Τείχη προστασίας

Νικόλαος Ε. Κολοκοτρώνης
Επίκουρος Καθηγητής

Τμήμα Πληροφορικής και Τηλεπικοινωνιών
Πανεπιστήμιο Πελοποννήσου
Email: nkolok@uop.gr
Web: http://www.uop.gr/~nkolok/

ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ

Περιεχόμενα

Περιεχόμενα

- The need for firewalls
- Firewall characteristics
- Types of firewalls
- Firewall basing
- Firewall configurations

The need for firewalls

- Internet connectivity is no longer optional for business
  - Individual users in any organization need Internet access
- Internet access provides benefits to an organization, but it enables the outside world to reach and interact with local network assets
  - This creates a threat to the organization
  - While it is possible to equip each workstation and server on the premises network with strong security features, this may not be sufficient and in some cases is not cost-effective

Firewalls at a glance

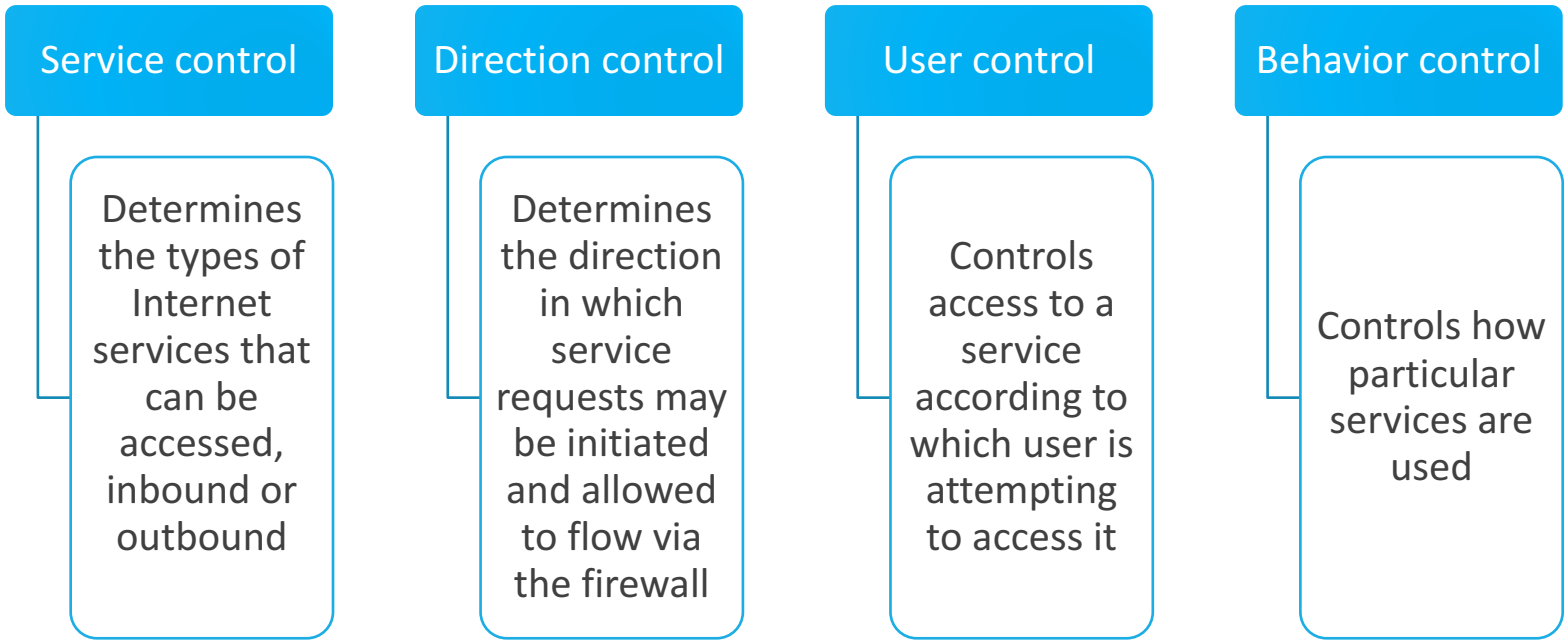
- An alternative, or at least complement, to host-based security services
- Inserted between local network and the Internet to set a controlled link and erect a security wall or perimeter
  - The aim of this perimeter is to protect the premises network from Internet-based attacks and to provide a single choke point where security and auditing can be imposed
- May be a single computer system or a set of two or more systems that cooperate to perform the firewall function

Firewall design goals

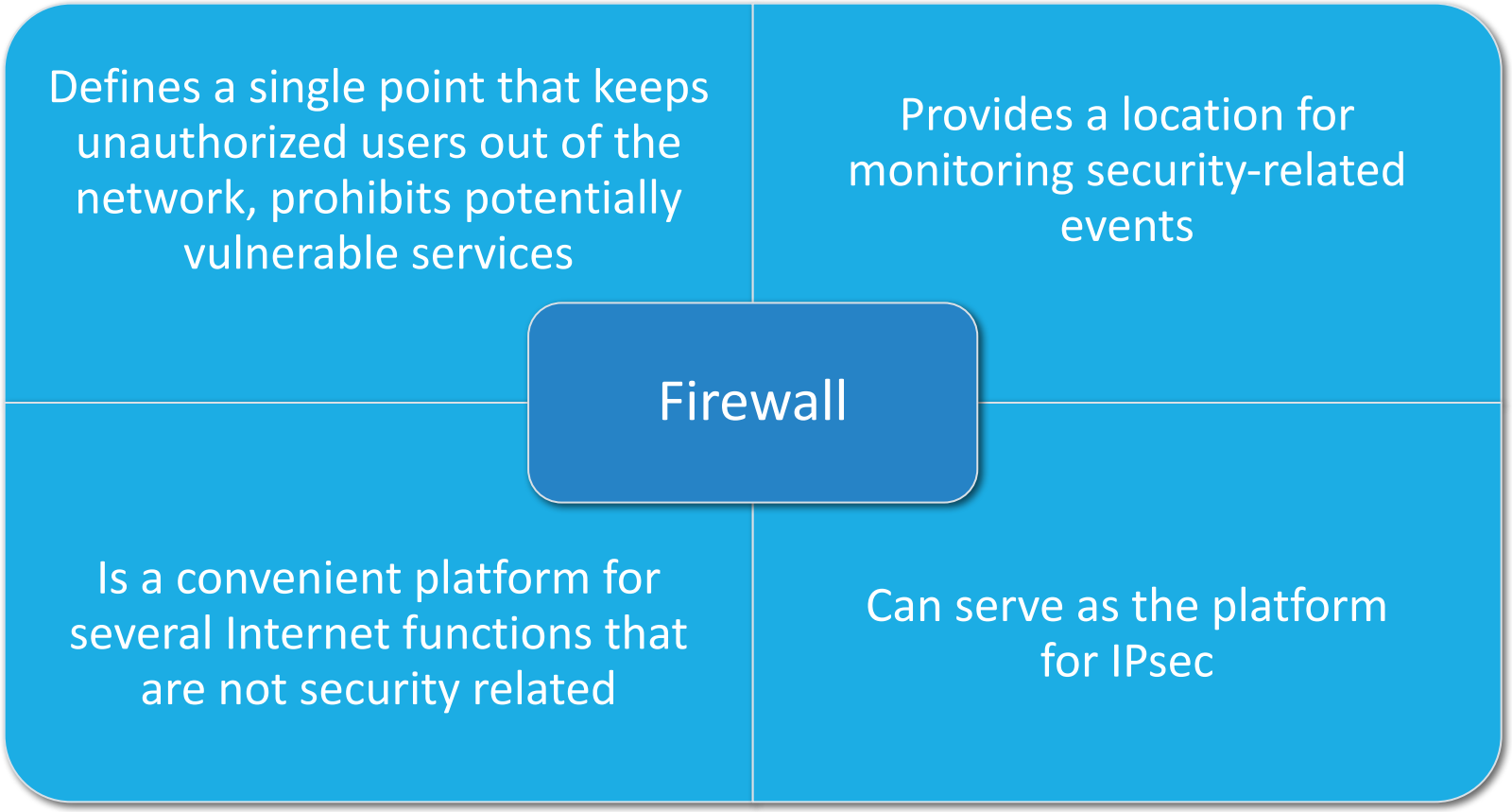
- All traffic from inside to outside, and vice versa, must pass through the firewall
- Only authorized traffic, as defined by the local security policy, will be allowed to pass
- The firewall itself is immune to penetration

Firewall techniques

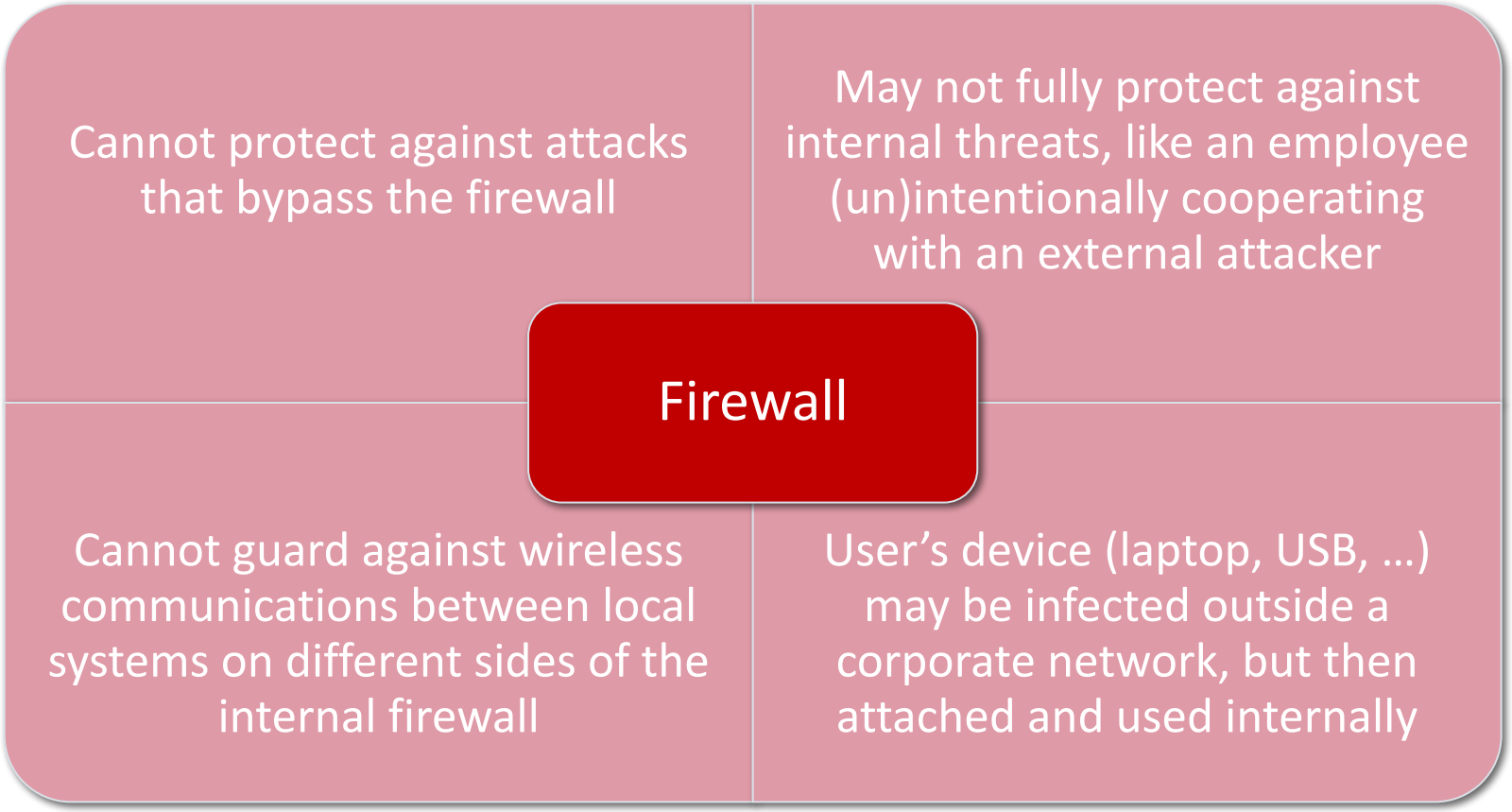
- Techniques that firewalls use to control access and enforce the site's security policy include



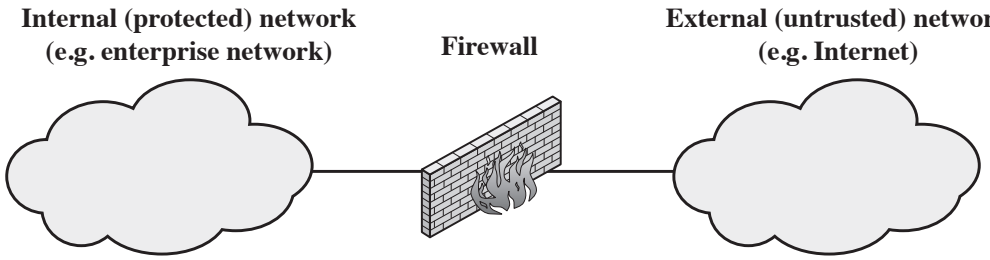
Firewall expectations



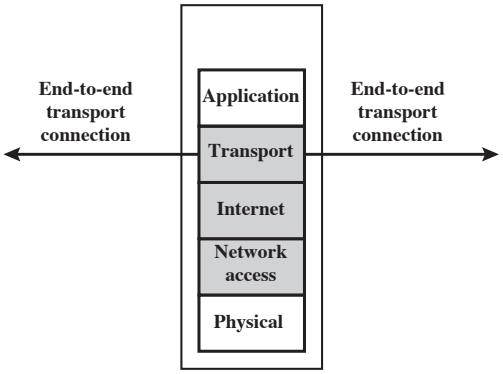
Firewall limitations



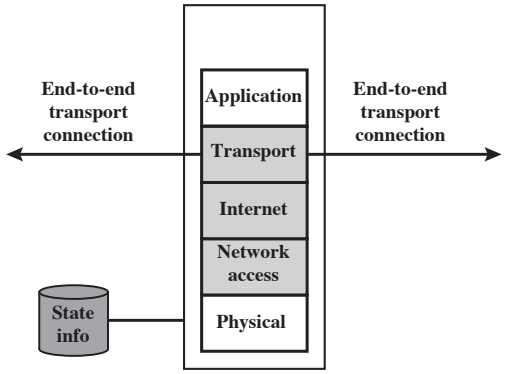
Types of firewalls



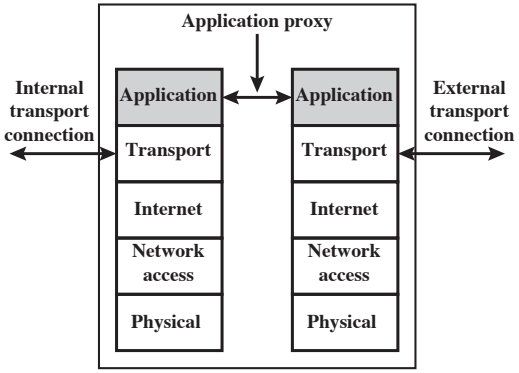
(a) General model



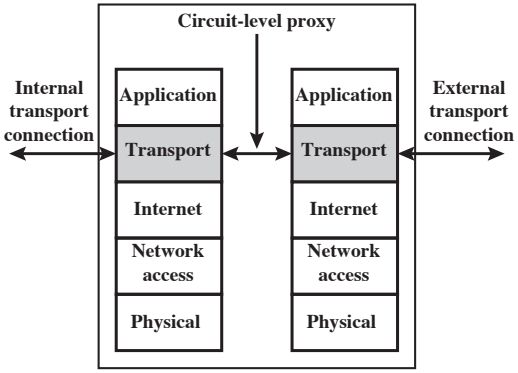
(b) Packet filtering firewall



(c) Stateful inspection firewall



(d) Application proxy firewall



(e) Circuit-level proxy firewall

Firewall policies

- Default forward policy
  - Allows all traffic; you add a rule to block a certain type of traffic
  - Increases ease of use for end users but provides reduced security
  - Security admin must react to new security threats as they arise
- Default discard policy
  - More conservative, everything is blocked (no traffic is allowed); you add rules to allow only certain types of traffic
  - Services must be added on a case-by-case basic
  - More visible to users who may see the firewall as an obstacle

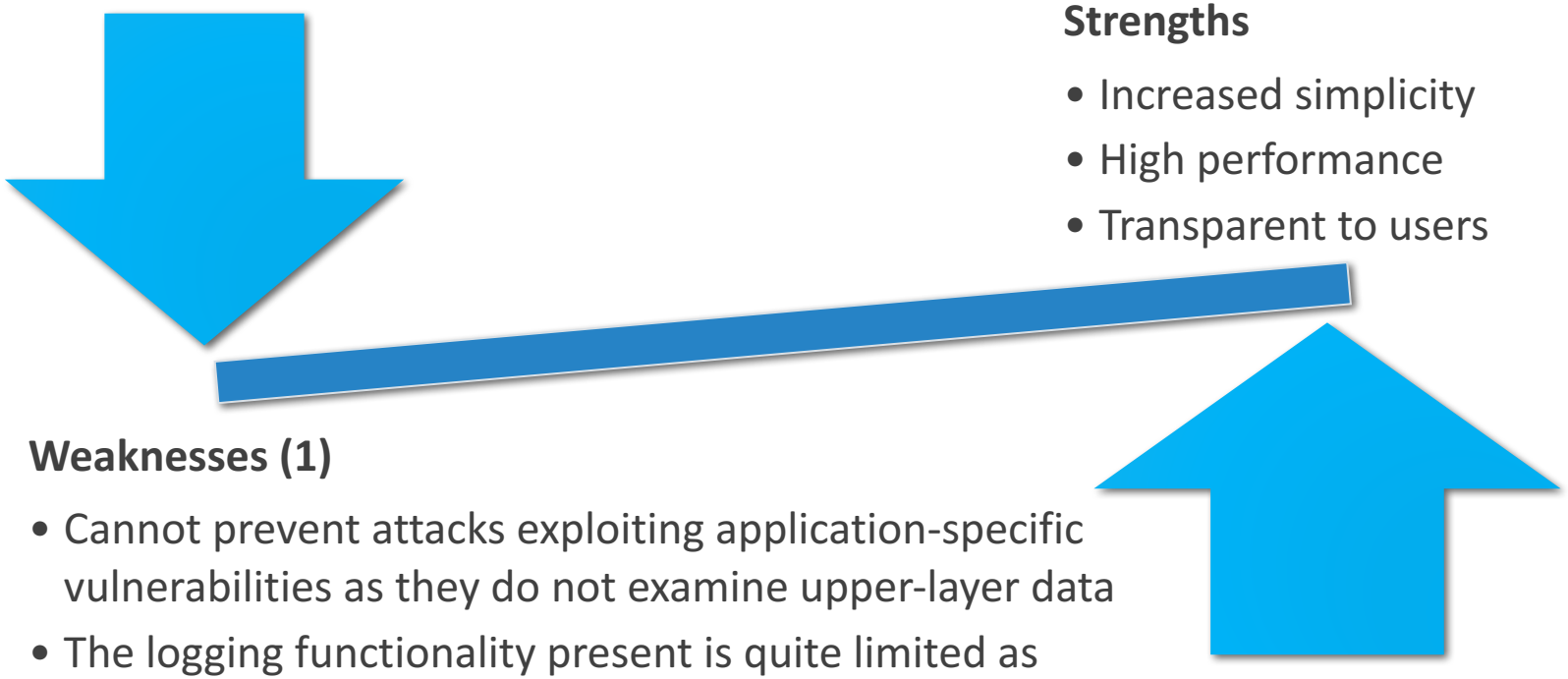
Packet filtering firewall

- Filtering rules are based on info contained in IP header
  - Source IP address: The IP address of the system that originated the IP packet (e.g., 192.178.1.1)
  - Destination IP address: The IP address of the system the IP packet is trying to reach (e.g., 192.168.1.2)
  - Source /destination transport level address: The transport-level (TCP or UDP) port number, which defines apps like SNMP or TELNET
  - IP protocol field: Defines the transport protocol
  - Interface: which interface of the firewall the packet came from or is destined to (if the firewall has three or more ports)

Packet filtering example

Rule	Direction	Src address	Dest addresss	Protocol	Dest port	Action
A	In	External	Internal	TCP	25	Permit
B	Out	Internal	External	TCP	>1023	Permit
C	Out	Internal	External	TCP	25	Permit
D	In	External	Internal	TCP	>1023	Permit
E	Either	Any	Any	Any	Any	Deny

Packet filtering firewalls



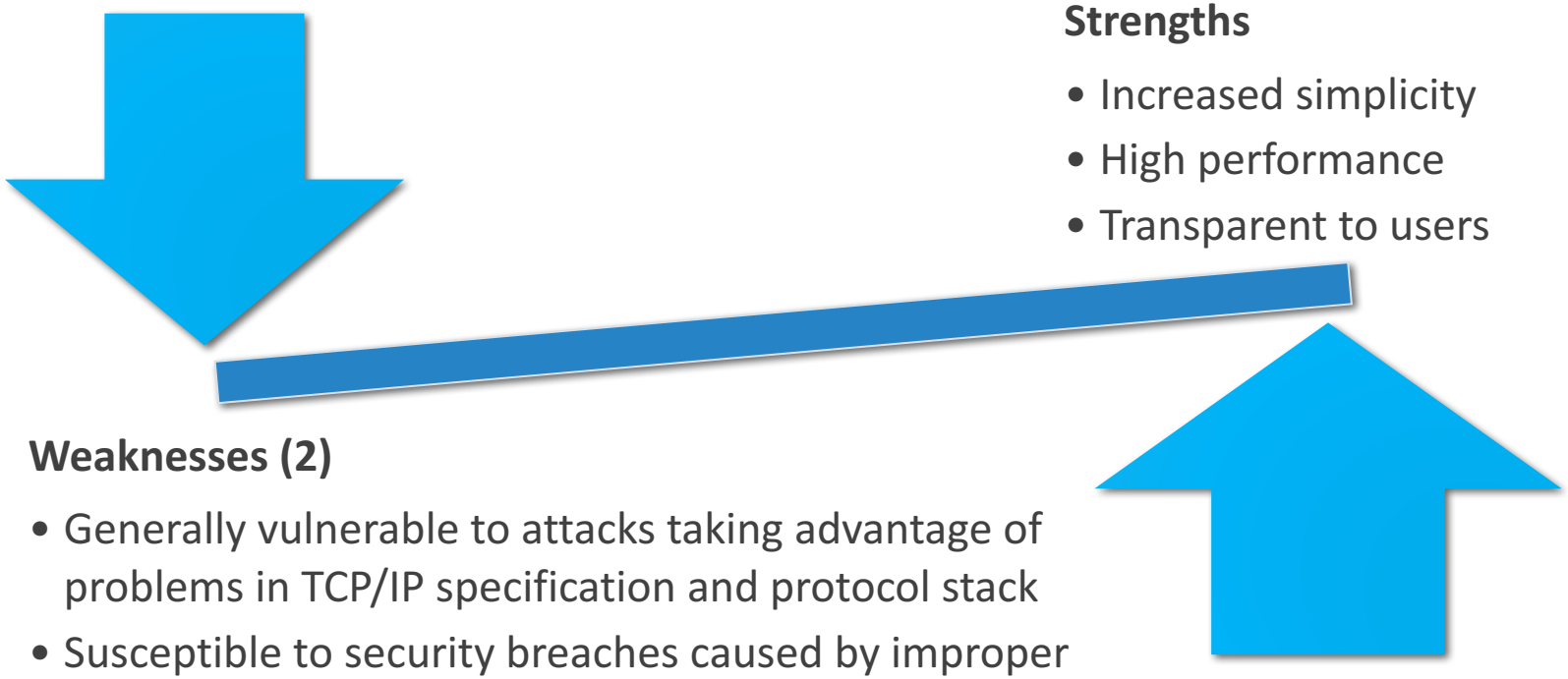
Strengths

- Increased simplicity
- High performance
- Transparent to users

Weaknesses (1)

- Cannot prevent attacks exploiting application-specific vulnerabilities as they do not examine upper-layer data
- The logging functionality present is quite limited as little information is available to the firewall
- Mostly do not support advanced user authentication

Packet filtering firewalls



Strengths

- Increased simplicity
- High performance
- Transparent to users

Weaknesses (2)

- Generally vulnerable to attacks taking advantage of problems in TCP/IP specification and protocol stack
- Susceptible to security breaches caused by improper configurations due to the small number of variables used in access control decisions

Attacks and countermeasures

IP address spoofing

Intruder transmits packets from the outside with source IP address that of an internal host

Countermeasure is to discard packets with inside source address if they arrive on ext. interface

Source routing attacks

Intruder specifies a route for a packet to bypass security tools not analyzing routing information

Countermeasure is to discard all packets that use this option

Tiny fragment attacks

Intruder uses the IP fragmentation to force the TCP header into to a separate packet fragment

Countermeasure is to enforce the first fragment of a packet having a min amount of transport header

Stateful firewall connection states

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.22.88.29	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
2122.22.123.32	2112	192.168.1.6	80	Established
210.922.212.18	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 *application proxy*
- Acts as a relay of application-level traffic
  - If the gateway does not implement the proxy code for an app, the service is not supported and cannot be forwarded via the firewall
  - Can be configured to support only specific features of an app that the security admin considers acceptable (denying the rest)
- Tends to be more secure than packet filters
- Disadvantages
  - The additional processing overhead on each connection

Circuit level gateway

- Also called *circuit-level proxy*
- Can be a stand-alone system or can be performed by an application-level gateway for certain applications
- Does not permit an end-to-end TCP connection
  - The security function determines which connections are allowed
  - Typical use is the case where security admin trusts internal users
  - Can be configured to support application-level or proxy service on inbound connections and circuit-level functions for outbound
- Example of implementation is the SOCKS package

Circuit level gateway: SOCKS

- SOCKS (RFC 1928) consists of the following components
  - The SOCKS server, which often runs on a UNIX-based firewall (also implemented on Windows systems)
  - The SOCKS client library, which runs on internal hosts protected by the firewall
  - SOCKS-ified versions of standard client programs such as FTP and TELNET; implementation of SOCKS protocol involves either
    - the recompilation or relinking of TCP-based client applications, or
    - the use of alternate dynamically loaded libraries, to use the appropriate encapsulation routines in the SOCKS library.

Bastion host

- A system identified by the firewall administrator as a critical strong point in the network's security
  - Executes a secure version of its operating system, making it a hardened system
  - Only the services that the network administrator considers essential are installed
  - May require additional authentication before a user is allowed access to the proxy services
- Typically serves as a platform for an application-level or circuit-level gateway

Bastion host

Common characteristics

- Each proxy is configured to support only a subset of the standard application's command set
- Each proxy is configured to allow access only to specific host systems
- Each proxy maintains detailed audit information by logging all traffic, each connection, and the duration of each connection
- Each proxy module is a very small software package specifically designed for network security
- Each proxy is independent of other proxies on the bastion host
- A proxy generally performs no disk access other than to read its initial configuration file
- Each proxy runs as a nonprivileged user in a private and secured directory on the bastion host

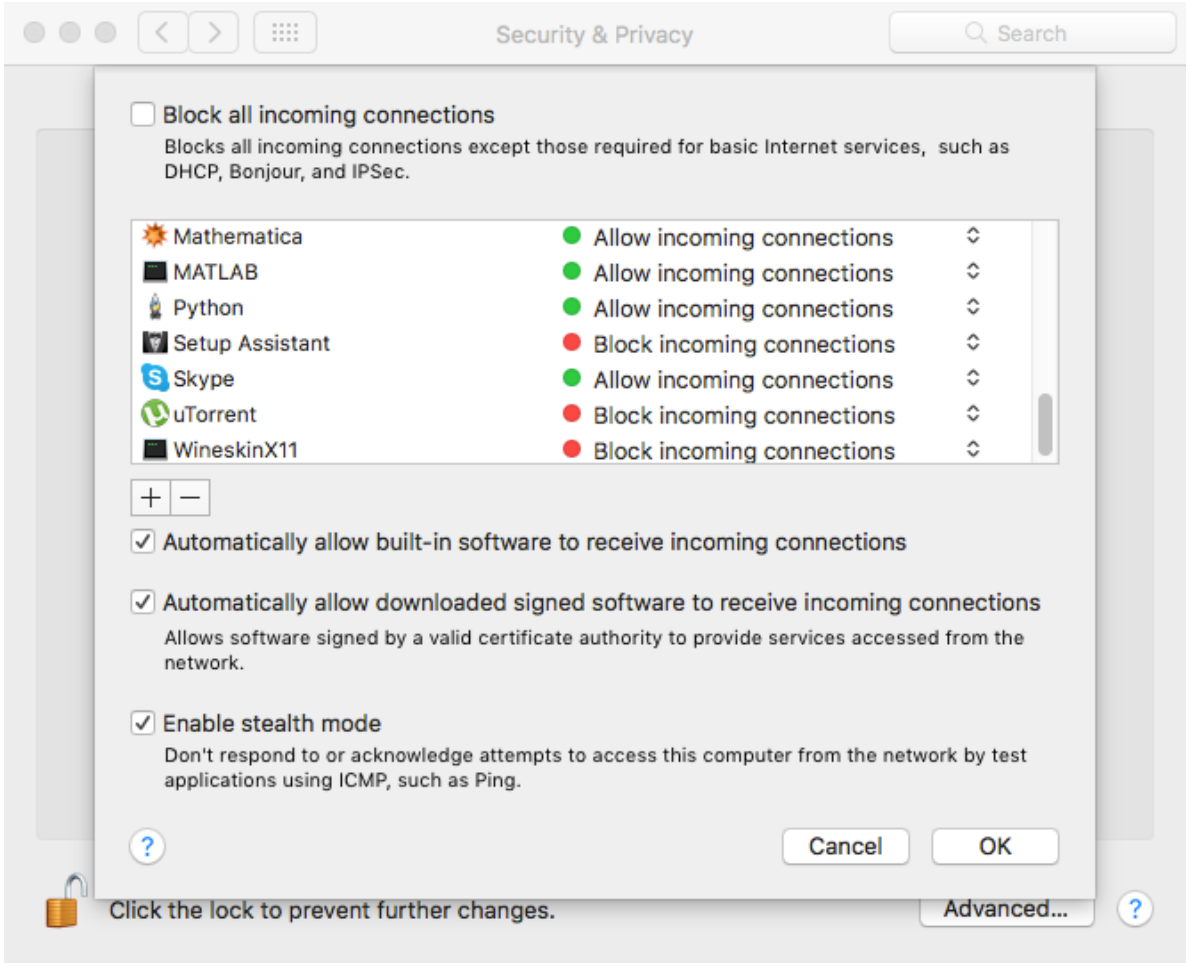
Host based firewall

- A software module used to secure an individual host
  - Available in many OSs or provided as an add-on package
  - Filters and restricts the flow of packets
  - Common location is a server
- Advantages
  - Filtering rules can be tailored to the host environment
  - Protection is provided independent of the topology
  - Used in conjunction with stand-alone firewalls to provide an additional layer of protection

Personal firewall

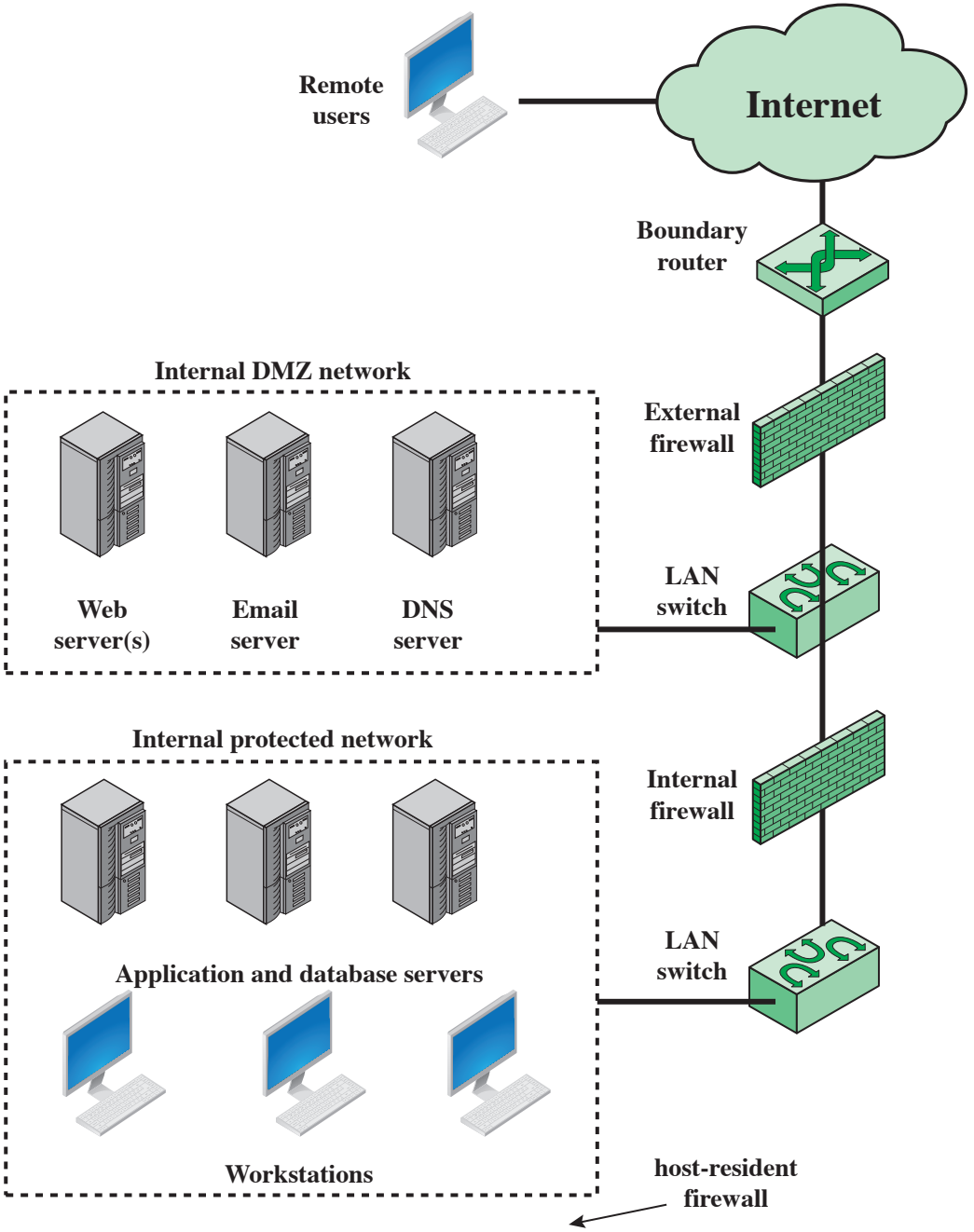
- Controls the traffic between a workstation on one side and the Internet or enterprise network on the other
  - Can be used in home environment or corporate intranets
  - Typically is a software module on the personal computer
  - Can also be housed in a router that connects all of the home computers to a DSL (or other) modem
- Role is to deny unauthorized remote access to a computer
- Can also monitor outgoing activity in an attempt to detect and block worms and other malware

Personal firewall: example GUI



Example firewall configurations

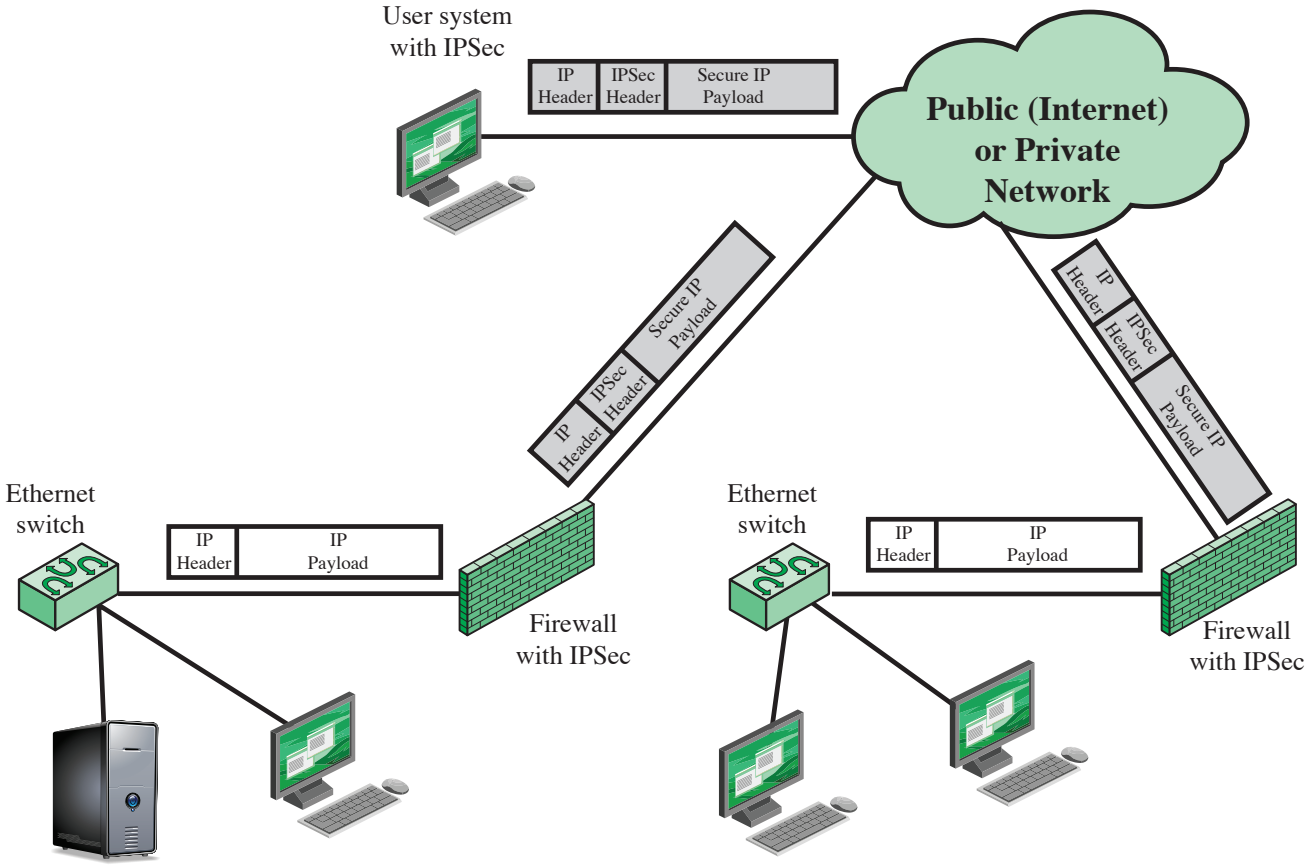
The simple case



DMZ networks

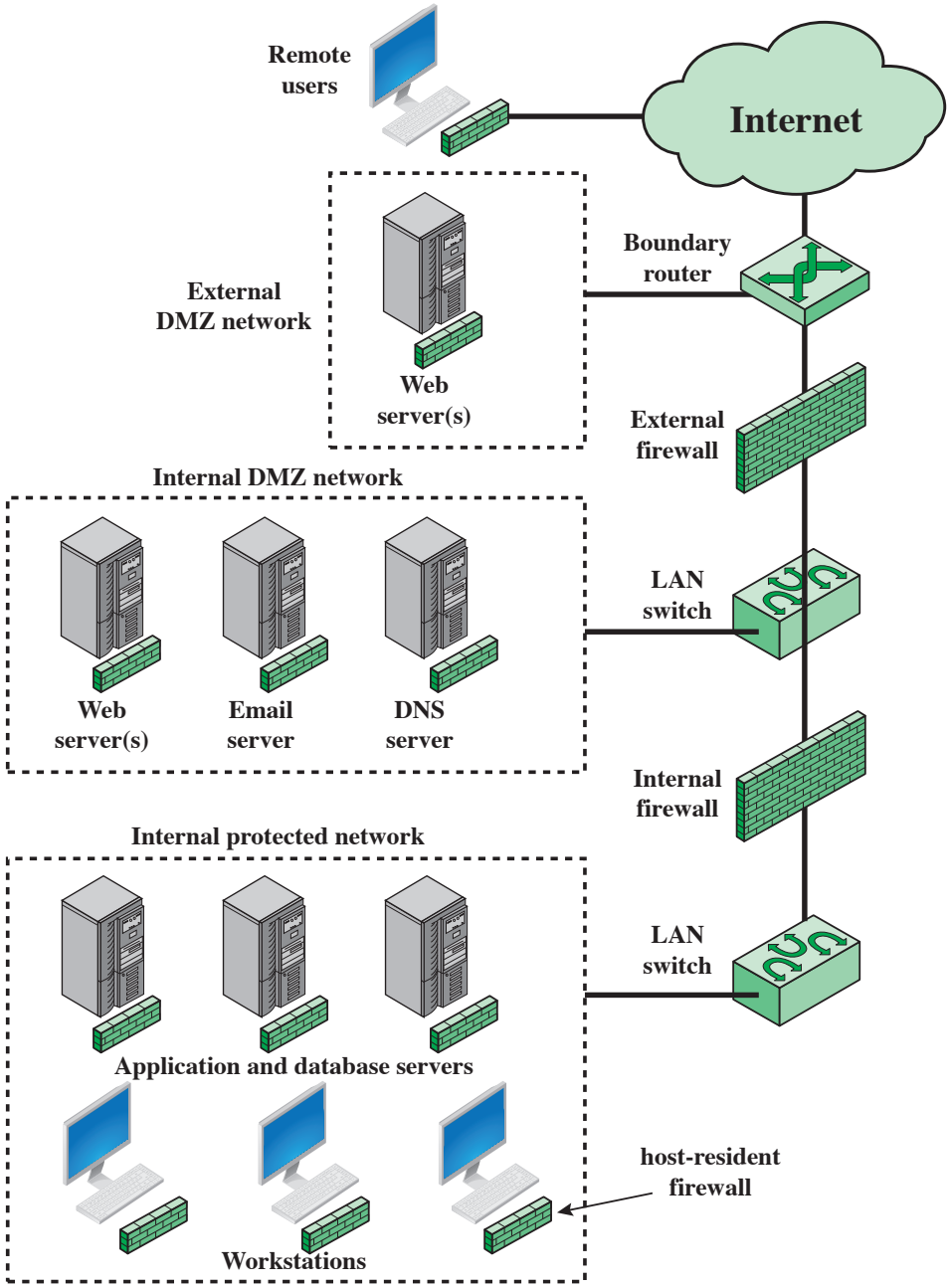
- The internal firewalls
  - Add more stringent filtering capability to protect servers
  - Provide two-way protection with respect to the DMZ
    - protect the rest of the network from attacks launched from DMZ (might originate from malware lodged in the DMZ)
    - protect the DMZ from attacks from the internal protected network
  - Many internal firewalls can be used to protect the internal network
    - e.g. internal servers could be protected from internal hosts and vice versa
    - common practice to place the DMZ on a different network interface on the external firewall from that used for internal networks

VPN security scenario



Example firewall configurations

The distributed case



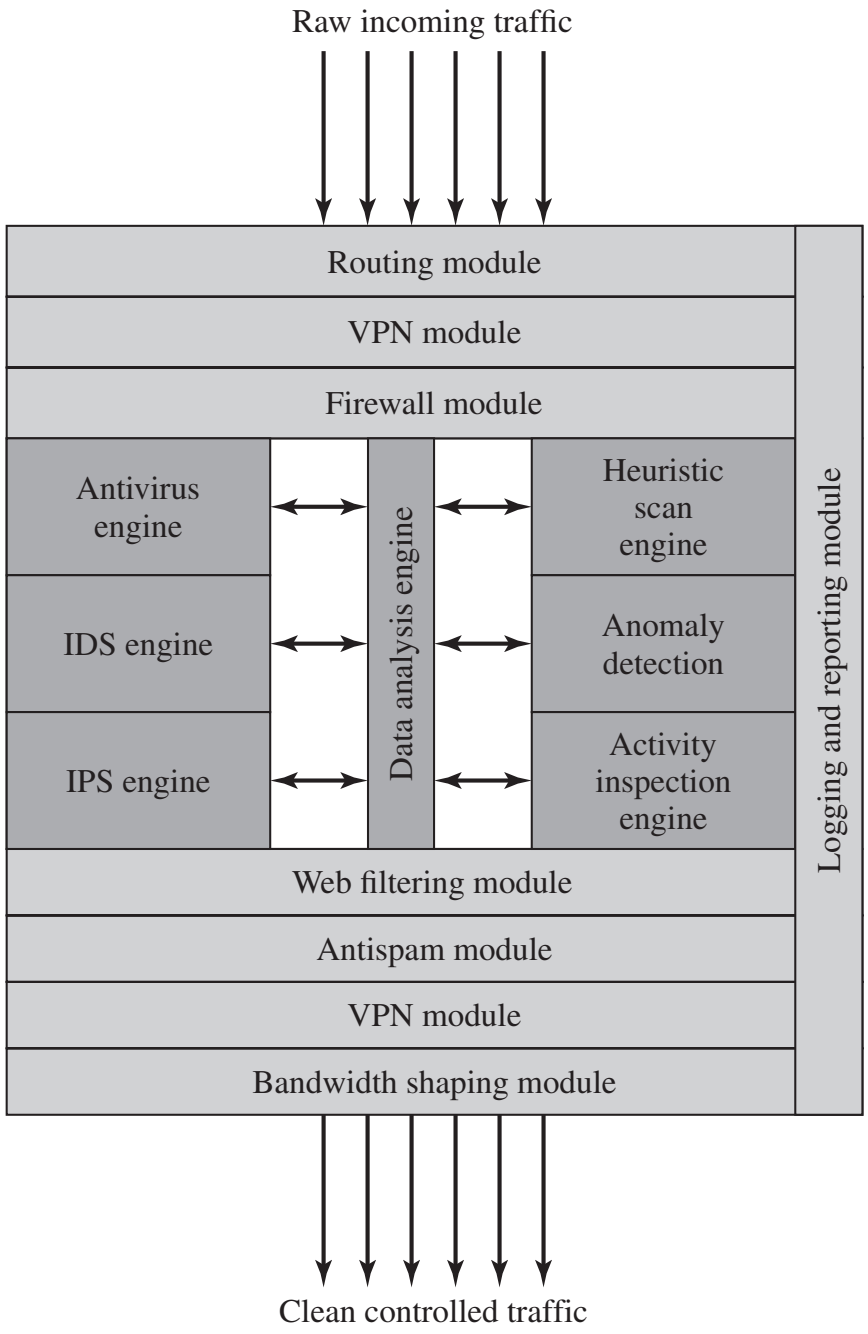
Summary of firewall aspects

- Host-resident firewall
  - includes personal and server firewall software
  - used alone or part of an in-depth firewall deployment
- Screening router
  - router between internal and external networks with full or stateless packet filtering
  - Typical for small/home office
- Single bastion inline
  - A single firewall between an internal and external router
  - the typical firewall appliance configuration for small-to-medium sized organizations
- Double bastion inline
  - DMZ is sandwiched between bastion firewalls

Summary of firewall aspects

- Single bastion T
  - As single bastion inline, but has a third network interface on bastion to a DMZ with externally visible servers
- Double bastion T
  - DMZ is on a separate network interface on the bastion firewall
- Distributed firewall configuration
  - Used by some large businesses and government organizations

Unified threat mgmt.



Unified threat mgmt.: functions

- Inbound traffic is can be decrypted before its initial inspection
- An initial firewall module filters traffic, discarding packets that violate rules
- A number of modules process individual packets and flows of packets at various protocols levels
- Incoming traffic may need to be re-encrypted to maintain flow security
- Detected threats are reported to the logging and reporting module
- The bandwidth-shaping module can use various priority and QoS algs. to optimize performance

Industrial personal firewalls

OPNsense

PfSense

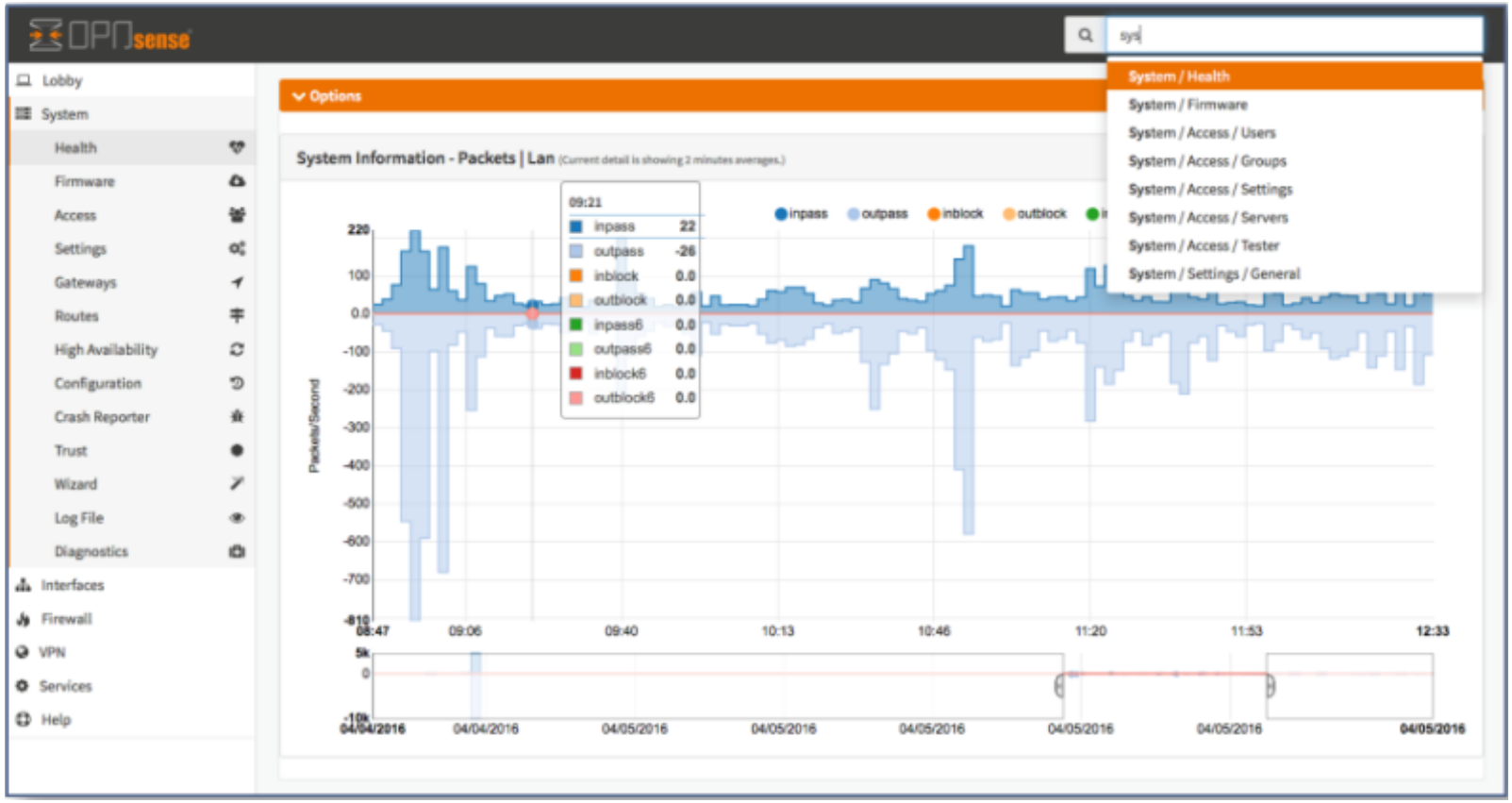
Shorewall

SmoothWall

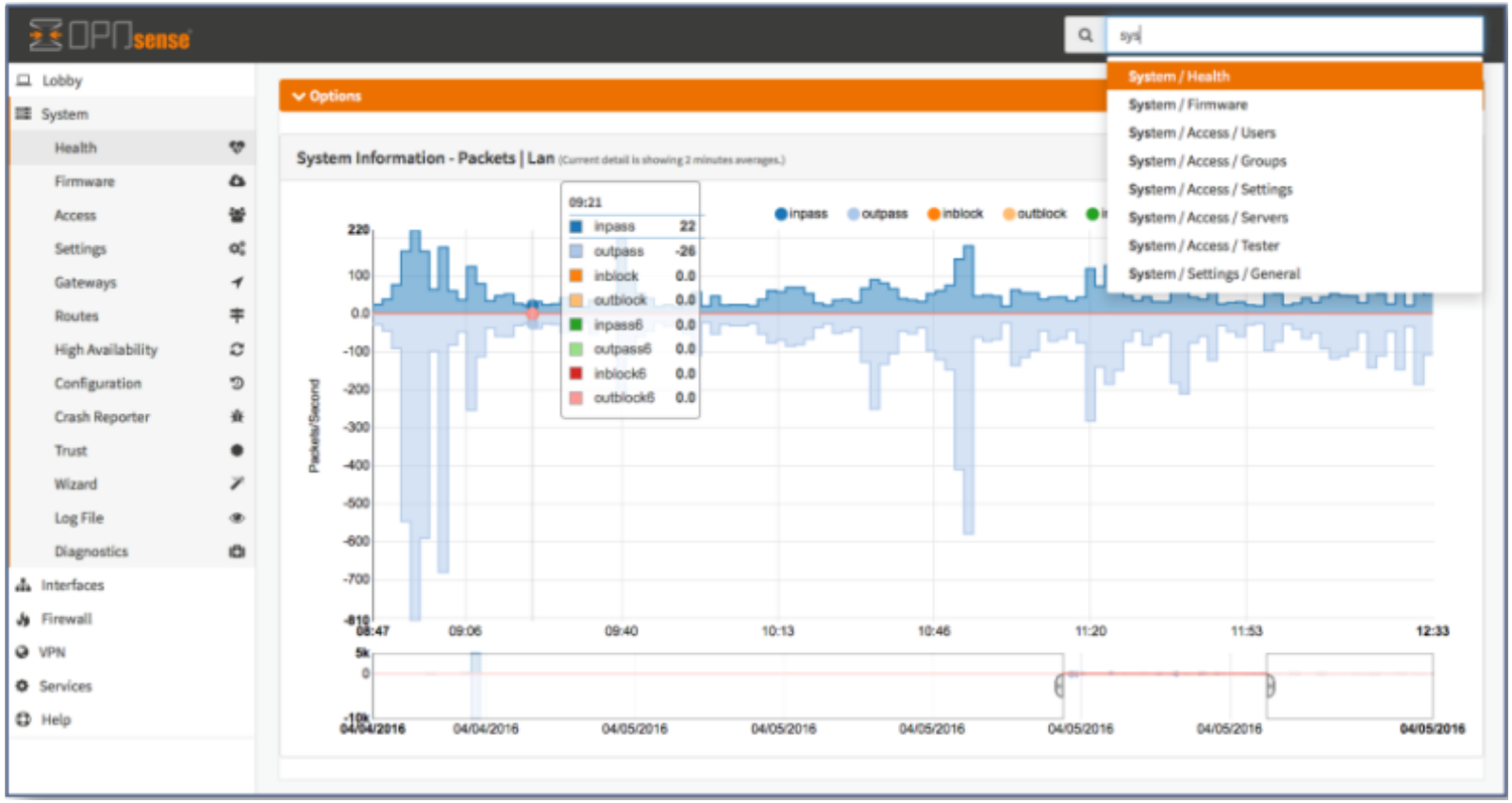
Untangle

WinGate

Personal firewalls: OPNsense GUI

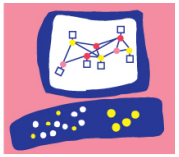


Personal firewalls: OPNsense GUI



NG firewalls: threat intelligence

INDICATIVE COMPANIES



Check point

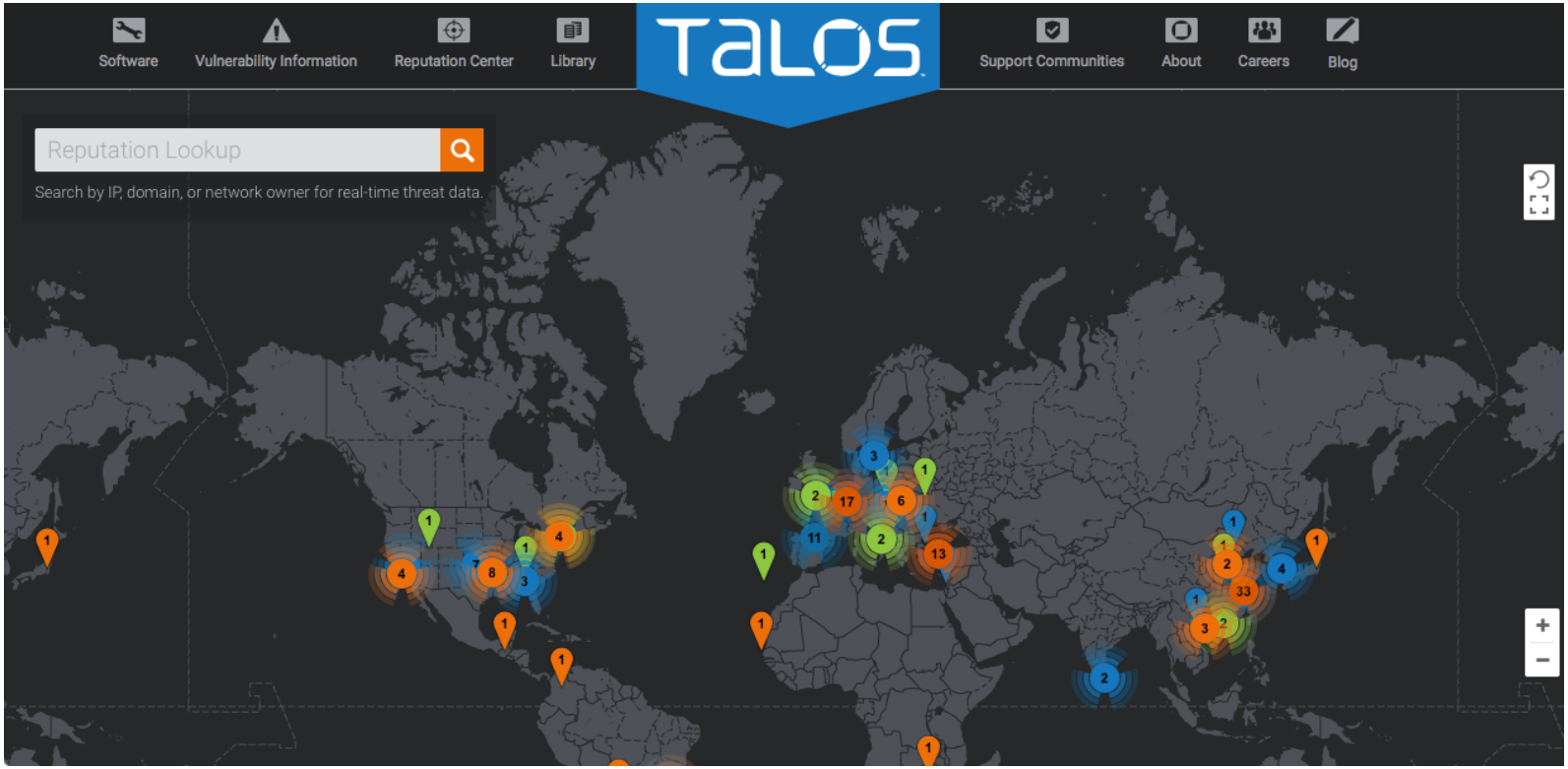
Cisco

Palo alto networks

EXAMPLES OF SERVICES

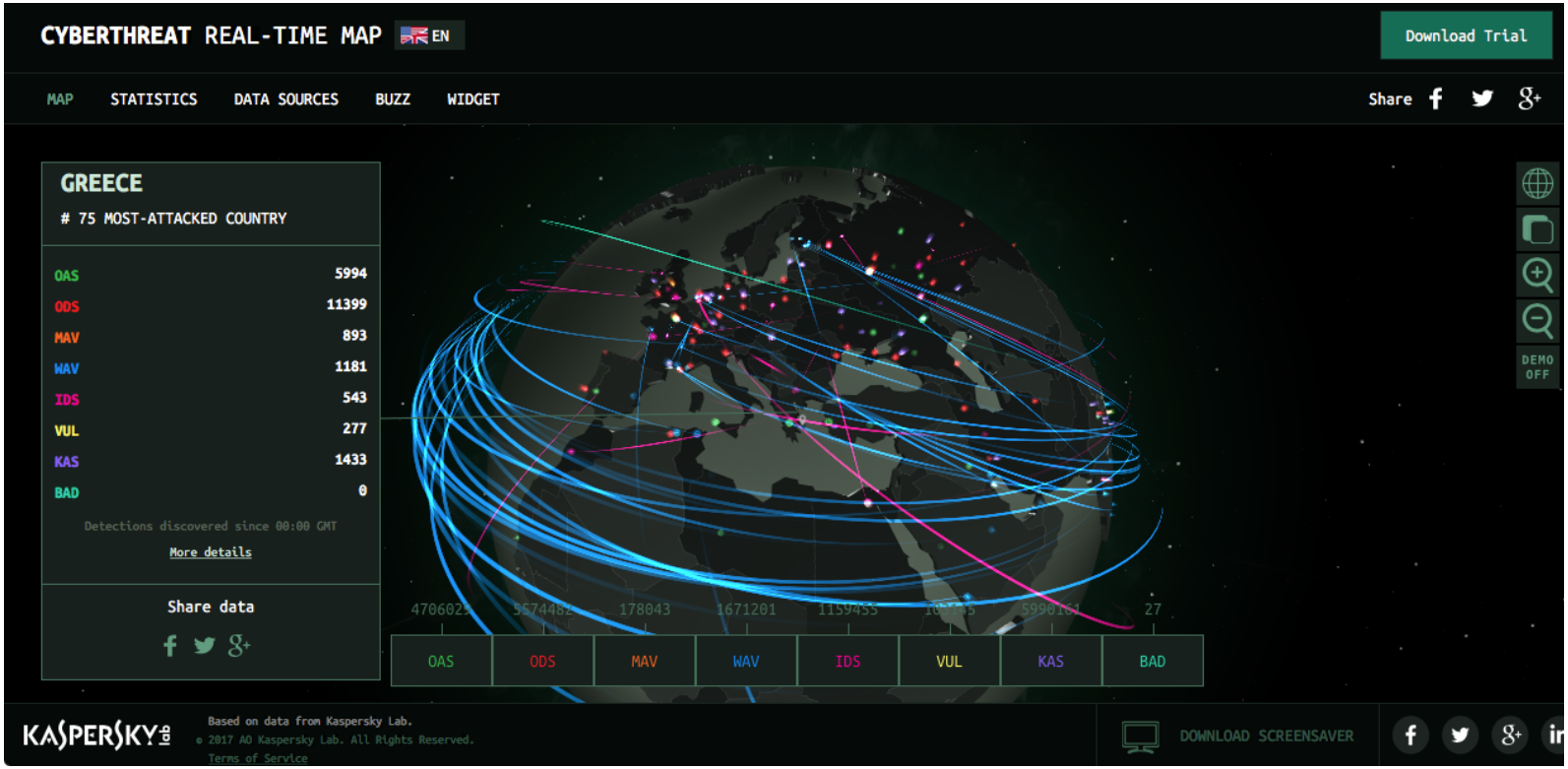
- Impact assessment
- Adaptive threat mgmt.
- Indicators of compromise
- Security awareness
- Adv. threat intelligence
- Threat containment

NG firewalls: threat intelligence



https://www.talosintelligence.com

NG firewalls: threat intelligence



https://cybermap.kaspersky.com

Προτεινόμενη βιβλιογραφία

- W. Stallings
  Cryptography and Network Security: Principles & Practice
  7th Ed., Prentice Hall, 2017
- W. Stallings and L. Brown
  Computer Security: Principles & Practice
  3rd Ed., Prentice Hall, 2015
- M. Bishop
  Computer Security: Art and Science
  Addison Wesley, 2003