IPv6 Firewalls

ITU/APNIC/MICT IPv6 Security Workshop

8th – 12th May 2017

Bangkok

Last updated 17th May 2016

Acknowledgements

- Contains material from
  - Stallings and Brown (2015)
  - Ian Welch (Victoria University of Wellington)

What is a Firewall?

- **Design goals (Bellovin and Cheswick 1994)**
  - All traffic from inside to outside, and vice versa, must pass through the firewall
  - Only authorized traffic as defined by the local security policy will be allowed to pass
  - The firewall itself is immune to penetration

The Need for Firewalls

- Host within an organisation need access to and potentially from the Internet
- But our hosts have vulnerabilities
  - we might not want to or be able to patch them
- We might want to control what internal hosts can access in the outside world
- Firewall acts as filter at network perimeter
  - Single choke point to impose security and auditing
- Routers were used in adhoc way to drop unwanted traffic
- Dedicated firewalls from late 1980s

What is a Firewall?

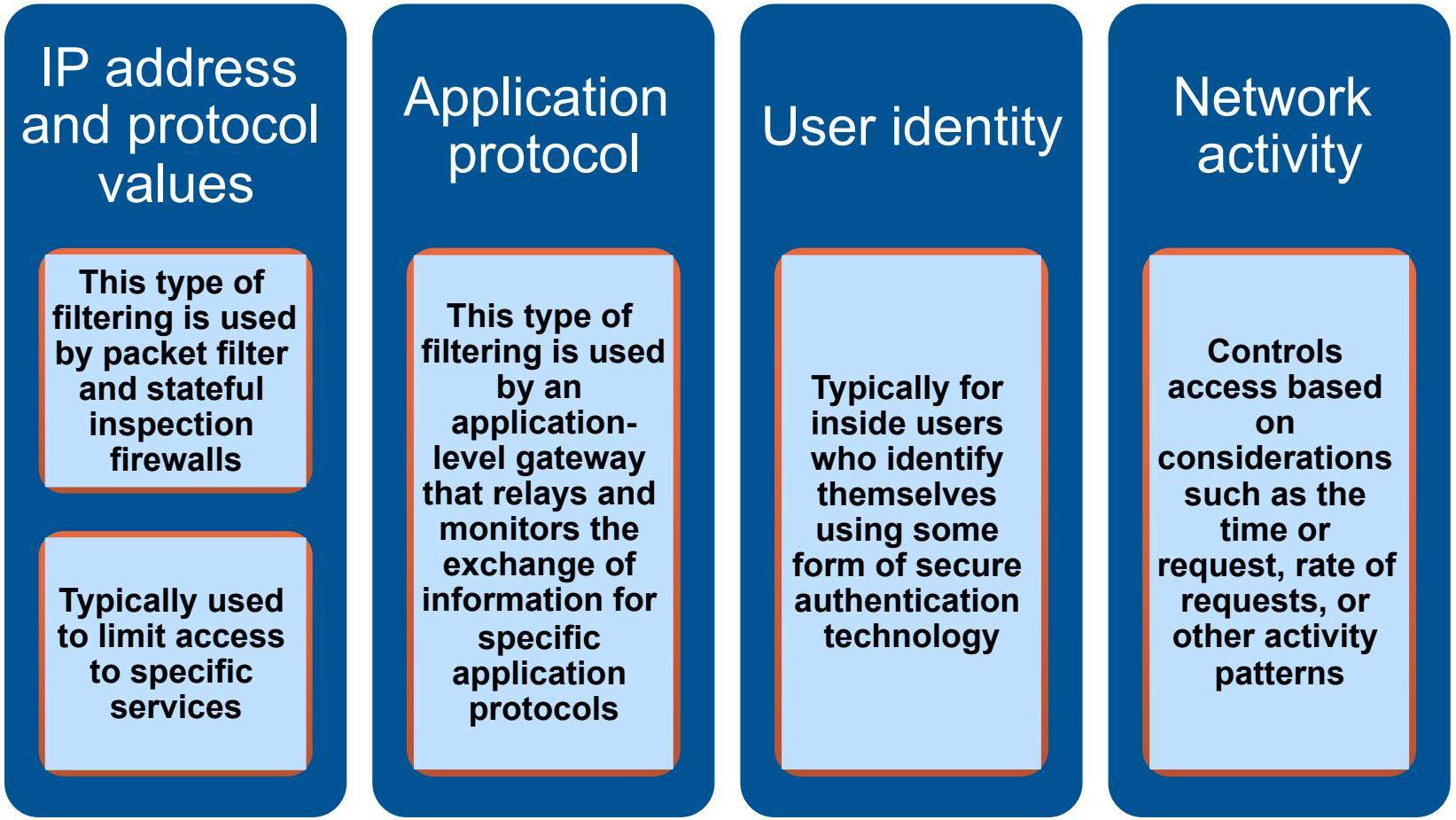
- Firewalls can be found anywhere:
  - On your laptop OS
  - On routers
  - On server OS
  - On network hardware appliances

Firewall Access Policy

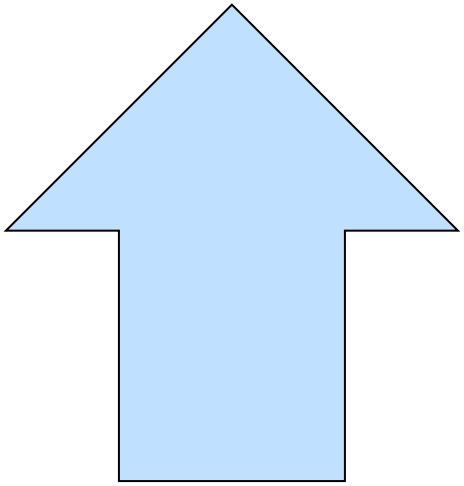
- Access policy defines what traffic is allowed.
  - What host?
  - What protocol layer?
  - What applications?
  - What content?
- **Not just a technical decision.**
- Details of what traffic is allowed pass depends also on where the firewall relative to the rest of the network
- Tradeoff:
  - Too broad a set of rules means potentially slow performance or annoyed users.
  - Too specific means that access might allowed that shouldn't
- Cannot set and forget
  - Changes in the set of hosts on the network or connectivity might lead to changes in the access policy

Firewall Filter Characteristics

Characteristics that a firewall access policy could use to filter traffic include:

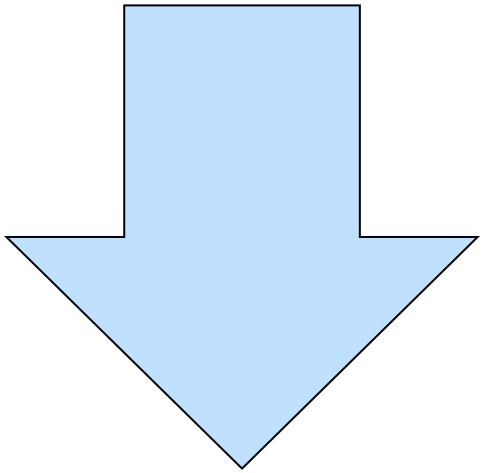


Firewall Capabilities And Limits



Capabilities:

- **Defines a single choke point**
- **Provides a location for monitoring security events**
- **Convenient platform for several Internet functions that are not security related**
- **Can serve as the platform for IPSec**



Limitations:

- **Cannot protect against attacks bypassing firewall**
- **May not protect fully against internal threats**
- **Improperly secured wireless LAN can be accessed from outside the organization**
- **Laptop, PDA, or portable storage device may be infected outside the corporate network then used internally**

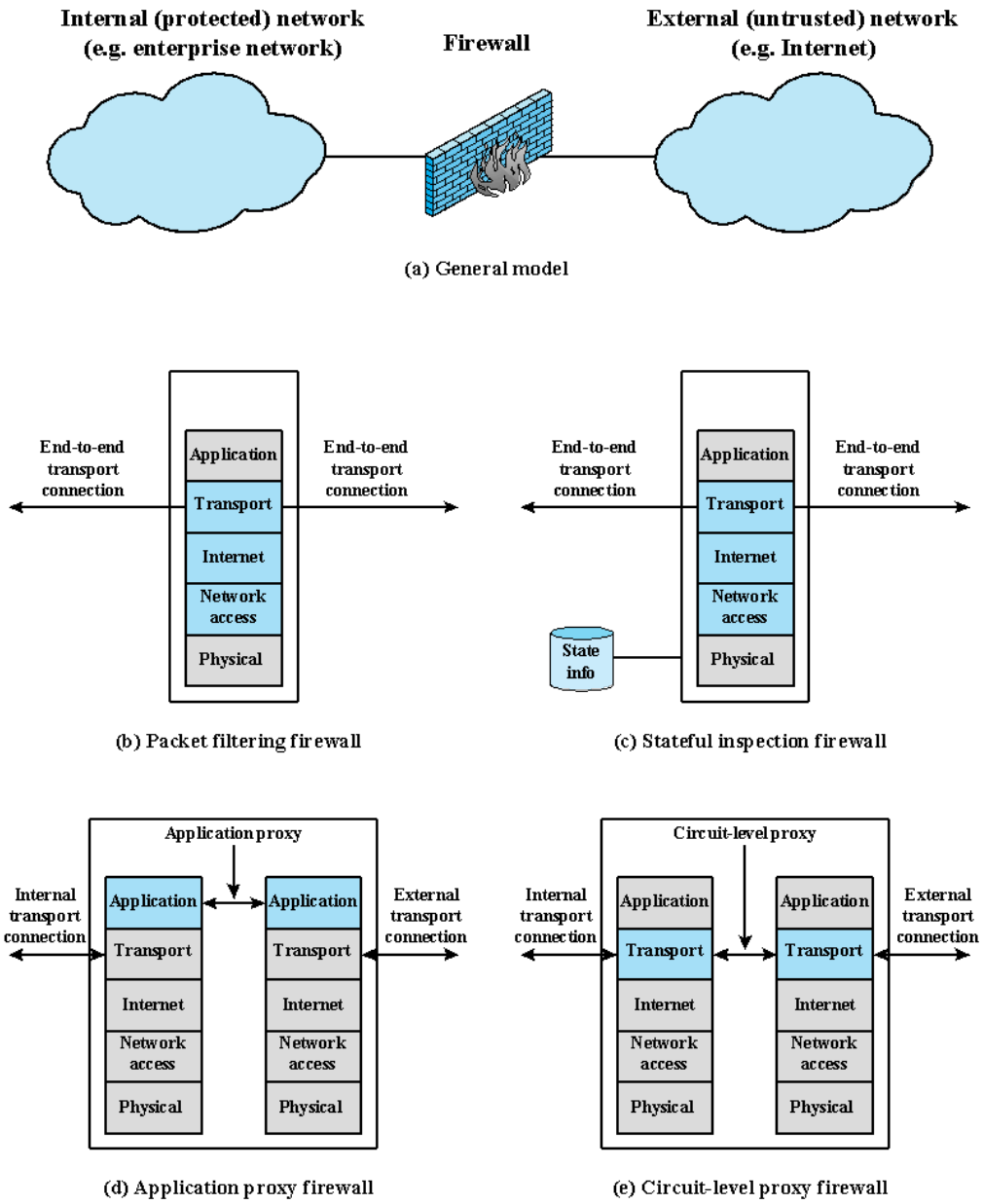


Figure 9.1 Types of Firewalls

Types of firewalls

- Packet Filters
  - Analyze network packets and decide a course of action based on configuration
- Stateful Filters
  - Track network “conversations” and maintain a table of which connections are in an active conversations
- Application layer
  - Layer 7 firewalls are able to detect if an unwanted protocol is attempting to bypass the firewall on an allowed port

Keeping State vs Stateless

- Stateful inspection refers to ability to track the state, or progress, of a network connection
- By storing information about each connection in a state table, a firewall is able to quickly determine if a packet passing through the firewall belongs to an already established connection.
- If it does, it is passed through the firewall without going through ruleset evaluation saving time and avoiding extra processing.

Typical features of a Firewall

- Rule Syntax
- NAT control
- Able to pass, redirect or drop traffic based on the rules
- Logging feature – to allow audit of activities and of traffic
- Stateful inspection – not all and may need to be enabled with extra config options
- Ability to be either inclusive or exclusive
  - An exclusive firewall allows all traffic through except for the traffic matching the ruleset (default is to allow)
  - An inclusive firewall does the reverse (default is to block)

What Firewalls Can Do

- Implement filters to protect networks from the wider Internet
- Implement filters to protect the Internet from a network's users
- Selective blocking of sources or destinations
- Inspection of content
- Address Translation for IPv4
- NB: Routers can do all of the above too!

What Firewalls Cannot Do

- Block spam, worms, malware and other malicious content
  - Users will find ways of circumventing L7 inspection
- Look inside encrypted links
  - VPNs, HTTPS,…
- Block Denial of Service Attacks
  - DOS attacks more than fill access links
  - RTBH and support of upstream network operator is the only way

Firewalls on Routers

- Can be simple packet filters on egress and ingress interfaces
  - Typically used to block
    - Unwanted traffic (IP destination)
    - Unwanted traffic (TCP/UDP/… destination)
    - Access to the router control plane
    - Specific internal or external destinations according to corporate policy
- Can be a "Firewall Feature" part of the router operating system
  - Operates as a L7 filter, able to look inside packets

Router Packet Filters:

- Example:
  - Packet filter application to a router interface
  - Most common application of firewall for any network

```
interface GigabitEthernet0/1
 description ISP link
 bandwidth 1548
 ip address 192.168.10.2 255.255.255.252
 ip access-group ipv4-in in
 ip access-group ipv4-out out
 ip verify unicast reverse-path
 ipv6 address 2001:DB8:34:10::1/127
 ipv6 verify unicast reverse-path
 ipv6 traffic-filter ipv6-in in
 ipv6 traffic-filter ipv6-out out
```

Router Packet Filters:

- IPv6 Access List
  - Example

```
ipv6 access-list ipv6-in
 deny tcp any any eq telnet
 deny tcp any any eq 135
 deny tcp any any eq 139
 deny tcp any any eq 445
 permit icmp any any
 permit tcp any any established
 permit tcp any any eq 22
 permit tcp any any eq www
 permit tcp any any eq domain
 permit udp any any eq domain
 permit udp any any gt 1023
 ...
 deny ipv6 any any log
!
ipv6 access-list ipv6-out
 permit icmp any any
 deny udp any any eq netbios-ns
 deny udp any any eq netbios-dgm
 permit ipv6 any any
!
```

Host Packet Filters

- IP6tables on a Linux host:
  - Allows DNS queries and incoming SSH

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p ipv6-icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p udp -m udp --dport 631 -j ACCEPT
-A INPUT -p udp -m udp --dport 53 -j ACCEPT
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp6-adm-prohibited
-A FORWARD -j REJECT --reject-with icmp6-adm-prohibited
COMMIT
```

Dedicated Firewall Devices

- Many equipment vendors offer all levels of Firewall product:
  - Small office/home office
    - Usually just a router!
  - Enterprises
    - Multi-megabits per second with dedicated hardware to speed up the processing of packets
  - DataCentres
    - Capable of multi-Gigabits per second
    - Multiple interfaces and support for multiple VLANs

Dedicated Firewall Devices

- Firewalls can be located:
  - Inline – the device sits between core and border routers, and takes an active part in the routing system
  - Transparent – physically inline between core and border routers but is "invisible" to the end user

Packet Filtering Firewall

Applies rules to each incoming and outgoing IP packet

- Typically a list of rules based on matches in the IP or TCP header
- **Forwards or discards** the packet based on rules match

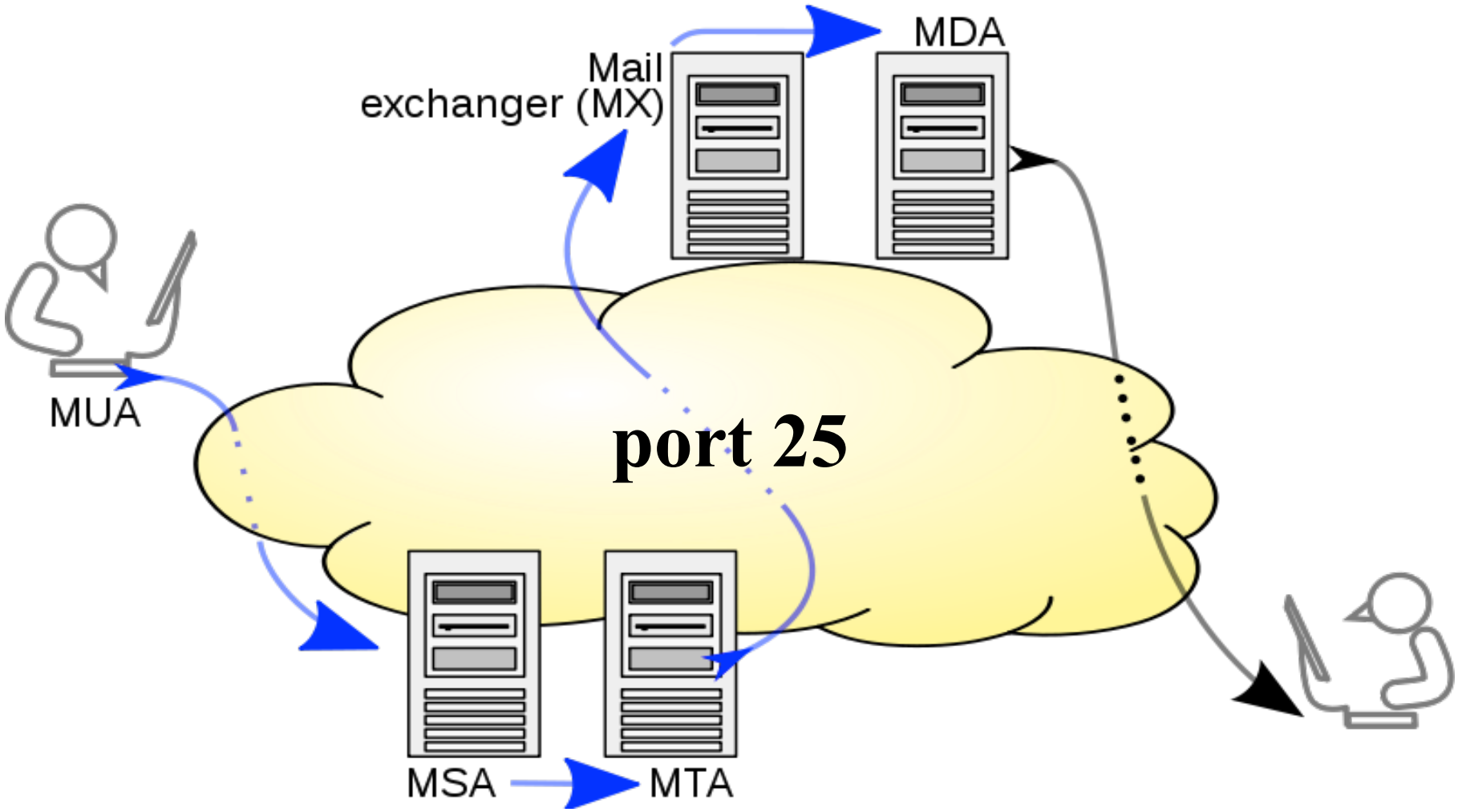
Filtering rules are based on information contained in a network packet

- Source IP address
- Destination IP address
- Source and destination transport-level address
- IP protocol field
- Interface

Two default policies:

- Discard - prohibit unless expressly permitted
  - More conservative, controlled, visible to users
- Forward - permit unless expressly prohibited
  - Easier to manage and use but less secure

Example: we want people to be able to send us mail



Example: we want people to be able to send us mail

Every ruleset is followed by an implicit rule reading like this.

action	ourhost	port	theirhost	port	comment
block	*	*	*	*	*default*

Example 1:

Suppose we want to allow inbound mail (SMTP, port 25) but only to our gateway machine. Also suppose that traffic from some particular site SPIGOT is to be blocked.

Solution: 1

action	ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	*we don't trust these people*
allow	OUR-GW	25	*	*	*connection to our SMTP port*

Example 2:

Now suppose that we want to implement the policy "any inside host can send mail to the outside".

Solution: 2

action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	*connection to their SMTP port*

This solution allows calls to come from any port on an inside machine, and will direct them to port 25 on the outside. Simple enough…

So why is it wrong?

So why is this wrong?

- Our defined restriction is based solely on the outside host's port number, which we have no way of controlling.
- Now an enemy can access any internal machines and port by originating his call from port 25 on the outside machine.

- What can be a better solution ?

A Better Solution

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		*our packets to their SMTP port*
allow	*	25	*	*	ACK	*their replies*

- The ACK signifies that the packet is part of an ongoing conversation
- Packets without the ACK are connection establishment messages, which we are only permitting from internal hosts

Security & Performance of Packet Filters

- Tiny fragment attacks
  - Split TCP header info over several tiny packets
  - Either discard or reassemble before check
- Degradation depends on number of rules applied at any point
- Order rules so that most common traffic is dealt with first
- Correctness is more important than speed

Implementation Options

- Packet filters can be implemented using a general purpose computer but this means it can be overwhelmed by packet arrivals
- ASIC (Application Specific Integrated Circuit) architecture.
- Chip optimised for specific functions:
  - used for very fast matching
  - great when can express rules as bitmaps
  - not so great for looking inside a packet

Packet Filter : Advantages And Weaknesses

Advantages

- Simplicity
- Typically transparent to users and are very fast

Weaknesses

- Cannot prevent attacks that employ application specific vulnerabilities or functions
- Limited logging functionality
- Do not support advanced user authentication
- Vulnerable to attacks on TCP/IP protocol bugs
- Improper configuration can lead to breaches

Importance of Context

- Most of the services we want to secure adopt a client-server model (TCP)
- Packet filters can include flags in match rules (for example, ACK)
- Each packet evaluated independently of the context of that packet within a TCP flow
- Can get past a flag rule by generating a fake packet with the flag set
- **What can be a better solution ?**

Each Packet has a Context

- Track flows (active TCP connections) between clients and server.
- Decisions made based upon the history of this current packet with respect to flow
- For example, only allow packet with ACK from a host if is in response to a SYN request sent to the host
- Requires the firewall to maintain state.

Stateful Inspection Firewall

Tightens rules for TCP traffic by creating a directory of outbound TCP connections

- There is an entry for each currently established connection
- Packet filter allows incoming traffic to high numbered ports only for those packets that fit the profile of one of the entries in this directory

Reviews packet information but also records information about TCP connections

- Keeps track of TCP sequence numbers to prevent attacks that depend on the sequence number
- Inspects data for protocols like FTP, IM and SIPS commands

Example Stateful Firewall Connection State Table

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established

Application-Level Gateway

- Also called an application proxy
- Acts as a relay of application-level traffic
  - User contacts gateway using a TCP/IP application
  - User is authenticated
  - Gateway contacts application on remote host and relays TCP segments between server and user
- When relaying the ALG inspects and may modify packets
- For example, CISCO security appliance can enforce maximum domain-name length on requests.

Application-Level Gateway

- Very powerful but requires code for each protocol supported
  - May restrict application features supported
- Tend to be more secure than packet filters
  - Easier to configure rules correctly because fewer of them!
- Disadvantage is the additional processing overhead on each connection

Circuit Level Gateway

- Sets up two TCP connections, one between itself and a TCP user on an inner host and one on an outside host
- Relays TCP segments from one connection to the other without examining contents
- Security function consists of determining which connections will be allowed
- Typically used when internal users are trusted
- May use application-level gateway inbound and circuit-level gateway outbound
- Lower overheads because no further packet inspection done

SOCKS Circuit Level Gateway

- SOCKS v5 defined in RFC1928
- Designed to provide a framework for client-server applications in TCP/UDP domains to conveniently and securely use the services of a network firewall
- Client application contacts SOCKS server, authenticates, sends relay request
- Server evaluates and either establishes or denies the connection

Bastion Hosts

- Computer that is fully exposed to attack.
- Platform for firewalls, gateways or services such as mail, web etc.
  - Common characteristics:
  - Runs secure O/S, only essential services
  - May require user authentication to access proxy or host
  - Each proxy can restrict features, hosts accessed
  - Each proxy is small, simple, checked for security
  - Each proxy is independent, non-privileged
  - Limited disk use, hence read-only code
- External firewalls are bastion host you buy, others are ones you make.

Host-Based Firewalls

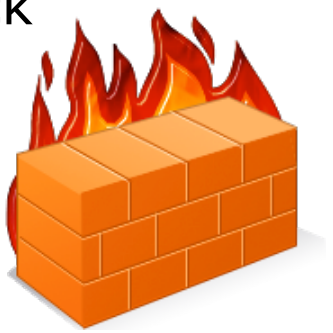
- Used to secure an individual host
- Available in operating systems or can be provided as an add-on package
- Filter and restrict packet flows
- Common location is a server

Advantages:

- Filtering rules can be tailored to the host environment
- Protection is provided independent of topology
- Provides an additional layer of protection

Personal Firewall

- Controls traffic between a personal computer or workstation and the Internet or enterprise network
- For both home or corporate use
- Typically is a software module on a personal computer
- Can be housed in a router that connects all of the home computers to a DSL, cable modem, or other Internet interface
- Typically much less complex than server-based or stand-alone firewalls
- Primary role is to deny unauthorized remote access
- May also monitor outgoing traffic to detect and block worms and malware activity



Distributed Firewall

- Stand-alone firewalls PLUS host-based firewalls
- Single point of administration.
- Increases manageability.
- Can collect audit logs to provide network wide view.
- Simplifies having multiple segments
- Figure shows an extra segment (External DMZ network)

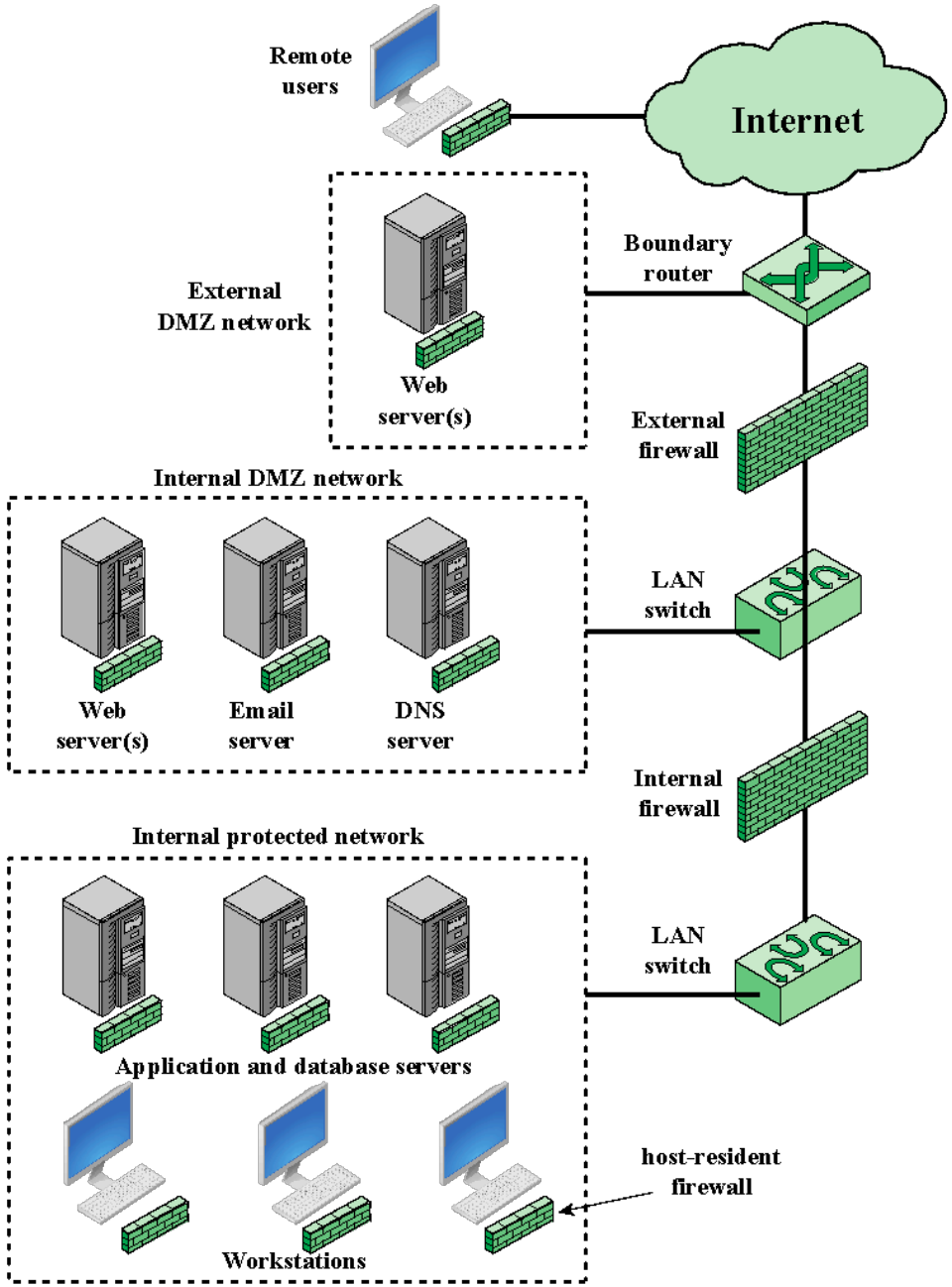


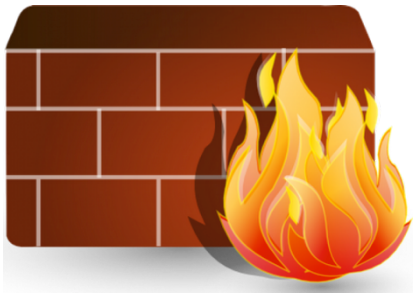
Figure 9.4 Example Distributed Firewall Configuration

Firewall Technologies

Host-resident firewall	• Includes personal firewall software and firewall software on servers
Screening router	• Single router between internal and external networks with stateless or full packet filtering
Single bastion inline	• Single firewall device between an internal and external router
Single bastion T	• Has a third network interface on bastion to a DMZ where externally visible servers are placed
Double bastion inline	• DMZ is sandwiched between bastion firewalls
Double bastion T	• DMZ is on a separate network interface on the bastion firewall
Distributed firewall configuration	• Used by large businesses and government organizations

Summary

- The need for firewalls
- Firewall characteristics and access policy
- Types of firewalls
  - Packet filtering firewall
  - Stateful inspection firewalls
  - Application-level gateway
  - Circuit-level gateway
- Firewall basing
  - Bastion host
  - Host-based firewalls
  - Personal firewall



- Firewall location and configurations
  - DMZ networks
  - Virtual private networks
  - Distributed firewalls
  - Firewall locations and topologies

IPv6 Firewalls

ITU/APNIC/MICT IPv6 Security Workshop

8th – 12th May 2017

Bangkok