Computer Networks

Mohammed El-Hajj

Jacobs University Bremen

October 10, 2021

JACOBS
UNIVERSITY

Course Content

1. Introduction
2. Fundamental Networking Concepts
3. Local Area Networks (IEEE 802)
4. Internet Network Layer (IPv4, IPv6)
5. Internet Routing (RIP, OSPF, BGP)
6. Internet Transport Layer (UDP, TCP)
7. Firewalls and Network Address Translators
8. Domain Name System (DNS)
9. Abstract Syntax Notation 1 (ASN.1)
10. External Data Representation (XDR)
11. Augmented Backus Naur Form (ABNF)
12. Electronic Mail (SMTP, IMAP)
13. Document Access and Transfer (HTTP, FTP)

Part 7: Firewalls and Network Address Translators

Section 27: Middleboxes

Middleboxes

Definition (RFC 3234)

A middlebox is any intermediary device performing functions other than the normal, standard functions of an IP router on the datagram path between a source host and destination host.

- A middlebox is not necessarily a physical box — it is usually just a function implemented in some other box.
- Middleboxes challenge the End-to-End principle and the hourglass model of the Internet architecture.
- Middleboxes are popular (whether we like this or not).

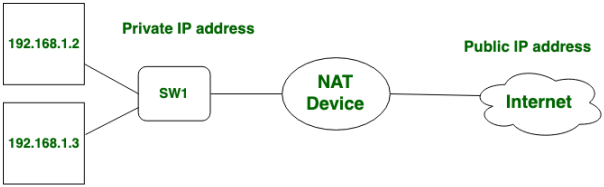
Concerns about Middleboxes

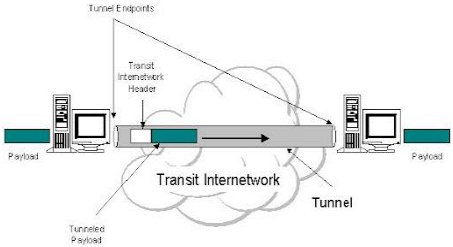
- Protocols designed without consideration of middleboxes may fail, predictably or unpredictably, in the presence of middleboxes.
- Middleboxes introduce new failure modes; rerouting of IP packets around crashed routers is no longer the only case to consider.
- Configuration is no longer limited to the two ends of a session; middleboxes may also require configuration and management.
- Diagnosis of failures and misconfigurations is more complex.

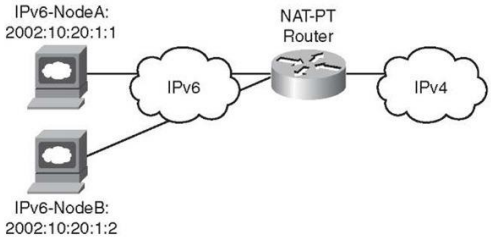
Types of Middleboxes

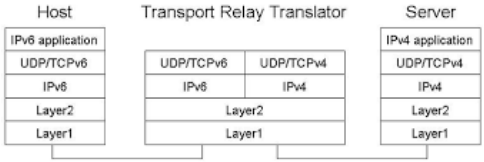
- *Network Address Translators (NAT)*: A function that dynamically assigns a globally unique address to a host that doesn't have one, without that host's knowledge.
- *NAT with Protocol Translator (NAT-PT)*: A function that performs NAT between an IPv6 host and an IPv4 network, additionally translating the entire IP header between IPv6 and IPv4 formats.
- *IP Tunnel Endpoints*: Tunnel endpoints, including virtual private network endpoints, use basic IP services to set up tunnels with their peer tunnel endpoints which might be anywhere in the Internet.
- *Transport Relays*: A middlebox which translates between two transport layer instances.

Types of Middleboxes









Types of Middleboxes (cont.)

- *Packet classifiers, markers and schedulers*: Packet classifiers classify packets flowing through them according to policy and either select them for special treatment or mark them, in particular for differentiated services.
- *TCP performance enhancing proxies*: “TCP spoofer” are middleboxes that modify the timing or action of the TCP protocol in flight for the purposes of enhancing performance.
- *Load balancers that divert/munge packets*: Techniques that divert packets from their intended IP destination, or make that destination ambiguous.
- *IP Firewalls*: A function that screens and rejects packets based purely on fields in the IP and Transport headers.
- *Application Firewalls*: Application-level firewalls act as a protocol end point and relay

Types of Middleboxes (cont.)

- *Application-level gateways (ALGs)*: ALGs translate IP addresses in application layer protocols and typically complement IP firewalls.
- *Transcoders*: Functions performing some type of on-the-fly conversion of application level data.
- *Proxies*: An intermediary program which acts as both a server and a client for the purpose of making requests on behalf of other clients.
- *Caches*: Caches are functions typically intended to optimise response times.
- *Anonymisers*: Functions that hide the IP address of the data sender or receiver. Although the implementation may be distinct, this is in practice very similar to a NAT plus ALG.
- …

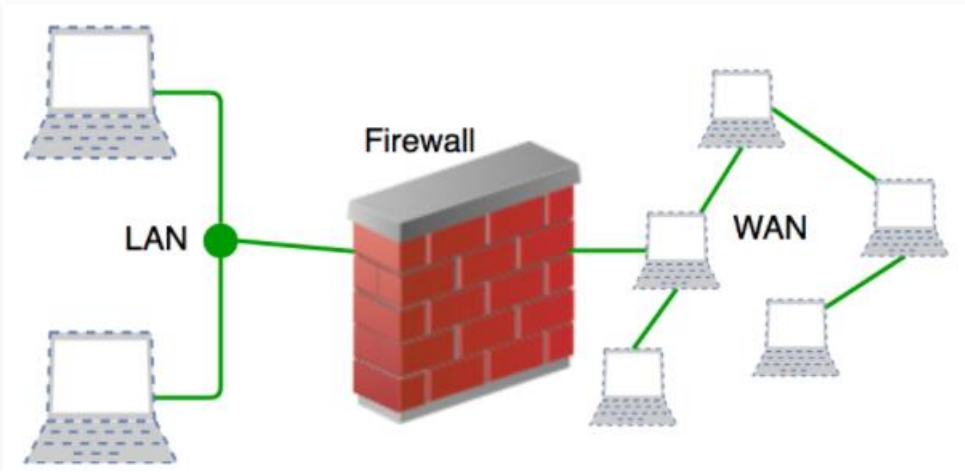
Section 28: Firewalls

Firewalls

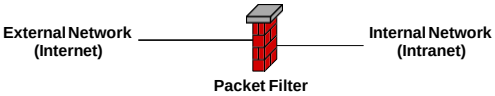
- A firewall is a system (or a set of systems) that enforce access control policies between two (or more) networks.
- *Conservative firewalls* allow known desired traffic and reject everything else.
- *Optimistic firewalls* reject known unwanted traffic and allow the rest.
- Firewalls typically consist of packet filters, transport gateways and application level gateways.
- Firewalls not only protect the “inside” from the “outside”, but also the “outside” from the “inside”.

⇒ There are many ways to avoid firewalls if internal and external hosts cooperate.

Firewalls



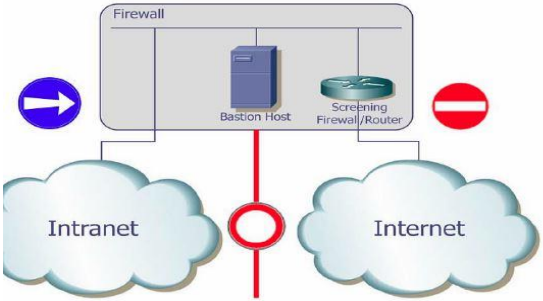
Firewall Architectures



	Source IP	Dest. IP	Source Port	Dest. Port	Action
1	192.168.21.0	--	--	--	deny
2	--	--	--	23	deny
3	--	192.168.21.3	--	--	deny
4	--	192.168.21.0	--	>1023	Allow

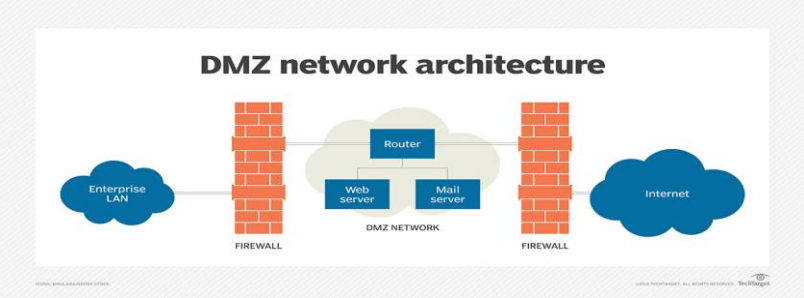
- The simplest architecture is a packet filter which is typically implemented within a router that connects the internal network with the external network.
- Sometimes called a “screening router”.

Firewall Architectures



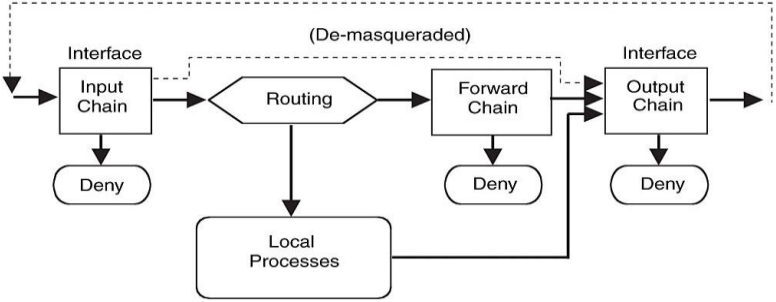
- A bastion host is a multihomed host connected to the internal and external network which does not forward IP datagrams but instead provides suitable gateways.
- Effectively prevents any direct communication between hosts on the internal network with hosts on the external network.

Firewall Architectures



- The most common architecture consists of two packet filters which create a demilitarized zone (DMZ).
- Externally visible servers and gateways are located in the DMZ.

Packetfilter Example: Linux ipchains



- Input chains are lists of filter rules applied to all incoming IP packets.
- Output chains are lists of filter rules applied to all outgoing IP packet.
- Forward chains are lists of fiter rules applied to all forwarded IP packets.

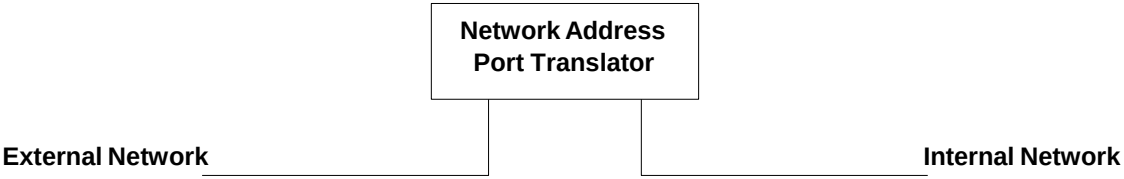
Section 29: Network Address Translators

Network Address Translators

- *Basic Network Address Translation (NAT)*:
  Translates private IP addresses into public IP addresses.
- *Network Address Port Translation (NAPT)*:
  Translates transport endpoint identifiers. NAPT allows to share a single public address among many private addresses (masquerading).
- *Bi-directional NAT (Two-Way NAT)*:
  Translates outbound and inbound and uses DNS-ALGs to facilitate bi-directional name to address mappings.
- *Twice NAT*:
  A variation of a NAT which modifies both the source and destination addresses of a datagram. Used to join overlapping address domains.

Network Address Port Translation Example

Ext. IP	Ext. Port	Int. IP	Int. Port
212.201.44.241	12345	10.50.1.1	1234
212.201.44.241	54321	10.50.1.2	1234
212.201.44.241	15243	10.50.1.1	4321



Full Cone NAT

- A full cone NAT is a NAT where all requests from the same internal IP address and port are mapped to the same external IP address and port.
- Any external host can send a packet to the internal host, by sending a packet to the mapped external address.

Restricted Cone NAT

- A restricted cone NAT is a NAT where all requests from the same internal IP address and port are mapped to the same external IP address and port.
- Unlike a full cone NAT, an external host (with IP address X) can send a packet to the internal host only if the internal host had previously sent a packet to IP address X.

Port Restricted Cone NAT

- A port restricted cone NAT is like a restricted cone NAT, but the restriction includes port numbers.
- Specifically, an external host can send a packet, with source IP address X and source port P, to the internal host only if the internal host had previously sent a packet to IP address X and port P.

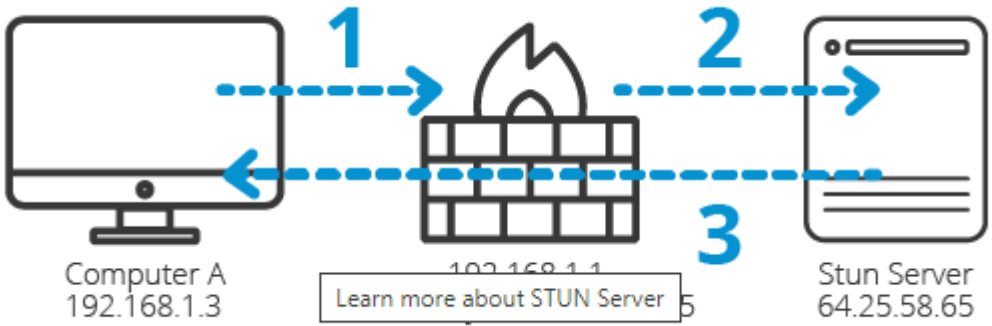
Symmetric NAT

- A symmetric NAT is a NAT where all requests from the same internal IP address and port, to a specific destination IP address and port, are mapped to the same external IP address and port.
- If the same host sends a packet with the same source address and port, but to a different destination, a different mapping is used.
- Only the external host that receives a packet can send a UDP packet back to the internal host.

STUN NAT Traversal (RFC 5389)

- Session Traversal Utilities for NAT (STUN)
- Client / server protocol used for NAT discovery:
  1. The client sends a request to a STUN server
  2. The server returns a response containing the IP address seen by the server (i.e., a mapped address)
  3. The client compares its IP address with the IP address returned by the server; if they are different, the client is behind a NAT and learns its mapped address
- RFC 5780 details a number of tests that can be performed using STUN to determine the behaviour of a NAT.

STUN NAT Traversal (RFC 5389)



References

B. Carpenter and S. Brim.
Middleboxes: Taxonomy andIssues.
RFC 3234, IBM Zurich Research Laboratory, February 2002.

P. Srisuresh and M. Holdrege.
IP Network Address Translator (NAT) Terminology and Considerations.
RFC 2663, Lucent Technologies, August 1999.

B. Carpenter.
Internet Transparency.
RFC 2775, IBM, February 2000.

N. Freed.
Behavior of and Requirements for Internet Firewalls.
RFC 2979, Sun, October 2000.

J. Rosenberg, J. Weinberger, C. Huitema, and R. Mahy.
STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs).
RFC 3489, dynamicsoft, Microsoft, Cisco, March 2003.

E. D. Zwicky, S. Cooper, and D. B. Chapman.
Building Internet Firewalls.
O'Reilly, 2 edition, 2000.