes fewer messages.
  - Main mode
    - All IPSec implementations must support main mode. Main mode utilizes 6 messages. The last two messages contain identity information and are encrypted. This provides identity protection.
  - Aggressive mode
    - Some IPSec implementations do not support aggressive mode. Aggressive mode utilizes 3 messages. No messages are encrypted.
- Identity information is used to locate policy. Phase 1 identity types supported by Integrated IPSec include:
  - An IPv4 address (this identity type should not be used when behind a NAT)
  - RFC 822 name (for example, email address)
  - Fully qualified domain name (FQDN)
  - x500 distinguished name (DN)
- Authentication modes
  - Preshared key
    - Security endpoint administrators agree to this value. The key is not directly used to encrypt data.
    - Often used during the initial stages of dynamic SA deployment
  - RSA signature
    - Require X509 certificates.
      - Certificates need to contain an endpoint's identity in the certificate's SubjectName (for DNs) or the SubjectAlternate name (for RFC 822 names, FQDNs, or IPv4 addresses).
    - Often used when dynamic SA are widely deployed.
- Diffie-Hellman is an algorithm that allows IKE to produce cryptographic keying material. Diffie-Hellman groups are defined in RFC 2409 (IKE). Original options are groups 1 and 2. Group 2 provides better security characteristics, but it also requires more computational power. Groups 5 and 14 are new for use with AES.

© 2009 IBM Corporation

Perfect Forward Secrecy

- Perfect forward secrecy
  - Refers to the notion that the compromise of a single key will only permit access to data protected by that key
    - Compromise of the keys negotiated in phase 1 will not compromise keys generated in phase 2
    - Compromise of the keys negotiated in phase 2 will not compromise future phase 2 keys or previously generated phase 2 keys
- PFS is optional
  - Accomplished by performing an optional Diffie-Hellman exchange during phase 2
    - The Diffie-Hellman exchange during Phase 1 SA is not optional
- Factors to consider
  - Frequency that IKE SAs are refreshed (Phase 1)
  - Frequency that IPSec SAs are refreshed (Phase 2)
  - Key size

© 2009 IBM Corporation

IPSec without NAT Traversal

- Tunnel mode with AH and/or ESP

Gateway to Gateway

Gateway to Host

Host to Gateway

- Tunnel or transport mode with AH and/or ESP

Host to Host

Legend

Security Endpoint

Data Endpoint

Protected Data

Unprotected Data

Data Endpoint same as Security Endpoint

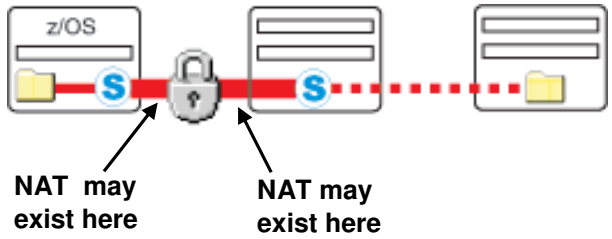
© 2009 IBM Corporation

IPSec with NAT (or NAPT) in the way

- **IPSec carries endpoint IP addresses in data (and they are secured)**
- **Solution is to encapsulate ESP packet in UDP packet**
- **NAT is discovered dynamically by IKE daemon**
  - Therefore, dynamic tunnels only
  - Additional flows in Phase 1 Exchange
- **If the responder of an SA negotiation is behind a NAT or NAPT firewall, a static NAT mapping should be used**

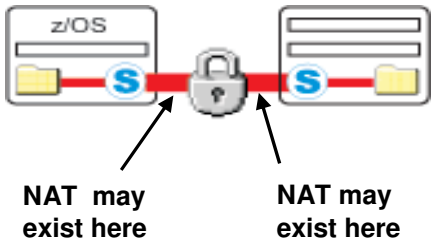
- Tunnel mode with ESP

Host to Gateway



- Tunnel or transport mode with ESP

Host to Host



© 2009 IBM Corporation

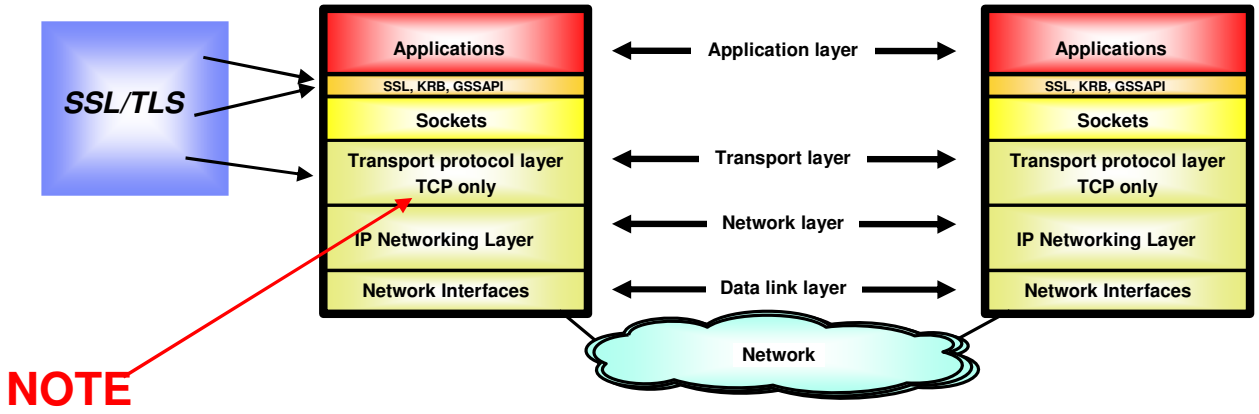
© 2009 IBM Corporation

Secure Sockets Layer and Transport Layer Security

- **SSL History**
- **Client and Server authentication**
- **SSL/TLS Protocols and Flows**

© 2009 IBM Corporation

SSL/TLS Overview



- **Transport Layer Security (TLS) is defined by the IETF (RFC 2246)**
  - Based on Secure Sockets Layer (SSL)
    - Above sockets layer, below application layer
    - SSL originally defined by Netscape to protect HTTP traffic
    - V1 no longer supported
    - V2 still exists, concerns about efficacy
    - V3 is common
    - TLS is V3.1; TLS implementers should drop to V3 if partner is back level
- **End to End Application "pipe"**
  - Requires reliable transport layer, therefore TCP only
  - Server always authenticated, client is optional
    - Always uses certificate
    - Client authentication is often ID/password, but encrypted
  - Application source code changes are generally needed to enable a Sockets program for TLS

© 2009 IBM Corporation

SSL/TLS Functions

- TLS provides:
  - Message privacy
    - Using symmetric key encryption.
    - Uses a handshake when initiating contact. The handshake establishes a session key and encryption algorithm, between both parties, prior to any messages being sent.
  - Message integrity
    - By using the combination of shared secret key and cryptographic hash functions.
    - This ensures that the content of any messages does not change.
  - Mutual authentication
    - Server and (optionally) client authenticate to each other.
    - This happens during the handshake.

© 2009 IBM Corporation

SSL/TLS Contrasted with IPSec

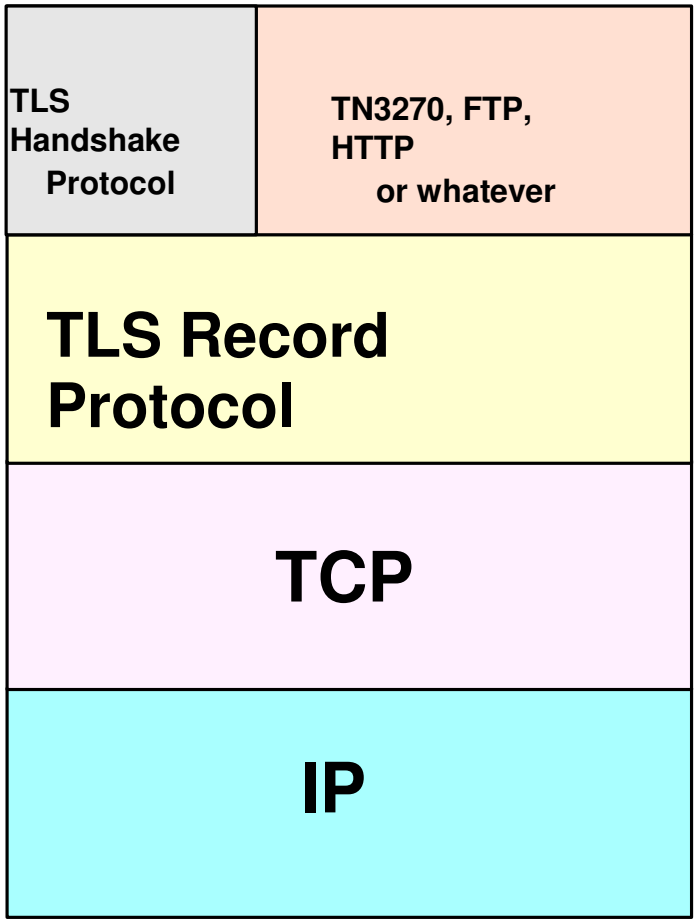
1. IPSec is stack-level
2. IPSec protects all traffic between specified address ranges
3. IPSec can protect any IP protocol
4. IPSec can do manual or dynamic tunnels
5. IPSec can do shared keys or certificate authentication
6. IPSec must authenticate both partners
7. IPSec can do data integrity, and optionally privacy (encryption)

1. SSL/TLS is application-specific
2. SSL/TLS protects all traffic on a specified TCP connection
3. SSL/TLS can only protect TCP
4. SSL/TLS can only do dynamic sessions
5. SSL/TLS must always use certificates
6. SSL/TLS must authenticate the server, and optionally the client
7. SSL/TLS always does privacy (encryption)

The same algorithms (DES, 3DES, AES, MD5, SHA, RSA, DSA.... are used by both SSL/TLS and IPSec.

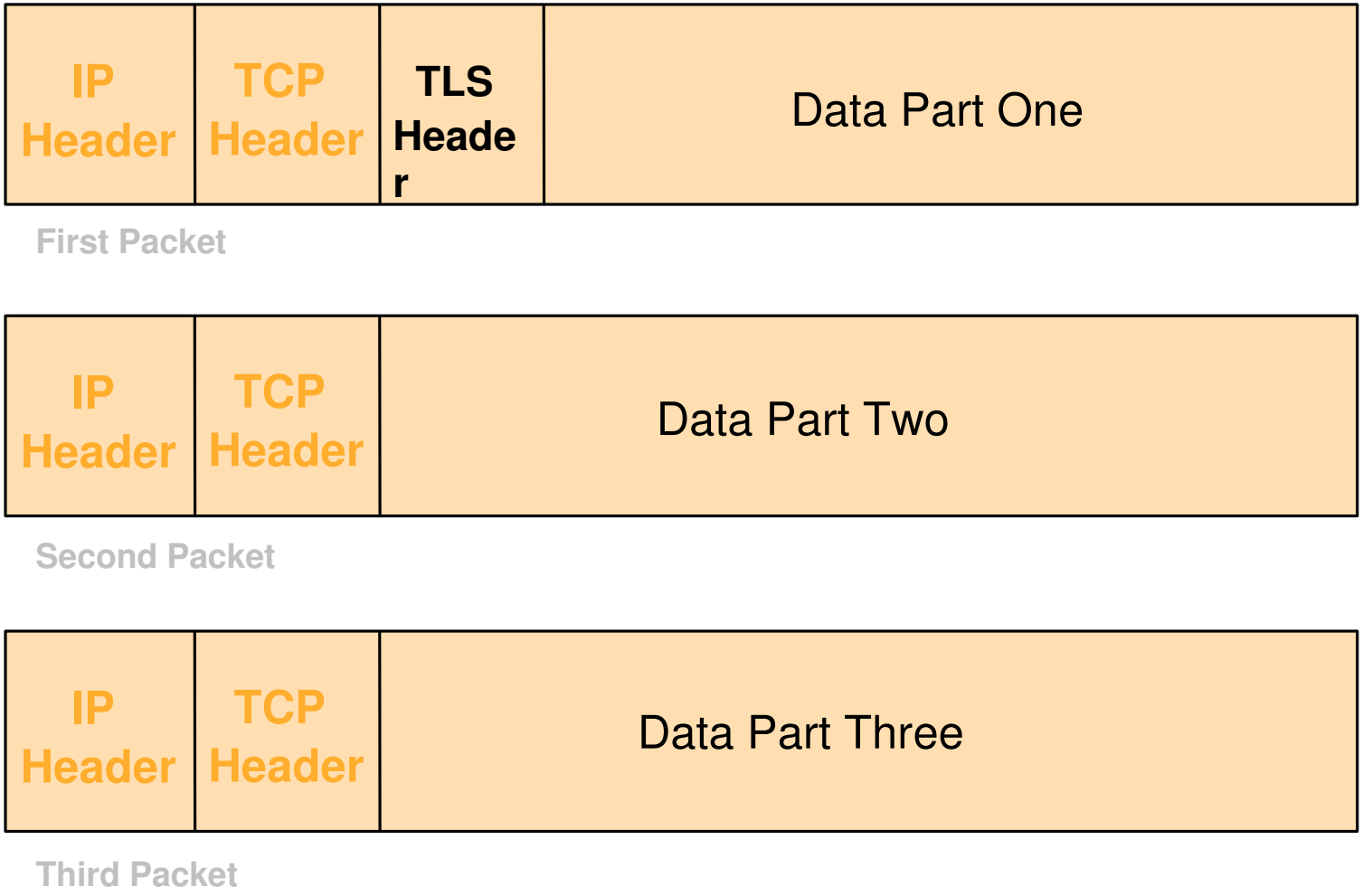
© 2009 IBM Corporation

SSL/TLS Protocol Stack



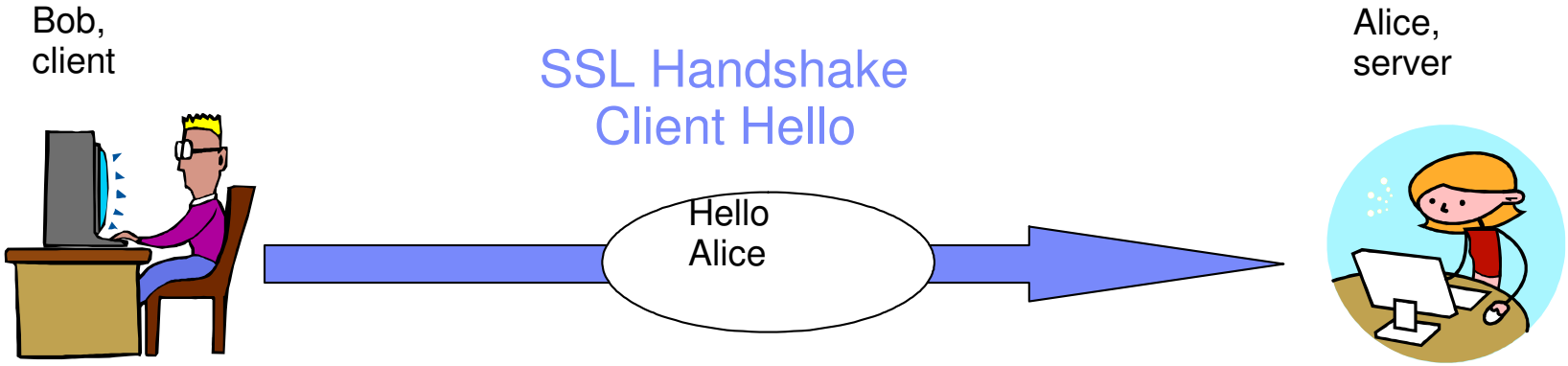
© 2009 IBM Corporation

SSL/TLS Packet Format



© 2009 IBM Corporation

SSL/TLS Handshake (1)

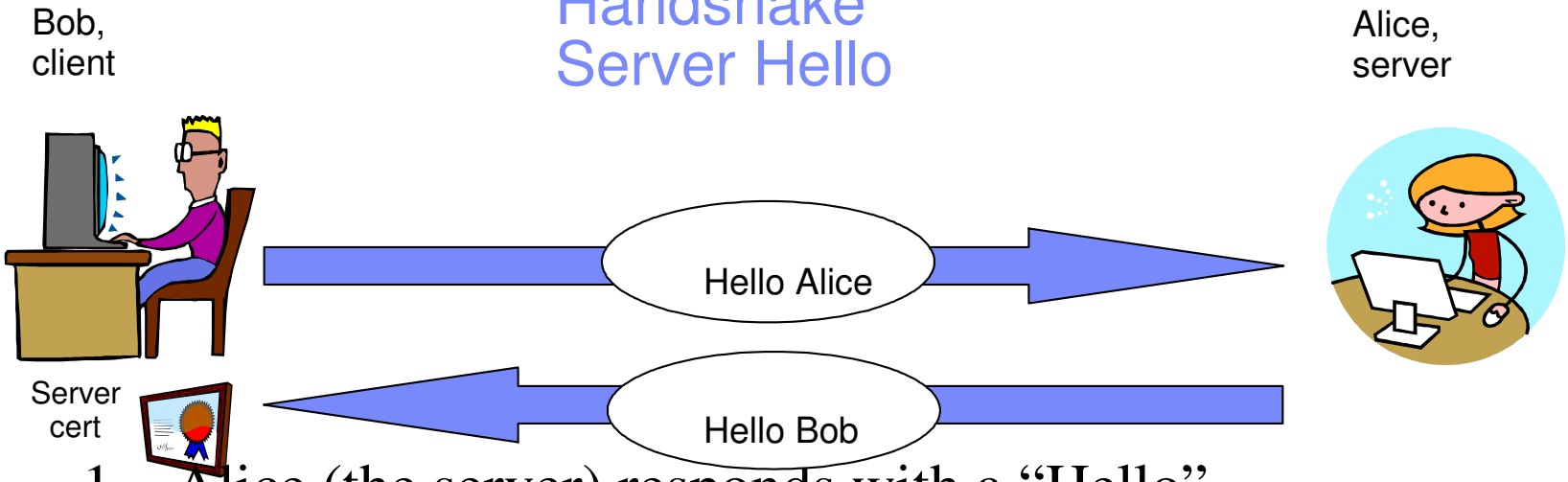


1. Bob sends Alice a hello message.
2. Within this initial contact message is a list of Cipher Suites that Bob (the client) can use.
3. The list is in client preference.
4. Bob is considered the client since he initiated communication.

© 2009 IBM Corporation

SSL/TLS Handshake (2)

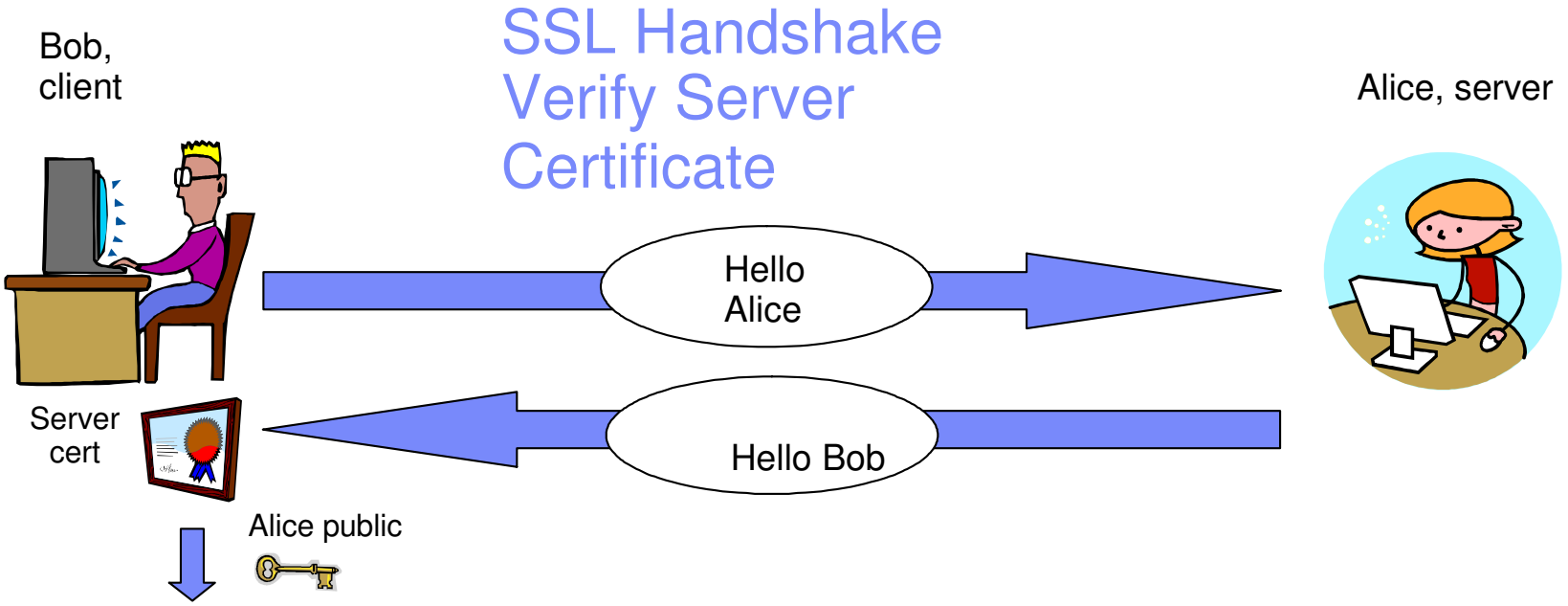
SSL Handshake Server Hello



1. Alice (the server) responds with a “Hello”
2. Alice also sends Bob a signed Digital Certificate containing her public key
3. Bob will already have a CA certificate in a key database, against which to verify Alice's certificate
4. This response contains the CipherSuite that Alice has selected from the list Bob sent her

© 2009 IBM Corporation

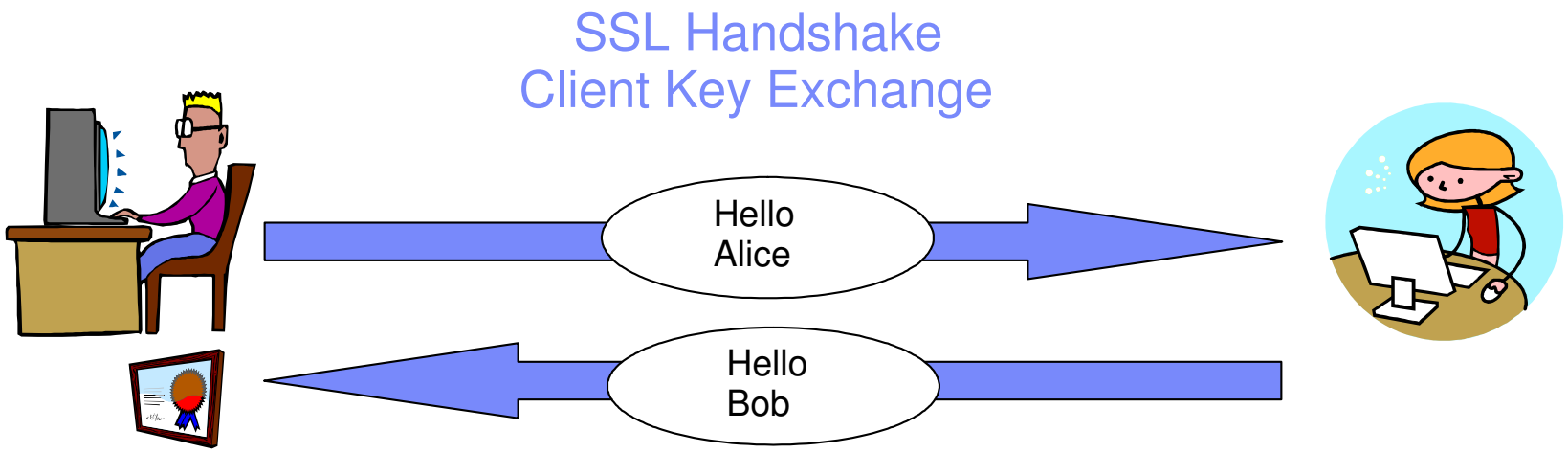
SSL/TLS Handshake (2a)



1. Receive Alice's public key
2. Check if the certificate has expired
3. Verify the certificate's signature against a CA certificate
4. If client authentication is being used, then Alice would request a digital certificate

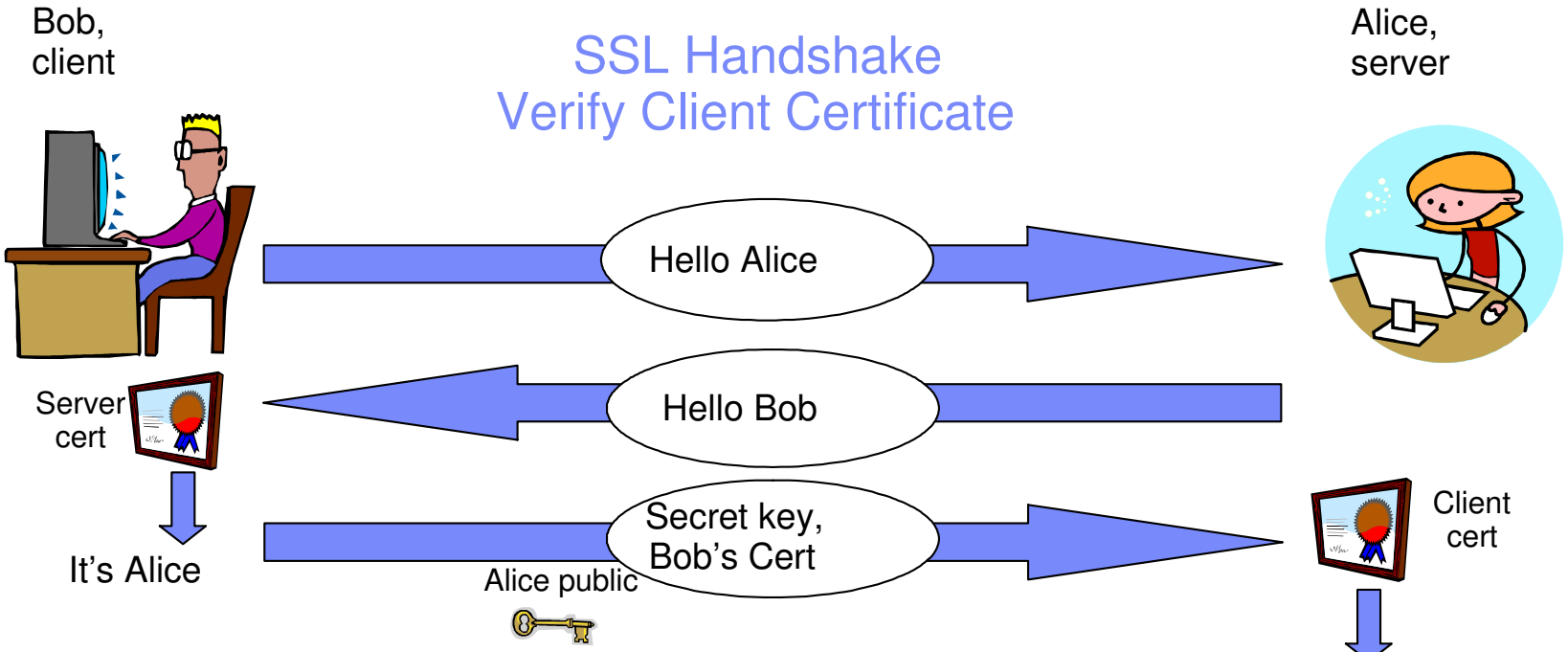
© 2009 IBM Corporation

SSL/TLS Handshake (3)



© 2009 IBM Corporation

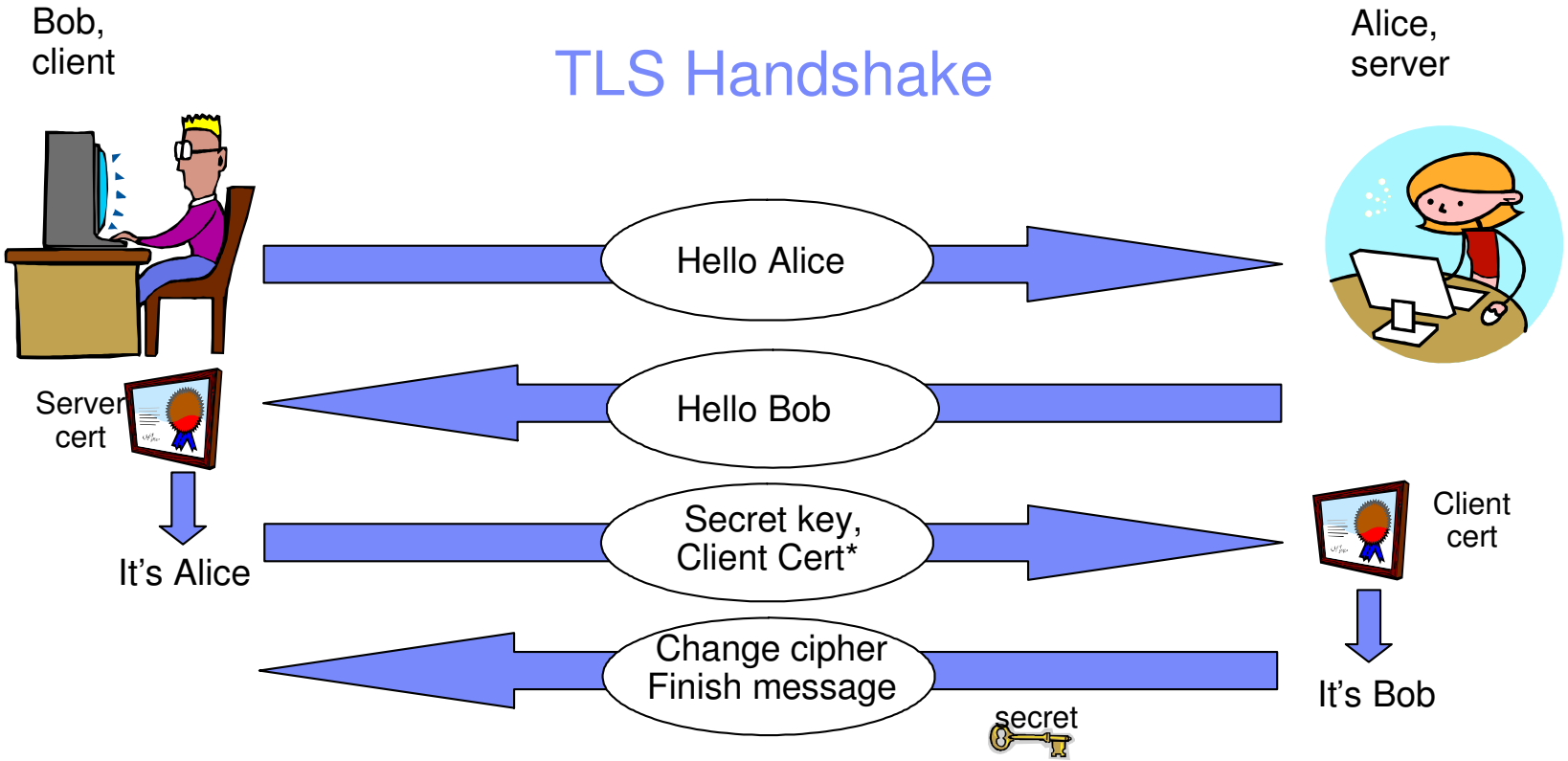
SSL/TLS Handshake (3a)



1. Verify the certificate against a keystore
2. Encrypt using Alice's public key
3. Client key exchange message
4. Change CipherSpec message
5. Finished message

© 2009 IBM Corporation

SSL/TLS Handshake (4)



* Optional if the server requires client certificate

1. Encrypted using secret key
2. Change CipherSuite message
3. Finish Message

© 2009 IBM Corporation