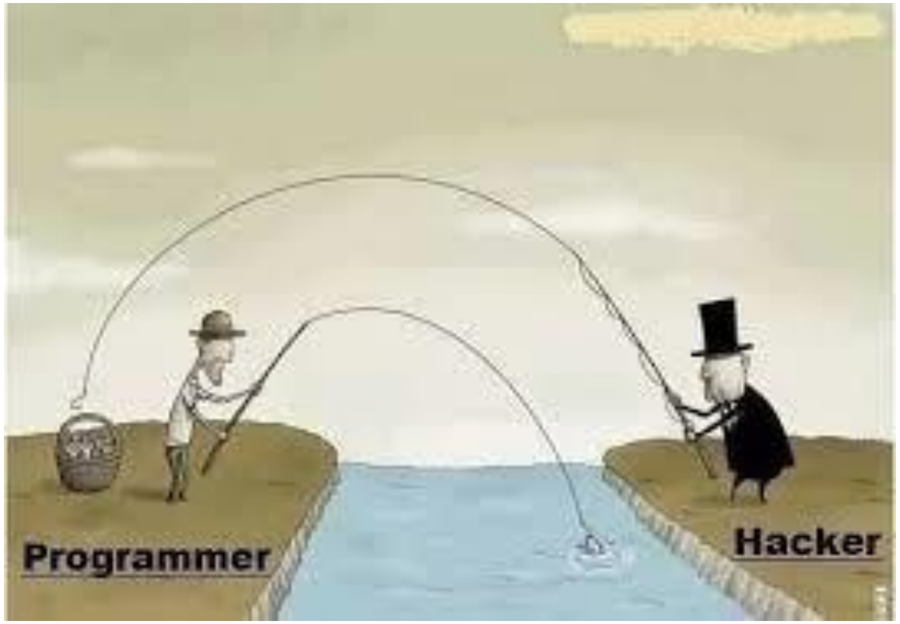
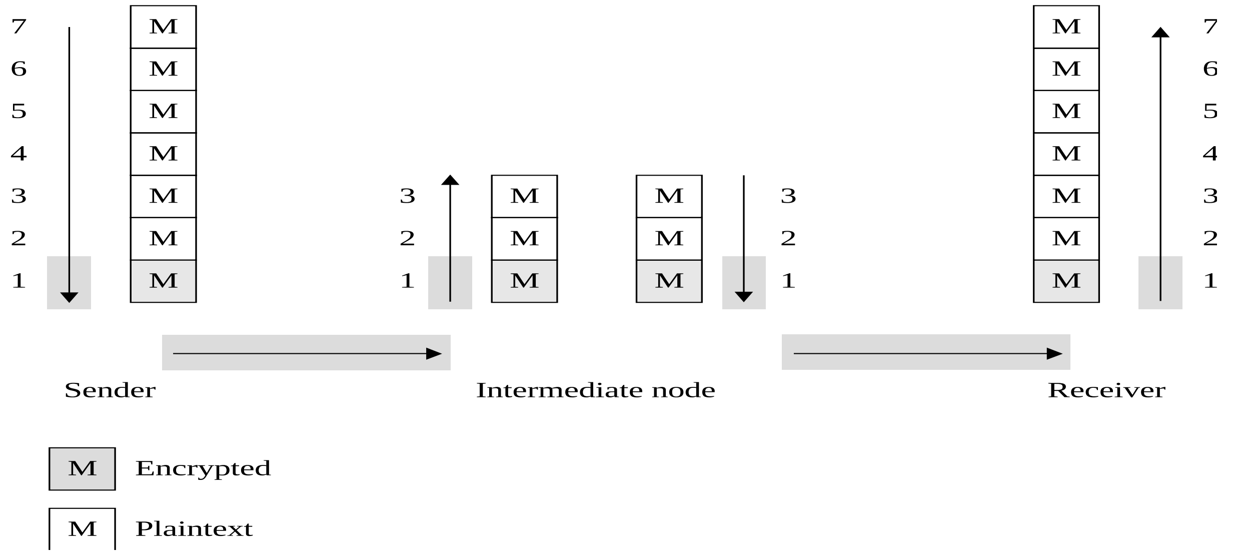
SECURITY IN COMPUTING, FIFTH EDITION

Chapter 6: Networks

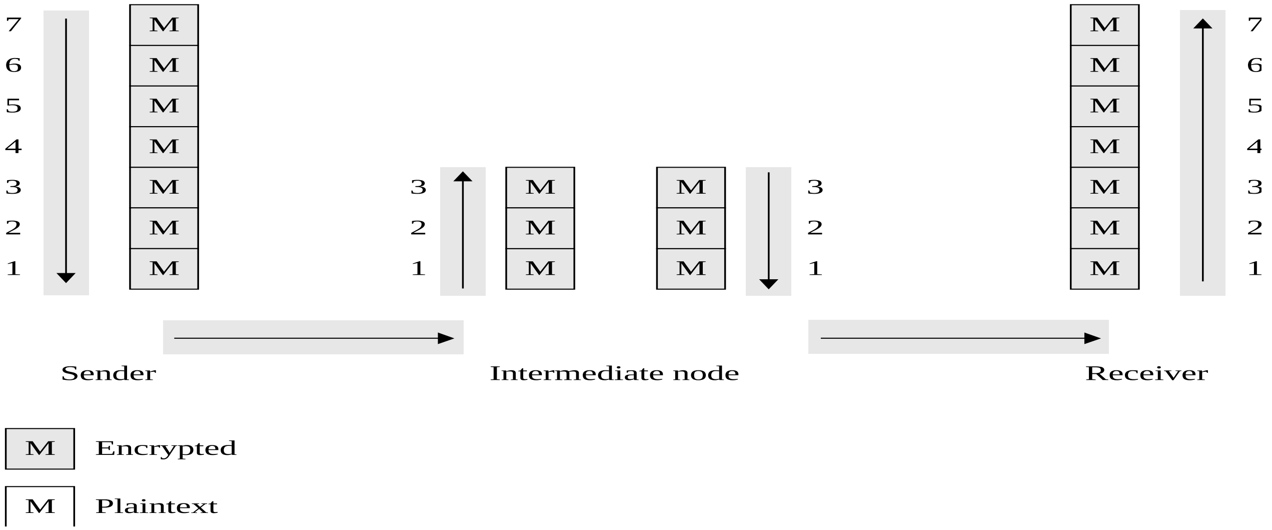


Link Encryption



- In link encryption, data are encrypted just before the system places them on the physical communications link and are decrypted just as they arrive at the destination system. In this graphic, we see that the data is encrypted only at layer 1 of the OSI stack.
- If the data is communicated through an intermediate node, that intermediate node will decrypt the data when it arrives, and then may re-encrypt it for the next link.
- Link encryption is appropriate when the transmission line is the point of greatest vulnerability, such as in wireless scenarios.

End-to-End Encryption

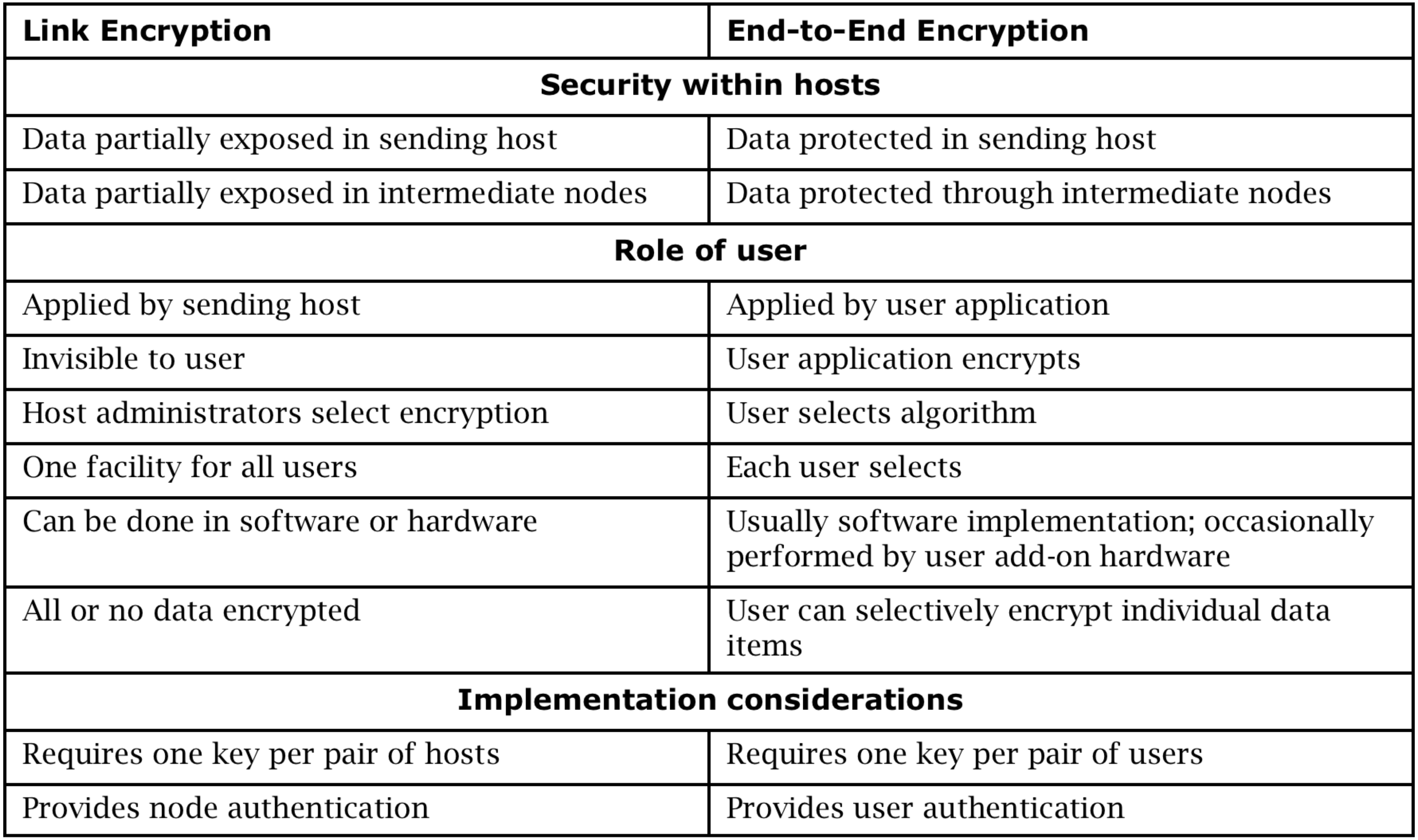


In contrast with the previous slide, this end-to-end encryption diagram shows our data encrypted all the way up to OSI layer 7, the application layer.

In real-world end-to-end encryption, such as those that use SSL, the data often isn’t encrypted all the way to layer 7; the important element is that intermediate nodes cannot decrypt the data.

End-to-end encryption is appropriate whenever sending sensitive data through untrustworthy intermediate nodes, such as over the Internet.

Link vs. End-to-End



Link Encryption	End-to-End Encryption
Security within hosts	
Data partially exposed in sending host	Data protected in sending host
Data partially exposed in intermediate nodes	Data protected through intermediate nodes
Role of user	
Applied by sending host	Applied by user application
Invisible to user	User application encrypts
Host administrators select encryption	User selects algorithm
One facility for all users	Each user selects
Can be done in software or hardware	Usually software implementation; occasionally performed by user add-on hardware
All or no data encrypted	User can selectively encrypt individual data items
Implementation considerations	
Requires one key per pair of hosts	Requires one key per pair of users
Provides node authentication	Provides user authentication

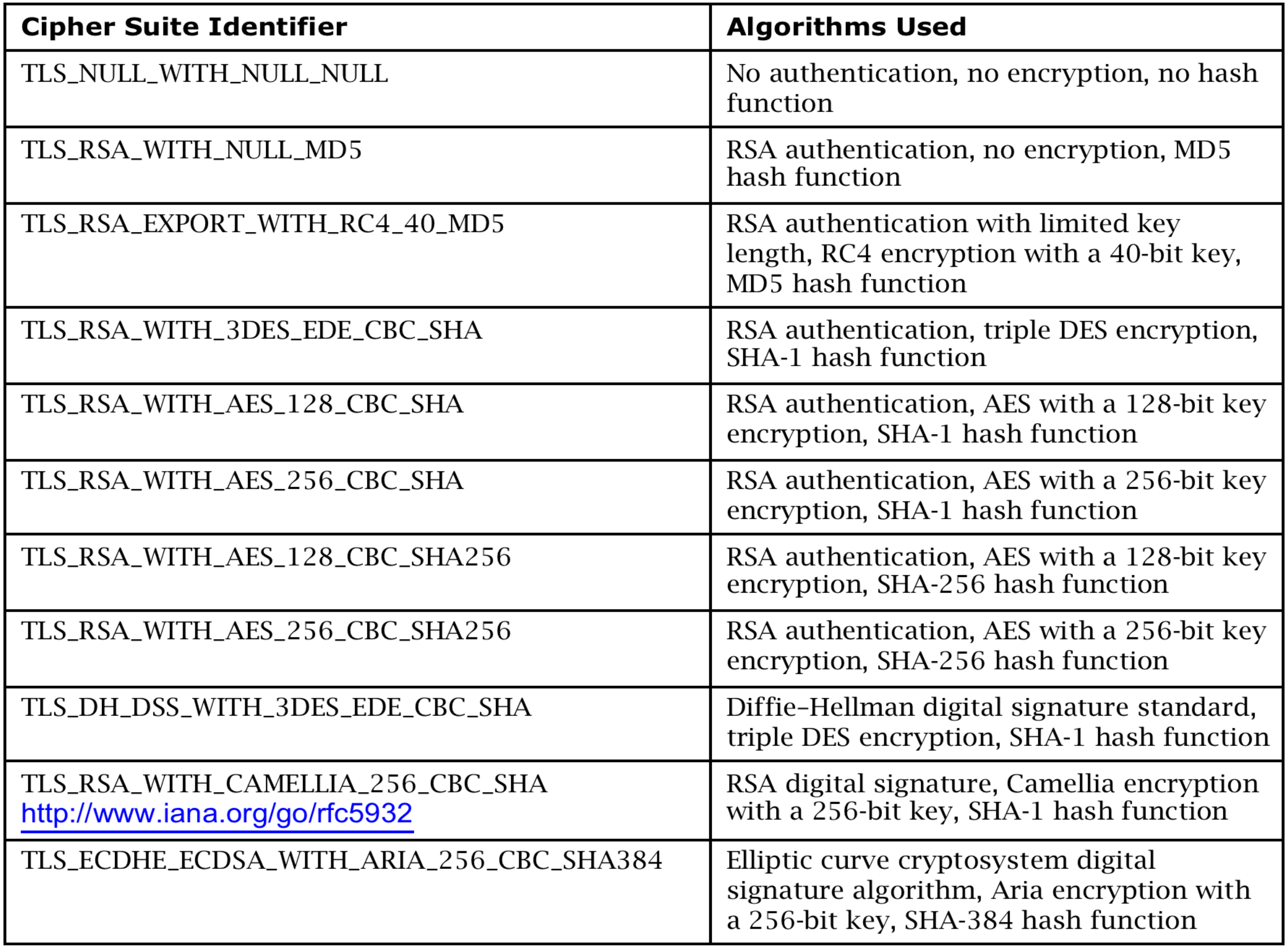
Malicious Autonomous Mobile Agents

- Working largely on their own, these programs can infect computers anywhere they can access, causing denial of service as well as other kinds of harm.
- Code does not develop, appear, or mutate on its own; there has to be a developer involved initially to set up the process and to establish a scheme for updates. Such an agent is sometimes called an inoculation agent.
- As bots or agents execute and acquire updates, not every agent will be updated at once.
- Autonomous Mobile Protective Agents

SSL and TLS

- Secure Sockets Layer (SSL) was designed in 1990s to protect communication between browser & server
- In a 1999 upgrade to SSL, it was renamed Transport Layer Security (TLS)
- While the protocol is still commonly called SSL, TLS is the modern, and much more secure, protocol
- SSL is implemented at OSI layer 4 (transport) and provides
  - Server authentication
  - Client authentication (optional)
  - Encrypted communication
- At start of an SSL session, the client & server negotiate encryption algorithms, known as the “cipher suite”
- The server sends a list of cipher suite options, and the client chooses an option from that list
- The cipher suite consists of
  - A digital signature algorithm for authentication
  - An encryption algorithm for confidentiality
  - A hash algorithm for integrity

SSL and TLS



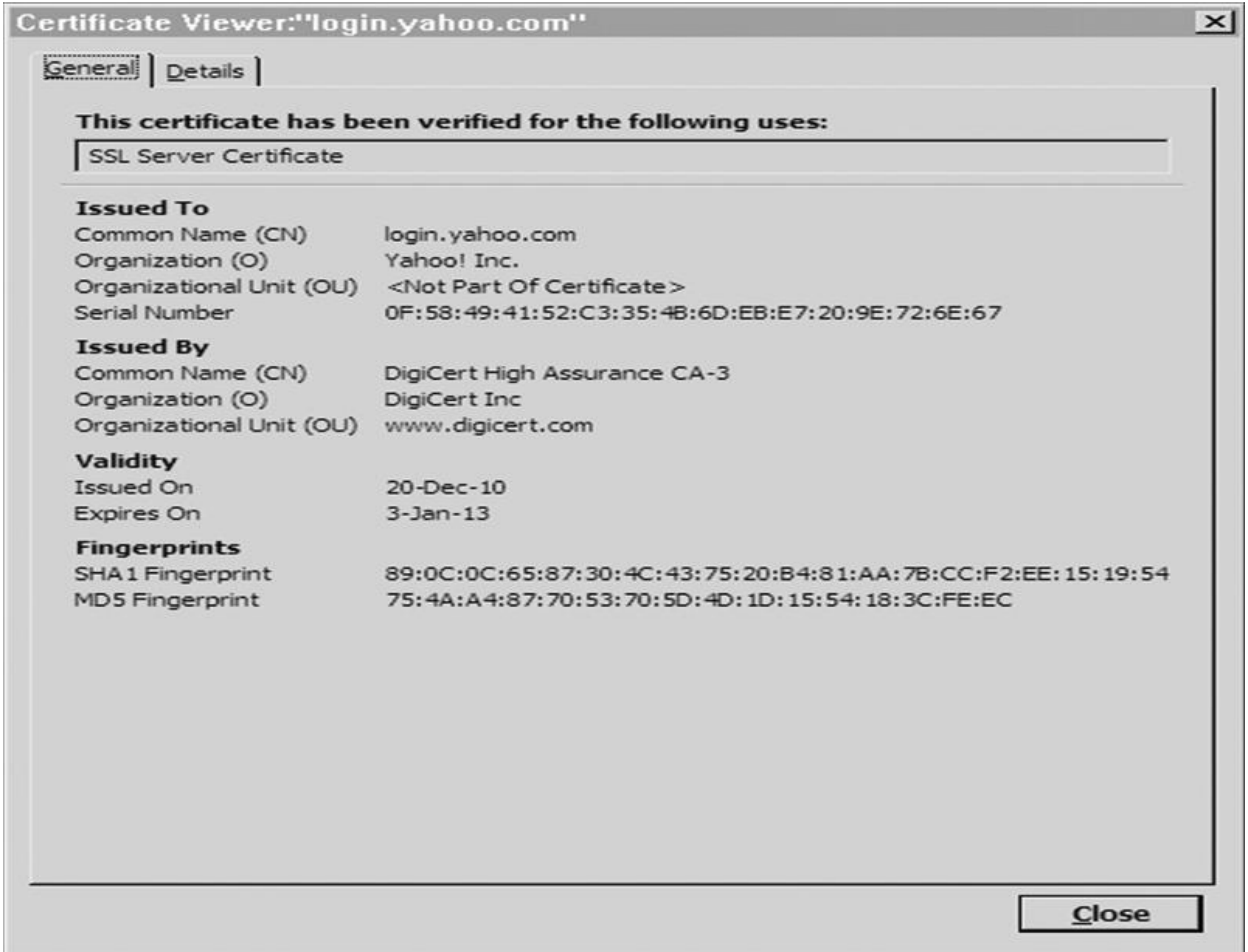
Cipher Suite Identifier	Algorithms Used
TLS_NULL_WITH_NULL_NULL	No authentication, no encryption, no hash function
TLS_RSA_WITH_NULL_MD5	RSA authentication, no encryption, MD5 hash function
TLS_RSA_EXPORT_WITH_RC4_40_MD5	RSA authentication with limited key length, RC4 encryption with a 40-bit key, MD5 hash function
TLS_RSA_WITH_3DES_EDE_CBC_SHA	RSA authentication, triple DES encryption, SHA-1 hash function
TLS_RSA_WITH_AES_128_CBC_SHA	RSA authentication, AES with a 128-bit key encryption, SHA-1 hash function
TLS_RSA_WITH_AES_256_CBC_SHA	RSA authentication, AES with a 256-bit key encryption, SHA-1 hash function
TLS_RSA_WITH_AES_128_CBC_SHA256	RSA authentication, AES with a 128-bit key encryption, SHA-256 hash function
TLS_RSA_WITH_AES_256_CBC_SHA256	RSA authentication, AES with a 256-bit key encryption, SHA-256 hash function
TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	Diffie–Hellman digital signature standard, triple DES encryption, SHA-1 hash function
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA http://www.iana.org/go/rfc5932	RSA digital signature, Camellia encryption with a 256-bit key, SHA-1 hash function
TLS_ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA384	Elliptic curve cryptosystem digital signature algorithm, Aria encryption with a 256-bit key, SHA-384 hash function

SSL and TLS

Cipher suite negotiation is at the center of a very common SSL configuration vulnerability. It is very common for servers to be configured to offer as many cipher suites as possible to provide broad compatibility.

However, if a server offers cipher suite options that have significant known vulnerabilities (many do), it presents the opportunity for a man-in-the-middle to negotiate on the client’s behalf for a weak cipher suite that the attacker can break.

SSL Certificate



This certificate has been verified for the following uses:

SSL Server Certificate

Issued To

Common Name (CN)	login.yahoo.com
Organization (O)	Yahoo! Inc.
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	0F:58:49:41:52:C3:35:4B:6D:EB:E7:20:9E:72:6E:67

Issued By

Common Name (CN)	DigiCert High Assurance CA-3
Organization (O)	DigiCert Inc
Organizational Unit (OU)	www.digicert.com

Validity

Issued On	20-Dec-10
Expires On	3-Jan-13

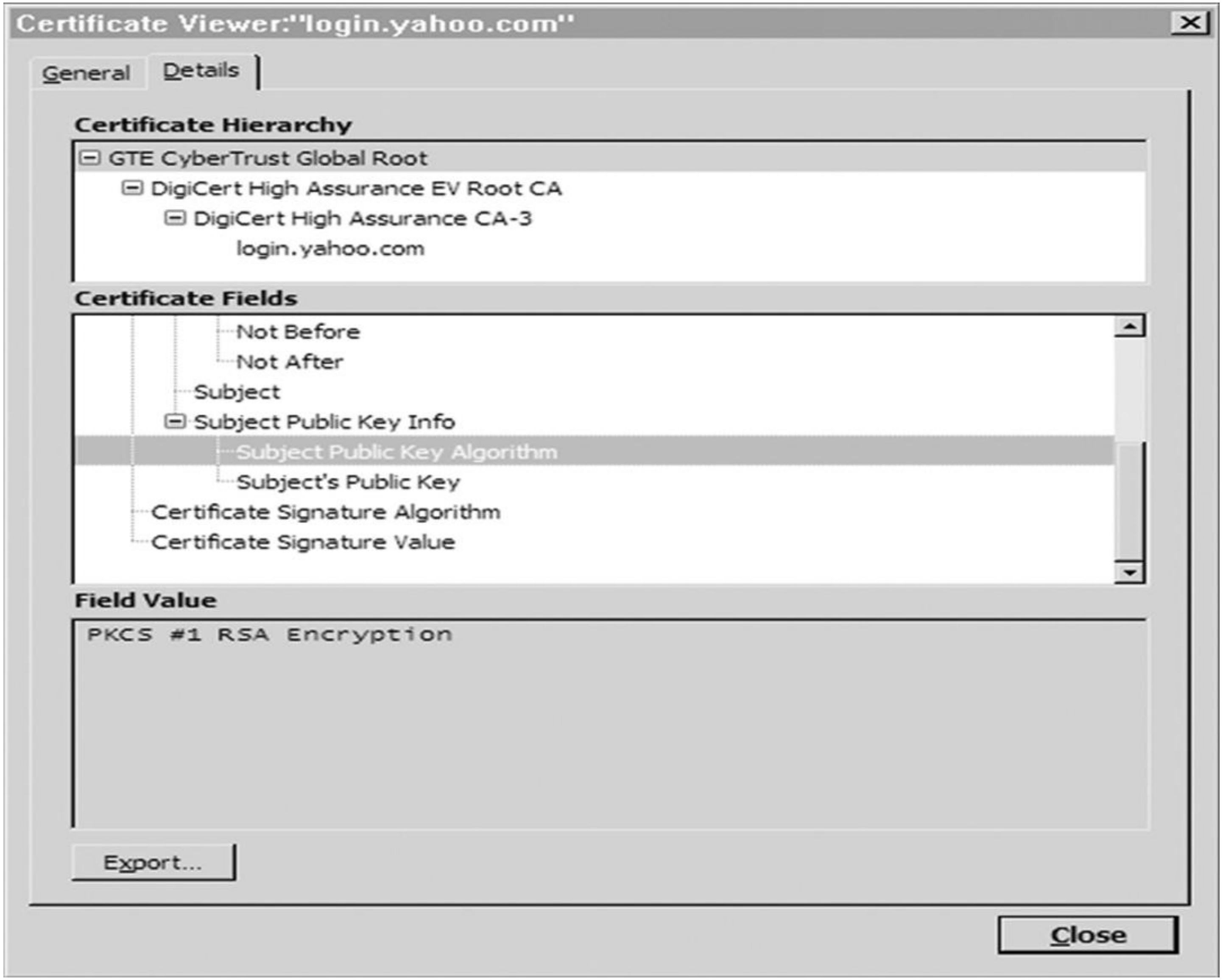
Fingerprints

SHA1 Fingerprint	89:0C:0C:65:87:30:4C:43:75:20:B4:81:AA:7B:CC:F2:EE:15:19:54
MD5 Fingerprint	75:4A:A4:87:70:53:70:5D:4D:1D:15:54:18:3C:FE:EC

SSL Certificate

- SSL/TLS certificates allow web browsers to identify and establish encrypted network connections to web sites using the SSL/TLS protocol.
- The certificate serves two primary functions: The certificate authenticates the identity of the server; and. The certificate binds a key pair to that server.
- In this dialog, we see the certificate details: the domain name being certified, the company that owns the site, the CA that issued the certificate, and the relevant dates.

Chain of Certificates



Certificate Hierarchy

- GTE CyberTrust Global Root
  - DigiCert High Assurance EV Root CA
    - DigiCert High Assurance CA-3
      - login.yahoo.com

Certificate Fields

- Not Before
- Not After
- Subject
- Subject Public Key Info
  - Subject Public Key Algorithm
  - Subject's Public Key
- Certificate Signature Algorithm
- Certificate Signature Value

Field Value

```
PKCS #1 RSA Encryption
```

Chain of Certificates

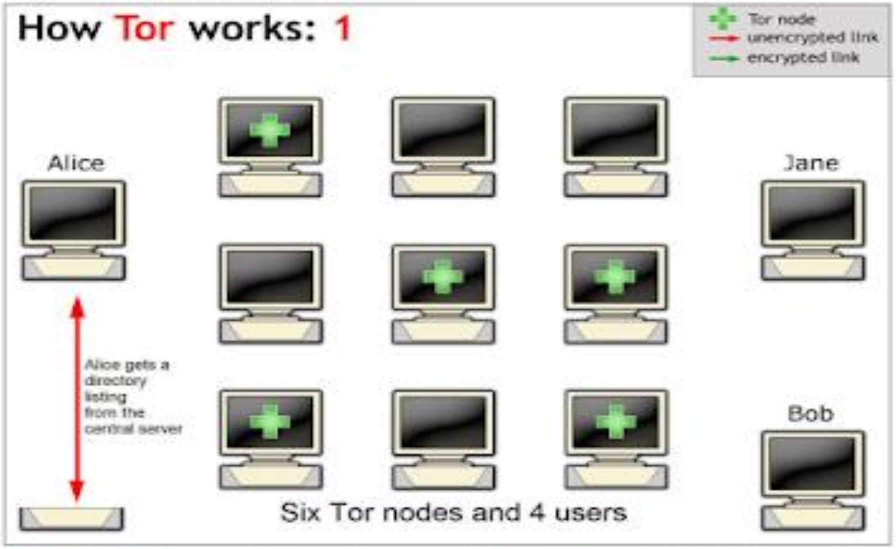
The chain of certificates, starting with GTE CyberTrust Global Root. This dialog also shows the algorithm used for signing the certificate.

If GTE CyberTrust is trusted by my browser, and it, or one of the CAs it authorizes, signs a certificate, then that certificate is valid as far as my browser is concerned.

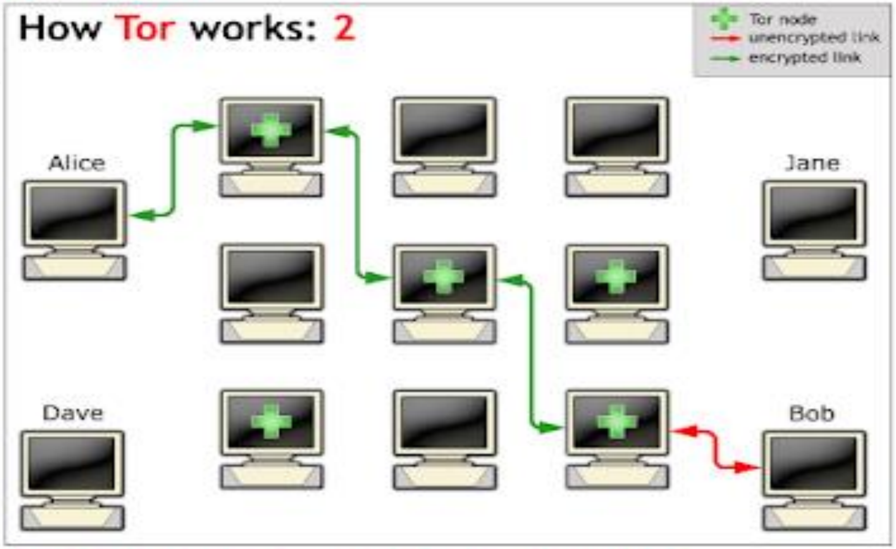
Onion Routing

- Onion routing prevents an eavesdropper from learning source, destination, or content of data in transit in a network
- This is particularly helpful for evading authorities, such as when users in oppressive countries want to communicate freely with the outside world
- Uses asymmetric cryptography, as well as layers of intermediate hosts, so that
  - The intermediate host that sends the message to the ultimate destination cannot determine the original sender, and
  - The host that received the message from the original sender cannot determine the ultimate destination

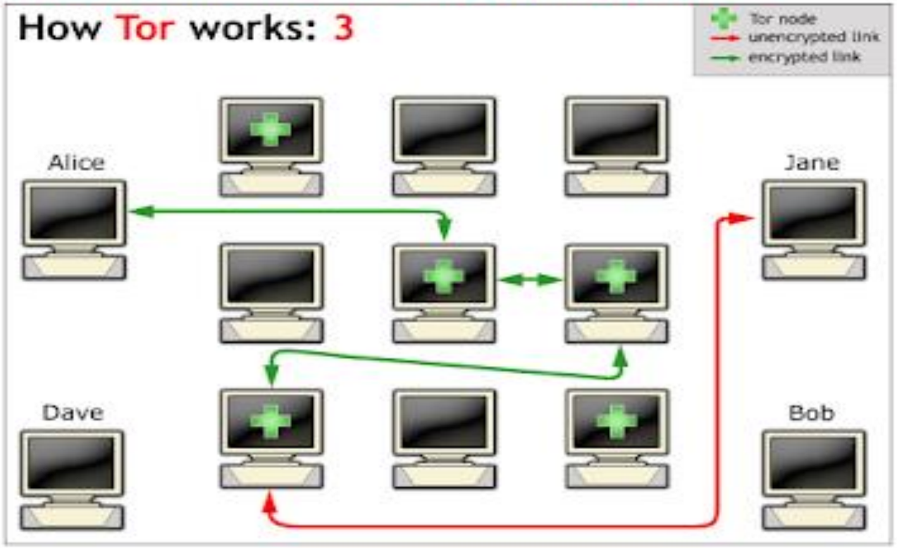
Connection set up


How Tor works: 1
Tor node
unencrypted link
encrypted link
Alice
Jane
Bob
Alice gets a directory listing from the central server
Six Tor nodes and 4 users

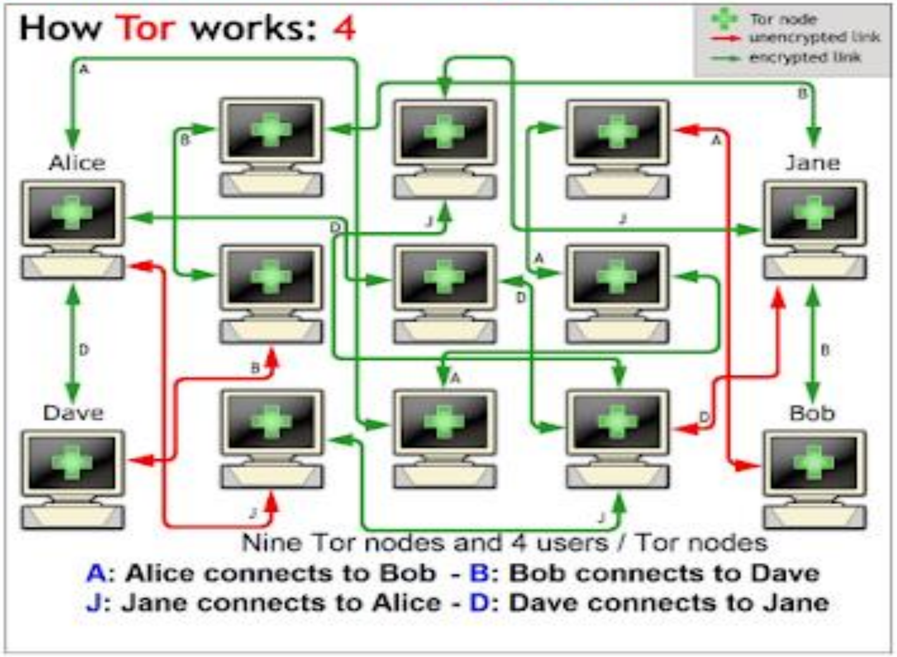
Connection



Connection Timeout - entry node change



A real scenario - multi purpose node



Nine Tor nodes and 4 users / Tor nodes

A: Alice connects to Bob - B: Bob connects to Dave

J: Jane connects to Alice - D: Dave connects to Jane

Onion Routing

- The model uses a collection of forwarding hosts, each of whom knows only from where a communication was received and to where to send it next.
- To send untraceable data from A to B, A picks some number of forwarding hosts, call them X, Y, and Z. A begins by encrypting the communication under B's public key.
- A then appends a header from Z to B, and encrypts the result under Z's public key. A then puts a header on that from Y to Z and encrypts that under Y's public key. A then puts a header on that communication from X to Y and encrypts that under X's public key.
- Finally, A puts on a header to send the package to X.

Onion Routing

- Upon receiving the package, X decrypts it and finds instructions to forward the inner package to Y. Y then decrypts it and finds instructions to forward the inner package to Z. Z then decrypts it and finds instructions to forward the inner package to B. The package is deconstructed like peeling the layers from an onion, which is why this technique is called onion routing.
- No intermediate host can know who the ultimate recipient is. Even Z cannot tell that B is the final destination, because what Z delivers to B is encrypted under B’s public key. Thus, X, Y, and Z know only that they are intermediaries, but they do not know which other intermediaries there are, how many of them there are, or where they are in the chain.
- Any intermediate recipients—those other than the original sender and ultimate recipient— know neither where the package originated nor where it will end.

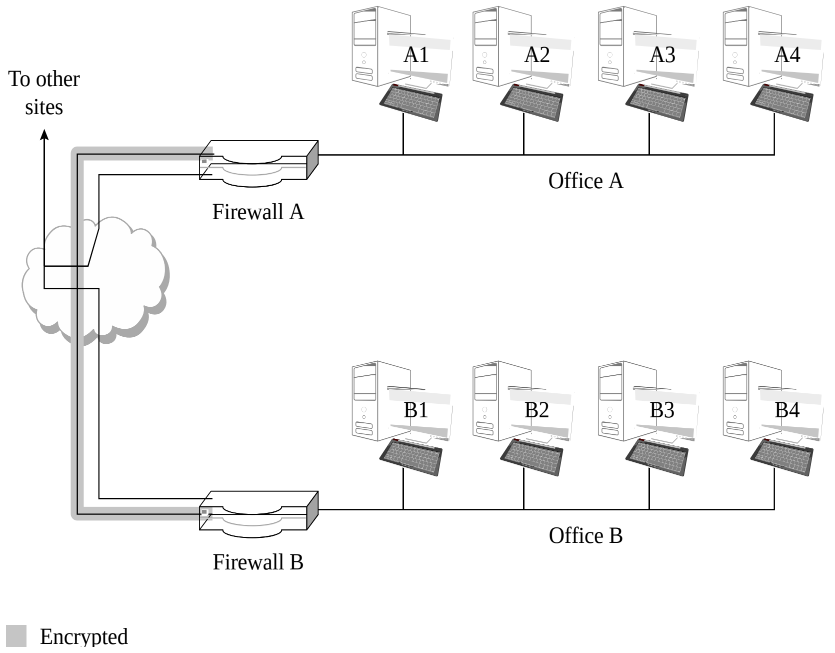
IP Security Protocol Suite (IPsec)

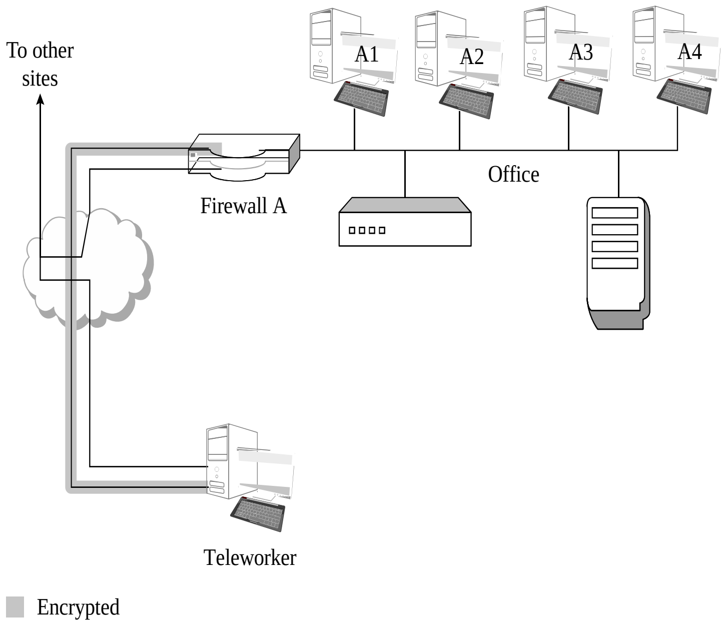
- IPsec, was adopted by the IETF. Designed to address fundamental shortcomings such as being subject to spoofing, eavesdropping, and session hijacking, the IPsec protocol defines a standard means for handling encrypted data.
- IPsec is implemented at the IP layer (3), so it protects data produced in all layers above it, in particular, TCP and UDP control information, as well as the application data. Therefore, IPsec requires no change to the existing large number of TCP and UDP protocols or applications.
- IPsec is somewhat similar to SSL, in that it supports authentication and confidentiality in a way that does not necessitate significant change either above it (in applications) or below it (in the TCP protocols).
- Like SSL, it was designed to be independent of specific cryptographic algorithms and to allow the two communicating parties to agree on amutually supported set of protocols.

IP Security Protocol Suite (IPsec)

- The fundamental data structures of IPsec are the authentication header (AH) and the encapsulated security payload (ESP).
- The ESP includes the conventional TCP header and data portion of a packet,
- Key Management
- Modes of Operation
- In transport mode (normal operation), the IP address header is unencrypted.
- In tunnel mode, the recipient's address is concealed by encryption, and IPsec substitutes the address of a remote device, such as a firewall, that will receive the transmission and remove the Ipsec encryption.

Virtual Private Networks (VPN)





A VPN—an encrypted tunnel that provides confidentiality and integrity for communication between two sites over public networks—connects Office A to Office B over the Internet so they appear to their users as one seamless, private network.

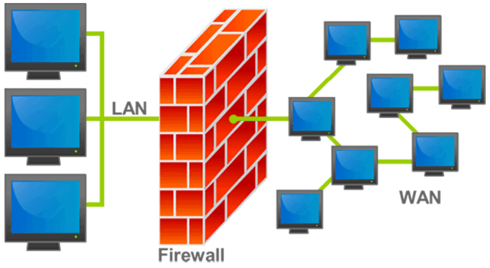
The VPN is terminated by firewalls at both ends, which is often the case in the real world.

In this VPN scenario, a teleworker uses a VPN to connect to a remote office.

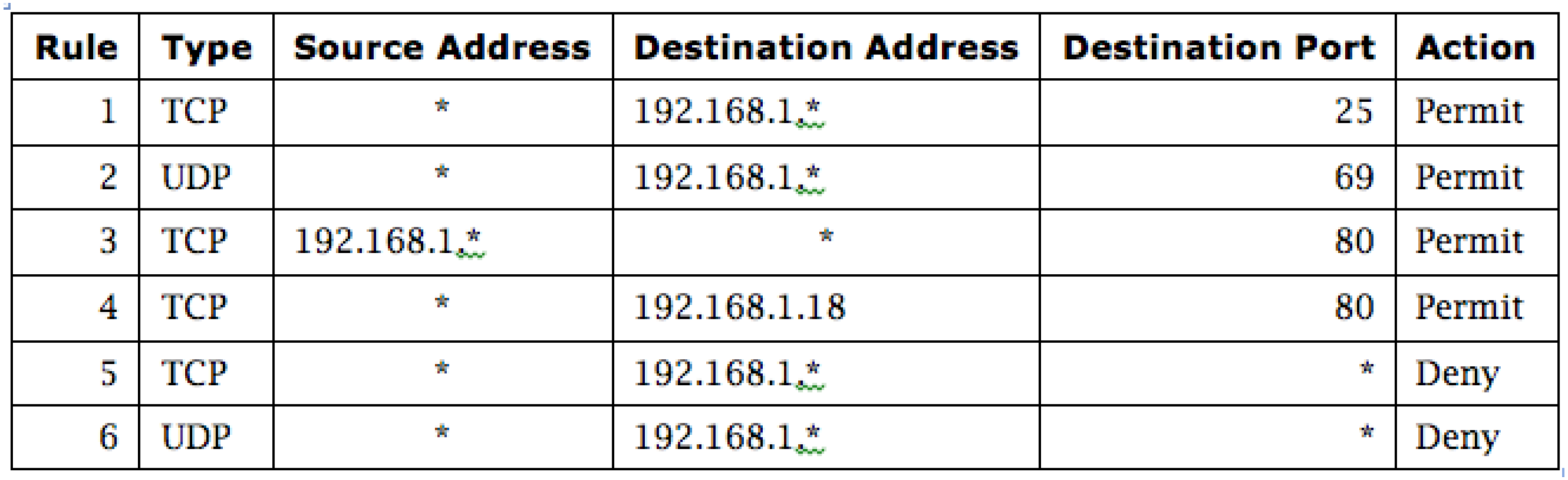
She authenticates to the firewall (that's acting as a VPN server), and the firewall passes that authentication information to the servers in the office so she can be appropriately access controlled.

Firewalls

- A device that filters all traffic between a protected or “inside” network and less trustworthy or “outside” network
- Most firewalls run as dedicated devices
  - Easier to design correctly and inspect for bugs
  - Easier to optimize for performance
- Firewalls implement security policies, or set of rules that determine what traffic can or cannot pass through
- A firewall is an example of a reference monitor, which means it should have three characteristics:
  - Always invoked (cannot be circumvented)
  - Tamperproof
  - Small and simple enough for rigorous analysis



Firewall Security Policy



Rule	Type	Source Address	Destination Address	Destination Port	Action
1	TCP	*	192.168.1.*	25	Permit
2	UDP	*	192.168.1.*	69	Permit
3	TCP	192.168.1.*	*	80	Permit
4	TCP	*	192.168.1.18	80	Permit
5	TCP	*	192.168.1.*	*	Deny
6	UDP	*	192.168.1.*	*	Deny

In this example firewall configuration…

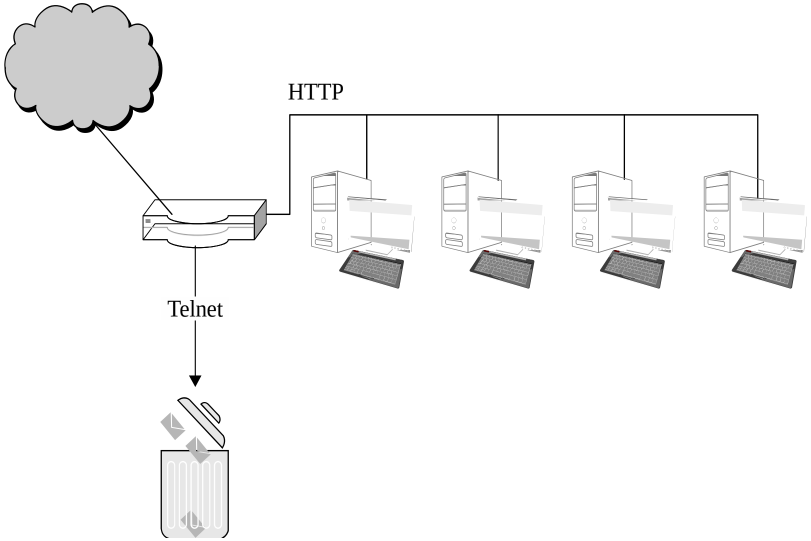
- External traffic can reach the entire internal network on TCP/25 and UDP/69.
- Internal traffic can go out to port 80 on the external network.
- External traffic can reach TCP/80 on one internal server.
- All other traffic from external to internal is disallowed.

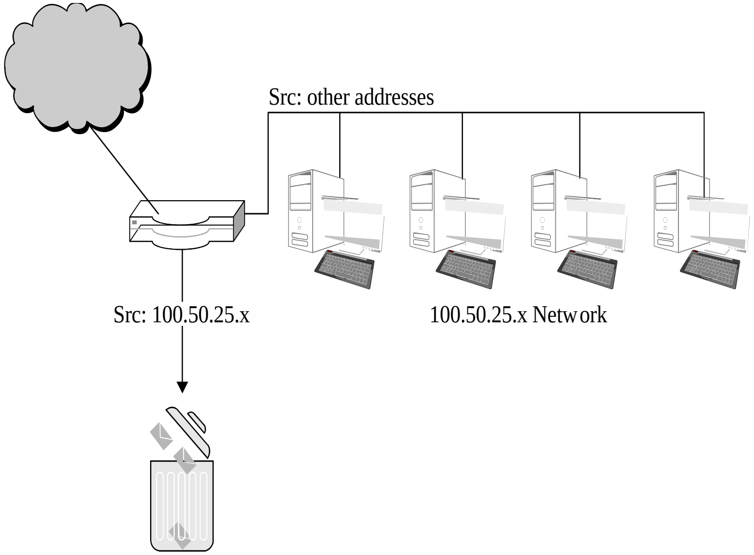
Types of Firewalls

- Packet filtering gateways or screening routers
- Stateful inspection firewalls
- Application-level gateways, also known as proxies
- Circuit-level gateways
- Guards
- Personal or host-based firewalls

Packet-Filtering Gateways

A packet-filtering gateway controls access on the basis of packet address and specific transport protocol type (e.g., HTTP traffic).





The firewall is filtering out Telnet traffic but allowing HTTP traffic in.

The firewall is filtering traffic on the basis of source IP rather than port. Filtering rules can also be based on combinations of addresses and ports/protocols.

Limitations of Packet-Filtering Gateways

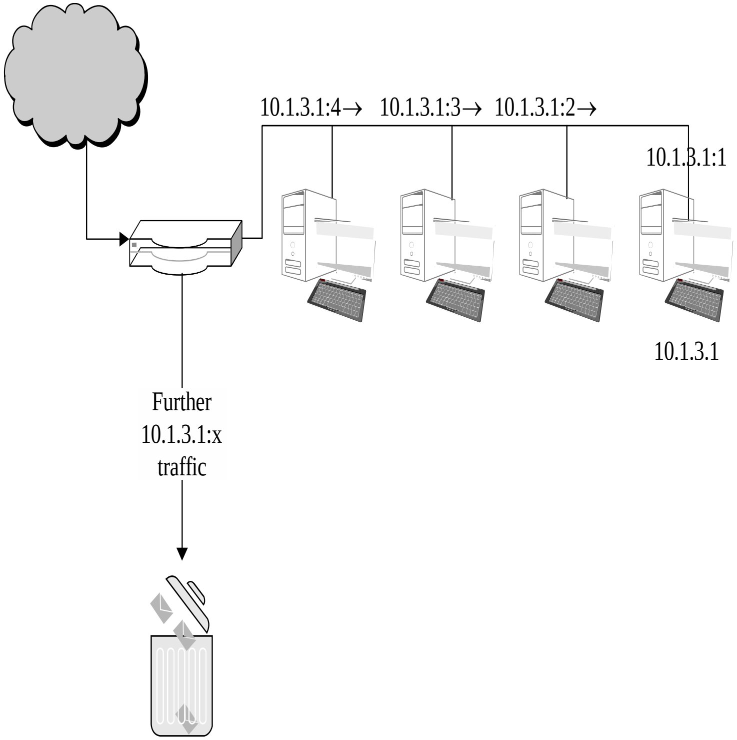
- A packet-filtering firewall may not prevent application layer attacks and is blind to application data
- Does not have state tracking capability.
- To perform sophisticated filtering, the rules set needs to be very detailed. A detailed rules set will be complex and therefore prone to error.
- For example, blocking all port 23 traffic (Telnet) is simple and straightforward. But if some Telnet traffic is to be allowed, each IP address from which it is allowed must be specified in the rules; in this way, the rule set can become very long

Stateful Inspection Firewall

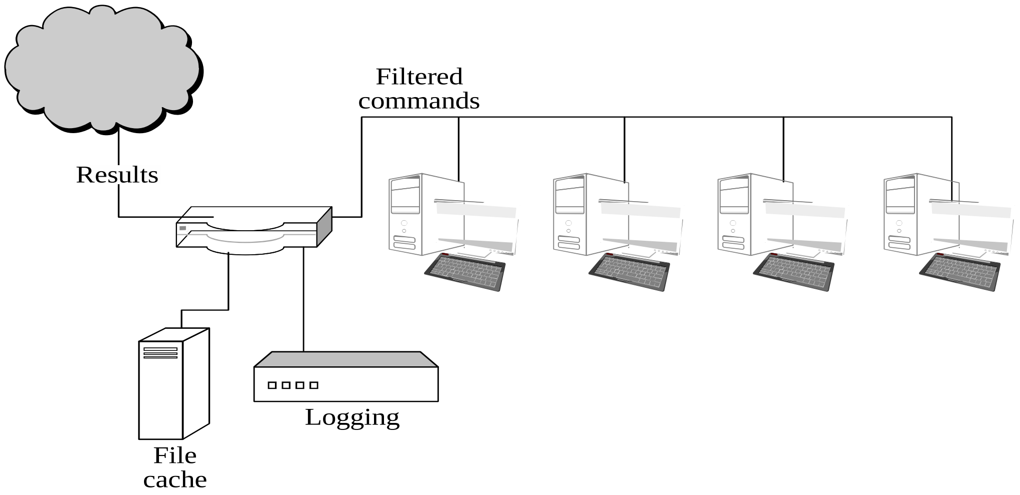
Packet-filtering gateways maintain no state from one packet to the next. They simply look at each packet's IP addresses and ports and compare them to the configured policies. Stateful inspection firewalls, on the other hand, maintain state information from one packet to the next.

In the example in the image, the firewall is counting the number of systems coming from external IP 10.1.3.1; after the external system reaches out to a fourth computer, the firewall hits a configured threshold and begins filtering packets from that address.

In real life, it can be difficult to define rules that require state/context and that attackers cannot circumvent.



Application Proxy

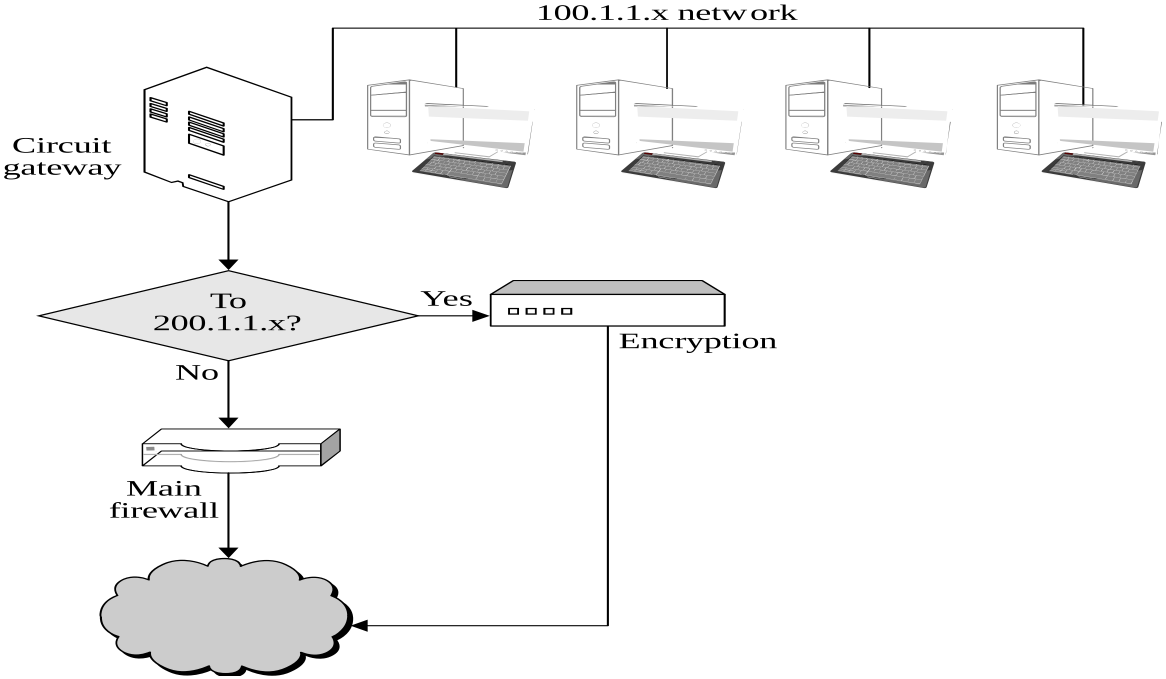


An application proxy simulates the behavior of an application at OSI layer 7 so that the real application receives only requests to act properly. Application proxies can serve several purposes:

- Filtering potentially dangerous application-layer requests
- Log requests/accesses
- Cache results to save bandwidth

Perhaps the most common form of application proxies in the real world is a web proxy, which companies often use to monitor and filter employee Internet use.

Circuit-Level Gateway

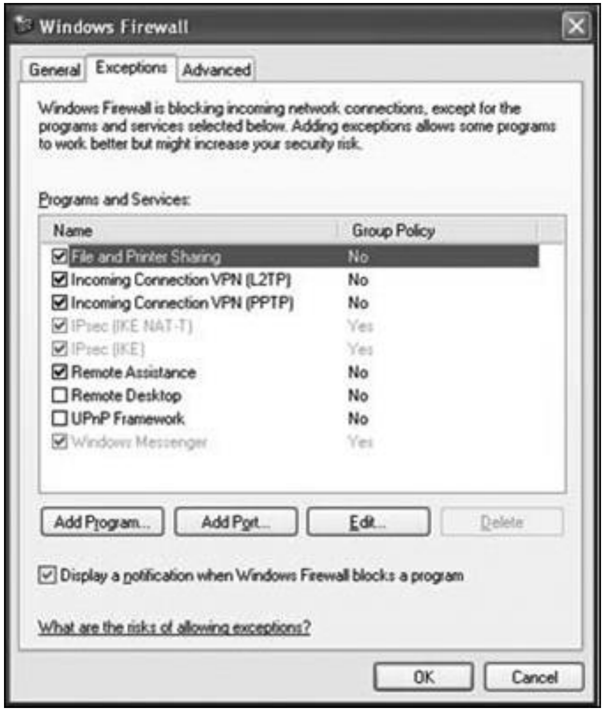


A circuit-level gateway is a firewall that essentially allows one network to be an extension of another. It operates at OSI layer 5, the session layer, and it functions as a virtual gateway between two networks. One use of a circuit-level gateway is to implement a VPN.

Guard

- A **guard** is a sophisticated firewall.
- Like a proxy firewall, it receives protocol data units, interprets them, and emits the same or different protocol data units that achieve either the same result or a modified result.
- The guard determines what services to perform on the user’s behalf in accordance with its available information, such as whatever it can reliably ascertain of the (outside) user’s identity, previous interactions, and so forth.
- A school wants its students to be able to access the World Wide Web but, because of the capacity of its connection to the web, it will allow only so many bytes per second (that is, allowing text mode and simple graphics but disallowing complex graphics, video, music, or the like).

Personal Firewalls



Windows Firewall is blocking incoming network connections, except for the programs and services selected below. Adding exceptions allows some programs to work better but might increase your security risk.

Programs and Services:

Name	Group Policy
☑ File and Printer Sharing	No
☑ Incoming Connection VPN (L2TP)	No
☑ Incoming Connection VPN (PPTP)	No
☑ IPsec (IKE NAT-T)	Yes
☑ IPsec (IKE)	Yes
☑ Remote Assistance	No
□ Remote Desktop	No
□ UPnP Framework	No
☑ Windows Messenger	Yes

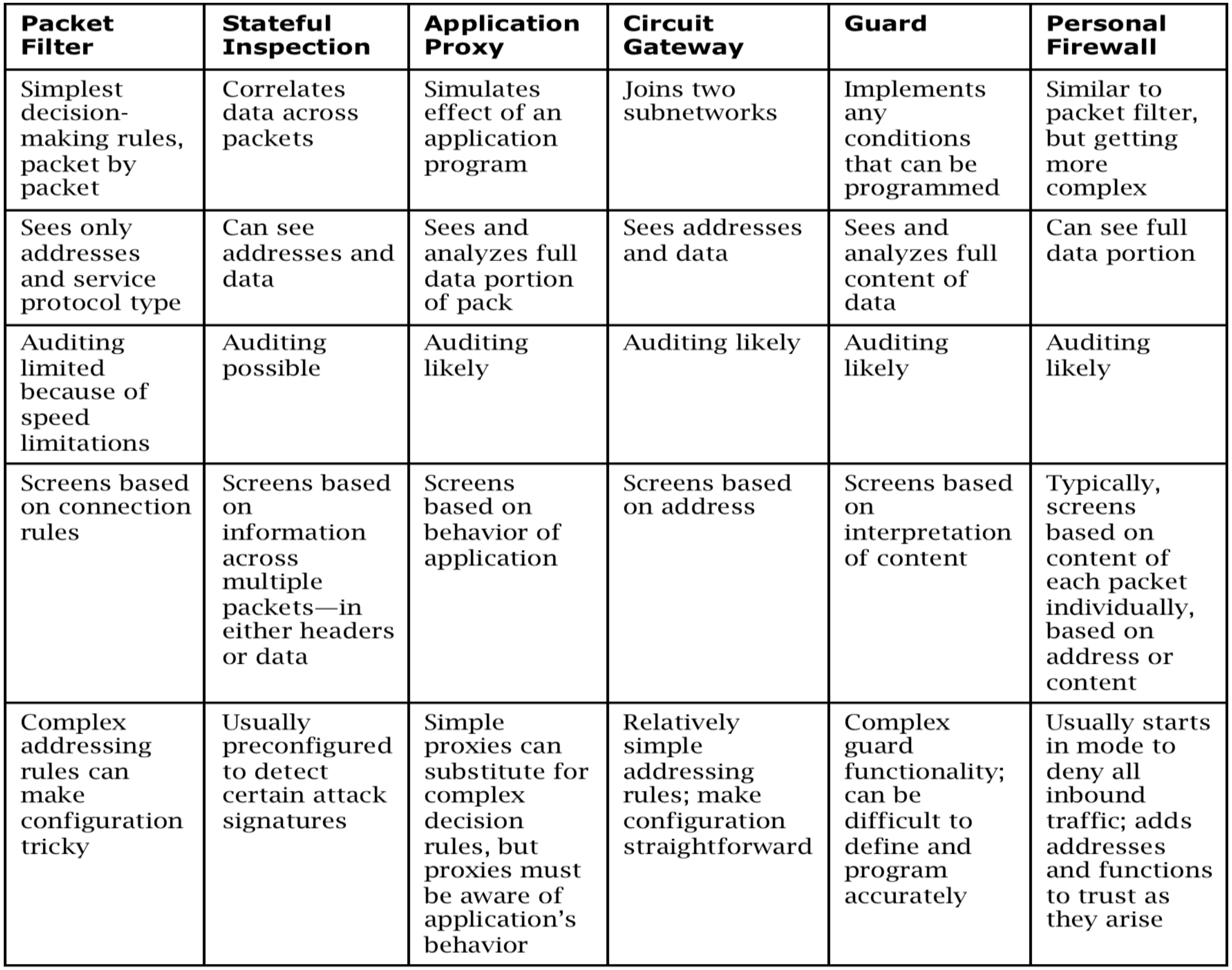
☑ Display a notification when Windows Firewall blocks a program

What are the risks of allowing exceptions?

A personal firewall runs on a workstation or server and can enforce security policy like other firewalls. In addition to restricting traffic by source IP and destination port, personal firewalls can restrict which applications are allowed to use the network.

In this example Windows firewall configuration dialog, an administrator can select which protocols and applications should be allowed to communicate to and from the host.

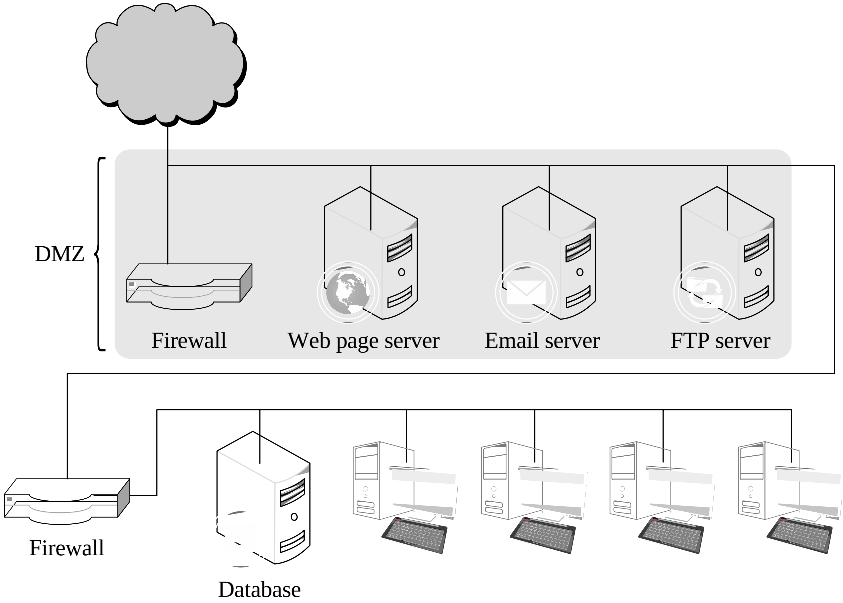
Comparison of Firewall Types



Packet Filter	Stateful Inspection	Application Proxy	Circuit Gateway	Guard	Personal Firewall
Simplest decision-making rules, packet by packet	Correlates data across packets	Simulates effect of an application program	Joins two subnetworks	Implements any conditions that can be programmed	Similar to packet filter, but getting more complex
Sees only addresses and service protocol type	Can see addresses and data	Sees and analyzes full data portion of pack	Sees addresses and data	Sees and analyzes full content of data	Can see full data portion
Auditing limited because of speed limitations	Auditing possible	Auditing likely	Auditing likely	Auditing likely	Auditing likely
Screens based on connection rules	Screens based on information across multiple packets—in either headers or data	Screens based on behavior of application	Screens based on address	Screens based on interpretation of content	Typically, screens based on content of each packet individually, based on address or content
Complex addressing rules can make configuration tricky	Usually preconfigured to detect certain attack signatures	Simple proxies can substitute for complex decision rules, but proxies must be aware of application's behavior	Relatively simple addressing rules; make configuration straightforward	Complex guard functionality; can be difficult to define and program accurately	Usually starts in mode to deny all inbound traffic; adds addresses and functions to trust as they arise

Demilitarized Zone (DMZ)

A DMZ is a form of network architecture in which a network enclave is dedicated to services that should be somewhat accessible from the outside.



In this example, a firewall protects a DMZ that contains web, email, and FTP servers, and a second firewall protects an internal network—that should not be reachable from the Internet—from the DMZ in case a DMZ host becomes compromised.

The benefit of such a configuration is that the hosts that need to be accessible from the Internet—and are therefore most at risk from outside attack—can only do limited damage to the internal hosts that do not need to be reachable from the Internet.

An even more careful option would separate web, email & FTP servers with further firewalls.

What Firewalls Can and Cannot Do

- Firewalls can protect an environment only if they control the entire perimeter
- Firewalls do not protect data outside the perimeter
- Firewalls are the most visible part of an installation to the outside, so they are an attractive target for attack
- Firewalls must be correctly configured, that configuration must be updated as the environment changes, and firewall activity reports must be reviewed periodically for evidence of attempted or successful intrusion
- Firewalls exercise only minor control over the content admitted to the inside, meaning that inaccurate or malicious code must be controlled by means inside the perimeter

Network Address Translation (NAT)

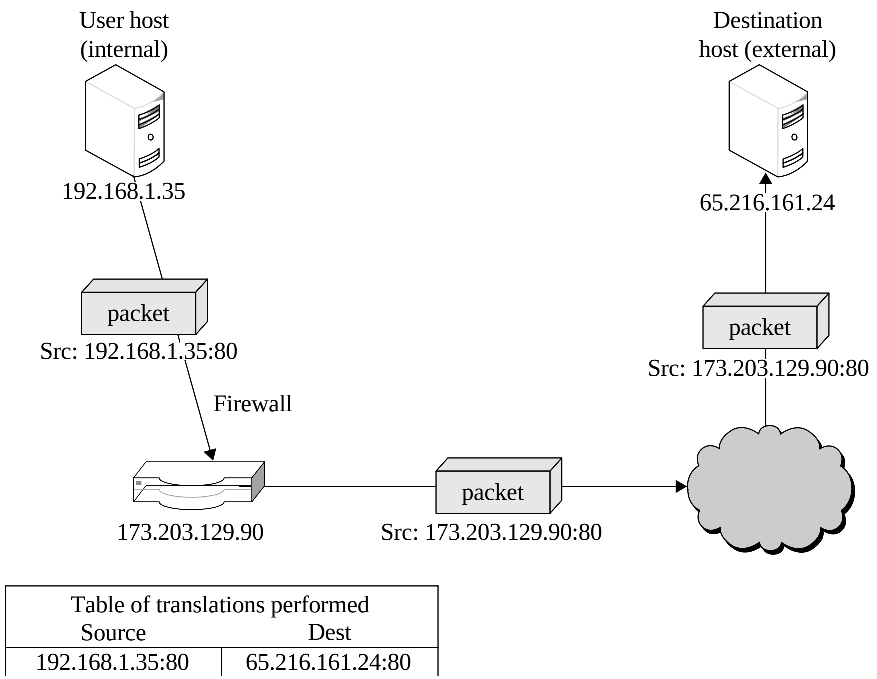


Table of translations performed

Source	Dest
192.168.1.35:80	65.216.161.24:80

With NAT, the source firewall converts the source address in the packet into the firewall's own address. The firewall also makes an entry in a translation table showing the destination address, the source port & the original source address to be able to forward any replies to the original source address. The firewall then converts the address back on any return packets.

This has the effect of concealing the true address of the internal host and prevents the internal host from being reached directly.

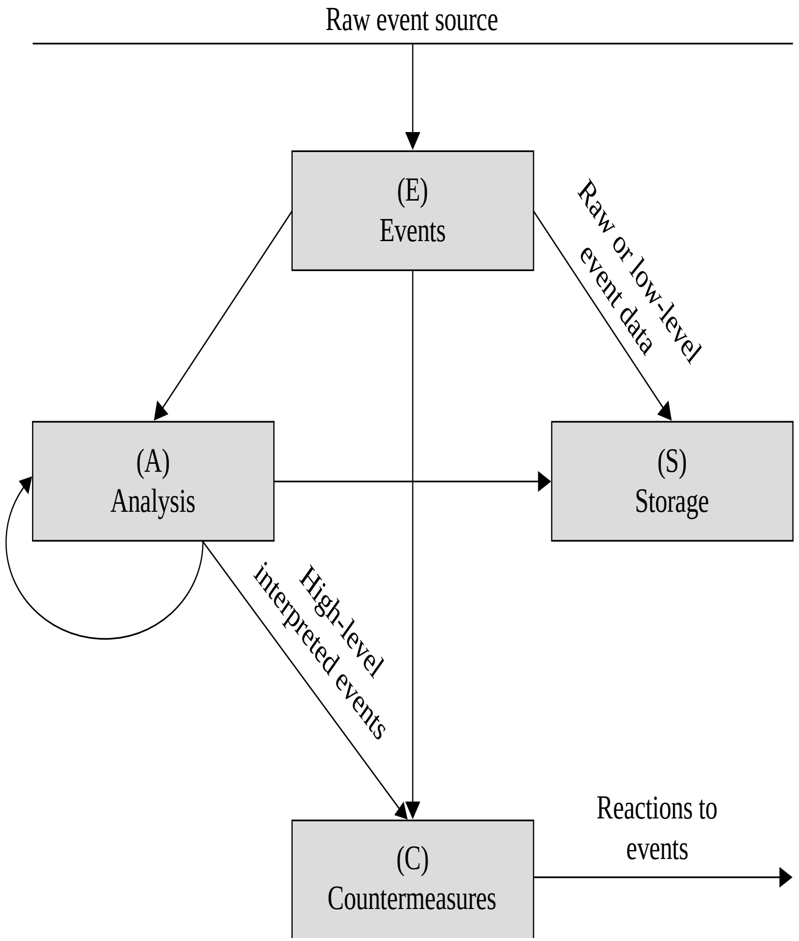
Data Loss Prevention (DLP)

- DLP is a set of technologies that can detect and possibly prevent attempts to send sensitive data where it is not allowed to go
- Can be implemented as
  - Agent installed as an OS rootkit
  - Guard
- Indicators DLP looks for:
  - Keywords
  - Traffic patterns
  - Encoding/encryption
- DLP is best for preventing accidental incidents, as malicious users will often find ways to circumvent it

Intrusion Detection Systems (IDS)

IDSs complement preventative controls as a next line of defense. IDSs monitor activity to identify malicious or suspicious events. IDSs may:

- Monitor user and system activity
- Audit system configurations for vulnerabilities and misconfigurations
- Assess integrity of critical system and data files
- Recognize known attack patterns in system activity
- Identify abnormal activity through statistical analysis
- Manage audit trails and highlight policy violations
- Install and operate traps to record information about intruders



Types of IDS

- Detection method
  - Signature-based, Heuristic
- Location
  - Front end, Internal
- Scope
  - Host-based IDS (HIDS), Network-based IDS (NIDS)
- Capability
  - Passive, Active, also known as intrusion prevention systems (IPS)

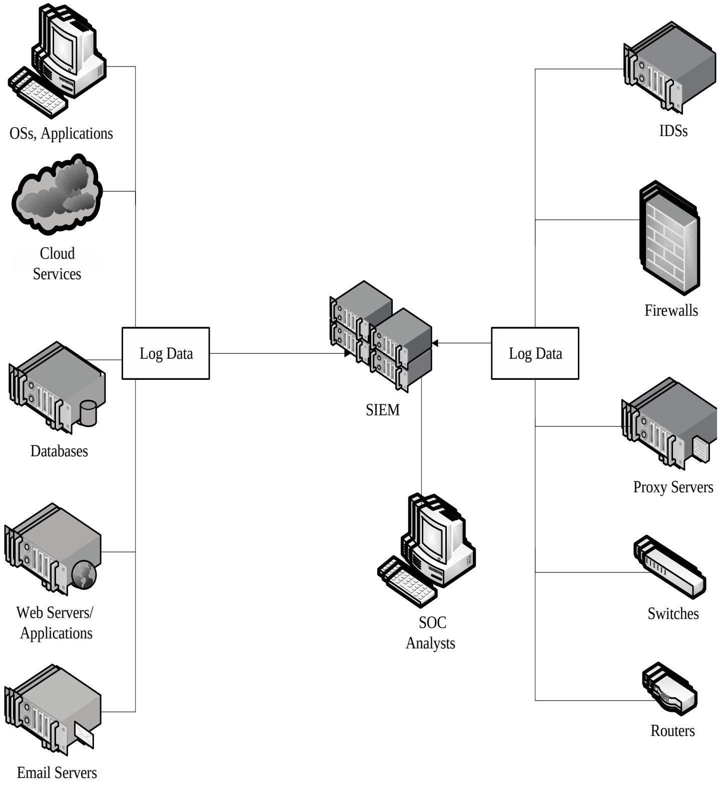
- A signature-based IDS can only detect known patterns.
- A heuristic IDS looks for patterns of behavior that are out of the ordinary.
- A front-end IDS looks at traffic as it enters the network, while an internal IDS monitors traffic within the network.
- A host-based IDS protects a single host by monitoring traffic from the OS.
- A network-based IDS is a server or appliance that monitors network traffic.
- An IPS is an IDS that tries to block or otherwise prevent suspicious or malicious behavior once it is detected.

Security Information and Event Management (SIEM)

SIEMs are software systems that collect security-relevant data—usually audit logs—from a variety of hardware and software products to create a unified security dashboard for security operations center personnel.

Without an SIEM, analysts would need to log into each device individually on a constant basis and would have to manually correlate events on one system against events on another, which is impossible on any reasonably sized system.

SIEMs range in functionality from simple ones that allow for basic search and alerting to complex platforms that allow for completely custom dashboards, reports, alerts, and correlation.



Summary

- Networks are threatened by attacks aimed at interception, modification, fabrication, and interruption
- WPA2 has many critical security advantages over WEP
- DoS attacks come in many flavors, but malicious ones are usually either volumetric in nature or exploit a bug
- Network encryption can be achieved using specialized tools—some for link encryption and some for end-to-end—such as VPNs, SSH, and the SSL/TLS protocols
- A wide variety of firewall types exist, ranging from very basic IP-based functionality to complex application-layer logic, and both on networks and hosts
- There are many flavors of IDS, each of which detects different kinds of attacks in very different parts of the network