Lecture 14 - 11/05/2019

Firewalls

- An additional layer of defence

Goals

- Single choke point
- Only authorized traffic can pass
- Immune to penetration

Provides

- Service control
- Direction control
- User control
- Behaviour control

Capabilities

- Single admin point
- Monitor sec-related events
- Platform for other (non-sec-related) functions
- Platform for ipsec (VPN in tunnel mode)

IPsec

Transport mode

- Protect (encrypt) the body of the message
- Take that packet and send it where it needs to go
- Nobody can see the contents of the packet in transit.

Tunnel mode

- Take the header and the body and encrypt the whole thing
- Take the encrypted message and make it the body of another packet
- You could modify the sender and receiver of the header

Limitations

- Can’t protect any traffic that does not go through it
    - Any traffic that bypasses the firewall, it will not be able to act on these packets.
- If you have a firewall on the perimeter of your network, It will not protect against internal attacks.
- Can’t protect against naive users.

Types of Filters

There are many different types, all essentially packet filters.

- Positive filter
    - Is a filter that will only allow packets that match a specific criteria.
- Negative filter
    - Is a filter that will only block packets that match a specific criteria.
- Examine only headers
    - Just examines the headers of packets and filters based on those
- Examine header & payload (“deep packet inspection”)
    - Looking at the full content of the packet.
- Examine the pattern generated by a sequence of packets
    - Something that may indicate a DoS attack

Main types of firewalls

Packet filtering firewall

- Applying any of the previously mentioned filters
- “The OG firewall as the kids might say” - Carlise Adams
- It’s going to specifically look at packets and let some through or deny some.

Stateful inspection firewall

- Essentially a packet filtering firewalls
- Also monitors TCP connections
- Keeps a table of src/dest addresses and the establishment state.
- Might also keep track of seq numbers to prevent against session hijacking

Application-level Firewall (Application proxy)

- Any connection that you want to make, it will break into two connections, it connects the user to itself and it connects itself to the service or destination.
- It can then do connection level filtering.
- Works nicely for whitelisted/blacklisted applications
- Lots of overhead

Circuit-level gateway (Circuit-level proxy)

- Same as the application, but happens at the circuit layer
- Happens at the TCP/UDP layer
- Does not look at content, simply looks at connections.

Firewall Installation

Perimeter Firewall

- Installed on the outside of an organization’s network to protect the entire network

Host based firewall

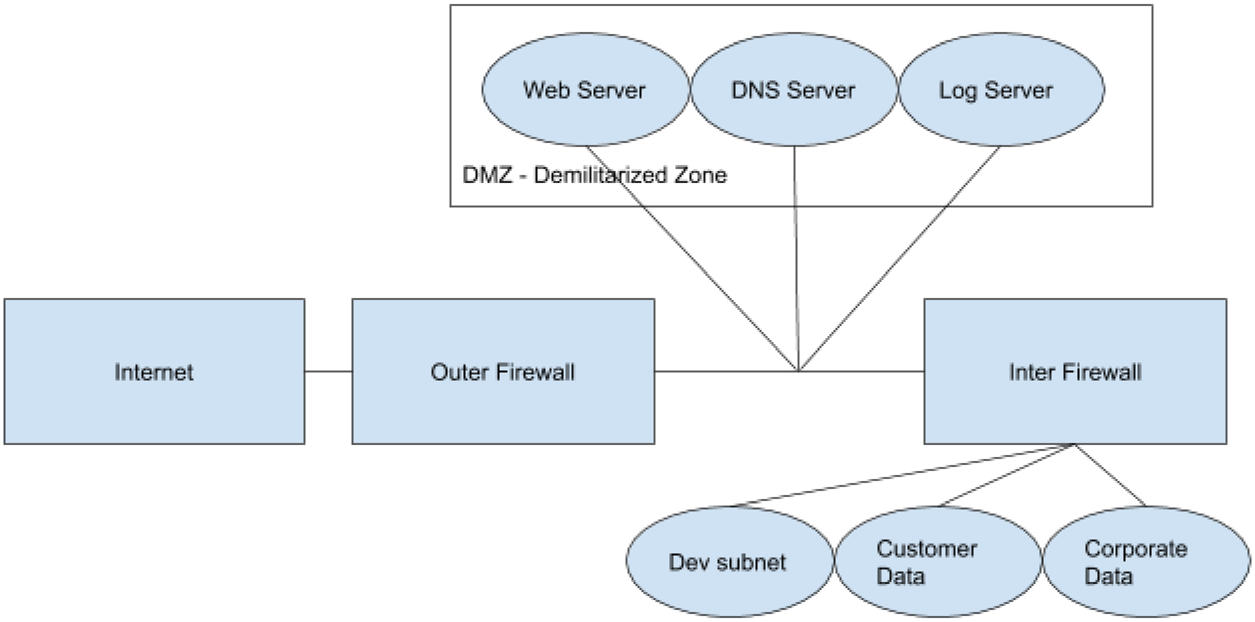
- Host-based firewall is a firewall installed on specific machines or servers within a network

Personal firewall

- Installed on a specific person’s computer
- Less complex than the previous two

Firewall Location

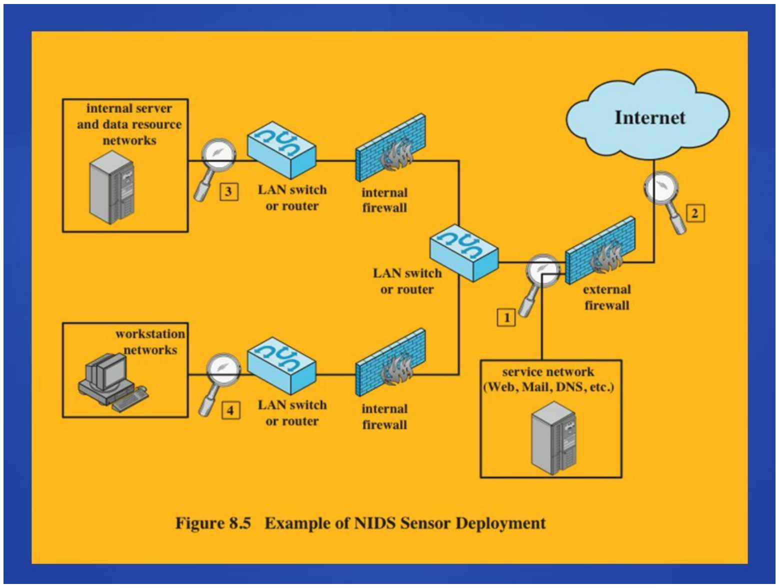
Most common corporate network architecture



Ultimately we want to protect inner services from outer services and do filtering in both directions.

- Any traffic coming in must be trustworthy
- Any traffic going from the DMZ to the internal servers must be scrutinized further.

Internal firewalls can be split up to protect internal resources from each other



Intrusion protection systems

- Is a combination of a firewall and an intrusion detection system
- Can be anywhere in a network, host firewall, perimeter firewall.

Unified threat management

Makes it easier for a system administrator to keep a network safe.

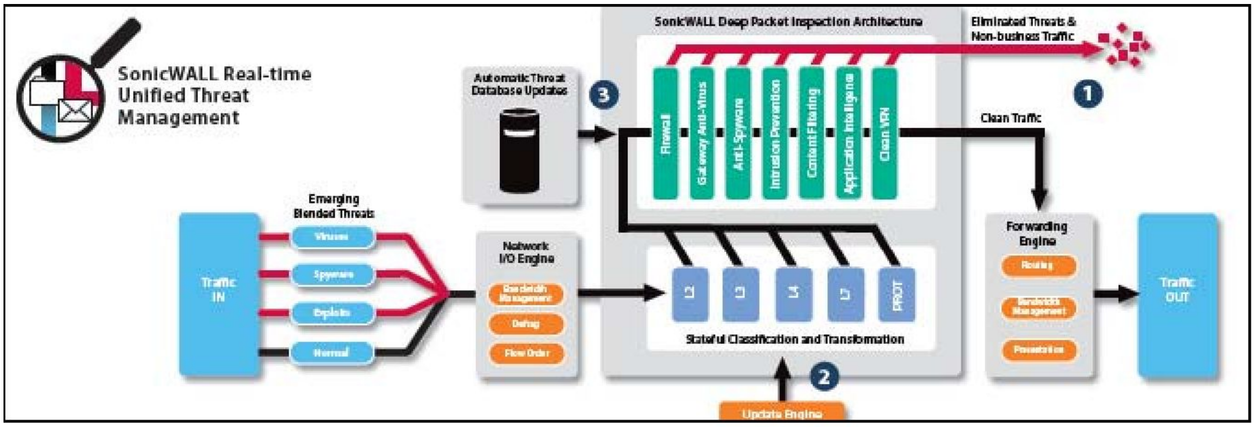


Figure 2: UTM Architecture adapted from SonicWALL 2007

Layers of a UTM will start easy and quick and slowly get more difficult.

Engines themselves will be hardware based so they can be as fast as possible.

Pro: easy to configure and use
Con: Huge hit on performance

Buffer Overflow

In 2000, nearly 45% of software problems were buffer overflow vulns

- Problem exists because C sucks at handling array overflow.
- Why is this still a problem?
    - Legacy code
    - Modern languages make calls to C libraries
- Stack is for argument params
- Heap is for fixed memory allocations