Lecture Two

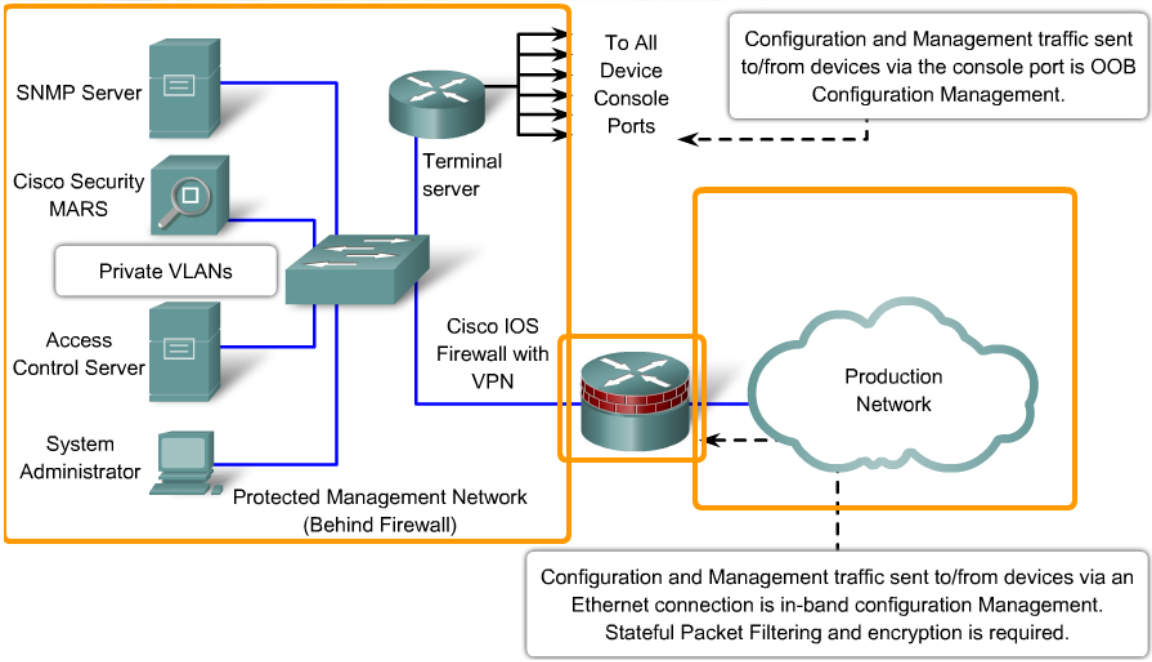
Network Security Devices

Dr. M. Mahfuzul Islam
Professor, Dept. of CSE, BUET

Securing Edge Router

Edge Router: The last router between the intranet network and an untrusted network such as the Internet

- Implements security actions based on the organization's security policies



Methods for securing Edge Router

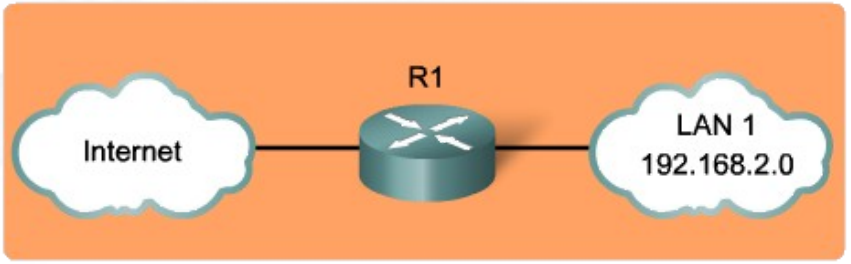
- Various perimeter router implementations
- Physical security, operating system security, and router hardening
- Secure administrative access
- Local versus remote router access

Securing Edge Router

Perimeter Implementations

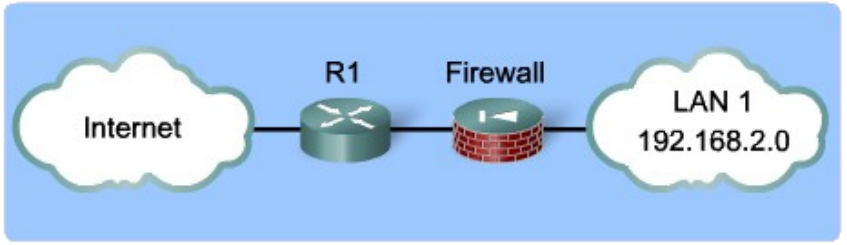
- **Single Router Approach**

  A single router connects the internal LAN to the Internet. All security policies are configured on this device.



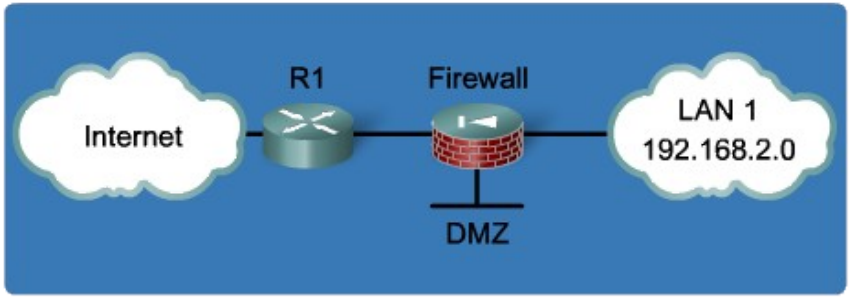
- **Defense-in-depth Approach**

  Passes everything through to the firewall. A set of rules determines what traffic the router will allow or deny.



- **DMZ Approach**

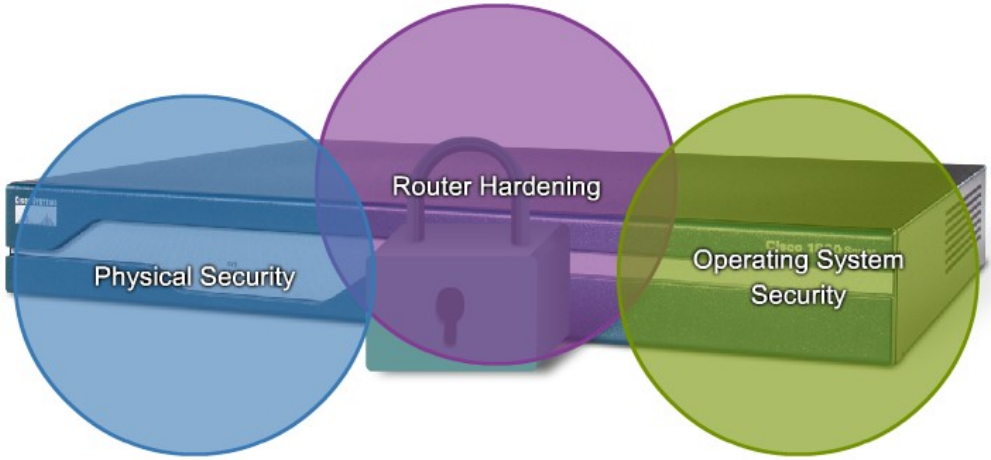
  The DMZ is set up between two routers. Most traffic filtering left to the firewall



Securing Edge Router

Areas of Router Security

- Physical Security
  - Place router in a secured, locked room
  - Install an uninterruptible power supply(UPS)
- Operating System Security
  - Configure the router with the maximum amount of memory possible.
  - Use the latest stable version that meets network requirements
  - Keep a copy of the IOS and configuration file as a backup
- Router Hardening
  - Secure administrative control
  - Disable unused ports and interfaces
  - Disable unnecessary services



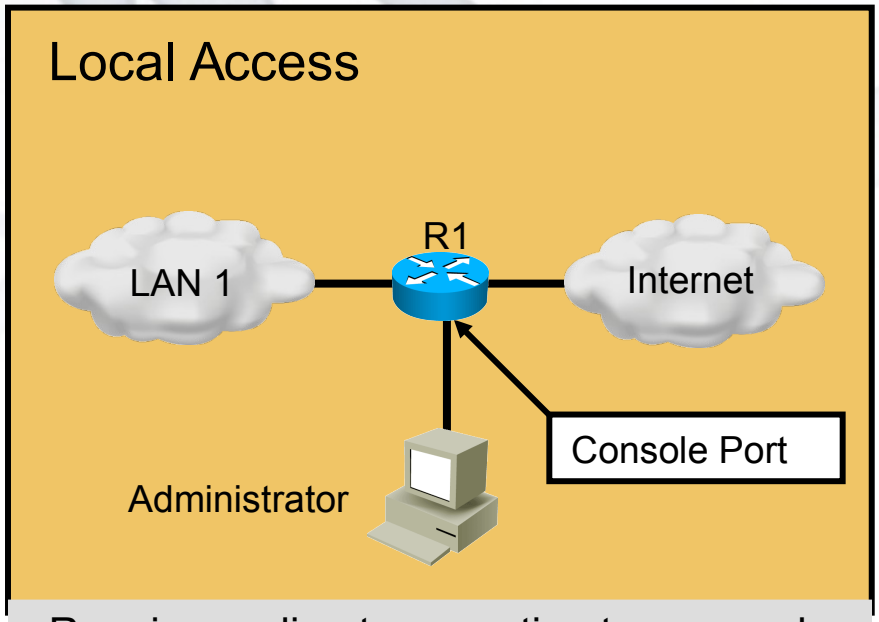
Securing Edge Router

Securing Administrative Access

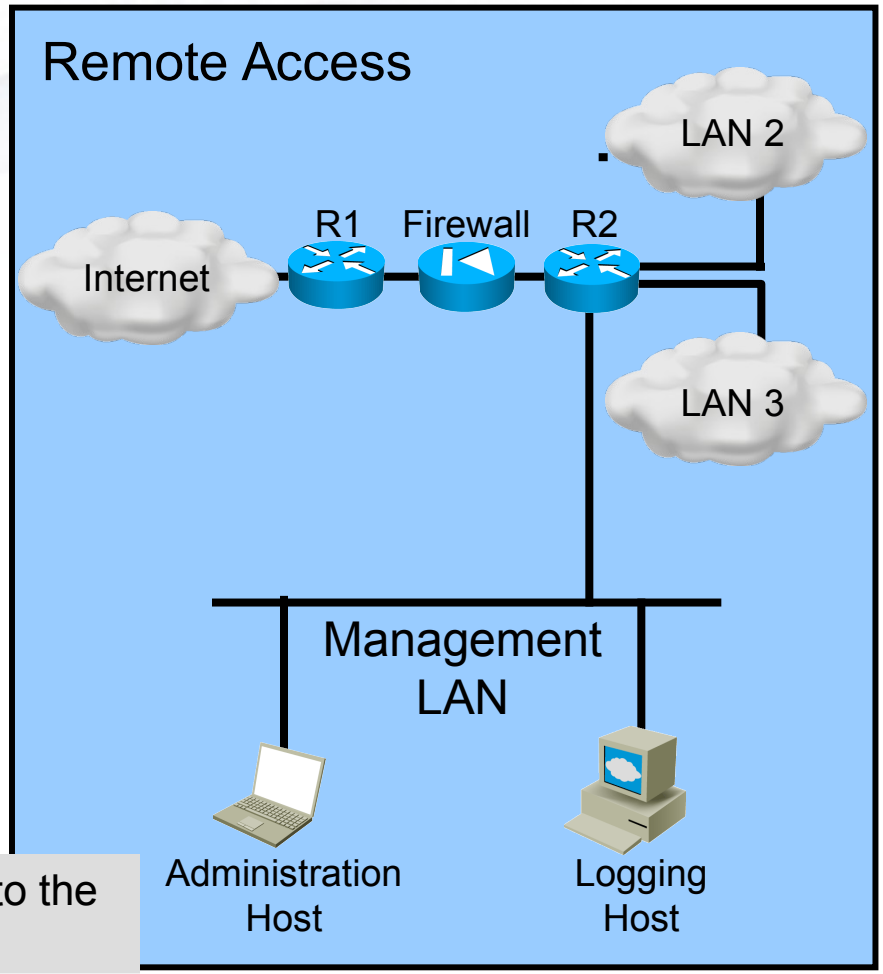
- Restrict Device Accessibility - Limit the accessible ports, restrict the permitted communicators and restrict the permitted methods of access.
- Log and Account for all Access - Record anyone who accesses a device.
- Authenticate Access - Ensure access is only granted to authenticated users, groups, and services.
- Authorize Actions - Restrict the actions and views permitted by any particular user, group, or service.
- Present Legal Notification - Display legal notice for interactive sessions.
- Ensure the Confidentiality of Data - Protect locally stored sensitive data from viewing and copying.

Securing Edge Router

Local Versus Remote Access



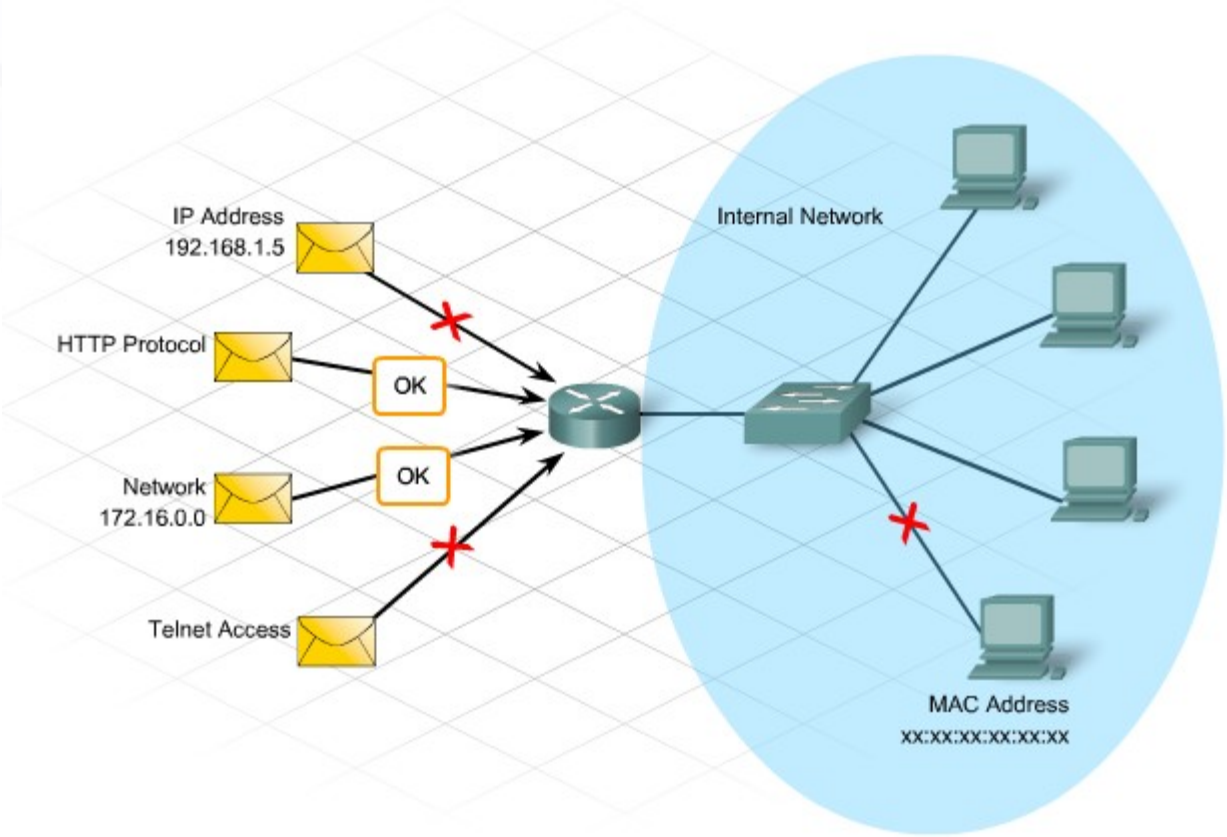
Requires a direct connection to a console port using a computer running terminal emulation software



Uses Telnet, SSH HTTP or SNMP connections to the router from a computer

Access Control List (ACL)

- ACLs filter traffic going through the router, or traffic to and from the router, depending on how it is applied



Protocol	Range
IP	1-99, 1300-1999
Extended IP	100-199, 2000-2699
Ethernet type code	200-299
Ethernet address	700-799
Transparent bridging (protocol type)	200-299
Transparent bridging (vendor code)	700-799
Extended transparent bridging	1100-1199
DECnet and extended DECnet	300-399
XNS	400-499
Extended XNS	500-599
AppleTalk	600-699
Source-route bridging (protocol type)	200-299
Source-route bridging (vendor code)	700-799
IPX	800-899
Extended IPX	900-999
IPX SAP	1000-1099
Standard VINES	1-100
Extended VINES	101-200
Simple VINES	201-300

Access Control List (ACL)

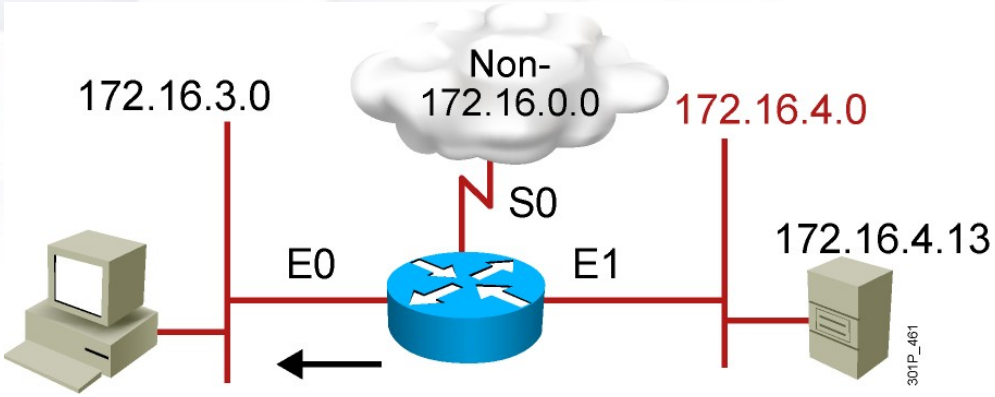
Standard IP ACL Format

```
Router(config)# access-list {1-99} {permit | deny}
source-addr [source-mask]
```

- The first value specifies the ACL number
- The second value specifies whether to permit or deny the configured source IP address traffic
- The third value is the source IP address that must be matched
- The fourth value is the wildcard mask to be applied to the previously configured IP address to indicate the range
- All ACLs assume an implicit deny statement . At least one permit statement should be included or all traffic will be dropped once that ACL is applied to an interface

Access Control List (ACL)

Standard IP ACL Example: Use a standard ACL to block all traffic from 172.16.4.0/24 network, but allow all other traffic




```
r1(config)# access-list 1 deny 172.16.4.0 0.0.0.255
r1(config)# access-list 1 permit any
r1(config)# interface ethernet 0
r1(config-if)# ip access-group 1 out
```

Access Control List (ACL)

Extended IP ACL Format

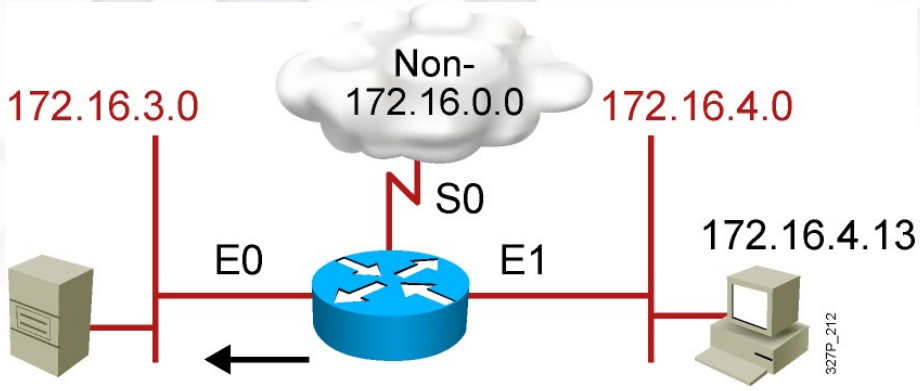
```
R1(config)# access-list 101 permit tcp 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 eq 22
```

There are several pieces of information logged:

- The action—permit or deny
- The protocol—TCP, UDP, or ICMP
- The source and destination addresses
- For TCP and UDP—the source and destination port numbers
- For ICMP—the message types

Access Control List (ACL)

Extended IP ACL Example: Use an extended ACL to block all FTP traffic from 172.16.4.0/24 network, but allow all other traffic




```
access-list 101 deny tcp 172.16.4.0 0.0.0.255
172.16.3.0 0.0.0.255 eq 21
access-list 101 deny tcp 172.16.4.0 0.0.0.255
172.16.3.0 0.0.0.255 eq 20
access-list 101 permit ip any any
```

Some Important Commands:

1. To ensure that only traffic from a subnet is blocked and all other traffic is allowed:

```
access-list 1 permit any
```

2. To place an ACL on the inbound E1 interface:

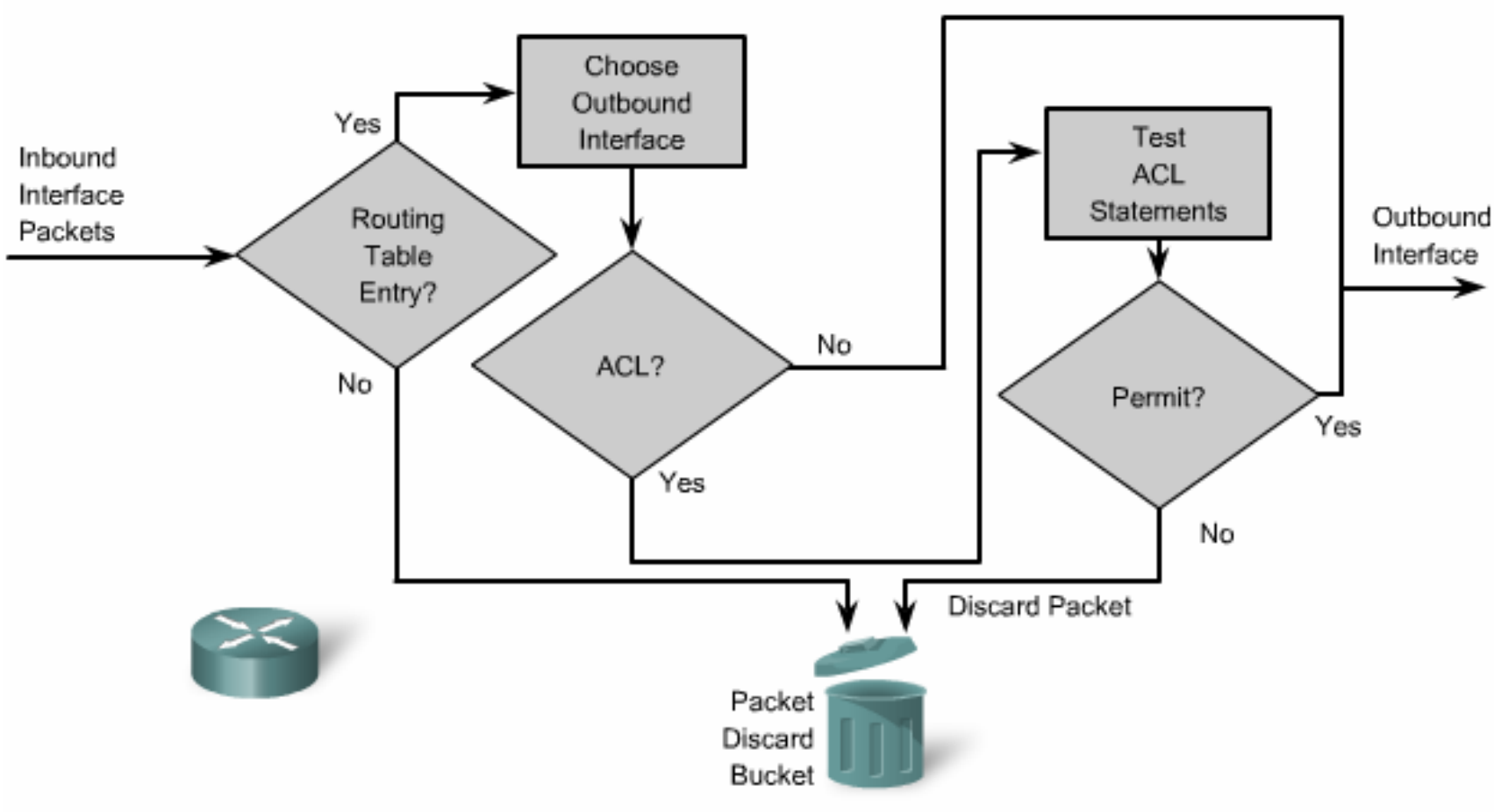
```
interface ethernet 1
ip access-group 101 in
```

3. To check the intended effect of an ACL:

```
show ip access-list
```

Access Control List (ACL)

How does ACL work?



Inbound ACL

Outbound ACL

Access Control List (ACL)

ACL Placement

Standard ACLs: as close to the destination as possible.

- Standard ACLs filter packets based on the source address only. If placed too close to the source, it can deny all traffic, including valid traffic.

Extended ACLs: as close as possible to the source.

- If placed too far from the source being filtered, there is inefficient use of network resources.

- ACLs can be used to mitigate many network threats:
  - IP address spoofing, inbound and outbound
  - DoS TCP SYN attacks
  - DoS smurf attacks
- ACLs can filter the following traffic:
  - ICMP messages, inbound and outbound
  - traceroute

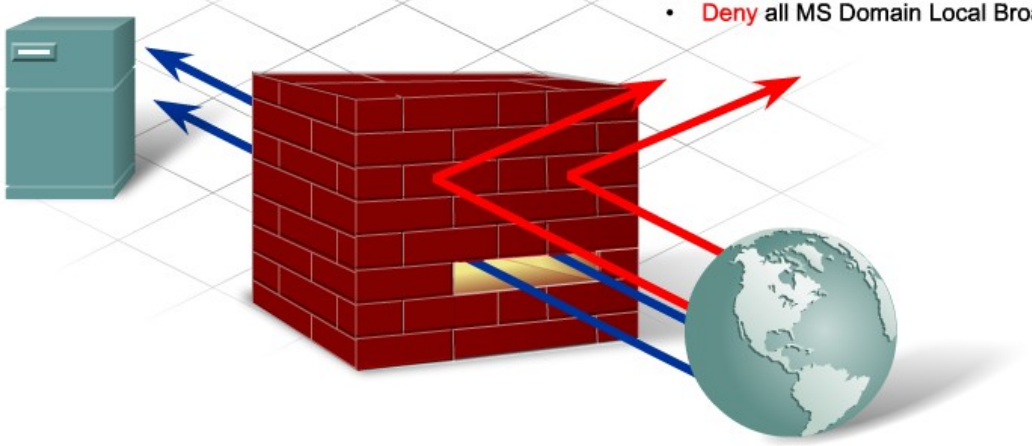
Firewalls

- A firewall is a system that enforces an access control policy between networks

- Common properties of firewalls:
  - ✓The firewall is resistant to attacks
  - ✓The firewall is the only transit point between networks
  - ✓The firewall enforces the access control policy

- Allow web traffic from any external address to the web server
- Allow traffic to FTP server
- Allow traffic to SMTP server
- Allow traffic to internal IMAP server

- Deny all inbound traffic with network addresses matching internal-registered IP addresses
- Deny all inbound traffic to server from external addresses
- Deny all inbound ICMP echo request traffic
- Deny all inbound MS Active Directory
- Deny all inbound MS SQL server ports
- Deny all MS Domain Local Broadcasts



Benefits of Firewalls

- Exposure of sensitive hosts and applications to untrusted users can be prevented.
- The protocol flow can be sanitized, preventing the exploitation of protocol flaws.
- Malicious data can be blocked from servers and clients.
- Security policy enforcement can be made simple, scalable, and robust with a properly configured firewall.
- Offloading most of the network access control to a few points in the network can reduce the complexity of security management.

Limitations of Firewalls

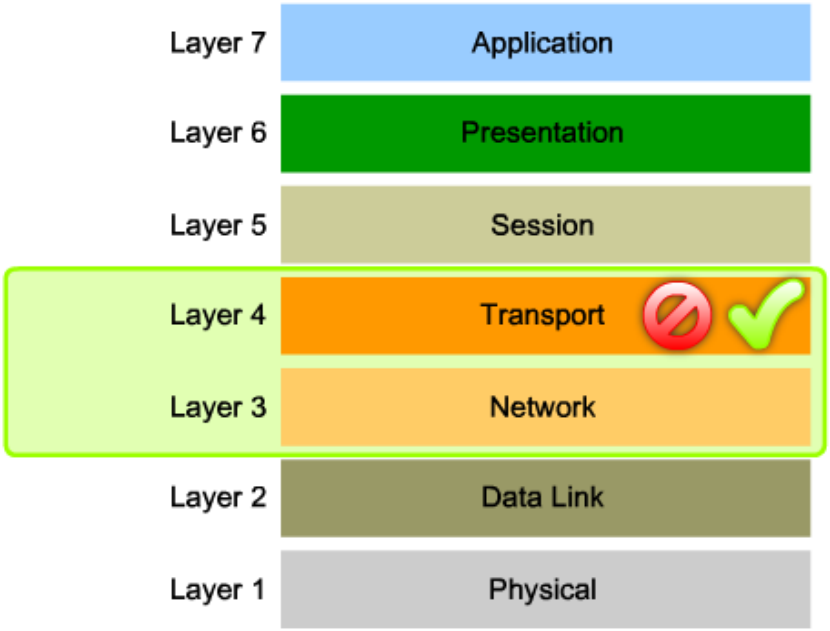
- If misconfigured, a firewall can have serious consequences (single point of failure).
- Many applications cannot be passed over firewalls securely.
- Users might proactively search for ways around the firewall to receive blocked material, exposing the network to potential attack.
- Network performance can slow down.
- Unauthorized traffic can be tunneled or hidden as legitimate traffic through the firewall.

Types of Firewalls

- **Packet-filtering** firewall—is typically a router that has the capability to filter on some of the contents of packets (examines Layer 3 and sometimes Layer 4 information)
- **Stateful** firewall—keeps track of the state of a connection: whether the connection is in an initiation, data transfer, or termination state
- **Application gateway** firewall (proxy firewall) —filters information at Layers 3, 4, 5, and 7. Firewall control and filtering done in software.
- **Address-translation** firewall—expands the number of IP addresses available and hides network addressing design.
- **Host-based** (server and personal) firewall—a PC or server with firewall software running on it.
- **Transparent** firewall—filters IP traffic between a pair of bridged interfaces.
- **Hybrid** firewalls—some combination of the above firewalls. For example, an application inspection firewall combines a stateful firewall with an application gateway firewall. 017 140 26808

Packet-Filtering Firewalls

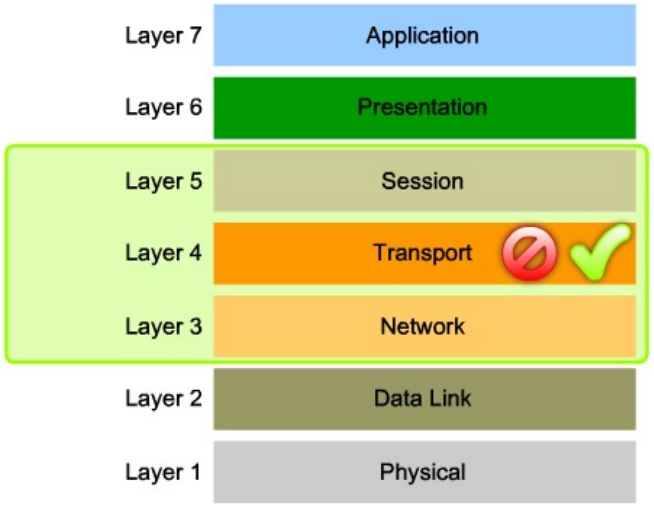
- Packet-filtering firewalls use a simple policy table lookup that permits or denies traffic based on specific criteria:
  - Source IP address
  - Destination IP address
  - Protocol
  - Source port number
  - Destination port number
  - Synchronize/start (SYN) packet receipt

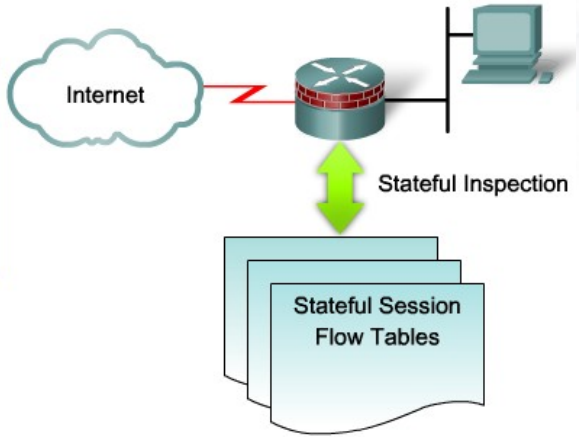


Packet-Filtering Firewalls

Advantages	• Simple permit or deny rule sets can be used to implement a packet filter. • Packet filters have a low impact on network performance. • Packet filters are easy to implement, and are supported by most routers. • An initial degree of security at a low network layer can be provided by a packet filter. • A packet filter can perform almost all tasks of a high end firewall at a much lower cost.
Disadvantages	• Packet filtering is susceptible to IP spoofing. Hackers send arbitrary packets that fit ACL criteria and pass through the filter. • Packet filters do not filter fragmented packets well. Because fragmented IP packets carry the TCP header in the first fragment and packet filters filter on TCP header information, all fragments after the first fragment are passed unconditionally. Decisions to use packet filters assume that the filter of the first fragment accurately enforces the policy. • Complex ACLs are difficult to implement and maintain correctly. • Packet filters cannot dynamically filter certain services. For example, sessions that use dynamic port negotiations are difficult to filter without opening access to a whole range of ports. • Packet filters are stateless. They examine each packet individually rather than in the context of the state of a connection.

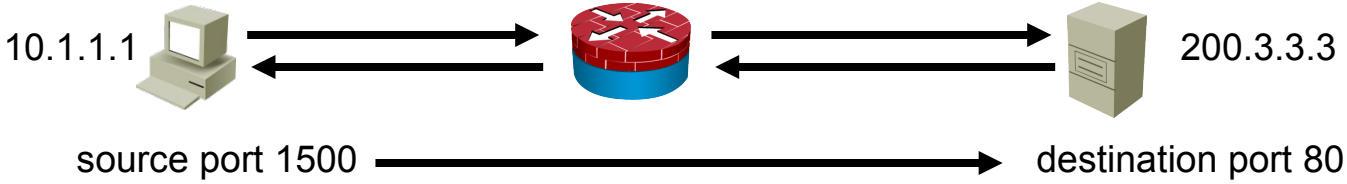
Statefall Firewalls





Provides four main functions:

- Traffic Filtering
- Traffic Inspection
- Intrusion Detection
- Generation of Audits and Alerts

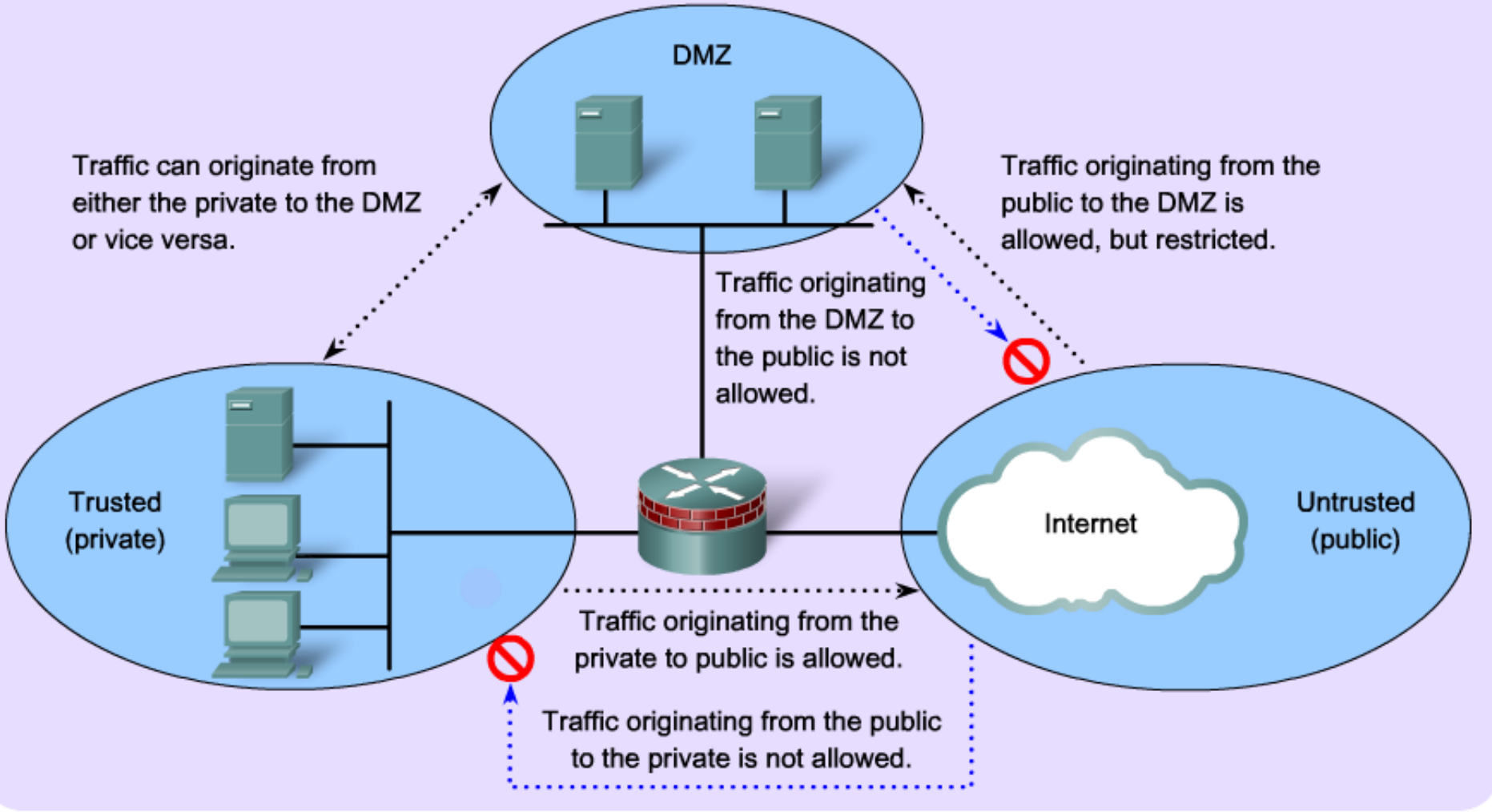


Inside ACL (Outgoing Traffic)	Outside ACL (Incoming Traffic)
permit ip 10.0.0.0 0.0.0.255 any	Dynamic: permit tcp host 200.3.3.3 eq 80 host 10.1.1.1 eq 1500 permit tcp any host 10.1.1.2 eq 25 permit udp any host 10.1.1.2 eq 53 deny ip any any

Advantages/disadvantages Statefall Firewalls

Advantages	• Often used as a primary means of defense by filtering unwanted, unnecessary, or undesirable traffic. • Strengthens packet filtering by providing more stringent control over security than packet filtering • Improves performance over packet filters or proxy servers. • Defends against spoofing and DoS attacks • Allows for more log information than a packet filtering firewall
Disadvantages	• Cannot prevent application layer attacks because it does not examine the actual contents of the HTTP connection • Not all protocols are stateful, such UDP and ICMP • Some applications open multiple connections requiring a whole new range of ports opened to allow this second connection • Stateful firewalls do not support user authentication

Design with DMZ (DeMilitarized Zone)



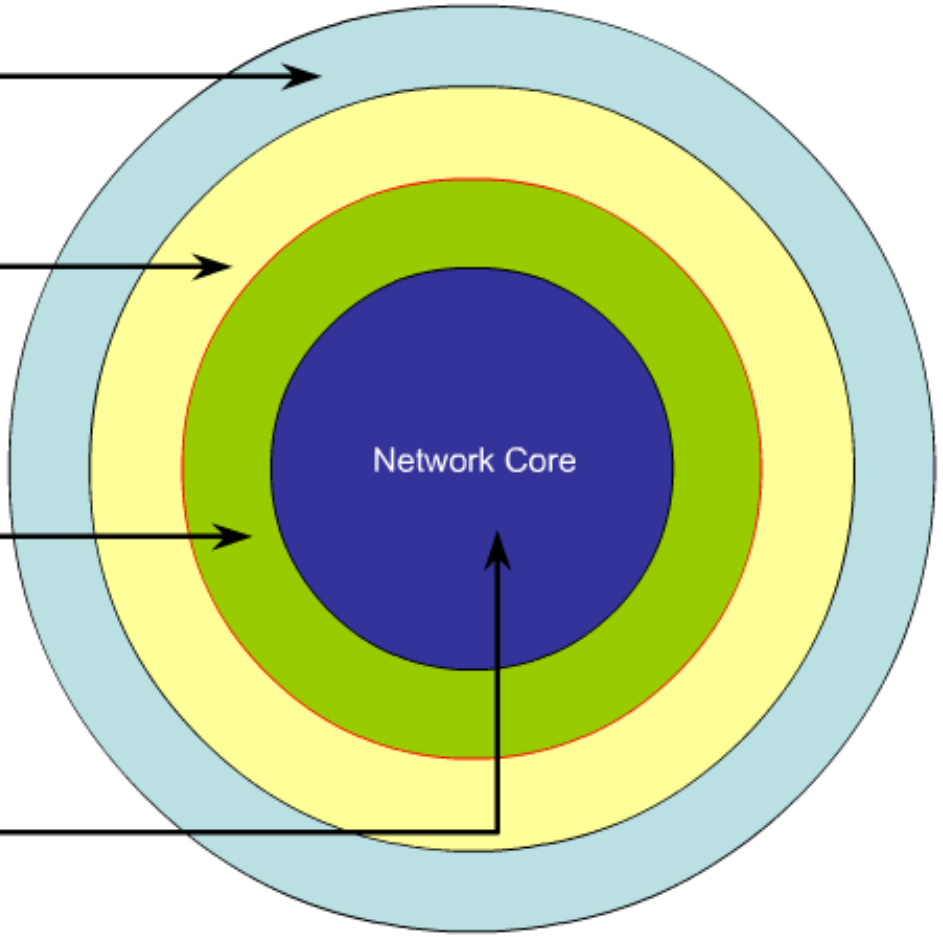
Layered Defense Scenario

Endpoint security:
Provides identity and device security policy compliance

Communications security:
Provides information assurance

Perimeter security:
Secures boundaries between zones

Core network security:
Protects against malicious software and traffic anomalies, enforces network policies, and ensures survivability



Disaster recovery:
Offsite storage and redundant architecture

Firewall Best Practices

- Position firewalls at security boundaries.
- Firewalls are the primary security device. It is unwise to rely exclusively on a firewall for security.
- Deny all traffic by default. Permit only services that are needed.
- Ensure that physical access to the firewall is controlled.
- Regularly monitor firewall logs.
- Practice change management for firewall configuration changes.
- Firewalls primarily protect from technical attacks originating from the outside.