

Gateway Security Devices

CSH5 Chapter 26

“Gateway Security Devices”

David Brussin & Justin Opatrny

1

Copyright © 2011 M. E. Kabay. All rights reserved.

Topics

- Introduction
- History & Background
- Network Security Mechanisms
- Deployment
- Network Security Device Evaluation



2

Copyright ©

Introduction



- Overview
- Changing Security Landscape
- Rise of Gateway Security Device
- Application Firewall: Beyond the Proxy

3

Copyright © 2011 M. E. Kabay. All rights reserved.

Overview

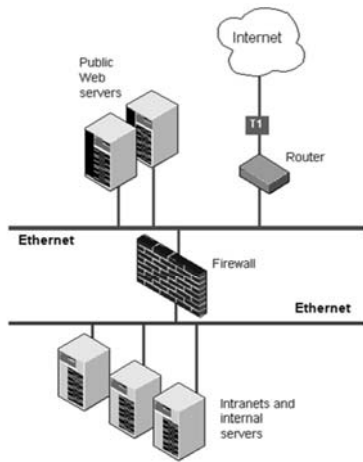
- What is a Firewall?
- Firewall rapidly accepted as perimeter security device
 - ❑ Even CEOs know about firewalls
- Original conception
 - ❑ Allow explicitly allowed communications
 - ❑ Deny all others
- Allowed paths became weakest links
 - ❑ Involve different (and insecure) protocols
 - ❑ Firewalls evolved to compensate for weak security in allowed protocols
- Successful use of firewalls depends on proper configuration



4

Copyright © 2011 M. E. Kabay. All rights reserved.

What is a Firewall?



A firewall is any *network-security device* that implements *security policies* by *restricting the ingress and egress of TCP/IP packets* according to *specific rules*.

Image from *Computer Desktop Encyclopedia*. Reproduced with permission. (c) 1981-2009 [The Computer Language Company Inc.](#)

Firewall Placement
An organization's public Web sites reside outside the firewall, but intranet servers and all internal computing resources are inside the firewall.

Changing Security Landscape (1)

- Pervasive changes in network architectures
 - ❑ Applications & work patterns require more open interactions
 - ❑ Perimeter less clearly defined
 - ❑ Increased centralization (e.g., servers)
 - ❑ Increased scrutiny of protocol traffic
- Borders dissolving
 - ❑ Outsourcing, hosted applications (e.g., CRM, e-mail, external storage, Web apps, cloud computing)
 - ❑ Enterprise applications linked to customer & 3rd party applications



Changing Security Landscape (2)

- Mobility (physical and logical)
 - ❑ Employees work from home, while traveling
 - ❑ Use kiosks, home systems, phones
 - ❑ Opens networks to attacks via compromised client systems
- Regulatory compliance
 - ❑ Increased demands for security
 - ❑ In USA, laws such as Gramm-Leach-Bliley (GLB), Health Information Portability and Accountability Act (HIPAA), and Sarbanes-Oxley (SOX) force protection of personally identifiable information (PII)



Rise of Gateway Security Device (1)

- Firewalls originally defined allowed paths for access (ports)
- Evolved into GSD to provide many security functions as shown below
- Gateway security device capabilities:
 - ❑ Processing power has increased
 - ❑ Now see multifunction platforms; e.g., role-based access controls (RBAC)
- Enterprise directory integration:
 - ❑ Lightweight Directory Access Protocol (LDAP) infrastructure for authorization

Rise of GSDs (2)

- Unified threat management:
 - ❑ Perimeter-based antivirus, antimalware, antispam
 - ❑ Intrusion detection & intrusion prevention
 - ❑ Content control
- Content control & data leakage prevention:
 - ❑ Deep inspection of packets in protocols such as HTTP, SMTP, IM
 - ❑ Dictionary-based and URL-list filters
 - ❑ Requiring encryption for sensitive data
- Archive & discovery
 - ❑ Message security & records for legal compliance

9

Copyright © 2011 M. E. Kabay. All rights reserved.

Application Firewall: Beyond the Proxy

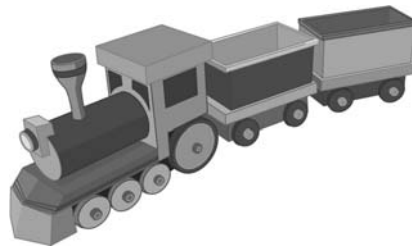
- Most significant allowed paths for most firewalls: Web access
 - ❑ HTTP & HTTPS (HTTP with SSL)
- Increased complexity
 - ❑ Rich-client applications; e.g., using AJAX
 - ✓ Aynchronous JavaScript & XML
 - ✓ AKA *remote scripting*
 - ✓ Allows user to interact *a field at a time* instead of *a page at a time*
 - ❑ Firewall now has to guard against misconfiguration & vulnerability in custom Web applications running over allowed HTTP

10

Copyright © 2011 M. E. Kabay. All rights reserved.

History & Background

- Changing Network Models
 - ❑ Mainframe
 - ❑ Client/Server
 - ❑ Web
- Firewall Architectures
- Firewall Platforms



Cross References in CSH5:

- Overview of computing and security history, see Chapter 1.
- Introduction to data communication basics, see Chapter 5.
- Introduction to local area networks, see Chapter 25.

11

Copyright © 2011 M. E. Kabay. All rights reserved.

Changing Network Models (1)

- Shift from mainframe-centric to LAN-centric to Internet-centric computing through 1980s through 1990s & 2000s
- Mainframe architectures
 - ❑ *Glass house* approach
 - ❑ Solitary systems with hardwired dumb or smart terminals (*green screens*)
 - ❑ Multiple mainframes linked within single data centers
 - ❑ WANs used leased lines (telephony)
- Virtualization began on mainframes
 - ❑ IBM MVS/VM
 - ❑ Strict partitions, mandatory access control

12

Copyright © 2011 M. E. Kabay. All rights reserved.

Changing Network Models (2)

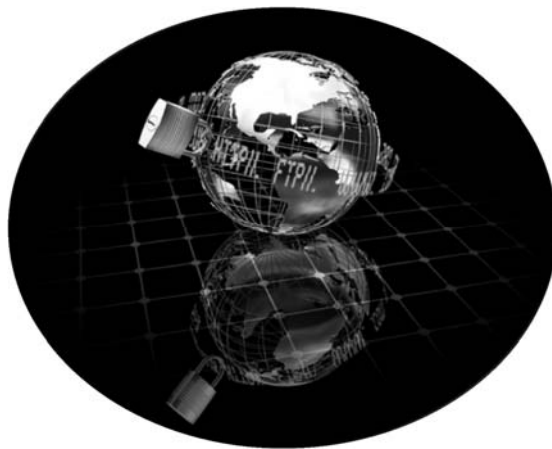
- Client/Server (1980s, early 1990s)
 - ❑ Midrange servers running Unix, NetWare, OS/2, Windows NT
 - ❑ Rapid increase in # & type of connections
 - ❑ Switch to PCs with local processing
- Security perimeter expanded
 - ❑ Out of data center to desktop
 - ❑ WANs expanded beyond enterprise
- Application security expanded across systems
 - ❑ Multiple allowed paths
 - ❑ Multiple possible attack paths

Changing Network Models (3)

- Web
 - ❑ HTTP/HTML started expanding 1989
 - ❑ Commercial Internet exploded starting in 1993 when .com opened in big way
 - ❑ Web applications replaced fat clients
- Mobile code complicated security issues
 - ❑ Asynchronous JavaScript & XML (AJAX)
 - ❑ Many customized & ad hoc protocols carry data over http
 - ❑ Firewalls increasingly focused on HTTP traffic

Firewall Architectures

- Access Control List
- Packet Filtering
- Stateful Inspection
- Application-Layer Gateway
- Multifunction Hybrid
- Host Environment Context



Access Control List (ACL)

- First FW were routers
 - ❑ Dedicated appliances
 - ❑ UNIX-based bastion hosts
- Routing appliances w/ ACLs
 - ❑ Still widely used
 - ❑ Decide on whether to allow packet into or out of network strictly one packet at a time
 - ❑ Examine packet data
 - ✓ Source, target addresses
 - ✓ Port, packet flags (e.g., SYN flag)
- Vulnerable to misconfigured packets
 - ❑ Fix problems using patches



Packet Filtering

- Pure packet-filtering FWs no longer common
 - ❑ Appliance or host-based
 - ❑ Use ACLs to apply policies
 - ❑ Typically provide logging
 - ❑ Support user-based authorization
 - ❑ Include intrusion detection & alerts
- Strengths
 - ❑ Ideally suited to load-balanced, high-availability environments
 - ❑ Can automatically share load among devices
- Weaknesses
 - ❑ Lack context information
 - ❑ Underlying operating system vulnerabilities affect security of FW
- Packet filtering has moved to non-security appliances such as load balancers, Web caches, switches

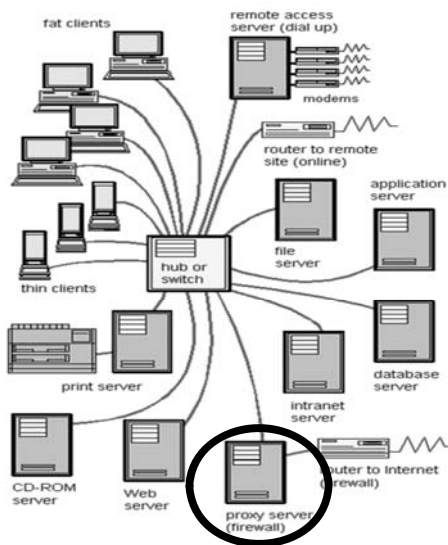


Stateful Inspection

- HTTP is a *connectionless protocol*
 - ❑ A communications architecture that does not require the establishment of a session between two nodes before transmission can begin. [*Computer Desktop Encyclopedia*]
- Stateful-inspection FW maintain connection information locally
 - ❑ Table in memory stores packet header data
 - ❑ Compare current packet info to session
 - ❑ Identify some abnormal packets used in attacks
 - ❑ But attacks that use uninspected portions can succeed
- Fast mode reduces inspection once connection opened successfully – strongly discouraged
- Performance can be good
 - ❑ Provide load balancing & failover with out-of-band data synchronization among devices running in parallel



What is a Proxy Server?

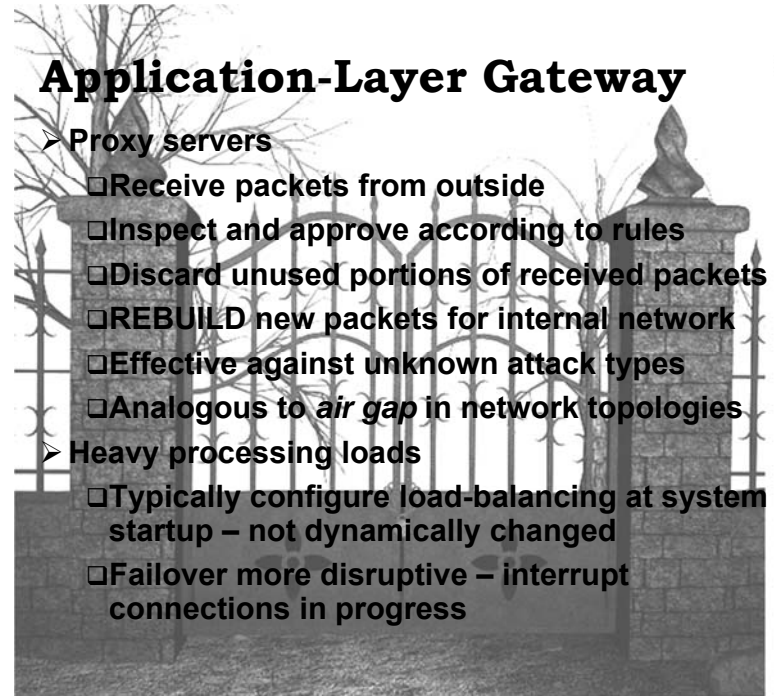


- “[An] application that breaks the connection between sender and receiver. All input is forwarded out a different port, closing a straight path between two networks and preventing a cracker from obtaining internal addresses and details of a private network.”

Image and text from *Computer Desktop Encyclopedia*. Reproduced with permission. (c) 1981-2009 [The Computer Language Company Inc.](#)

Application-Layer Gateway

- Proxy servers
 - ❑ Receive packets from outside
 - ❑ Inspect and approve according to rules
 - ❑ Discard unused portions of received packets
 - ❑ REBUILD new packets for internal network
 - ❑ Effective against unknown attack types
 - ❑ Analogous to *air gap* in network topologies
- Heavy processing loads
 - ❑ Typically configure load-balancing at system startup – not dynamically changed
 - ❑ Failover more disruptive – interrupt connections in progress



Multifunction Hybrid

- Most commercial firewalls today are hybrids
- Apply stateful inspection techniques to most protocols
- Use application-layer gateway proxies for specific protocols (e.g., HTTP, SMTP)
- Can shift to fast mode for stateful inspection once connection established



21

Host Environment Context

- Host-based security more granular than perimeter-based devices
 - Define specific applications / services
 - Regulate types of data allowed per process
 - Use sandbox or virtual machine to test code
- FWs can run on host or communicate with host
 - Use protocols such as Universal Plug and Play (UPnP) for data exchange
 - E.g., evaluate processes running when packet inspection being performed
 - Open and close specific ports as function of need

22

Copyright © 2011 M. E. Kabay. All rights reserved.

Firewall Platforms

- Routing
- Host Based
- Appliance
- Personal and Desktop Agent
- Virtual
- Embedded



23

Copyright © 2011 M. E. Kabay. All rights reserved.

FW Platforms: Routing

- Router
 - Heart of TCP/IP networks
 - Forwards packets from one network to another
 - Internal routing tables allow determination of where to forward each incoming packet
 - Destination address determines where outgoing packets are sent
 - Current load on different connections determine which line to use for each packet or group of packets
- ACL allow / deny statements restrict packets
- Hardware modules (blades) can share processing to increase throughput (bandwidth)

24

Copyright © 2011 M. E. Kabay. All rights reserved.

FW Platforms: Host-Based

- Dedicated server-based firewalls provide additional functions

- Protocol traffic inspection
- Contextual traffic inspection
- Comprehensive logging & alerts
- Air-gap proxy servers



- Typically run on Unix or Windows
 - Often have special *hardening* (security features) such as modifications of network stack
 - Consequences of increased complexity include increased bugs, vulnerabilities

FW Platforms: Appliance

- Extension of host-based FW: put FW into its own specialized processor w/ no other functions
- Total control of operating system
 - Control versions, patches specifically for functionality of FW
 - Prevent unauthorized, unwanted changes
- *Soft appliances*
 - Vendor specifies exact characteristics of hardware for user to buy & install
 - Provides full software – boot from vendor-supplied disk



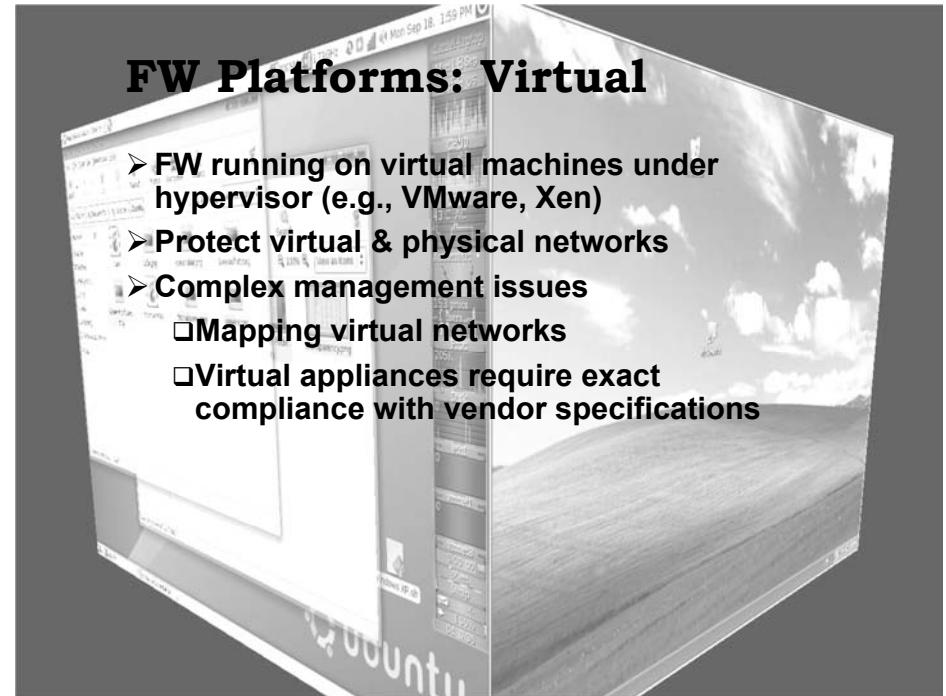
FW Platforms: Personal and Desktop Agent

- Software FW
 - Host-based systems
 - Commonplace today
 - Running on workstations
 - Integrated systems often include antivirus functions
- Evolve into host intrusion-prevention system (H-IPS)
- Require more maintenance than network-based FW
 - Constant signature updates
 - Regular patches of client software
 - Difficulties for management in wide-area networks



FW Platforms: Virtual

- FW running on virtual machines under hypervisor (e.g., VMware, Xen)
- Protect virtual & physical networks
- Complex management issues
 - Mapping virtual networks
 - Virtual appliances require exact compliance with vendor specifications



FW Platforms: Embedded

- Web-server-based plugins
 - ❑ Create customized *application* FWs
 - ❑ Scale to support consumers, small/medium business requirements
- Integrate tightly with Web server
 - ❑ Use downloaded signatures
 - ❑ Develop specific protection for specific applications
 - ❑ Allows contextual scanning unavailable to application gateways
- Often become all-in-one security appliances
 - ❑ Integrate FW, network intrusion-prevention, antivirus....

Network Security Mechanisms

- Recognition of value of network security mechanisms
 - ❑ IT managers have increased expertise
 - ❑ Increasingly recognized need
 - ❑ Often have unrealistic expectations
- Next slides:
 - ❑ Basic Roles
 - ❑ Personal & Desktop Agents
 - ❑ Additional Roles

Basic Roles

- Allowed Paths
- Intrusion Detection
- Intrusion Prevention/Response



Allowed Paths

- GSDs create physical perimeters
- Also create logical perimeter extending within protected networks
- Constitute least-privilege gateway
- Mechanisms for regulating access
 - ❑ Tunneling: Transmitting data structured in one protocol within the format of another.” (*Computer Desktop Encyclopedia*)
 - ❑ Antispoofing: preventing forged network addresses (e.g., blocking *inbound* packets with *internal* addresses and vice versa; blocking packets with originating addresses in *reserved address-space*)
 - ❑ Network Address Translation (NAT): see following

Network Address Translation (NAT)



- Masks address of internal nodes
 - ❑ Private address space accessed by internal tables
 - ❑ Limits determination of internal network size & topology
 - ❑ Restricts access to specific endpoints
- Static NAT
 - ❑ Manual, permanent assignment of IP address to each internal node
- Dynamic NAT
 - ❑ Pool of addresses assigned as required
- Port Address Translation (PAT)
 - ❑ AKA Nat overloading
 - ❑ Different TCP port # used for each client session

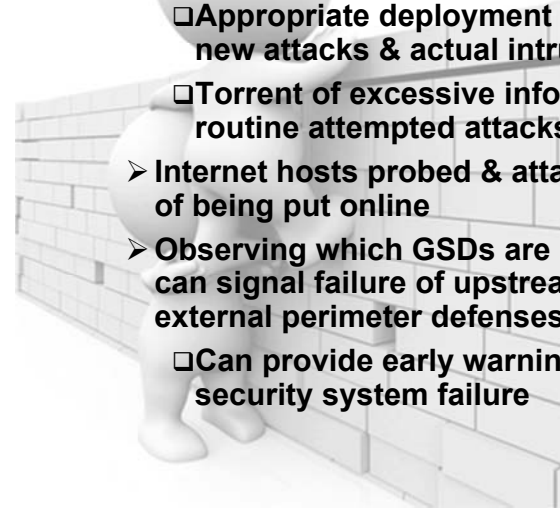
33

Copyright © 2011 M. E. Kabay. All rights reserved.

Intrusion Detection



- Alerts may be good or bad
 - ❑ Appropriate deployment of alarms over new attacks & actual intrusions good
 - ❑ Torrent of excessive information about routine attempted attacks → shutoff
- Internet hosts probed & attacked within hours of being put online
- Observing which GSDs are reporting attacks can signal failure of upstream devices (more external perimeter defenses)
 - ❑ Can provide early warning of impending security system failure



reed.

Intrusion Prevention & Response (1)



Several types of reaction to intrusions:

- Connection termination:
 - ❑ Stop traffic using RST (connection reset)
 - ❑ On User Datagram Protocol (UDP), can use packet dropping to terminate connection
 - ❑ Good for known attacks on allowed paths
 - ❑ Can allow denial of service
 - ❑ Not useful in preventing unknown types
- Dynamic rule modification
 - ❑ Target specific originating addresses
 - ❑ But opens even more to denial of service

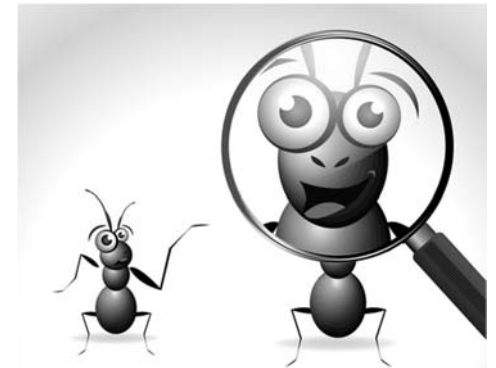
35

Copyright © 2011 M. E. Kabay. All rights reserved.

Intrusion Prevention & Response (2)



- System-level actions
 - ❑ Monitor for compromise
 - ❑ Firewall deactivation
 - ❑ But be sure that shutting down FW STOPS traffic, not leaves it open!
- Application inspection
 - ❑ Check for known protocol-specific exploits
 - ❑ E.g., use signatures to spot HTTP-specific attacks such as cross-site scripting (XSS) & SQL query injection attacks
- Antimalware
 - ❑ Spot malware in transit
 - ❑ Hijack Web session to divert download to quarantine



36

Copyright © 2011 M. E. Kabay. All rights reserved.

Personal & Desktop Agents

- Individual hosts (workstations)
 - ❑ Must be protected individually
 - ❑ Can use sophisticated contextual scanning
- End Point Protection
 - ❑ Mobile devices (laptop, phone) become extensions of network protection profile
 - ❑ Network location: Rules may vary depending on whether device is inside or outside perimeter
 - ❑ Application access: restrict inbound and outbound access depending on which program is running
 - ❑ Hybrid protections: spot particular patterns tied to known attack scenarios



37

Copyright © 2011 M. E. Kabay. All rights reserved.

Additional Roles

- Encryption
- Acceleration
- Content Control
- IPv6



38

Copyright © 2011 M. E. Kabay. All rights reserved.

Encryption (1)

- Many GSDs support encryption
 - ❑ Important because encrypted packets could contain dangerous payload
- Inspection
 - ❑ Termination: packet decrypted at perimeter
 - ✓ Contents inspected
 - ✓ May be re-encrypted for transmission to internal end-point
 - ❑ Alternative is passive (simultaneous) decryption using escrowed keys
 - ✓ But original encrypted packet continues to target while FW decrypts contents
 - ✓ Thus there are issues of synchronization



39

Copyright © 2011 M. E. Kabay. All rights reserved.

Encryption (2): VPNs

- Virtual Private Networks
- Extend security perimeter to include remote systems
- Increasingly popular
- But should consider special rules for VPN clients
 - ❑ May not be owned by organization
 - ❑ Need to establish clean operating environment
 - ❑ Especially important to prevent malware from entering corporate systems

See CSH5 Chapter 32 for more about VPNs

38

Copyright © 2011 M. E. Kabay. All rights reserved.

Acceleration

- **SSL (Secure Sockets Layer)**
 - ❑ Most frequently used encryption protocol
 - ❑ Defines HTTPS
 - ❑ Widely used on Web for e-commerce
- **Many high-volume servers equipped with dedicated encryption appliances**
 - ❑ Manage throughput
 - ❑ Avoid letting encryption/decryption become bottleneck on processing

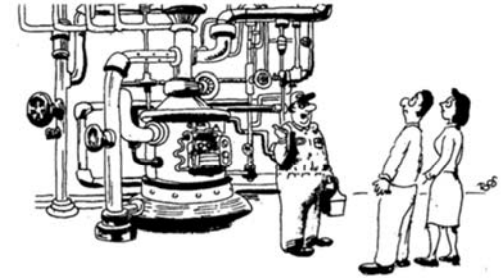


41

Copyright © 2011 M. E. Kabay. All rights reserved.

Content Control (1)

- **Content filtering**
 - ❑ Policy enforcement
 - ❑ Address-based filtering can block some sites (sometimes by mistake)
 - ❑ Keyword scanning has many false positives
- **Antimalware**
 - ❑ Pervasive element of all networks and workstations
 - ❑ Includes scans for harmful e-mail attachments, spam
 - ❑ Often uses appliances on network side to speed throughput



"This is just the water filter. The faucet is in the kitchen."

42

Copyright © 2011 M. E. Kabay. All rights reserved.

Content Control (2)

See CSH5 Chapter 17 for more about mobile code

- **Active Content**
 - ❑ Flash, QuickTime, ActiveX, VBScript, JavaScript
 - ❑ Many GSDs scan for and block such code
 - ❑ Others use signatures and sandboxes to screen hostile code
- **Caching**
 - ❑ Proxy servers keep copies of frequently-used items
 - ❑ Typically for HTTP, FTP, streaming media
- **Policy Enforcement**
 - ❑ Can scan e-mail for sensitive keywords
 - ❑ Can require encryption for specific communications



43

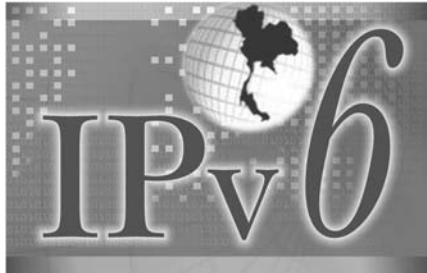
Copyright © 2011 M. E. Kabay. All rights reserved.

IPv6 (1)

- **Successor to IPv4 (current standard)**
- **Support & compatibility**
 - ❑ GSDs must support appropriate protocols
 - ✓ Neighbor discovery (ND)
 - ✓ Router solicitation/advertisement (RS/RA)
 - ✓ Multicast listener discovery (MLD)
 - ❑ Stateless autoconfiguration
 - ✓ IPv6 nodes may assign their own addresses
 - ✓ Can discover their own routers using NS, RS/RA – but may break user/address audit trail (use MAC addresses for hardware nodes)

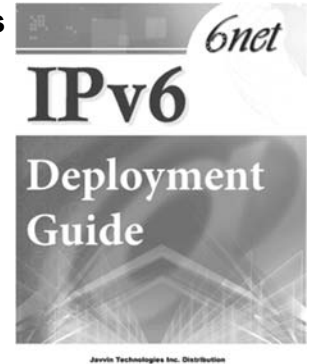
IPv6 (2)

- Address shortage resolved
 - ❑ IPv4 address space = $2^{32} \approx 10^9$
 - ❑ IPv6 address space = $2^{128} \approx 10^{38}$
 - ❑ Ratio is IPv6:IPv4::solar system:stamp!
- Be careful about IPv6 traffic tunneling through IPv4 infrastructure
 - ❑ E.g., antispoofing benefits of IPv6 lost when using IPv4-to-IPv6 gateways



IPv6 (3)

- NAT not intended to survive transition
 - ❑ IPv6 may expose IPv4 nodes when NAT removed
- Single IP address associated with specific device (node)
 - ❑ Can carry address from internal network to external network
 - ❑ Example: laptop starts session in office but moves to café – same IP address
 - ❑ Will need new developments to cope with device-specific IPv6 addresses



Deployment

- Screened Subnet FW Architectures
- Gateway Protection Device Positioning
- Management & Monitoring Strategies



Screened Subnet FW Architectures

- Service Networks
 - ❑ New design strategy: don't lump Web, DNS, e-mail into single network (NW)
 - ❑ Break functional components into separate, protected NW
 - ❑ Defines *service NW* with their own security configurations, policies
- Redirect Back-End Traffic Through FW
 - ❑ Just because FW decrypts packet doesn't mean it's necessarily safe
 - ❑ Reroute decrypted packet through FW before allowing it to reach internal destination



Gateway Protection Device Positioning (1)

- Encrypting protocols (e.g., SSL & IPSec) can pose problems
 - ❑ Bandwidth chokepoints due to processing requirements
 - ❑ Ideally, deploy GSDs where there is little encrypted traffic
- Two major approaches (details on following slides):
 - ❑ Put GSDs inline
 - ❑ Avoid encrypted traffic

Gateway Protection Device Positioning (2)

- Inline
 - ❑ Configure *span port* to replicate data from one or more switch ports to monitoring port
 - ❑ Problems
 - ✓ Can overload the monitor (too many inputs)
 - ✓ Passive devices don't offer protection, only alerts (so dangerous packets already gone)
 - ❑ Thus should put GSD inline with traffic
 - ✓ Provides choke point (but device can have *wire speed* bandwidth)
 - ✓ Allows active prevention (blockage)
 - ✓ But be sure to configure properly to avoid DoS

Gateway Protection Device Positioning (3)

- Avoid encrypted traffic
 - ❑ Encrypted packets defeat GSDs
 - ❑ Therefore GSD must evaluate packets on unencrypted side of encrypted connection
 - ✓ E.g., on backside of SSL terminator
 - ✓ On unencrypted side of VPN connection
 - ❑ Implies likelihood of more than one GSD

Management & Monitoring Strategies

- Monitoring
- Policy
- Auditing/Testing
- Maintenance
- Logging & Alerting
- Secure Configurations
- Disaster Recovery



Monitoring

- Device Health (may be part of GSD system)
 - ❑ Processor utilization
 - ❑ Available RAM
 - ❑ Number of connections
 - ❑ May have to use SNMP, RMON tools
 - ❑ Restrict access by monitoring tools
 - ❑ Examine trends
- Availability
 - ❑ Periodically test functionality
 - ❑ *ping, traceroute*
- Integrity
 - ❑ Ensure that operating code cannot be / has not been modified without authorization
 - ❑ Checksums, utility scanner....

Policy (1)

- *GSDs instantiate policy!*
 - ❑ Look for centralized management consoles
- Firewall-allowed paths
 - ❑ Every allowed path must relate to specific *required* external service
 - ❑ Start with deny-all basis and add allowed paths
 - ❑ To degree possible, identify endpoints in rules
 - ❑ Keep track of *direction* of connections (inbound vs outbound)

Policy (2)

- Complexity of GSD policies
 - ❑ Standard FW rules are simple Boolean logic
 - ❑ But GSDs may require multistage rules
 - ✓ Origination addresses
 - ✓ Message contents
 - ✓ Attachments virus-free
- Change management
 - ❑ Must control & track policy changes & implementation
 - ❑ Can thus backout mistakes
 - ❑ Audit trail important for security incident analysis

Policy (3)

- Secondary validation
 - ❑ Making changes can be easy
 - ❑ But complex systems can result in unexpected errors
 - ❑ Having second network / system admin check proposed change helpful
 - ✓ Avoid errors
 - ✓ Share knowledge
 - ✓ Enforce security principle of shared responsibility, checks-and-balances

Auditing/Testing

- How do we know our GSDs are working?
 - ❑ **Auditing:** do the actual rules comply with the rules we claim to want according to policy?
 - ❑ **Assessment:** are the rules working as we want / expect?
- Vulnerability assessment (VA)
 - ❑ Walkthrough, tools for examining parameters
- Penetration testing (Pen Testing)
 - ❑ Actually trying to break through the GSD

See CSH5 Chapter 46 for VA/Pen Testing & Chapter 54 for audits

Maintenance

- Patching – see CSH5 Chapter 40
- Pattern updates
 - ❑ Automatic updates a must to get files promptly
 - ❑ But production environment cannot automatically trust patches
 - ✓ Have monitor-mode to see if new signatures work properly & safely
 - ✓ Then enable for action as approved by QA team
 - ❑ Alternative is to install on completely separate non-production systems for testing

Logging & Alerting

- Logging essential
 - ❑ Must be able to access data on allowed / denied packets
 - ❑ Record of system changes
- Alert mechanisms
 - ❑ Configurable
 - ❑ Whom to alert?
 - ❑ How (e-mail? IM? Phone w/ robot voice?)
- Log files
 - ❑ Can eat up disk space
 - ❑ Plan for backups to cheaper media
 - ❑ May configure to exclude safe traffic
 - ❑ Need log file utilities to extract & format data

Secure Configurations

- Ensure that GSDs are themselves secure against tampering, error
- Define baseline secure configurations
- Default configuration may be inadequate
- Implied rules
 - ❑ Must be made explicit & examined
 - ❑ May modify or disable as required
- Ancillary exposures
 - ❑ Administrative console can reveal unsuspected functions, services
 - ❑ Can disable unused functions, services

Disaster Recovery

See CSH5 Chapters 56-59

- FW or GSD outage can cripple system or leave it wide open to attack
- Fail-over/high availability
 - ❑ May need to configure active/standby units
 - ✓ Instant cutover
- Load-balancing configurations
 - ❑ Provide better throughput
 - ❑ Also serves for business continuity
- Backup/restore
 - ❑ Be sure all configuration scripts are backed up
 - ❑ Be able to re-establish known-good configuration ASAP

Network Security Device Evaluation

- Current Infrastructure Limitations
- New Infrastructure Requirements
- Performance
- Management
- Usability
- Price
- Vendor Considerations
- Managed Security Service Providers

§26.5 provides checklists for evaluating GDSs

Will Firewalls Ever Be Perfect?



"It's programmed to override their firewall."

DISCUSSION