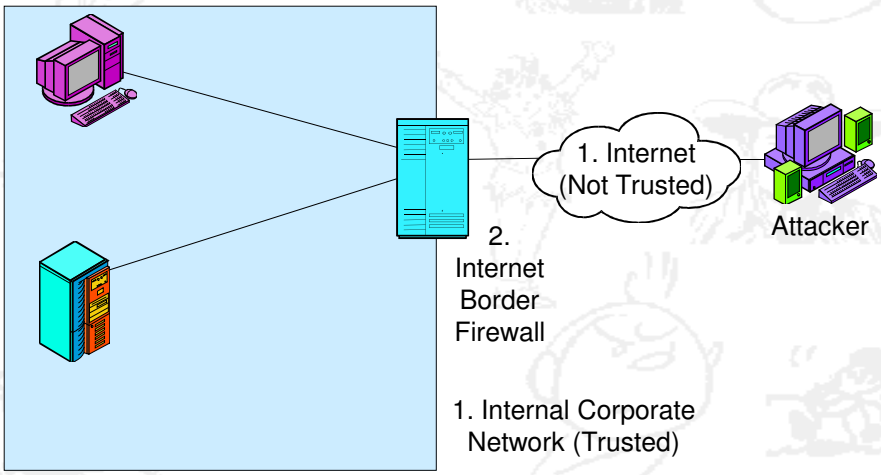
Reti di Calcolatori II

I Firewall

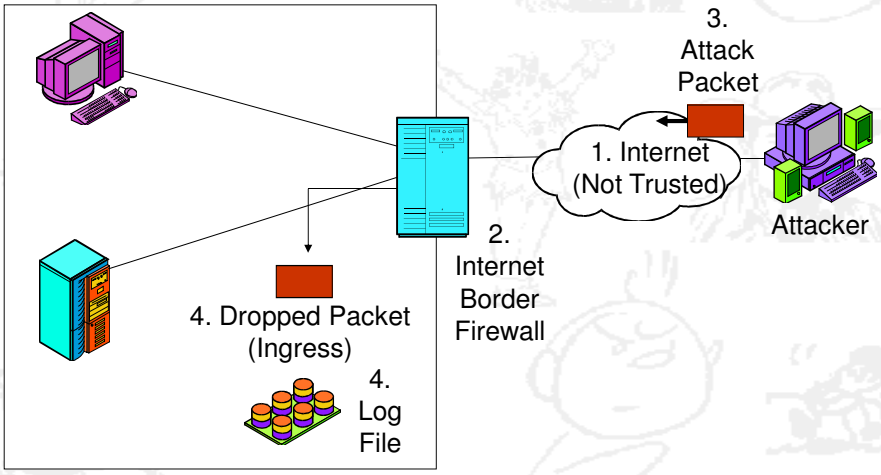
Giorgio Ventre

Dipartimento di Informatica e Sistemistica
Università di Napoli Federico II

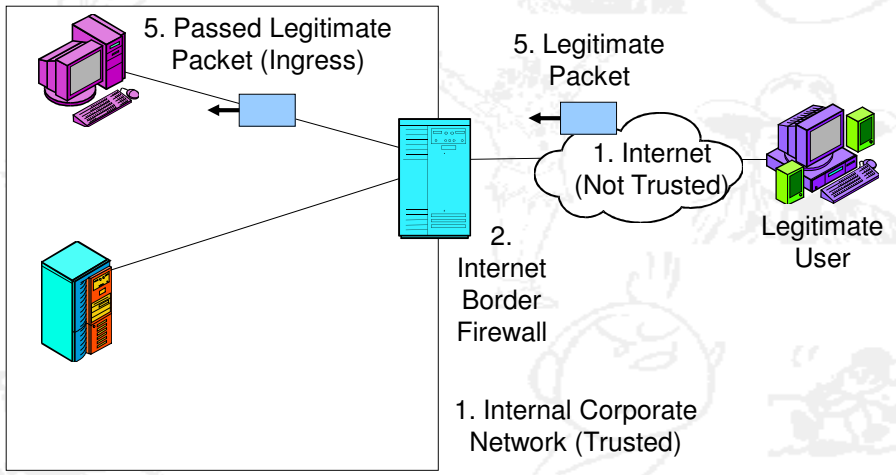
Border Firewall



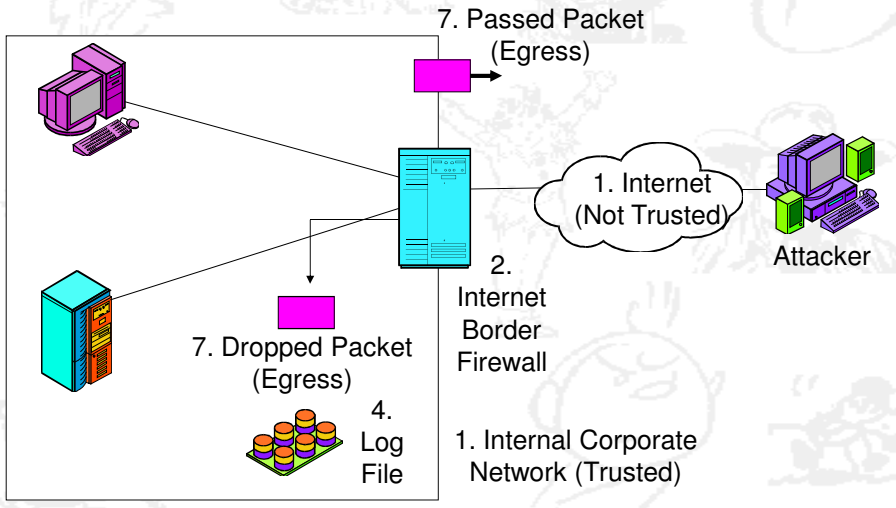
Border Firewall



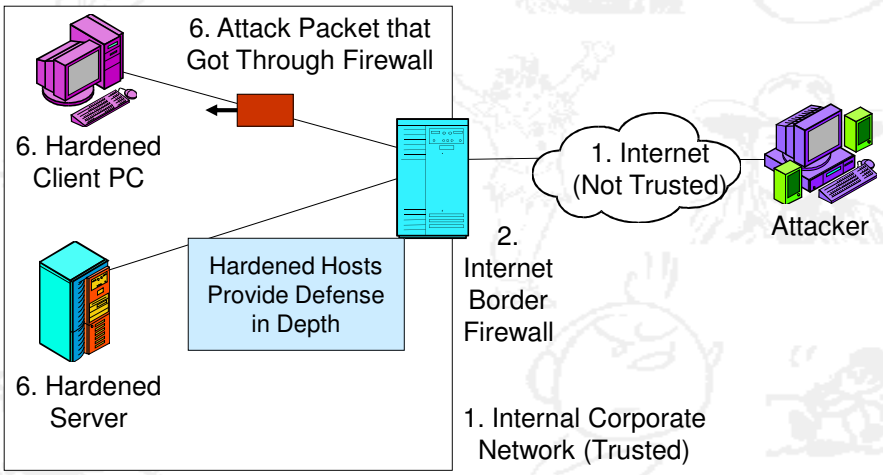
Border Firewall



Border Firewall



Border Firewall



Types of Firewall Inspection

- Virtual Private Network Handling
  - » Virtual private networks offer message-by-message confidentiality, authentication, message integrity, and anti-replay protection
  - » Packets are encrypted for confidentiality, so firewall inspection is impossible
  - » VPNs typically bypass firewalls, making border security weaker

Firewalls

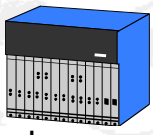
- Firewall Hardware and Software
  - » Screening router firewalls
  - » Computer-based firewalls
  - » Firewall appliances
  - » Host firewalls (firewalls on clients and servers)
- Inspection Methods
- Firewall Architecture
- Configuring, Testing, and Maintenance

Firewall Hardware and Software

- Screening Router Firewalls
  - » Add firewall software to router
  - » Usually provide light filtering only
  - » Expensive for the processing power—usually must upgrade hardware, too

Firewall Hardware and Software

- Screening Router Firewalls



  - » Screens out incoming “noise” of simple scanning attacks to make the detection of serious attacks easier
  - » Good location for egress filtering—can eliminate scanning responses, even from the router

Firewall Hardware and Software

- Computer-Based Firewalls

  - » Add firewall software to server with an existing operating system: Windows or UNIX
  - » Can be purchased with power to handle any load
  - » Easy to use because know operating system

Firewall Hardware and Software

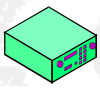
- Computer-Based Firewalls
  - » Firewall vendor might bundle firewall software with hardened hardware and operating system software
  - » General-purpose operating systems result in slower processing

Firewall Hardware and Software

- Computer-Based Firewalls
  - » Security: Attackers may be able to hack the operating system
    - – Change filtering rules to allow attack packets in
    - – Change filtering rules to drop legitimate packets

Firewall Hardware and Software

- Firewall Appliances



  - » Boxes with minimal operating systems
  - » Therefore, difficult to hack
  - » Setup is minimal
  - » Not customized to specific firm's situation
  - » Must be able to update

Firewall Hardware and Software

- Host Firewalls

  - » Installed on hosts themselves (servers and sometimes clients)
  - » Enhanced security because of host-specific knowledge
    - – For example, filter out everything but webserver transmissions on a webserver

Firewall Hardware and Software

- Host Firewalls

  - » Defense in depth
    - – Normally used in conjunction with other firewalls
    - – Although on single host computers connected to the Internet, might be only firewall

Firewall Hardware and Software

- Host Firewalls

  - » The firm must manage many host firewalls
  - » If not centrally managed, configuration can be a nightmare
  - » Especially if rule sets change frequently

Firewall Hardware and Software

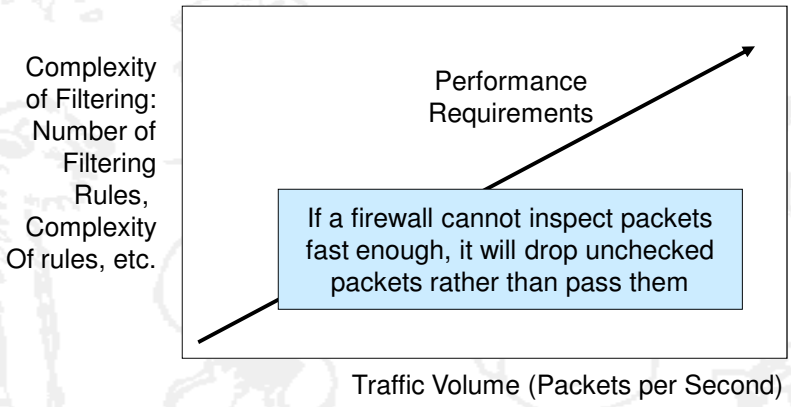
- Host Firewalls

  - » Client firewalls typically must be configured by ordinary users
    - – Might misconfigure or reject the firewall
    - – Need to centrally manage remote employee computers

Perspective

- Computer-Based Firewall
  - » Firewall based on a computer with a full operating system
  - » Traffic is traversing the computer
- Host Firewall
  - » A firewall on a host (client or server)
  - » Traffic is ending on the host

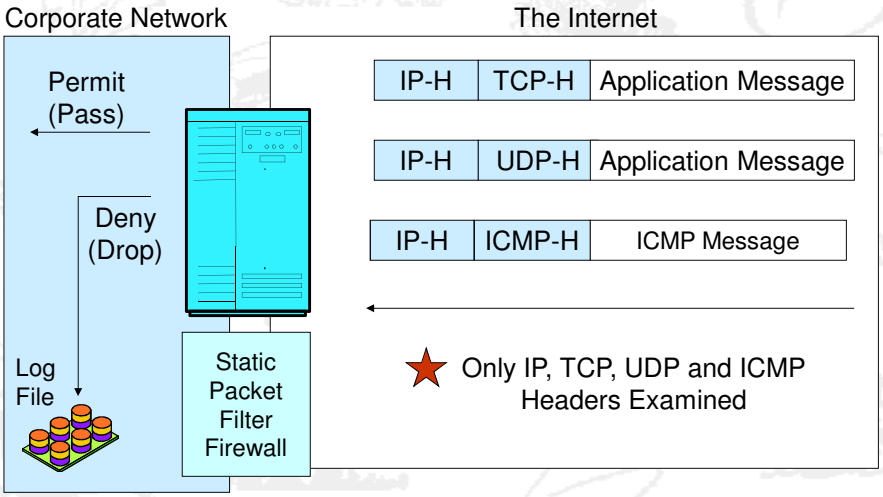
Drivers of Performance Requirements: Traffic Volume and Complexity of Filtering



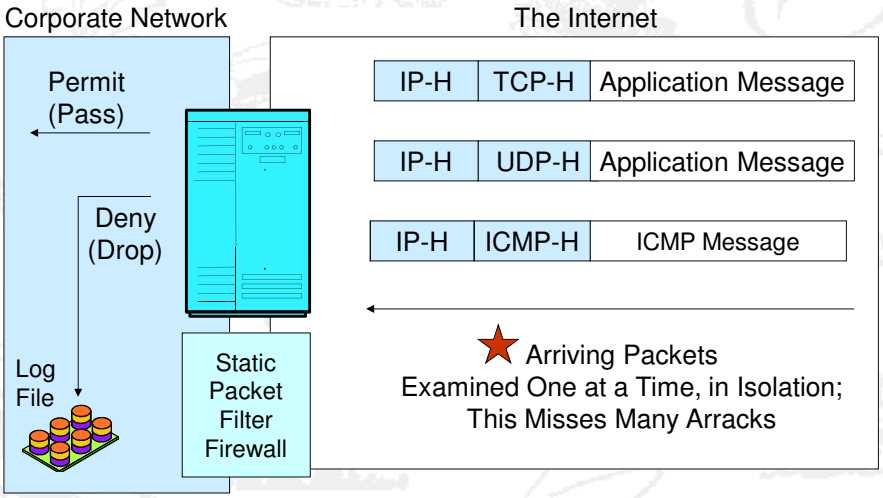
Firewalls

- Firewall Hardware and Software
- Inspection Methods
  - **Static Packet Inspection**
  - Stateful Packet Inspection
  - NAT
  - Application Firewalls
  - IPSs
- Firewall Architecture
- Configuring, Testing, and Maintenance

Static Packet Filter Firewall



Static Packet Filter Firewall



Access Control List (ACL) For Ingress Filtering at a Border Router

- 1. If source IP address = 10.*.*.*, DENY *[private IP address range]*
- 2. If source IP address = 172.16.*.* to 172.31.*.*, DENY *[private IP address range]*
- 3. If source IP address = 192.168.*.*, DENY *[private IP address range]*
- 4. If source IP address = 60.40.*.*, DENY *[internal address range]*

Access Control List (ACL) for Ingress Filtering at a Border Router

- 5. If source IP address = 1.2.3.4, DENY *[black-holed address of attacker]*
- 6. If TCP SYN=1 AND FIN=1, DENY *[crafted attack packet]*

Access Control List (ACL) for Ingress Filtering at a Border Router

- 7. If destination IP address = 60.47.3.9 AND TCP destination port=80 OR 443, PASS *[connection to a public webserver]*
- 8. If TCP SYN=1 AND ACK=0, DENY *[attempt to open a connection from the outside]*

Access Control List (ACL) for Ingress Filtering at a Border Router

- 9. If TCP destination port = 20, DENY *[FTP data connection]*
- 10. If TCP destination port = 21, DENY *[FTP supervisory control connection]*
- 11. If TCP destination port = 23, DENY *[Telnet data connection]*
- 12. If TCP destination port = 135 through 139, DENY *[NetBIOS connection for clients]*

Access Control List (ACL) for Ingress Filtering at a Border Router

- 13. If TCP destination port = 513, DENY *[UNIX rlogin without password]*
- 14. If TCP destination port = 514, DENY *[UNIX rsh launch shell without login]*
- 15. If TCP destination port = 22, DENY *[SSH for secure login, but some versions are insecure]*
- 16. If UDP destination port=69, DENY *[Trivial File Transfer Protocol; no login necessary]*

Access Control List (ACL) for Ingress Filtering at a Border Router

- 17. If ICMP Type = 0, PASS *[allow incoming echo reply messages]*
- DENY ALL

Access Control List (ACL) for Ingress Filtering at a Border Router

- DENY ALL
  - » Last rule
  - » Drops any packets not specifically permitted by earlier rules
  - » In the previous ACL, Rules 8-16 are not needed; Deny all would catch them

Access Control List (ACL) for Egress Filtering at a Border Router

- 1. If source IP address = 10.*.*.*, DENY *[private IP address range]*
- 2. If source IP address = 172.16.*.* to 172.31.*.*, DENY *[private IP address range]*
- 3. If source IP address = 192.168.*.*, DENY *[private IP address range]*
- 4. If source IP address NOT = 60.47.*.*, DENY *[not in internal address range]*
  - » *Rules 1-3 are not needed because of this rule*

Access Control List (ACL) for Egress Filtering at a Border Router

- 5. If ICMP Type = 8, PASS *[allow outgoing echo messages]*
- 6. If Protocol=ICMP, DENY *[drop all other outgoing ICMP messages]*
- 7. If TCP RST=1, DENY *[do not allow outgoing resets; used in host scanning]*

Access Control List (ACL) for Egress Filtering at a Border Router

- 8. If source IP address = 60.47.3.9 and TCP source port = 80 OR 443, PERMIT *[public webserver responses]*
  - » *Needed because next rule stops all packets from well-known port numbers*
- 9. If TCP source port=0 through 49151, DENY *[well-known and registered ports]*
- 10. If UDP source port=0 through 49151, DENY *[well-known and registered ports]*

Access Control List (ACL) for Egress Filtering at a Border Router

- 11. If TCP source port =49152 through 65,536, PASS *[allow outgoing client connections]*
- 12. If UDP source port = 49152 through 65,536, PASS *[allow outgoing client connections]*
  - » *Note: Rules 9-12 only work if all hosts follow IETF rules for port assignments (well-known, registered, and ephemeral). Windows computers do. Unix computers do not*

Access Control List (ACL) for Egress Filtering at a Border Router

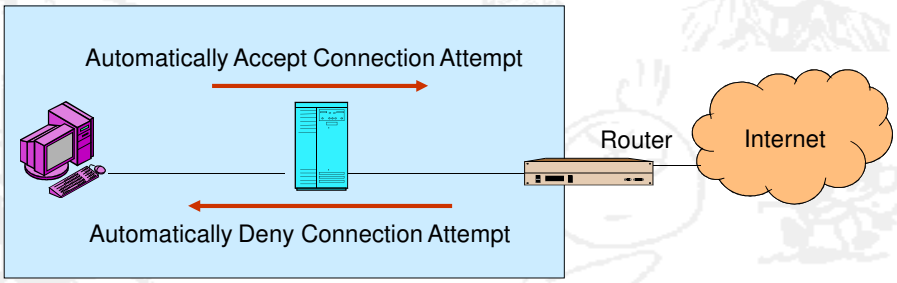
- 13. DENY ALL
  - » No need for Rules 9-10

Firewalls

- Firewall Hardware and Software
- Inspection Methods
  - » Static Packet Inspection
  - » **Stateful Packet Inspection**
  - » NAT
  - » Application Firewalls
- Firewall Architecture
- Configuring, Testing, and Maintenance

Stateful Inspection Firewalls

- Default Behavior
  - » Permit connections initiated by an internal host
  - » Deny connections initiated by an external host
  - » Can change default behavior with ACL



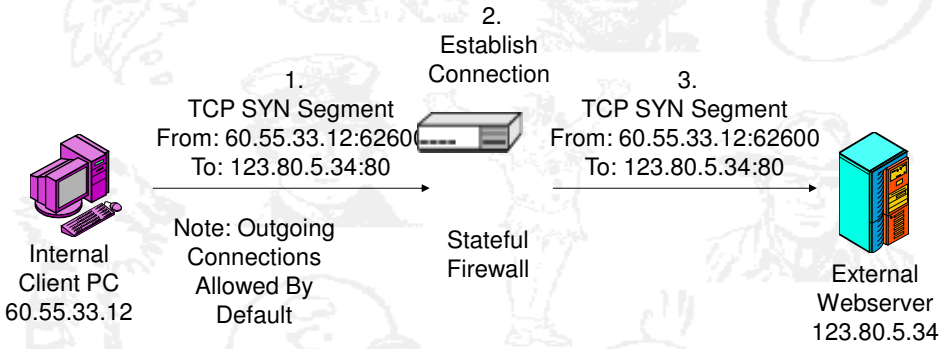
Stateful Inspection Firewalls

- State of Connection: Open or Closed
  - » State: Order of packet within a dialog
  - » Often simply whether the packet is part of an open connection

Stateful Inspection Firewalls

- Stateful Firewall Operation
  - » If accept a connection…
  - » Record the two IP addresses and port numbers in state table as OK (open) (Figure 5-9)
  - » Accept future packets between these hosts and ports with no further inspection
    - – This can miss some attacks

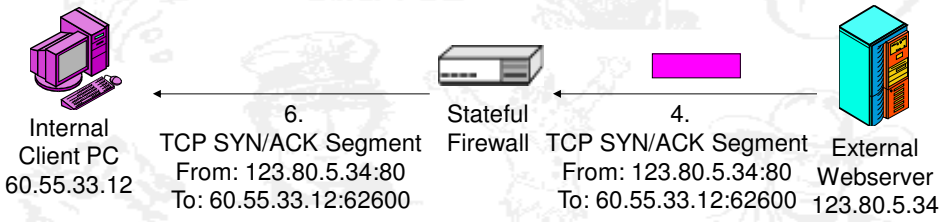
Stateful Inspection Firewall Operation I



Connection Table

Type	Internal IP	Internal Port	External IP	External Port	Status
TCP	60.55.33.12	62600	123.80.5.34	80	OK

Stateful Inspection Firewall Operation I



5.
Check Connection
OK;
Pass the Packet

Connection Table

Type	Internal IP	Internal Port	External IP	External Port	Status
TCP	60.55.33.12	62600	123.80.5.34	80	OK

Stateful Inspection Firewalls

- Stateful Firewall Operation
  - » For UDP, also record two IP addresses and port numbers in the state table

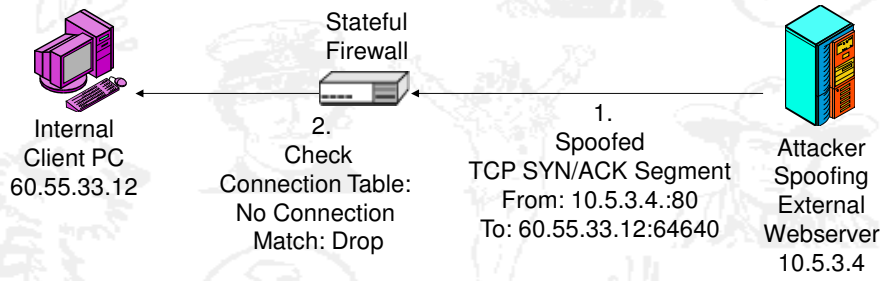
Connection Table

Type	Internal IP	Internal Port	External IP	External Port	Status
TCP	60.55.33.12	62600	123.80.5.34	80	OK
UDP	60.55.33.12	63206	1.8.33.4	69	OK

Stateful Inspection Firewalls

- Static Packet Filter Firewalls are Stateless
  - » Filter one packet at a time, in isolation
  - » If a TCP SYN/ACK segment is sent, cannot tell if there was a previous SYN to open a connection
  - » But stateful firewalls can (Figure 5-10)

Stateful Firewall Operation II



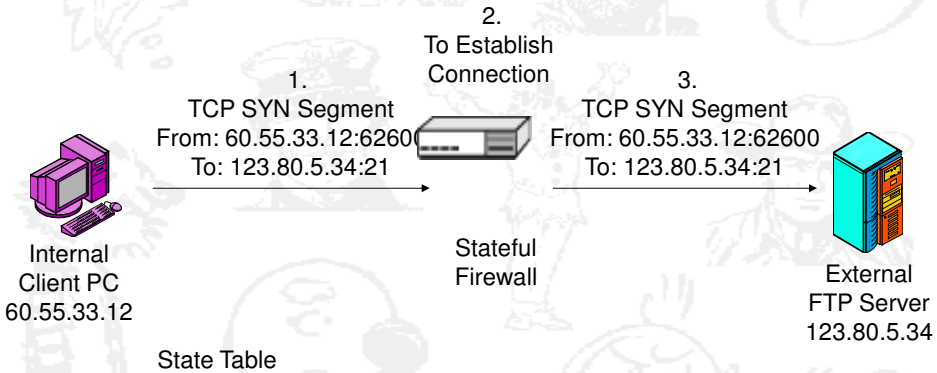
Connection Table

Type	Internal IP	Internal Port	External IP	External Port	Status
TCP	60.55.33.12	62600	123.80.5.34	80	OK
UDP	60.55.33.12	63206	222.8.33.4	69	OK

Stateful Inspection Firewalls

- Static Packet Filter Firewalls are Stateless
  - » Filter one packet at a time, in isolation
  - » Cannot deal with port-switching applications
  - » But stateful firewalls can (Figure 5-11)

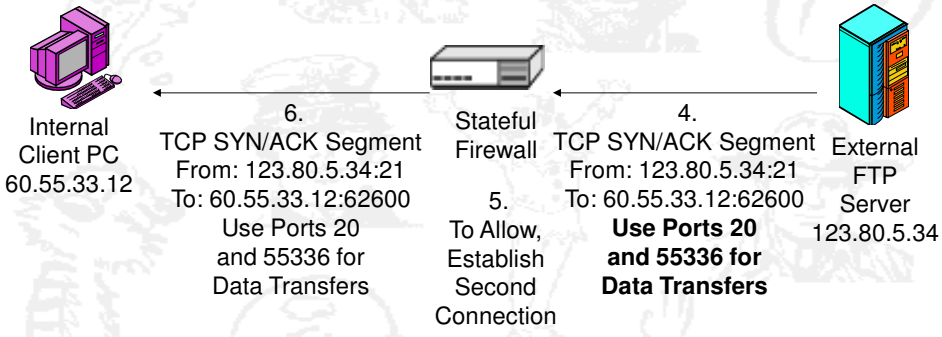
Port-Switching Applications with Stateful Firewalls



State Table

	Type	Internal IP	Internal Port	External IP	External Port	Status
Step 2 →	TCP	60.55.33.12	62600	123.80.5.34	21	OK

Port-Switching Applications with Stateful Firewalls



State Table

	Type	Internal IP	Internal Port	External IP	External Port	Status
Step 2 →	TCP	60.55.33.12	62600	123.80.5.34	21	OK
Step 5 →	TCP	60.55.33.12	55336	123.80.5.34	20	OK

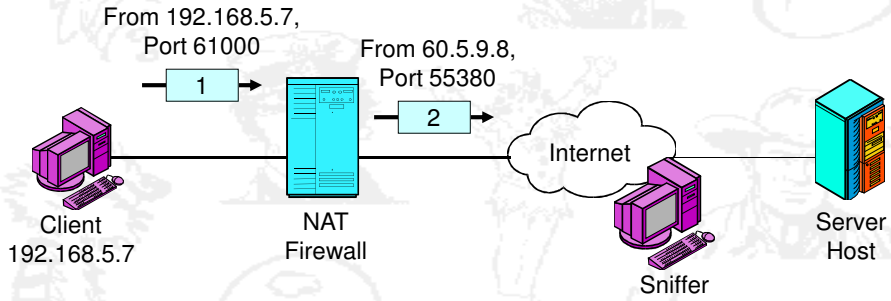
Stateful Inspection Firewalls

- Stateful Inspection Access Control Lists (ACLs)
  - Primary allow or deny applications (port numbers)
  - Simple because no need for probe packet rules because they are dropped automatically
  - Simplicity of stateful firewall gives speed and therefore low cost
  - Stateful firewalls are dominant today for the main corporate border firewalls

Firewalls

- Firewall Hardware and Software
- Inspection Methods
  - Static Packet Inspection
  - Stateful Packet Inspection
  - **NAT**
  - Application Firewalls
  - IPSs
- Firewall Architecture
- Configuring, Testing, and Maintenance

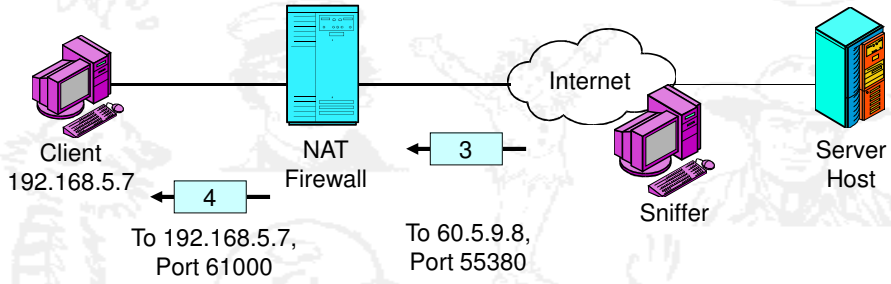
Network Address Translation (NAT)



Translation Table

Internal		External	
IP Addr	Port	IP Addr	Port
192.168.5.7	61000	60.5.9.8	55380
. . .	. . .	. . .	. . .

Network Address Translation (NAT)



Translation Table

Internal		External	
IP Addr	Port	IP Addr	Port
192.168.5.7	61000	60.5.9.8	55380
. . .	. . .	. . .	. . .

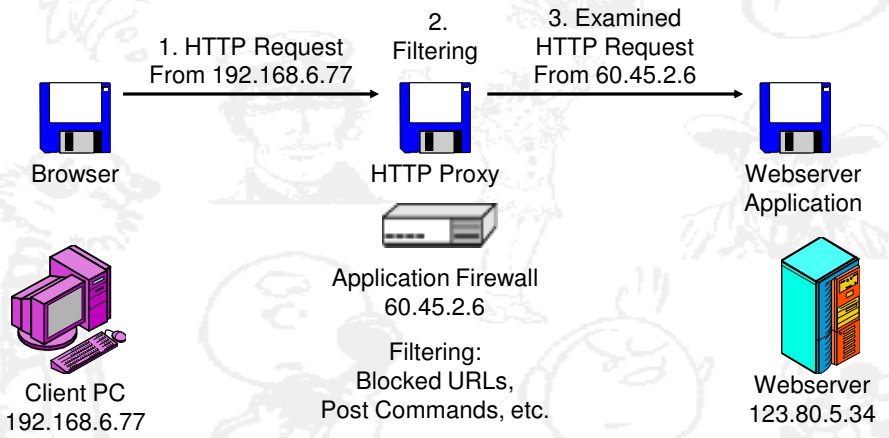
Network Address Translation (NAT)

- Sniffers on the Internet cannot learn internal IP addresses and port numbers
  - » Only learn the translated address and port number
- By themselves, provide a great deal of protection against attacks
  - » External attackers cannot create a connection to an internal computers

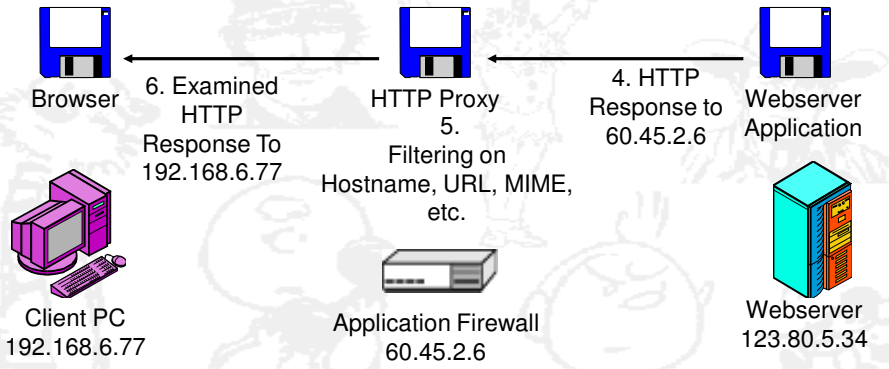
Firewalls

- Firewall Hardware and Software
- Inspection Methods
  - » Static Packet Inspection
  - » Stateful Packet Inspection
  - » NAT
  - » **Application Firewalls**
  - » IPSs
- Firewall Architecture
- Configuring, Testing, and Maintenance

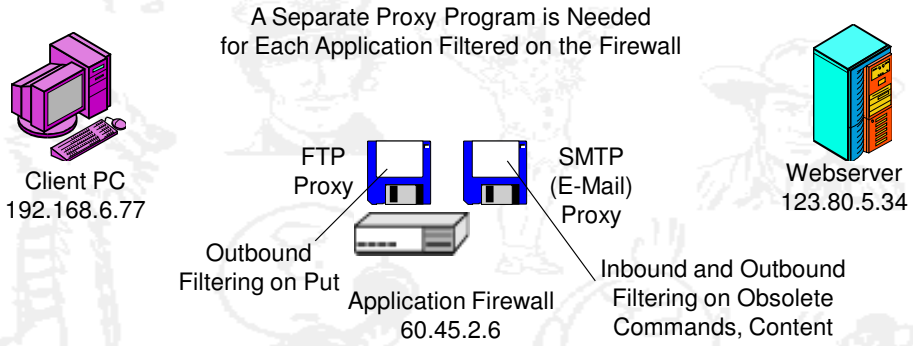
Application Firewall Operation



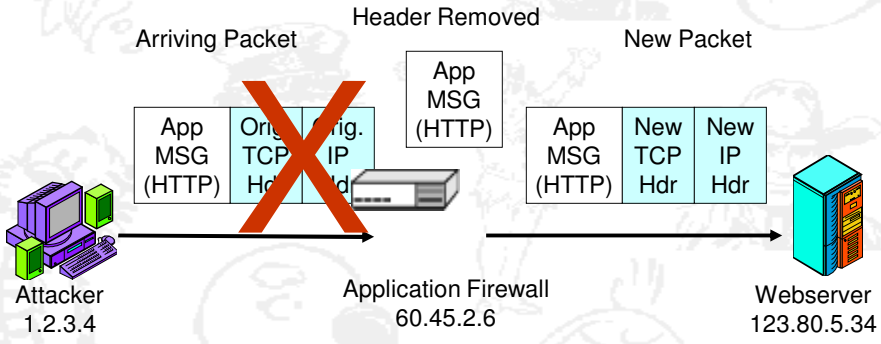
Application Firewall Operation



Application Firewall Operation

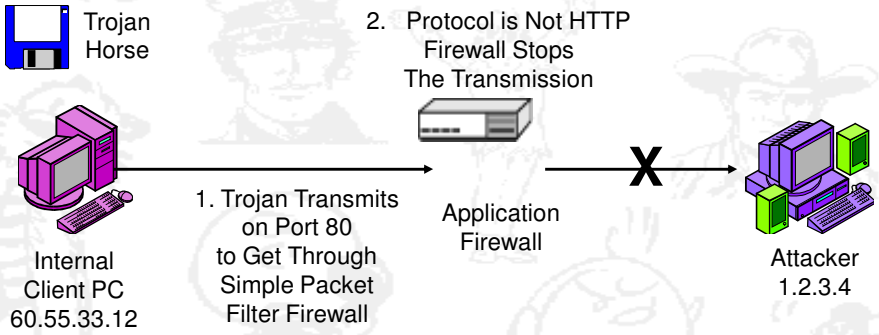


Header Destruction With Application Firewalls



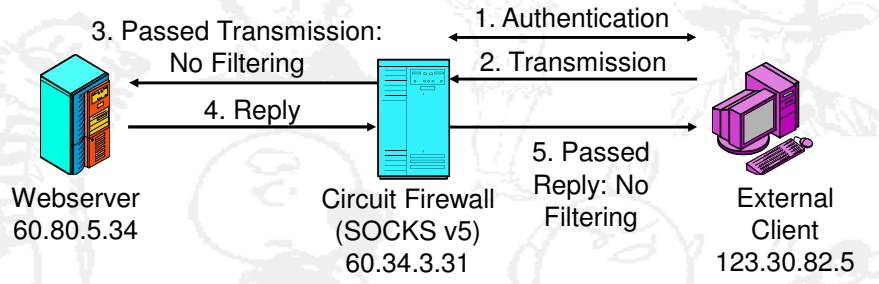
Application Firewall Strips Original Headers from Arriving Packets
Creates New Packet with New Headers
This Stops All Header-Based Packet Attacks

Protocol Spoofing



Circuit Firewall

Generic Type of Application Firewall



Firewalls

New

- Firewall Hardware and Software
- Inspection Methods
  - » Static Packet Inspection
  - » Stateful Packet Inspection
  - » NAT
  - » Application Firewalls
  - » **IPSs**
- Firewall Architecture
- Configuring, Testing, and Maintenance

Intrusion Prevention System (IPS)

- Provide More Sophisticated Inspection
- Examine Streams of Packets
  - » Look for patterns that cannot be diagnosed by looking at individual packets (such as denial-of-service attacks)
  - » And cannot be diagnosed by simply accepting packets that are part of a connection
- Do Deep Packet Inspection
  - » Examine all headers at all layers
    - – network, transport, and application

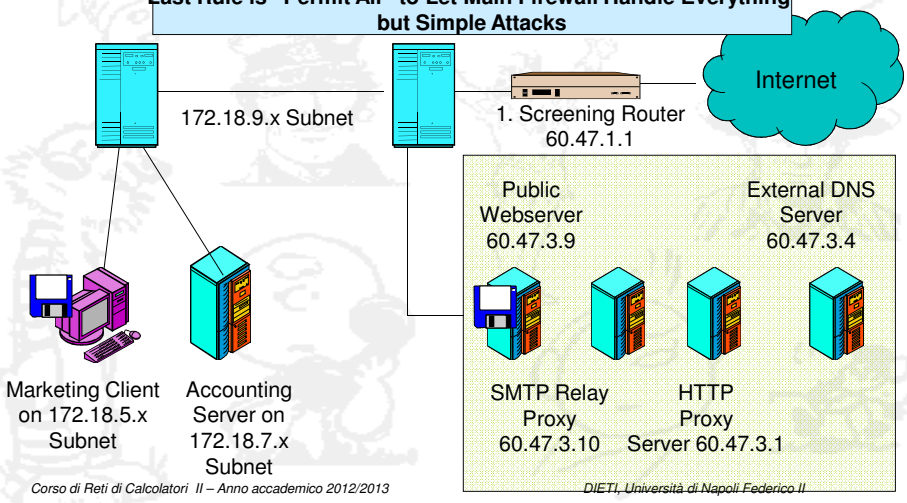
Intrusion Prevention System (IPS)

- IPSs Act Proactively
  - » Once an attack is diagnosed, future packets in the attacks are blocked
  - » This frightens many firms because if an IPS acts incorrectly, it effectively generates a self-serve denial-of-service attack
  - » First use of IPSs may only permit the most definitively identifiable attacks to be blocked, such as SYN flood denial of service attacks

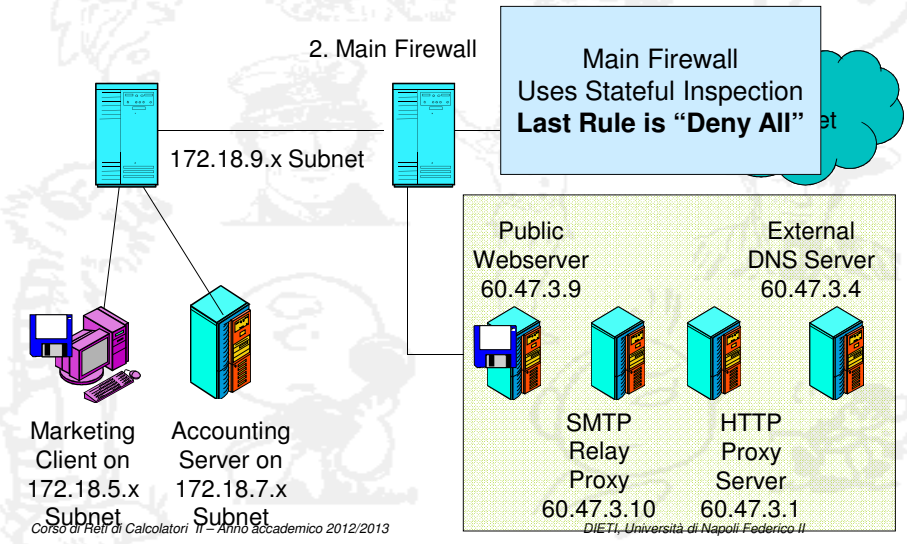
Firewalls

- Types of Firewalls
- Inspection Methods
- Firewall Architecture
  -  » Single site in large organization
  - » Home firewall
  - » SOHO firewall router
  - » Distributed firewall architecture
- Configuring, Testing, and Maintenance

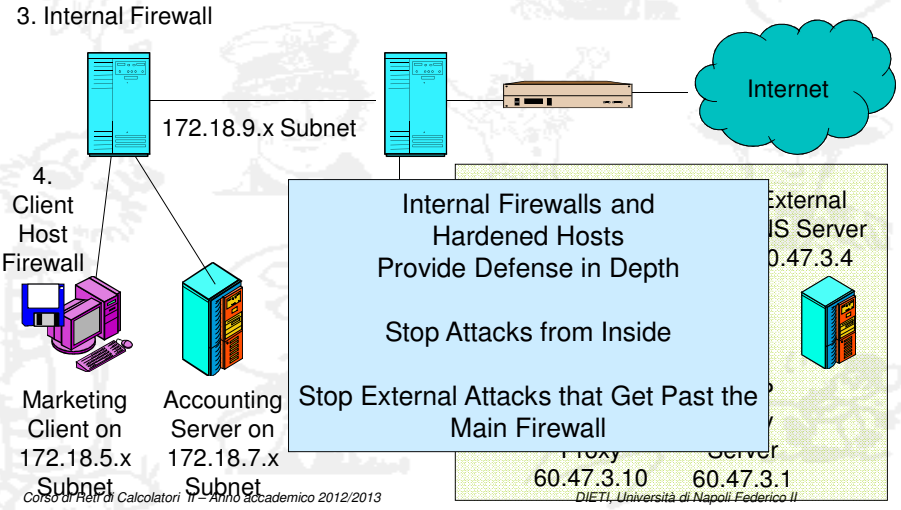
Single-Site Firewall Architecture for a Larger Firm with a Single Site



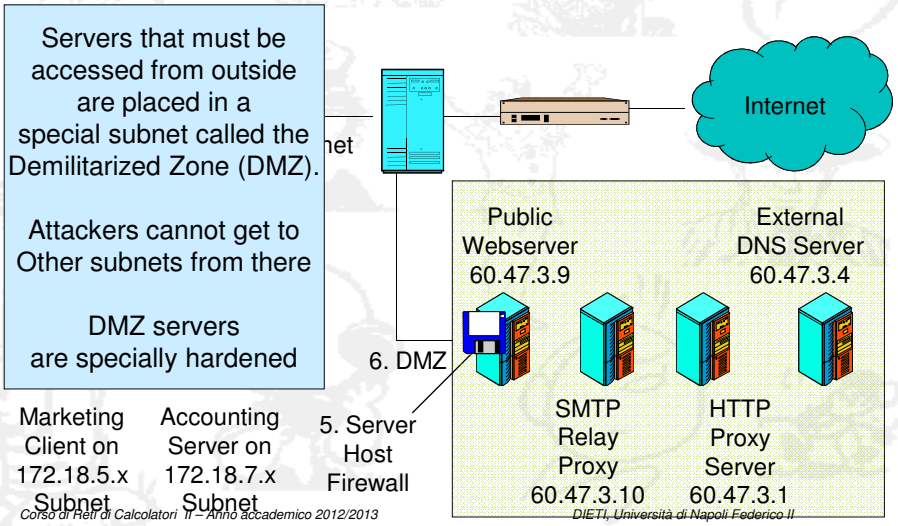
Single-Site Firewall Architecture for a Larger Firm with a Single Site



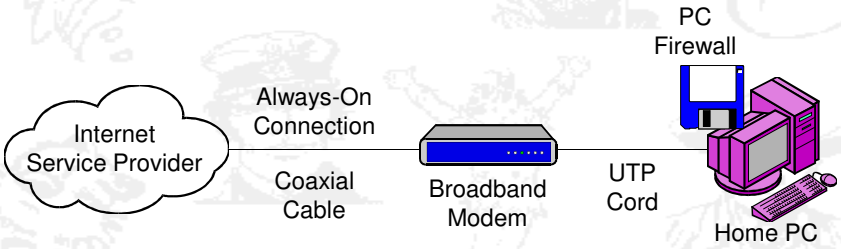
Single-Site Firewall Architecture for a Larger Firm with a Single Site



Single-Site Firewall Architecture for a Larger Firm with a Single Site



Home Firewall

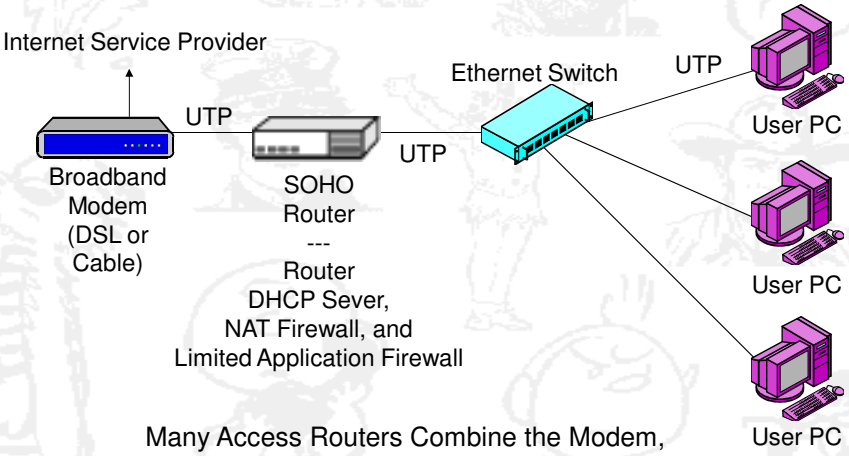


Windows has an internal firewall

Originally called the Internet Connection Firewall
Disabled by default

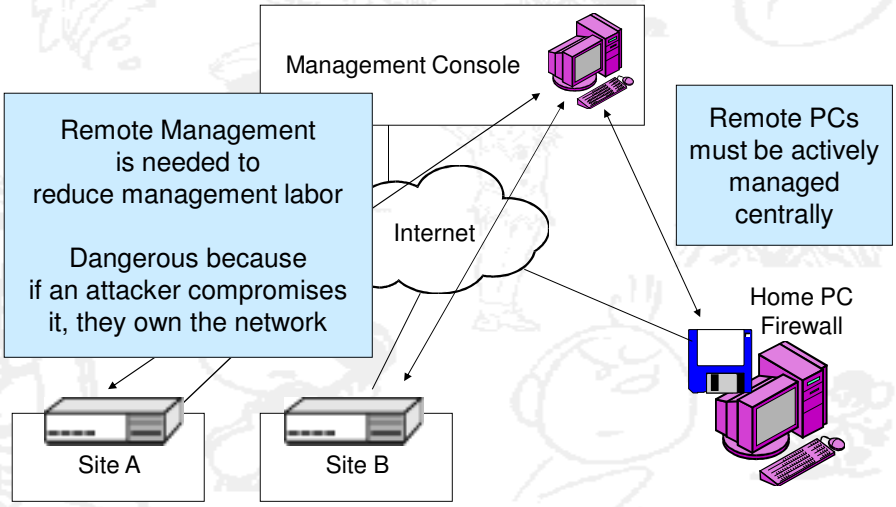
After called the Windows Firewall
Enabled by default

SOHO Firewall Router



Many Access Routers Combine the Modem, Router and Ethernet Switch in a Single Box

Distributed Firewall Architecture



Firewalls

- Types of Firewalls
- Inspection Methods
- Firewall Architecture
- Configuring, Testing, and Maintenance

Configuring, Testing, and Maintaining Firewalls

- Firewall Misconfiguration is a Serious Problem
  - » ACL rules must be executed in series
  - » Easy to make misordering problems
  - » Easy to make syntax errors

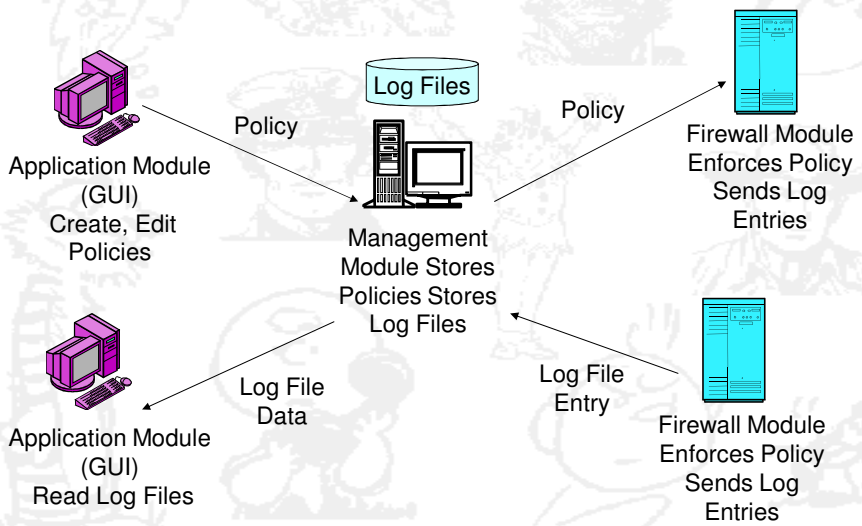
Configuring, Testing, and Maintaining Firewalls

- Create Policies Before ACLs
  - » Policies are easier to read than ACLs
  - » Can be reviewed by others more easily than ACLs
  - » Policies drive ACL development
  - » Policies also drive testing

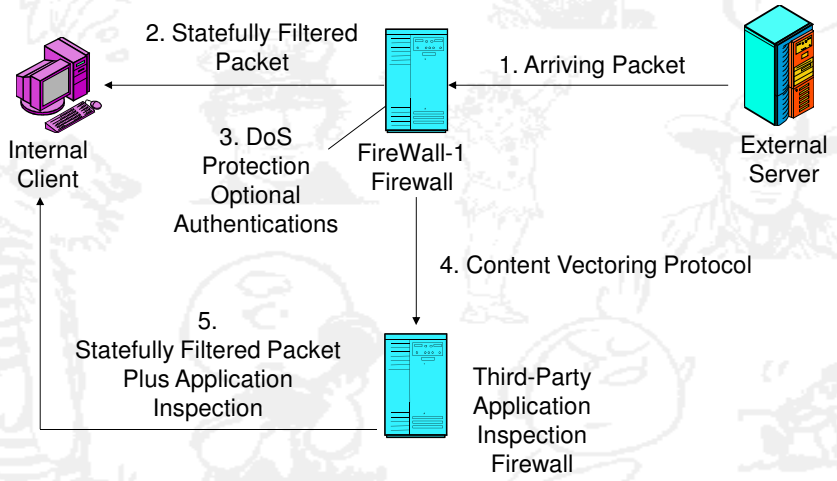
Configuring, Testing, and Maintaining Firewalls

- Must test Firewalls with Security Audits
  - » Attack your own firewall based on your policies
  - » Only way to tell if policies are being supported
- Maintaining Firewalls
  - » New threats appear constantly
  - » ACLs must be updated constantly if firewall is to be effective

FireWall-1 Modular Management Architecture



FireWall-1 Service Architecture



Security Level-Based Stateful Filtering in PIX Firewalls