Aalto University

Network Security: Firewall: further issues

Tuomas Aura

CS-E4300 Network security

Aalto University

TRANSPORT AND APPLICATION-LAYER FIREWALLS

TCP payload and packet filters

- Some firewalls try to perform deep packet inspection (DPI), i.e., filter TCP, UDP, or SCTP packets based on the payload data
  - HTTP or CoAP request:

    ```
    GET /index.html HTTP/1.1
    Host: thepiratebay.org
    ```

  - Specific byte strings, e.g., `Tiananmen Square`
- However, this is not reliable:
  - TCP payload data can be split arbitrarily to many TCP segments
  - Sender can confuse the firewall with invalid segments and non-standard resending behavior
  - IP packets may be fragmented
  - Most connections are now encrypted
- Reliable filtering can be done in a proxy that terminates the connection

SOCKS proxy

- Transport-layer proxy
  - When an intranet client needs to connect to a server outside, it connects to the proxy instead
  - Proxy terminates TCP and UDP connections. Creates a second connection to the server in the Internet
  - Proxy can act as an application-layer firewall and filter inbound and outbound payload data
  - Proxy is simpler than a host and easier to harden against attacks
- SOCKS is management protocol between the client and proxy
  - Client requests new connections from firewall
  - Supports authentication of client requests, e.g., Kerberos with GSSAPI
  - SOCKS is supported by most web browsers

Application proxies

- Application-layer proxies can terminate encryption (TLS) and filter payload data
  - Web application firewall
  - Web proxy
  - Reverse web proxy
  - CoAP proxy
  - TLS gateway
  - API gateway
  - Email gateway

FIREWALL DISCUSSION

Firewall traversal

- Network admins prefer to drop traffic by default
  → new applications and protocols will not work
- New applications will not become popular if an administrative decision is needed at each site → application developers (and users) do their best to circumvent firewalls
  - Most applications use port 443 or encrypt the data
  - NAT and firewall traversal is an art: STUN, TURN, ICE

History: In the early days of Internet, new network applications were standardized and got a registered port number from IANA. From the late 1990s, ports 80 and 443 were used for everything because they were open in firewalls. This created a heated debate because firewalls could no longer block specific applications.

Filtering outbound connections

Firewalls can also filter outbound traffic from intranet to Internet, but why?

- Security:
  - Prevent access to untrusted services or dangerous or embarrassing content
  - Prevent compromised machines in the intranet from attacking others, e.g., sending spam emails, DDoS etc.
  - More difficult for malware to exfiltrate data or set up command and control (C&C) channels
- Cost reduction:
  - If ISP charges by megabyte, prevent access to P2P, VoIP
- Productivity:
  - How do employees spend their time?
- Liability:
  - Does unrestricted Internet access by employees or visitors expose the company to legal risks? (e.g. BitTorrent)

Debugging firewall rules

- Firewall rules are difficult to configure
  - Order of rules matters → fragile configurations
  - Configuration language and its exact semantics vary between implementations
  - Stateless packet filters have limited expressive power
- Performance depends on hardware support
  - Router may become slow when filtering is enabled, or when specific filters are deployed. Which rules and how many of them can be processed in hardware?
- Redundancy in the firewall policy may indicate errors, but not always:
  - Rule is shadowed if another rule above prevents it from ever matching. Is this intentional?
  - Overlapping rules match some of the same packets. Do they specify the same action or different ones?
  - When a network path traverses multiple firewalls, do you want to filter at every firewall or at only one?

Internet ossification

- Traditionally, a strict policy with sanity checks for every packet header field is considered the good. Examples:
  - IP version must be 4 or 6
  - Unused IP and TCP flags must be zero
- Prevents deployment of new protocols and protocol features
  - Packets with new values in any packet header field will be dropped
  - Solution: encrypt everything that can encrypted, randomize plaintext header fields and bits that are currently unused

Firewall limitations (1)

- May prevent people from doing their work
  - Try to convince a network admin to open a port for your server!
- Network admins are often reluctant to change firewall policies in case something breaks
- Makes network diagnostics harder
- Firewall configuration errors are common
- Only coarse-grained rules can be managed effectively
- Most applications now use TCP port 80 or 443, or use other clever tricks to traverse firewalls

Firewall limitations (2)

- Perimeter defence is ineffective in large networks
  - There are always some compromised nodes inside
- Potential unfiltered ingress routes that circumvent firewalls:
  - Historical threat: dial-up modem connections in and out
  - Unauthorized wireless access points
  - Outbound VPN connections
  - Laptops move in and out of the intranet, “bring your own device” culture
  - Laptops have both cellular data and intranet connections
  - Apps installed from the web may be Trojan horses
  - Servers are now in cloud and accessed from inside and outside the network

Other firewall-related topics

- IPv6 rules
- Host firewall
- NAT and firewall traversal
- Firewall and VPN connections
- Routing and firewall between VLANs, VLAN trunking (802.1Q)
- Network virtualization, domain isolation
- Network access control (Cisco NAC, Microsoft NAP)
- Guest networks

Related reading

- William Stallings. Network security essentials: applications and standards, 3rd/5th ed.: chapter 11
- William Stallings. Cryptography and Network Security, 4th ed.: chapter 20
- Kaufmann, Perlman, Speciner. Network security, 2nd ed.: chapter 23
- Ross Anderson. Security Engineering, 2nd ed.: chapter 21.4.2
- Dieter Gollmann. Computer Security, 2nd ed.: chapter 13.6; 3rd ed.: chapter 17.3

Exercises

- Why cannot ingress filtering by gateway routers and ISPs ever stop all IP spoofing attacks?
- Do you find any mistakes or shortcomings in the firewall policy examples of this lecture? Can they be improved?
- Find out what kind of firewall capabilities your home gateway router/NAT has.
- Why has it been claimed that IPv6 exposes intranets to attacks from Internet?
- Configure your home router to filter IPv6. Try to enable only the necessary protocols and filter everything else. Configure also multiple network segments (VLANs) and a guest WLAN.
- Find the firewall configuration of a small network. Try to understand each line of the policy. Have compromises on security been made to achieve better performance, to simplify management, or because of limitations in the firewall platform?
- Stateless firewall typically passes all inbound TCP packets with the ACK flag set. On a 1 GB/s network, how difficult is it for external attackers to spoof some TCP packets (e.g., RST) that match the sequence numbers of a TCP connection on the target host in the intranet? Does ingress filtering help?
- Translate the examples in these slides to policies for iptables or a commercial firewall product (e.g., Cisco, pfSense, EdgeRouter, MicroTik)