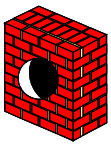
Firewall Threat Defense Features

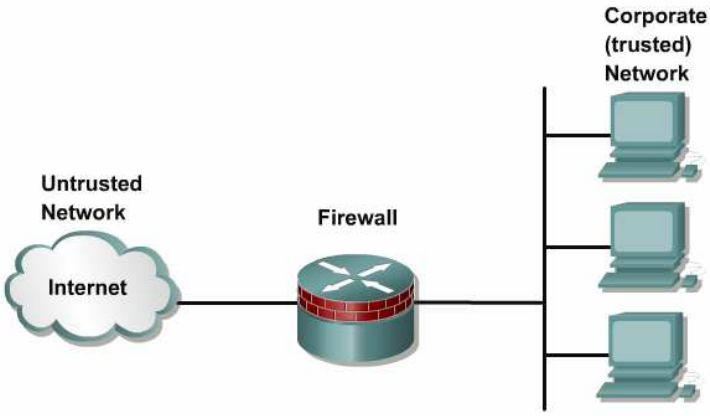
Introducing the Cisco IOS Firewall

Firewalls



- The most well-known security device is the firewall.
- By conventional definition, a firewall is a partition made of fireproof material designed to prevent the spread of fire from one part of a building to another.
- A firewall can also be used to isolate one compartment from another. When applying the term firewall to a computer network, a firewall is a system or group of systems that enforces an access control policy between two or more networks

Firewalls



A firewall is a system or group of systems that enforces an access control policy between two or more networks.

Firewalls

All firewalls fall within three classes:

- **Appliance-based firewalls** – Appliance-based firewalls are hardware platforms that are designed specifically as dedicated firewalls. The appliance may serve other functions, but they are secondary to the firewall feature set.
- **Server-based firewalls** – A server-based firewall consists of a firewall application that runs on a network operating system (NOS) such as UNIX, NT or Win2K, or Novell. The underlying operating system is still present, so vulnerabilities and resource use of the operating system must be taken into consideration when implementing a this type of firewall.
- **Integrated firewalls** – An integrated firewall is implemented by adding firewall functionality to an existing device.

Who needs a firewall ?

Network Attacks

- Reconnaissance attacks
- Access attacks
- Denial of service attacks
- Worms, viruses, and Trojan horses

Specific Attack Types

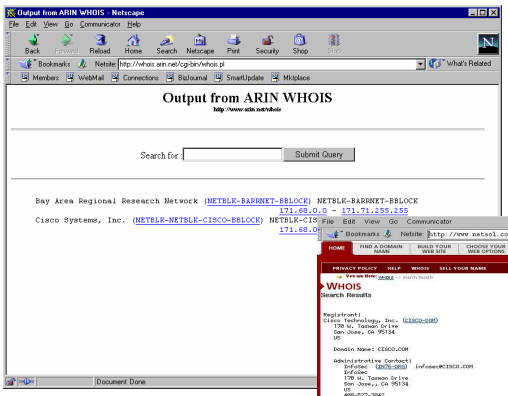
- Packet sniffers
- IP weaknesses
- Password attacks
- DoS or DDoS
- Man-in-the-middle attacks
- Application layer attacks
- Trust exploitation
- Port redirection
- Virus
- Trojan horse
- Operator error
- Worms

Reconnaissance Attack

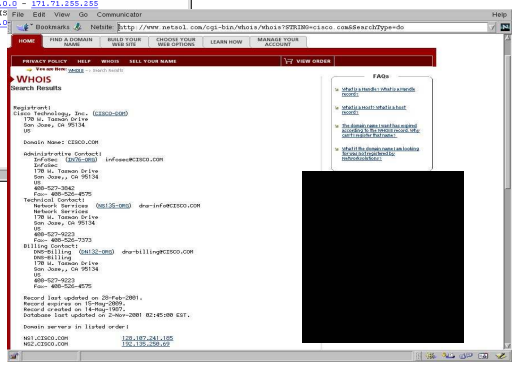
- **Network reconnaissance refers to the overall act of learning information about a target network by using publicly available information and applications. Network reconnaissance cannot be prevented entirely.**

IDSs (at the network and host levels can usually notify an administrator when a reconnaissance gathering attack (for example, ping sweeps and port scans) is under way.

Reconnaissance Attack Example



- **Sample IP address query**



Sample domain name query

Packet Sniffers

A packet sniffer is a software application that uses a network adapter card in promiscuous mode to capture all network packets. The following are the packet sniffer features:

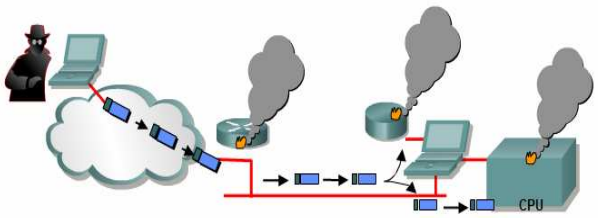
- Packet sniffers exploit information passed in clear text. Protocols that pass information in the clear include the following:
  - Telnet
  - FTP
  - SNMP
  - POP
- Packet sniffers must be on the same collision domain.

IP Spoofing

- IP spoofing occurs when a hacker inside or outside a network impersonates the conversations of a trusted computer.
- Two general techniques are used during IP spoofing:
  - A hacker uses an IP address that is within the range of trusted IP addresses.
  - A hacker uses an authorized external IP address that is trusted.
- Uses for IP spoofing include the following:
  - IP spoofing is usually limited to the injection of malicious data or commands into an existing stream of data.
  - A hacker changes the routing tables to point to the spoofed IP address, then the hacker can receive all the network packets that are addressed to the spoofed address and reply just as any trusted user can.

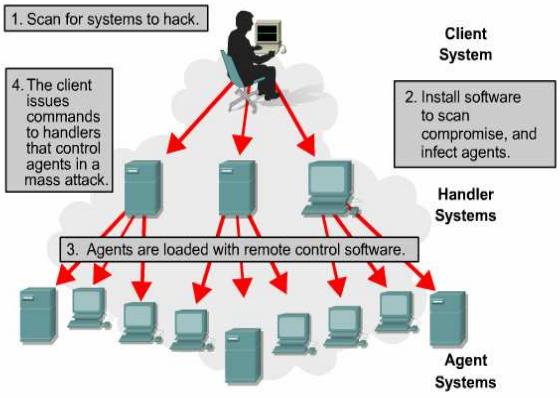
DoS Attacks

DoS attacks prevent authorized people from using a service by using up system resources.



Resource overloads	Malformed data
• Disk space, bandwidth, buffers, and so on. • Ping floods: smurf, and so on. • Packet storms: UDP bombs, fraggle, and so on.	• Oversized packets: ping of death, and so on. • Overlapping packets: winuke, and so on. • Un-handled data: teardrop, and so on.

DDoS Attack Example



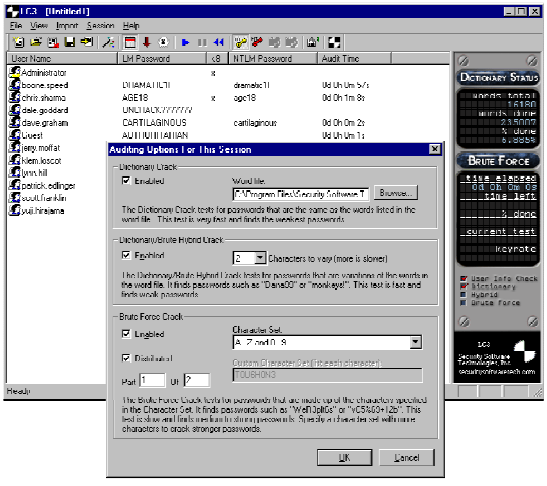
In a Distributed Denial of Service attack (DDoS) a hacker tricks other machines into flooding the target machine with nuisance traffic that robs system performance.

Password Attacks

- **Hackers can implement password attacks using several different methods:**
  - **Brute-force attacks**
  - **Dictionary Attacks**
  - **Trojan horse programs**
  - **IP spoofing**
  - **Packet sniffers**

Password Attacks

L0phtCrack can take the hashes of passwords and generate the clear text passwords from them.
Passwords are computed using two different methods:
- **Dictionary cracking**
- **Brute force computation**



Man-in-the-Middle Attacks

A man-in-the-middle attack requires that the hacker have access to network packets that come across a network.

A man-in-the-middle attack is implemented using the following:

- Network packet sniffers
- Routing and transport protocols

Possible man-in-the-middle attack uses include the following:

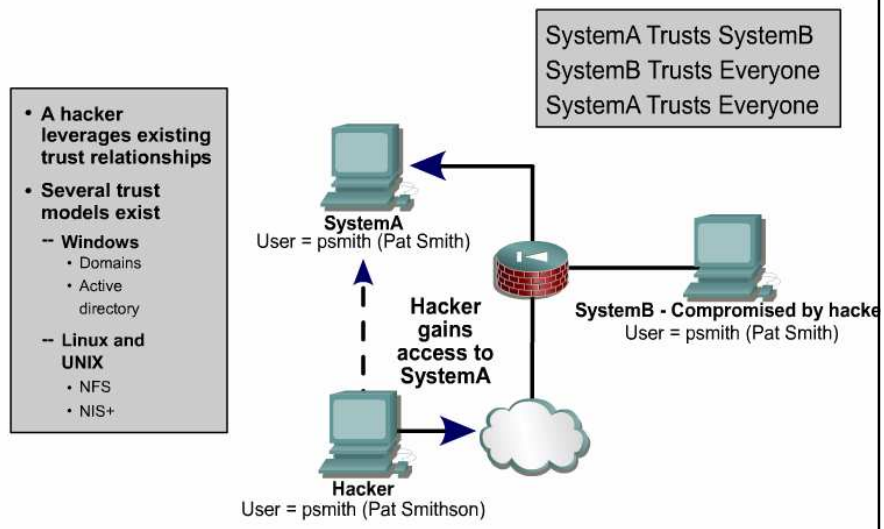
- Theft of information
- Hijacking of an ongoing session
- Traffic analysis
- DoS
- Corruption of transmitted data
- Introduction of new information into network sessions

Application Layer Attacks

- Application layer attacks have the following characteristics:
  - Exploit well known weaknesses, such as protocols, that are intrinsic to an application or system (for example, send mail, HTTP, and FTP)
  - Often use ports that are allowed through a firewall (for example, TCP port 80 used in an attack against a web server behind a firewall)
  - Can never be completely eliminated, because new vulnerabilities are always being discovered

Trust Exploitation

- A hacker leverages existing trust relationships
- Several trust models exist
  - -- Windows
    - Domains
    - Active directory
  - -- Linux and UNIX
    - NFS
    - NIS+

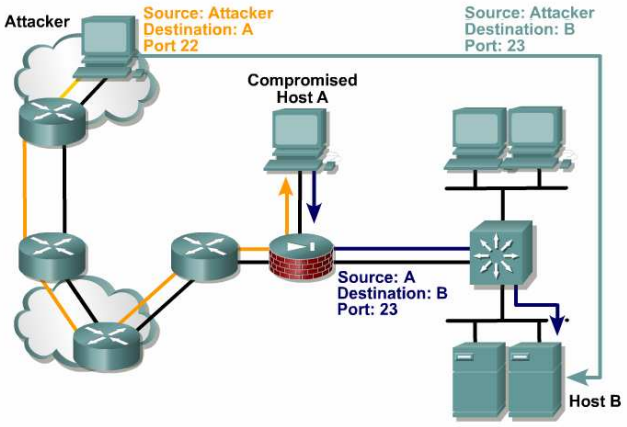


Port Redirection

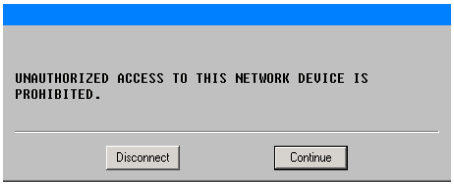
Port redirection is a type of trust-exploitation attack that uses a compromised host to pass traffic through a firewall that would otherwise be dropped.

It is mitigated primarily through the use of proper trust models.

Antivirus software and host-based IDS can help detect and prevent a hacker installing port redirecting utilities on the host.



Unauthorized Access



Unauthorized access includes any unauthorized attempt to access a private resource:

- **Not a specific type of attack**
- **Refers to most attacks executed in networks today**
- **Initiated on both the outside and inside of a network**

The following are mitigation techniques for unauthorized access attacks:

- **Eliminate the ability of a hacker to gain access to a system**
- **Prevent simple unauthorized access attacks, which is the primary function of a firewall**

Virus and Trojan Horses

Viruses refer to malicious software that are attached to another program to execute a particular unwanted function on a user's workstation. End-user workstations are the primary targets.

A Trojan horse is different only in that the entire application was written to look like something else, when in fact it is an attack tool. A Trojan horse is mitigated by antivirus software at the user level and possibly the network level.

Implementing a Firewall

- Personal software firewall – a software that is installed on a single PC to protect only that PC
- All-in-one firewall – can be a single device that offers the following features and functionality : router, Ethernet switch, wireless access point, firewall
- Small-to medium office firewalls , Enterprise firewalls – dedicated firewalls devices

Most common rules and features of firewalls

- Packet filtrering
- Block incoming network traffic based on sourse or destination
- Block outgoing network traffic based on sourse or destination
- Block network traffic based on content
- Make internal resourse available (DMZ)
- Allow connections to internal network
- Report on network traffic and firewall activites

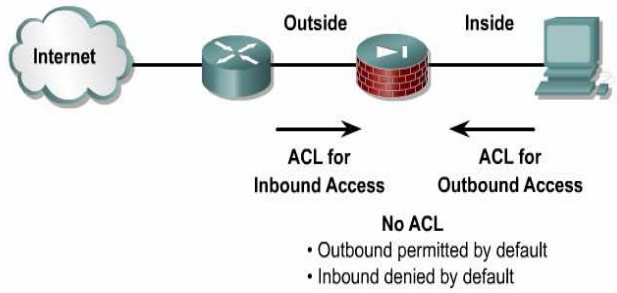
Packet filtering

- Packet filtering is the selective passing or blocking of data packets as they pass through a network interface. The criteria that uses when inspecting packets are based on the Layer 3 (IPv4 and IPv6) and Layer 4 (TCP, UDP, ICMP, and ICMPv6) headers.
- The most often used criteria are source and destination address, source and destination port, and protocol.

Access control list (ACL)

- Firewall can use packet filtering to limit information entering a network, or information moving from one segment of a network to another.
- Packet filtering uses access control lists (ACLs), which allow a firewall to accept or deny access based on packet types and other variables

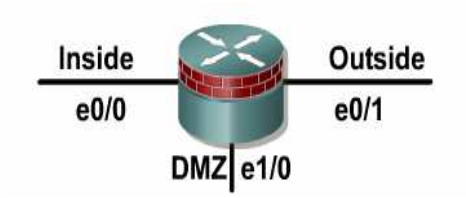
Access Policy
Access control list



Firewall appliance access-control policy is interface dependant.

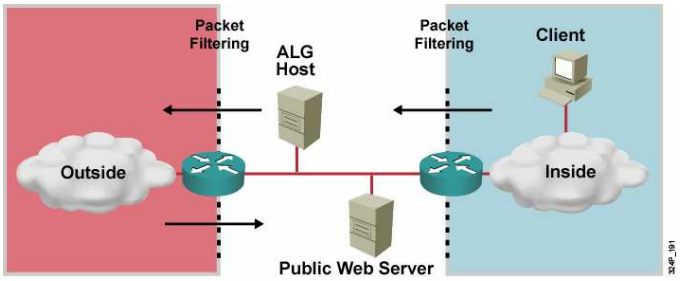
- Interface ACL permits or denies the initial packet incoming on that interface.
- ACL needs to describe only the initial packet of the application; no need to think about return traffic.
- If no ACL is attached to an interface, the following ASA policy applies:
  - Outbound packet is permitted by default.
  - Inbound packet is denied by default.

DMZ demilitarized zone



A DMZ is an interface that sits between a trusted network segment (your network) and an untrusted segment network segment (Internet), providing physical isolation between the two networks that is enforced by a series of connectivity rules within the firewall.

DMZ



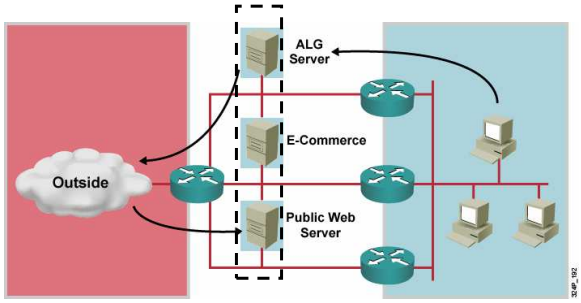
- A DMZ is established between security zones.
- DMZs are buffer networks that are neither the Inside nor the Outside network.

Layered Defense Features

- Access control is enforced on traffic entering and exiting the buffer network to all security zones by:
  - Classic routers
  - Dedicated firewalls
- DMZs are used to host services:
  - Exposed public services are served on dedicated hosts inside the buffer network.
  - The DMZ may host an application gateway for outbound connectivity.
- A DMZ blocks and contains an attacker in the case of a break-in.

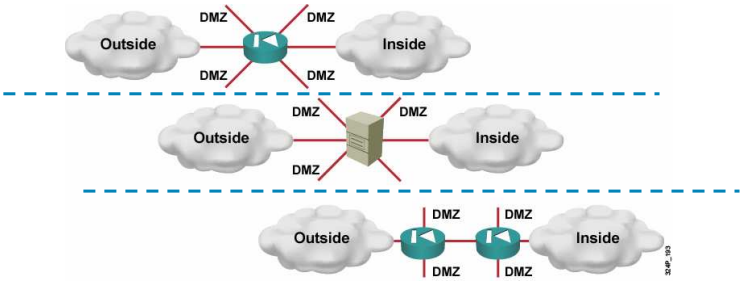
Multiple DMZs

Three Separate DMZs



- Multiple DMZs provide better separation and access control:
  - Each service can be hosted in a separate DMZ.
  - Damage is limited and attackers contained if a service is compromised.

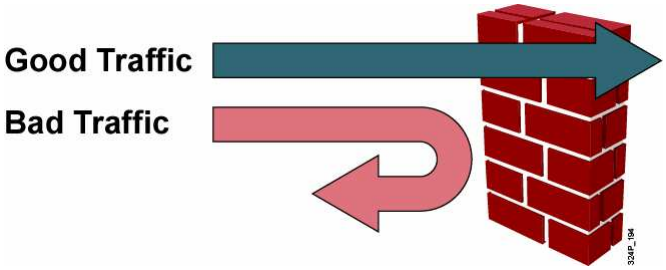
Modern DMZ Design



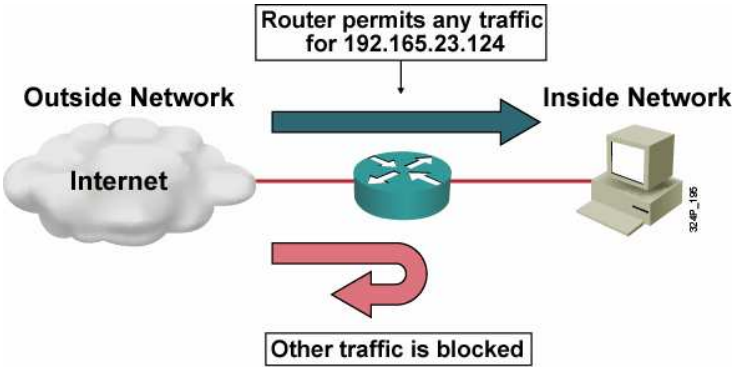
- Various systems (a stateful packet filter or proxy server) can filter traffic.
- Proper configuration of the filtering device is critical.

Firewall Technologies

- Firewalls use three technologies:
  - Packet filtering
  - Application layer gateway (ALG)
  - Stateful packet filtering

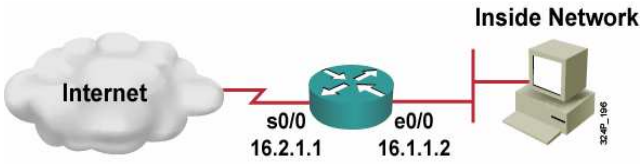


Packet Filtering



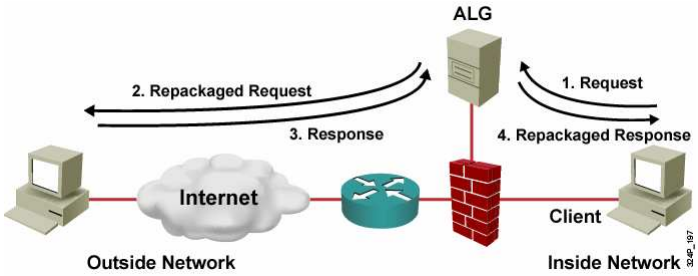
- Packet filtering limits traffic into a network based on the destination and source addresses, ports, and other flags that you compile in an ACL.

Packet Filtering Example



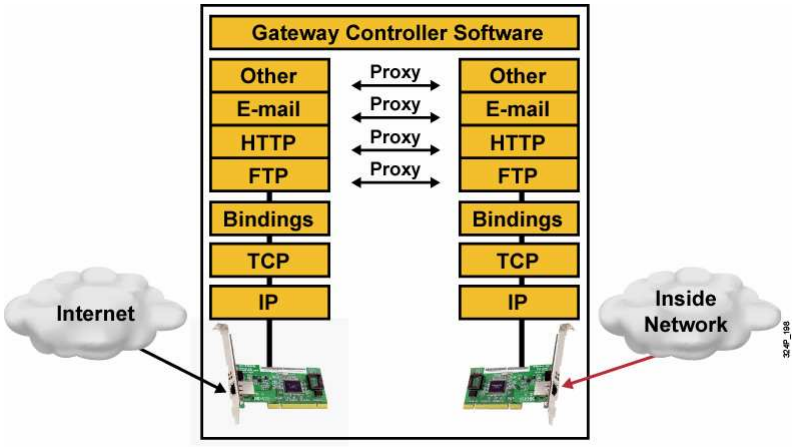

```
Router(config)# access-list 100 permit tcp any 16.1.1.0
0.0.0.255 established
Router(config)# access-list 100 deny ip any any log
Router(config)# interface Serial0/0
Router(config-if)# ip access-group 100 in
Router(config-if)# end
```


Application Layer Gateway

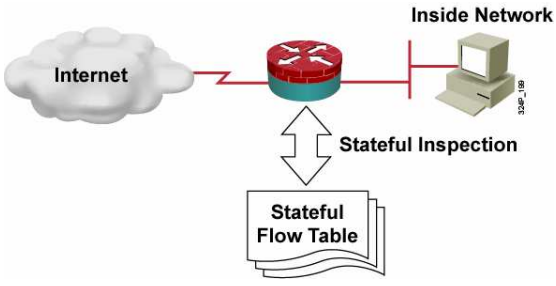


- The ALG intercepts and establishes connections to the Internet hosts on behalf of the client.

ALG Firewall Device



Stateful Packet Filtering



- Stateless ACLs filter traffic based on source and destination IP addresses, TCP and UDP port numbers, TCP flags, and ICMP types and codes.
- Stateful inspection then remembers certain details, or the state of that request.

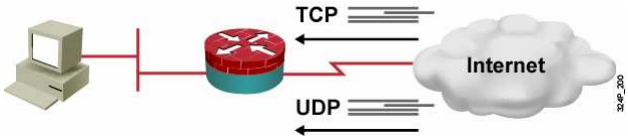
Stateful Firewalls

- Also called “stateful packet filters” and “application-aware packet filters.”
- Stateful firewalls have two main improvements over packet filters:
  - They maintain a session table (state table) where they track all connections.
  - They recognize dynamic applications and know which additional connections will be initiated between the endpoints.
- Stateful firewalls inspect every packet, compare the packet against the state table, and may examine the packet for any special protocol negotiations.
- Stateful firewalls operate mainly at the connection (TCP and UDP) layer.

The Cisco IOS Firewall Feature Set

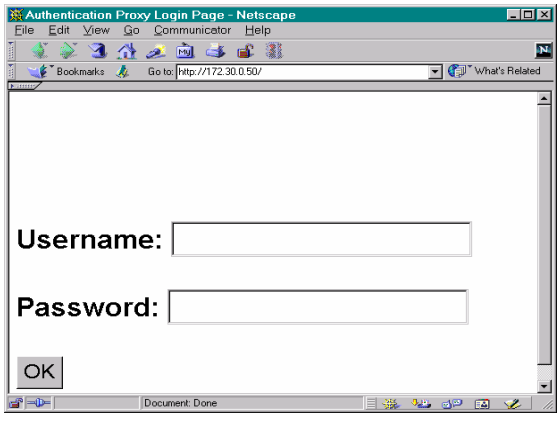
- The Cisco IOS Firewall Feature Set contains these features:
  - Standard and extended ACLs
  - Cisco IOS Firewall
  - Cisco IOS Firewall IPS
  - Authentication proxy
  - Port-to-Application Mapping (PAM)
  - NAT
  - IPsec network security
  - Event logging
  - User authentication and authorization

Cisco IOS Firewall



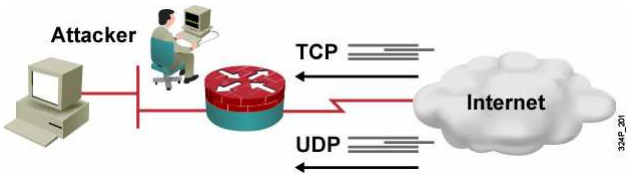
- Packets are inspected when entering the Cisco IOS firewall if the packets are not specifically denied by an ACL.
- Cisco IOS Firewall permits or denies specified TCP and UDP traffic through a firewall.
- A state table is maintained with session information.
- ACLs are dynamically created or deleted.
- Cisco IOS Firewall protects against DoS attacks.

Cisco IOS Authentication Proxy



- HTTP, HTTPS, FTP, and Telnet authentication
- Provides dynamic, per-user authentication and authorization via TACACS+ and RADIUS protocols

Cisco IOS IPS

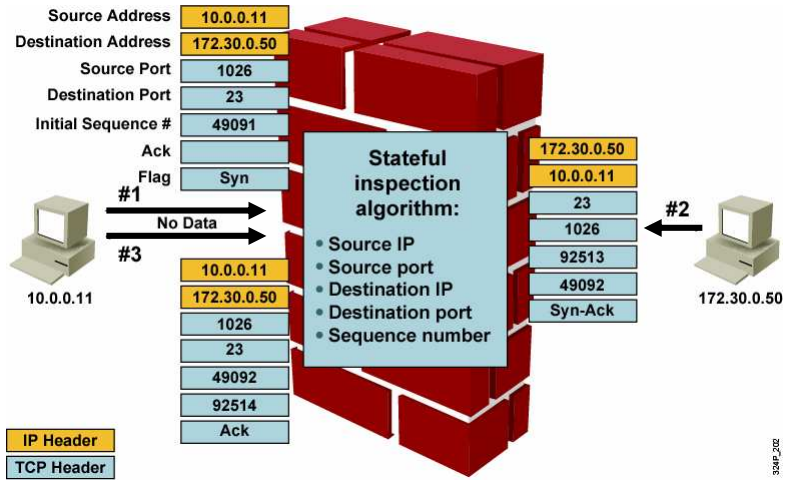


- Acts as an inline intrusion prevention sensor—traffic goes through the sensor
- When an attack is detected, the sensor can perform any of these actions:
  - Alarm: Send an alarm to SDM or syslog server.
  - Drop: Drop the packet.
  - Reset: Send TCP resets to terminate the session.
  - Block: Block an attacker IP address or session for a specified time.
- Identifies 700+ common attacks

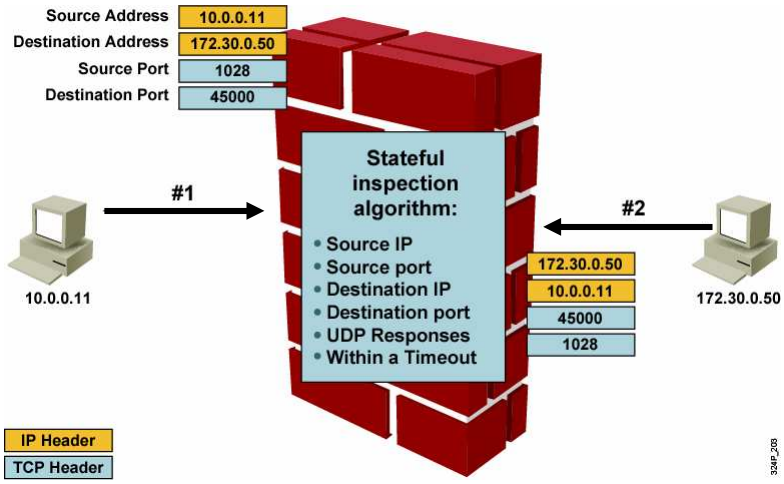
Cisco IOS ACLs Revisited

- ACLs provide traffic filtering by these criteria:
  - Source and destination IP addresses
  - Source and destination ports
- ACLs can be used to implement a filtering firewall leading to these security shortcomings:
  - Ports opened permanently to allow traffic, creating a security vulnerability.
  - The ACLs do not work with applications that negotiate ports dynamically.

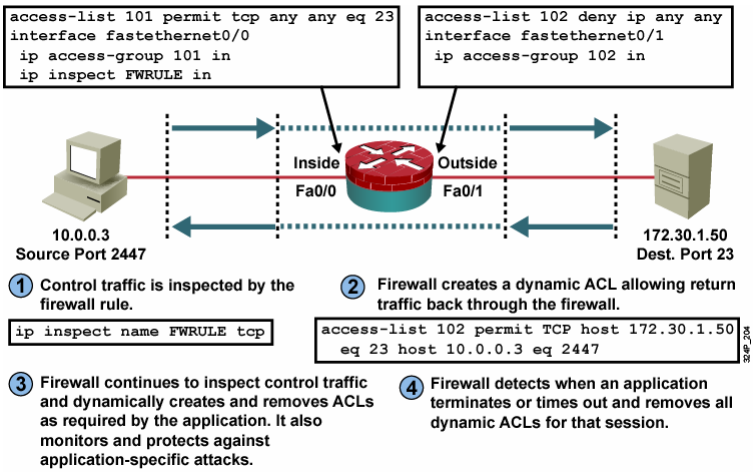
Cisco IOS Firewall TCP Handling



Cisco IOS Firewall UDP Handling

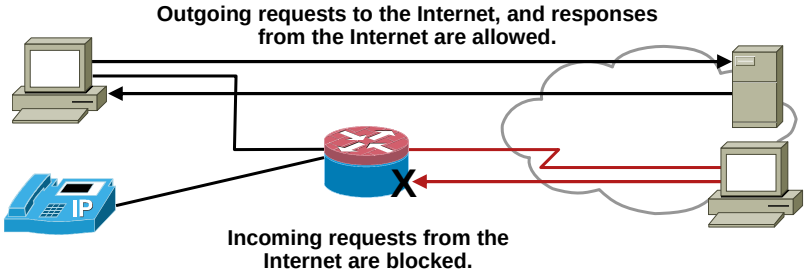


How Cisco IOS Firewall Works



Cisco IOS Firewall Supported Protocols

- Regardless of the application layer protocol, Cisco IOS Firewall will inspect:
  - All TCP sessions
  - All UDP connections
- Enhanced stateful inspection of application layer protocols

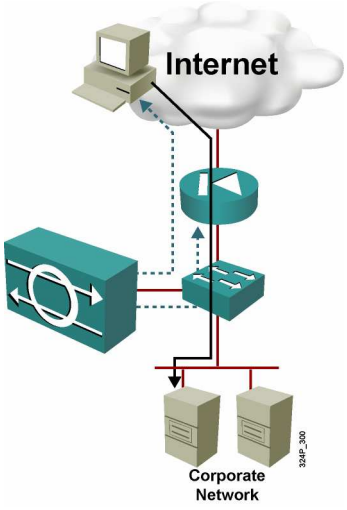


Alerts and Audit Trails

- Cisco IOS Firewall generates real-time alerts and audit trails.
- Audit trail features use syslog to track all network transactions.
- With Cisco IOS Firewall inspection rules, you can configure alerts and audit trail information on a per-application protocol basis.

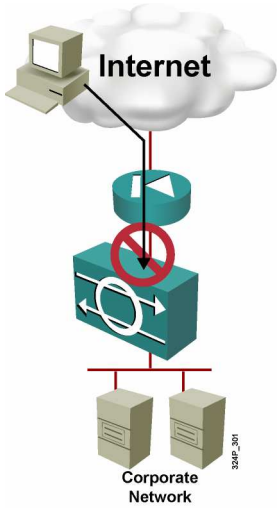
Intrusion Detection System

- IDS is a passive device:
  - Traffic does not pass through the IDS device.
  - Typically uses only one promiscuous interface.
- IDS is reactive:
  - IDS generates an alert to notify the manager of malicious traffic.
- Optional active response:
  - Further malicious traffic can be denied with a security appliance or router.
  - TCP resets can be sent to the source device.



Intrusion Protection System

- IPS is an active device:
  - All traffic passes through IPS.
  - IPS uses multiple interfaces.
- Proactive prevention:
  - IPS denies all malicious traffic.
  - IPS sends an alert to the management station.



Combining IDS and IPS

- IPS actively blocks offending traffic:
  - Should not block legitimate data
  - Only stops “known malicious traffic”
  - Requires focused tuning to avoid connectivity disruption
- IDS complements IPS:
  - Verifies that IPS is still operational
  - Alerts you about any suspicious data except “known good traffic”
  - Covers the “gray area” of possibly malicious traffic that IPS did not stop