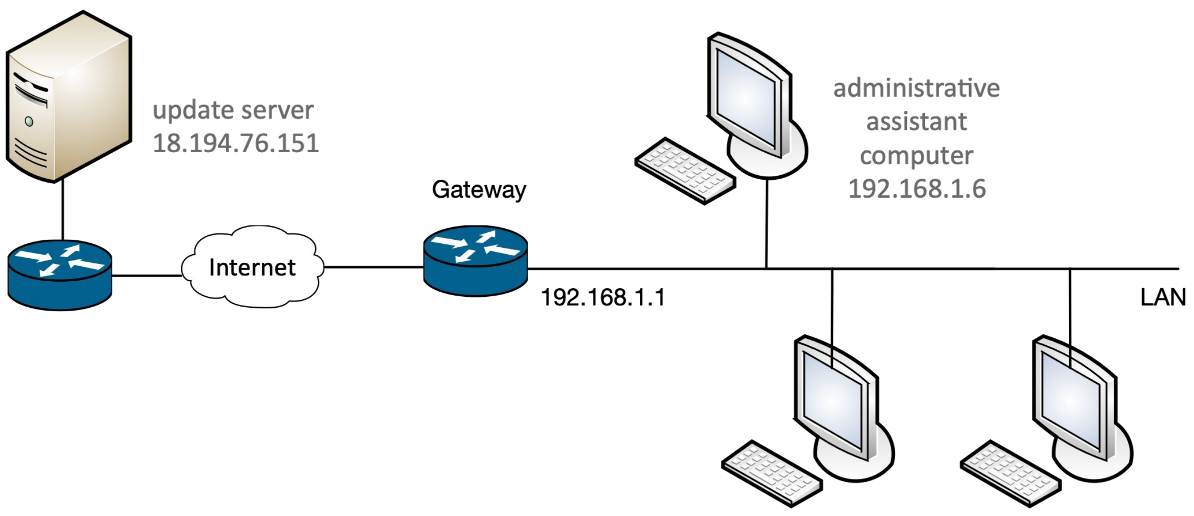
Exercises
Network Protocols Attacks
&
Secure Network Architectures

Computer Security

Question

As part of your job as a security analyst, one of your clients discovers that their network is compromised. In particular, from an early analysis, they have ground to suspect that the start of the compromise was a network attack against the computer of the administrative assistant.

Consider the following (simplified) schema of the company network.



1. Your client managed to capture the network traffic on the administrative assistant's computer (IP address *192.168.1.6* and MAC address *dc:a9:04:7a:ce:29*) when the attack was taking place. During the traffic capture, the computer was automatically updating a well-known accounting software from the software vendor's web server (IP address *18.194.76.151* and MAC address *dc:a6:03:01:02:fe*). You also know that the IP address of the LAN interface of the company's network gateway is *192.168.1.1*, and its MAC address is *b6:28:97:ca:b7:48*.

1 dc:a9:04:7a:ce:29 → ff:ff:ff:ff:ff:ff **ARP** *Who has 192.168.1.1? Tell 192.168.1.6*
2 38:60:77:b9:79:98 → dc:a9:04:7a:ce:29 **ARP** *192.168.1.1 is at 38:60:77:b9:79:98*
3 b6:28:97:ca:b7:48 → dc:a9:04:7a:ce:29 **ARP** *192.168.1.1 is at b6:28:97:ca:b7:48*
4 192.168.1.6 (dc:a9:04:7a:ce:29) → 18.194.76.151 (38:60:77:b9:79:98) **TCP** *SYN*
5 18.194.76.151 (38:60:77:b9:79:98) → 192.168.1.6 (dc:a9:04:7a:ce:29) **TCP** *SYN, ACK*
6 38:60:77:b9:79:98 → dc:a9:04:7a:ce:29 **ARP** *192.168.1.1 is at 38:60:77:b9:79:98*
7 192.168.1.6 (dc:a9:04:7a:ce:29) → 18.194.76.151 (38:60:77:b9:79:98) **TCP** *ACK*
8 38:60:77:b9:79:98 → dc:a9:04:7a:ce:29 **ARP** *192.168.1.1 is at 38:60:77:b9:79:98*
9 192.168.1.6 (dc:a9:04:7a:ce:29) → 18.194.76.151 (38:60:77:b9:79:98) **TCP** *HTTP GET /downloads/software-update.exe*
10 18.194.76.151 (38:60:77:b9:79:98) → 192.168.1.6 (dc:a9:04:7a:ce:29) **TCP** *HTTP 200 OK ...*

(assume that the traffic is captured directly from the network interface card of the employee's PC)

1.1 [2 points]. Describe the attack going on in the network, specifying the name and providing a short explanation of how the attack works *in general*.

1.1 [2 points]. Describe the attack going on in the network, specifying the name and providing a short explanation of how the attack works *in general*.

ARP spoofing, see slide.

1.2 [1 point]. What is the goal of the attack, in this specific case? Motivate your answer.

1.2 [1 point]. What is the goal of the attack, <u>in this specific case</u>? Motivate your answer.

Sniffing or manipulation of the traffic to\from the compromised machine. We can rule out DOS as the traffic passes (there are responses from the server).

Likely, given the scenario (malware infection), the attack is targeted at tampering with the data in transit rather than (or in addition to) sniffing.

1.3 [1 point]. Can you tell the IP address of the attacker? And the MAC address?

1.3 [1 point]. Can you tell the IP address of the attacker? And the MAC address?

IP address: no

MAC address: the attacker is using 38:60:77:b9:79:98, but it could very well be a spoofed address.

1.4 [1 point]. Given only the above packet capture, can you tell whether the attacker is located (i.e., on the LAN, on the same network of the web server, or on an arbitrary Internet-connected network)? Why?

1.4 [1 point]. Given only the above packet capture, can you tell whether the attacker is located (i.e., on the LAN, on the same network of the web server, or on an arbitrary Internet-connected network)? Why?

The attacker is located on the same network of the target machine, i.e., on the LAN.

Question

Suppose that you are the network security administrator of the network `131.168.0.0/24`, with gateway `131.168.0.1` and DNS servers `131.168.0.100` and `131.168.0.101`. While examining the network activity, you notice a DHCP offer packet coming from IP `131.168.0.10` with gateway set to `131.168.0.5`. Answer the following questions and provide a reason. Answers with no reason will not give any point.

- What kind of attack do you suspect, and how does it work?

- What kind of attack do you suspect, and how does it work?

DHCP poisoning. Someone is trying to trick a client connected to 131.168.0.0/24 into believing that `131.168.0.5` *is the gateway, by sending a crafted DHCP offer before, which comes before the real offer sent out by the real DHCP server.*

- Why such an attack works?

- Why such an attack works?

Because the DHCP protocol does not support authentication, so the client must blindly believe any DHCP offer that it sees, and because an arbitrary client can race (and win) against the real DHCP server.

- Can you tell the IP address of the host where those packets come from?

- Can you tell the IP address of the host where those packets come from?

Not really. 131.168.0.10 is the sender of the DHCP offer, but the address may be spoofed. We could look at the MAC address of the scender, but it could be spoofed as well.

- Can you tell the IP address or network address of the victim?

- Can you tell the IP address or network address of the victim?

From the above information there is little evidence to say that, although the potential victims are those that will receive and accept the spoofed DHCP offers. So, likely, 131.168.0.0/24.

Question

A network analyst is analyzing some traffic captured from a network belonging to Politecnico di Milano. The network is: 131.175.0.0/16. In particular, we suspect that a database server, whose IP address is 131.175.14.12, is victim of an attack. Indeed, observing the network traffic, we notice the following pattern:

131.175.14.12 → 131.175.255.255 (broadcast)	[ICMP] Echo (ping) request
131.175.0.2 → 131.175.14.12	[ICMP] Echo (ping) reply
7a:ce:29 → ff:ff:ff (broadcast)	[ARP] Who has 131.175.14.12? Tell 131.175.0.2
4b:74:28 → 7a:ce:29	[ARP] 131.175.14.12 is at 4b:74:28
131.175.0.3 → 131.175.14.12	[ICMP] Echo (ping) reply
131.175.0.4 → 131.175.14.12	[ICMP] Echo (ping) reply
⋮	
131.175.255.251 → 131.175.14.12	[ICMP] Echo (ping) reply
131.175.255.252 → 131.175.14.12	[ICMP] Echo (ping) reply
131.175.255.253 → 131.175.14.12	[ICMP] Echo (ping) reply

1. [2 point] Describe what attack you think is going on, and what is the feature (or lack thereof) of the involved protocol(s) that enable this attack.

1. [2 point] Describe what attack you think is going on, and what is the feature (or lack thereof) of the involved protocol(s) that enable this attack.

PING Smurf - see slides ....

Authentication

2. [2 point] Describe what you think is the **concrete** goal(s) of the attack in this scenario

2. [2 point] Describe what you think is the **concrete** goal(s) of the attack in this scenario

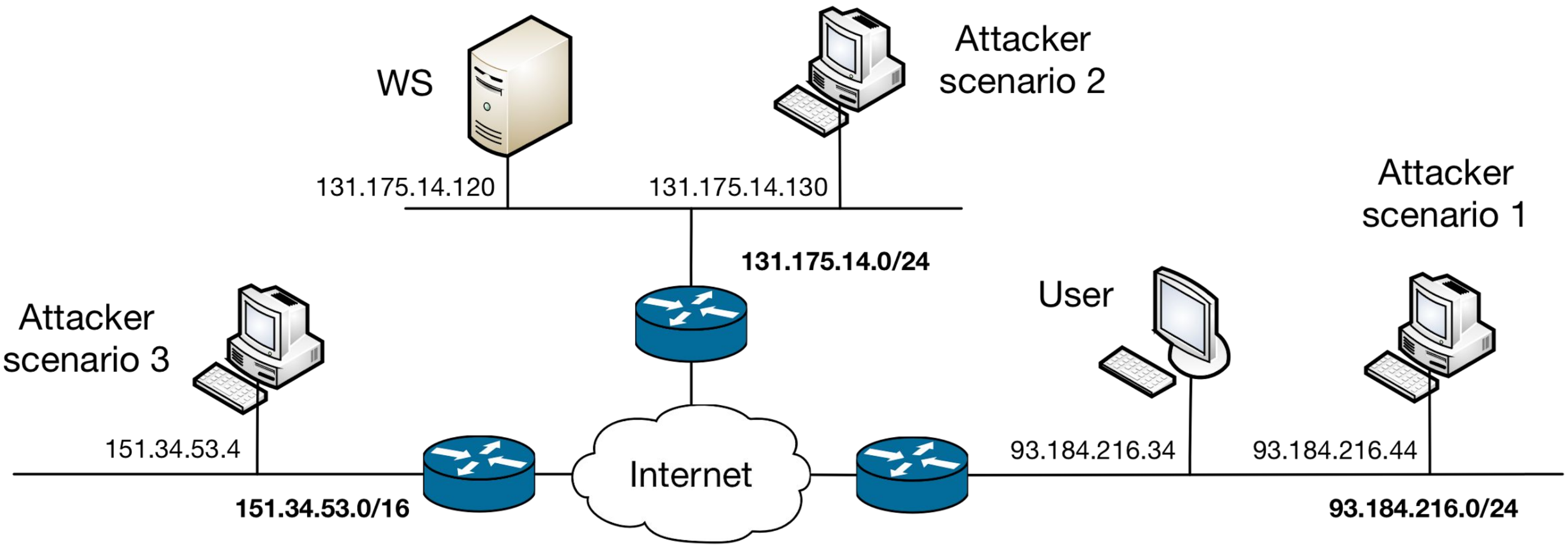
The goal is to saturate the resources of the victim using other machines on the network as an amplification mean. This results in a denial of service.

3. [1 point] Can you tell the IP and MAC address of the attacker? Why?

3. [1 point] Can you tell the IP and MAC address of the attacker? Why?

No, the IP address is spoofed for sure, and the MAC address can be spoofed as well.

Consider the following network diagram:



A user, with IP address 93.184.216.34, is attempting to download a software executable from a webserver in the Politecnico di Milano network, http://downloads.polimi.it, with IP address 131.175.14.120, over the HTTP protocol (no HTTPS, no signatures, nothing). Assume that the user's browser already cached the IP address of downloads.polimi.it (i.e., it does not perform any DNS request), and that there is no firewall involved. An attacker, who knows that the user is about to download this software, wants to target our user by carrying out an attack to replace the downloaded software with a piece of malware.

For each of the following attack scenarios, state whether the attacker is able to fulfill his\her goals. If you deem it possible, describe an attack that allows to do so: state the name of the class of attacks, and describe all the steps needed to make it work in this specific scenarios. If multiple classes of attacks are possible, focus on the simplest one that gets the job done. If no attack is possible, please explain why.

Scenario 1 (attacker: 93.184.216.44; same network and broadcast domain of the user):

Scenario 2 (attacker: 131.175.14.130; same network of web server, but different than user):

Scenario 3 (attacker: 151.34.53.4; attacker, user and webserver on three different networks):

For each of the following attack scenarios, state whether the attacker is able to fulfill his\her goals. If you deem it possible, describe an attack that allows to do so: state the name of the class of attacks, and describe all the steps needed to make it work in this specific scenarios. If multiple classes of attacks are possible, focus on the simplest one that gets the job done. If no attack is possible, please explain why.

Scenario 1 (attacker: 93.184.216.44; same network and broadcast domain of the user):

ARP spoofing ...

Scenario 2 (attacker: 131.175.14.130; same network of web server, but different than user):

Scenario 3 (attacker: 151.34.53.4; attacker, user and webserver on three different networks):

For each of the following attack scenarios, state whether the attacker is able to fulfill his\her goals. If you deem it possible, describe an attack that allows to do so: state the name of the class of attacks, and describe all the steps needed to make it work in this specific scenarios. If multiple classes of attacks are possible, focus on the simplest one that gets the job done. If no attack is possible, please explain why.

Scenario 1 (attacker: 93.184.216.44; same network and broadcast domain of the user):

ARP spoofing ...

Scenario 2 (attacker: 131.175.14.130; same network of web server, but different than user):

ARP spoofing ... (same as before but this time target the server)

Scenario 3 (attacker: 151.34.53.4; attacker, user and webserver on three different networks):

For each of the following attack scenarios, state whether the attacker is able to fulfill his\her goals. If you deem it possible, describe an attack that allows to do so: state the name of the class of attacks, and describe all the steps needed to make it work in this specific scenarios. If multiple classes of attacks are possible, focus on the simplest one that gets the job done. If no attack is possible, please explain why.

Scenario 1 (attacker: 93.184.216.44; same network and broadcast domain of the user):

ARP spoofing …

Scenario 2 (attacker: 131.175.14.130; same network of web server, but different than user):

ARP spoofing … (same as before but this time target the server)

Scenario 3 (attacker: 151.34.53.4; attacker, user and webserver on three different networks):

No attack possible, because HTTP uses TCP and, if sequence numbers are correctly implemented, not possible to perform TCP hijacking. Also, DNS poisoning not possible as DNS response already cached.

For the next questions consider ONLY scenario 3. Assume that each involved computer and server implements a custom TCP/IP stack that, for performance reasons, sets the TCP initial sequence number in the SYN and SYN+ACK packets as the most significant bits of the current timestamp.

2. [2 points]. Describe the security issue with the proposed ISN implementation, and propose a way to solve the issue

For the next questions consider ONLY scenario 3. Assume that each involved computer and server implements a custom TCP/IP stack that, for performance reasons, sets the TCP initial sequence number in the SYN and SYN+ACK packets as the most significant bits of the current timestamp.

2. [2 points]. Describe the security issue with the proposed ISN implementation, and propose a way to solve the issue

Can predict ISN -> solve by using random ISN

For the next questions <u>consider ONLY scenario 3</u>. Assume that each involved computer and server implements a custom TCP/IP stack that, for performance reasons, sets the TCP initial sequence number in the SYN and SYN+ACK packets as <u>the most significant bits of the current timestamp</u>.

3. [2 points]. Describe how the attacker can perform the above attack, this time *exploiting the security issues raised by the custom ISN implementation*. Describe all the steps and assumptions that you need to perform this attack.

For the next questions <u>consider ONLY scenario 3</u>. Assume that each involved computer and server implements a custom TCP/IP stack that, for performance reasons, sets the TCP initial sequence number in the SYN and SYN+ACK packets as <u>the most significant bits of the current timestamp</u>.

3. [2 points]. Describe how the attacker can perform the above attack, this time *exploiting the security issues raised by the custom ISN implementation*. Describe all the steps and assumptions that you need to perform this attack.

TCP hijacking. We can guess the ISN of the SYN packet sent by the victim (the user), we can spoof the webserver IP and send a "correct" SYN+ACK to it and, if we can guess the content of the request (we do), subsequent packets. This way we can send a different payload. In parallel we can also use TCP hijacking to send a fake RST to the actual server spoofing the user's IP address.
Problem\assumption: we need to know the ephemeral port used by the client to initiate the connection.

For the next questions consider ONLY scenario 3. Assume that each involved computer and server implements a custom TCP/IP stack that, for performance reasons, sets the TCP initial sequence number in the SYN and SYN+ACK packets as the most significant bits of the current timestamp.

4. [1 points]. Assume you are the network security administrator of the network of the attacker (in the scenario 3 and assuming the custom TCP initial sequence number implementation), and that you control the border router between the network 151.34.53.0/24 and the rest of the Internet. Propose a way to prevent the attack. Can the administrator of the other two border routers in the diagram deploy the same mitigation, and obtain the same result? Why?

For the next questions consider ONLY scenario 3. Assume that each involved computer and server implements a custom TCP/IP stack that, for performance reasons, sets the TCP initial sequence number in the SYN and SYN+ACK packets as the most significant bits of the current timestamp.

4. [1 points]. Assume you are the network security administrator of the network of the attacker (in the scenario 3 and assuming the custom TCP initial sequence number implementation), and that you control the border router between the network 151.34.53.0/24 and the rest of the Internet. Propose a way to prevent the attack. Can the administrator of the other two border routers in the diagram deploy the same mitigation, and obtain the same result? Why?

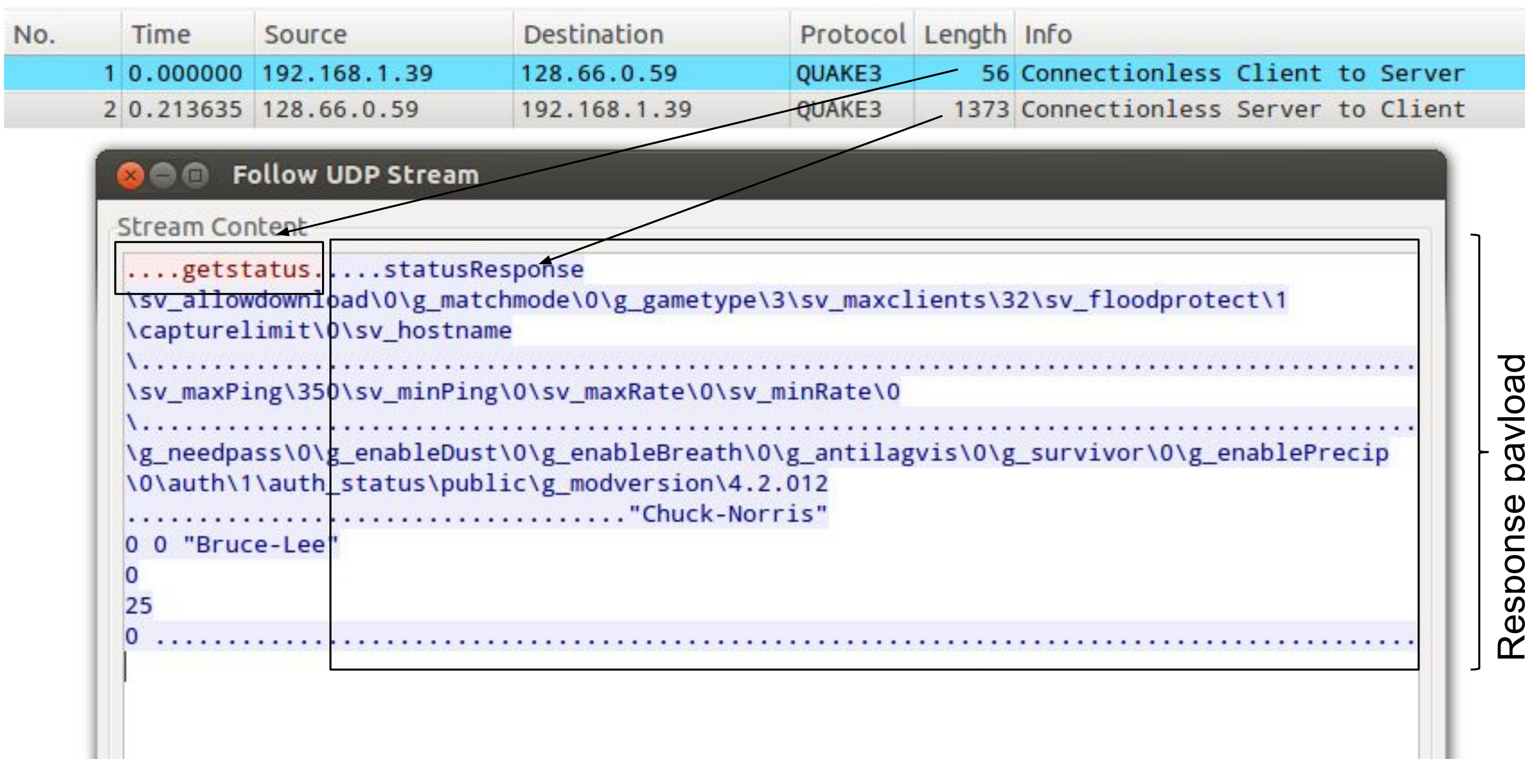
We can filter the packets with source IPs not belonging to our network. Other routers can't do this, they can only filter out packets coming from "outside" with spoofed IPs belonging to their network, but it's of little use in this scenario.

Question

Consider the “Quake III Arena Network Protocol”, a stateless client-server protocol used by the classic multi-player game. Quake III supports multiple game servers (indeed, anyone can run their server, expose it to the whole Internet, and even have it indexed by the “master server” for easy discovery).

When a client connects to one of the many available servers, it needs to retrieve some information. To this purpose, the Quake III protocol implements the command “`gestatus`”, accessible without authentication. When the server receives this command (via an UDP packet, destination port 27960), it replies with various information, such as: the list of enabled options, the hostname, the number of connected clients, and the type of supported game.

The image below is an example of protocol exchange, as shown in Wireshark, a packet capture tool: a client (192.168.1.39) sends a `getstatus` message to a server (128.66.0.59); the server replies with a `statusResponse` message, containing the information about the server in its payload.



2. [2 points] The part of the Quake III Arena protocol described in the previous page can be "misused" to *ease* a DoS attack against a victim. Please explain how an attack can misuse this protocol for this purpose, showing a concrete scenario where an attacker (who controls the server with IP address 93.184.216.32) aims to launch a DoS against the IP address 131.175.14.19. Make sure you mention in your answer the "feature" of this protocol that allows the misuse for DoS purpose.

2. [2 points] The part of the Quake III Arena protocol described in the previous page can be "misused" to *ease* a DoS attack against a victim. Please explain how an attack can misuse this protocol for this purpose, showing a concrete scenario where an attacker (who controls the server with IP address 93.184.216.32) aims to launch a DoS against the IP address 131.175.14.19. Make sure you mention in your answer the "feature" of this protocol that allows the misuse for DoS purpose.

The protocol allows an amplification-based denial of service: in fact, it is a UDP-based protocol, where a request of length 56 triggers a response of 1373 (in the example above), leading to a bandwidth amplification factor (BAF) of 24, i.e., "amplifying" the attacker's bandwidth of a factor of 24 (which means that, extremely roughly, if the attacker has a 100 Mbps network, given enough open Quake III servers with enough bandwidth each, it can flood the victim with a 2400 Mbps traffic).

*Concretely, the attacker (given he\she is in a network that allows IP spoofing) looks on the Internet for N open Quake III servers. It spoofs the victim's IP address, and sends to such servers M UDP "getstatus" packets. Each server will reply, for each packet received, with with the (long) information packet --- but, as the source IP is spoofed, the M * N packets will go to the victim, instead of the attacker.*

We discovered in the wild a DoS attack that exploits this protocol. The network administrators of the company that was hit by this attack were able to capture the following headers of some suspect packets at their network's border firewall:

```
IP 87.98.244.20 (src port 27960)  > 104.28.1.1 (dst port 12345)  UDP, length 1373
IP 87.98.244.20 (src port 27960)  > 104.28.1.1 (dst port 12345)  UDP, length 1373
IP 188.138.125.254 (src port 27960)   > 104.28.1.1 (dst port 32451)  UDP, length 1400
IP 188.138.125.254 (src port 27960)   > 104.28.1.1 (dst port 32451)  UDP, length 1400
IP 188.138.125.254 (src port 27960)   > 104.28.1.1 (dst port 32451)  UDP, length 1400
IP 188.138.125.254 (src port 27960)   > 104.28.1.1 (dst port 32451)  UDP, length 1400
IP 188.138.125.254 (src port 27960)   > 104.28.1.1 (dst port 32451)  UDP, length 1400
IP 5.196.85.159 (src port 27960)  > 104.28.1.1 (dst port 32451)  UDP, length 978
```

3. [1 point] Can you identify the attacker's IP address? And the victim's one? Why?

3. [1 point] Can you identify the attacker's IP address? And the victim's one? Why?

<u>Attacker</u>: no, the IP address you see in the logs are the ones of the vulnerable Quake III servers, not of the victim. Also, the vulnerable Quake servers can't identify the attacker's IP address as they're spoofed with the victim's IP.

<u>Victim</u>: yes, it's 104.28.1.1 (actually it could also be the border firewall or, in general, the company's network)

4. [1 point] As the network security administrator for the network hit by this attack (i.e., you control the border firewall and can add arbitrary rules), can you mitigate the effect of this attack or prevent it altogether? Why?

4. [1 point] As the network security administrator for the network hit by this attack (i.e., you control the border firewall and can add arbitrary rules), can you mitigate the effect of this attack or prevent it altogether? Why?

No. Due of the amplifying properties of the protocol, if the attacker has enough bandwidth that, amplified by the 24x factor of the protocol, is >= the victim's bandwidth, the attacker always succeeds.

However, if in this specific scenario the victim is the specific machine 104.28.1.1 and the bottleneck is not given by the (network bandwidth of the Internet → company link), but from something else (e.g., the bandwidth of an internal network link, the capabilities of the machine itself, the capabilities of some network middlebox, ...) implementing a firewall rule to drop UDP packet from source port 27960 can mitigate the attack (and thus it would be a good idea to implement).

In general, though, a more powerful DoS attack may be launched to defeat this mitigation…

5. [1 point] Consider the following mitigation implemented by the Quake III Arena server: "*when an IP address sends a* `getstatus` *command, the server will check if sender IP address has exceeded a pre-defined rate limit of 10 commands in a period of one second; if the rate limit is exceeded, the IP address is banned from the server forever*".

Is this solution effective to mitigate the impact of the DoS scenario in the above attack? Why?

5. [1 point] Consider the following mitigation implemented by the Quake III Arena server: "*when an IP address sends a* `getstatus` *command, the server will check if sender IP address has exceeded a pre-defined rate limit of 10 commands in a period of one second; if the rate limit is exceeded, the IP address is banned from the server forever*".

Is this solution effective to mitigate the impact of the DoS scenario in the above attack? Why?

No. While this mitigation restricts an attacker to exploit a vulnerable server as an amplifier at most 10 packets per second (i.e., 13730 bytes/s, i.e., about 100 kbps), given that enough vulnerable servers are available the attacker can just use multiple vulnerable Quake III servers at once to defeat the rate limit.

Moreover, if the attacker is targeting a network and not a specific IP address, it can spoof multiple IP of the same network, defeating the rate limiting.

6. [1 point] As the author(s) of Quake III Arena, you want to change the protocol to remove completely the issue that allows it from being exploited for DoS attacks. How would you <u>change the protocol</u> to achieve this goal?

6. [1 point] As the author(s) of Quake III Arena, you want to change the protocol to remove completely the issue that allows it from being exploited for DoS attacks. How would you change the protocol to achieve this goal?

Solution 1: Implement an handshake at the UDP protocol level (making sure it does not have amplifying capabilities). E.g., the client sends getinfo, the server responds with a nonce, and the client sends the nonce back to the server, then the server sends the "long" information message.

Solution 2: Move the protocol to TCP instead of UDP as a transport protocol. Due to the three-way handshake, TCP is immune to the amplification issue.

Question

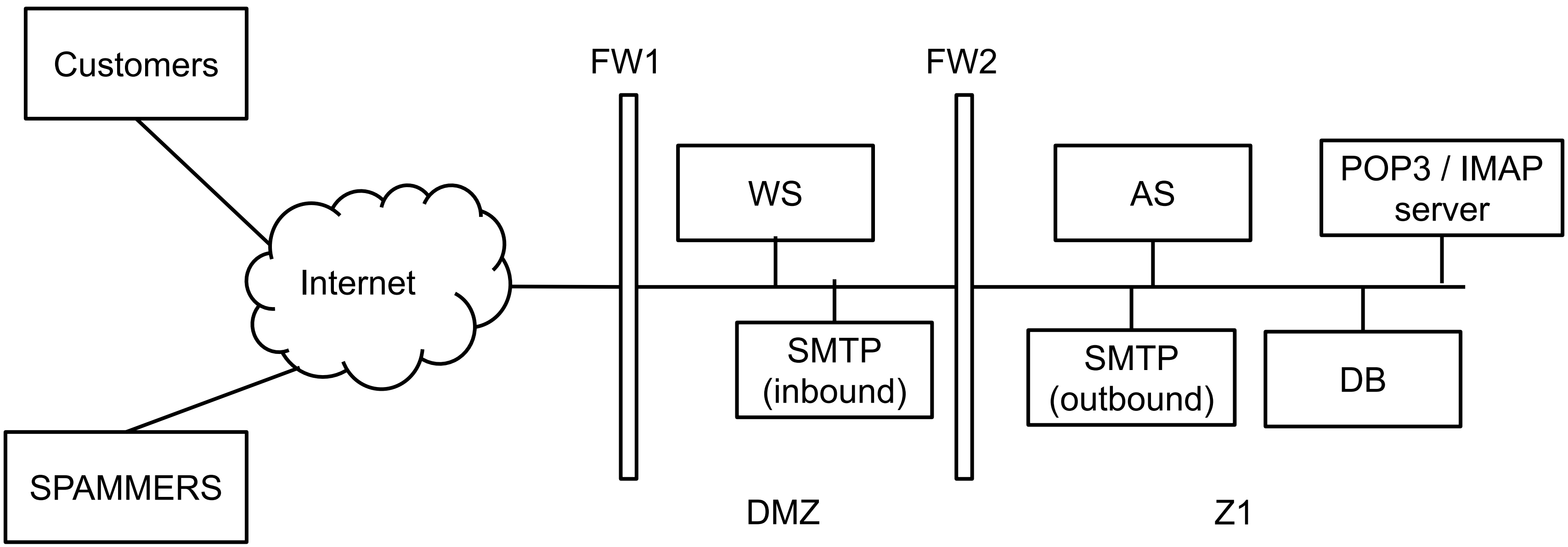
FreeMail is an anti-spam company that aims to fight spam using an innovative “vigilante” approach. FreeMail’s customers report their spam e-mails to FreeMail. Then, FreeMail leaves a generic complaint for each spam e-mail reported by users. FreeMail operates on the assumption that, as the community grows, the flow of complaints from hundreds of thousands of computers will apply enough pressure on spammers and their clients to convince them to stop spamming.

Users can report spam e-mails either through a web application (accessible over HTTPS) or by forwarding the spam messages to a dedicated e-mail address (i.e., inbound e-mails are received by a dedicated SMTP server). The web server uses application logic deployed on an application server. The logic implemented on the application server automatically visits every website advertised by the URLs in the spam messages and leaves complaints on those websites. Complaints are left in the website’s contact forms or, if the application logic can’t find any contact form, by sending an email to the spammer provider’s abuse contact (obtained by querying the WHOIS service). Furthermore, the application server saves in a SQL database information about the spam messages that are reported.

Read **all** the following questions and **then** answer one by one:

1. [1 points] Draw FreeMail’s network layout and assign distinct names to any machine and zone. [1 points] Draw FreeMail’s network layout and assign distinct names to any machine and zone.

1. [1 points] Draw FreeMail's network layout and assign distinct names to any machine and zone. [1 points] Draw FreeMail's network layout and assign distinct names to any machine and zone.



1. [3 points] Write the firewall rules, assuming firewalls to be stateful packet filters (i.e. you can consider the response rules implicit)

Firewall	Src IP	Src PORT	Direction of the 1st packet	Dst IP	Dst PORT	Policy	Description
FW1 (example)	10.0.0.1 (example)	ANY	zone 1 -> zone 2	192.168.0.2 (example)	443	DENY	(example: the X server in zone 1 cannot contact the Y server)

Firewall	Src IP	Src PORT	Direction of the 1st packet	Dst IP	Dst PORT	Policy	Description
FW1 (example)	10.0.0.1 (example)	ANY	zone 1 -> zone 2	192.168.0.2 (example)	443	DENY	(example: the X server in zone 1 cannot contact the Y server)
FW1	*ALL*	*ANY*	*ANY*	*ALL*	*ANY*	*DENY*	*Default deny*
FW1	*ANY*	*ANY*	*Internet -> DMZ*	*WS_IP*	*443 (HTTPS)*	*ALLOW*	*The webserver is publicly reachable*
FW1	*ANY*	*ANY*	*Internet -> DMZ*	*SMTPIN_IP*	*25*	*ALLOW*	*The SMTP server is publicly reachable*
FW2	*ALL*	*ANY*	*ANY*	*ALL*	*ANY*	*DENY*	*Default deny*
FW2	*WS_IP*	*ANY*	*DMZ → Z1*	*AS_IP*	*CUST*	*ALLOW*	*The webserver connects to the application server*
FW2	*SMTPIN_IP*	*ANY*	*DMZ → Z1*	*IMAP_IP*	*587*	*ALLOW*	*SMTPIn relays the incoming e-mails to the POP3\IMAP server (used by the application server)*
FW2	*AS_IP*	*ANY*	*Z1 → DMZ*	*ANY*	*80, 443*	*ALLOW*	*The application server connects to the spammer's websites*
FW1	*AS_IP*	*ANY*	*DMZ → Internet*	*ANY*	*80, 443*	*ALLOW*	*The application server connects to the spammer's websites*
FW2	*SMTPOUT_IP*	*ANY*	*Z1 → DMZ*	*ANY*	*25*	*ALLOW*	*The application server sends email to the abuse contacts (relayed by the SMTPOut server)*
FW1	*SMTPOUT_IP*	*ANY*	*DMZ → Internet*	*ANY*	*25*	*ALLOW*	*The application server sends email to the abuse contacts (relayed by the SMTPOut server)*
FW2	*AS_IP*	*ANY*	*Z1 → DMZ*	*ANY*	*WHOIS*	*ALLOW*	*The application server contacts the WHOIS servers*
FW1	*AS_IP*	*ANY*	*DMZ → Internet*	*ANY*	*WHOIS*	*ALLOW*	*The application server contacts the WHOIS servers*

After a short while since the beginning of their operations, FreeMail's public web site comes under a massive **DDoS attack** that uses **SYN flooding**.

1. Briefly describe **SYN flooding** attack and how the attack can cause a denial-of-service.

After a short while since the beginning of their operations, FreeMail's public web site comes under a massive **DDoS attack** that uses **SYN flooding**.

1. Briefly describe **SYN flooding** attack and how the attack can cause a denial-of-service.

A SYN flooding attack sends a stream of TCP "initial SYN" packets to the targeted server. Each packet appears to represent a request to establish a new connection. An attack that employs a large botnet, for example, might not use spoofing. : For each incoming SYN packet, the server both responds and consumes memory because it records information (state) associated with the impending new connection. The attack primarily aims to exhaust the server's available memory for keeping this state.

After a short while since the beginning of their operations, FreeMail's public web site comes under a massive **DDoS attack** that uses **SYN flooding**.

1. [2 points] Briefly describe **one countermeasure** that FreeMail could use to defend itself from this attack.

After a short while since the beginning of their operations, FreeMail's public web site comes under a massive **DDoS attack** that uses **SYN flooding**.

1. [2 points] Briefly describe **one countermeasure** that FreeMail could use to defend itself from this attack.

Syn cookies

After a short while since the beginning of their operations, FreeMail's public web site comes under a massive **DDoS attack** that uses **SYN flooding**.

1. [2 points] Can FreeMail use a stateful **packet-filter firewall** to defend itself against the SYN flooding-based DDoS? If so, describe what sort of rule or rules the firewall would need to apply, and what "collateral damage" the rules would incur. If not, explain why not.

After a short while since the beginning of their operations, FreeMail's public web site comes under a massive **DDoS attack** that uses **SYN flooding**.

1. [2 points] Can FreeMail use a stateful **packet-filter firewall** to defend itself against the SYN flooding-based DDoS? If so, describe what sort of rule or rules the firewall would need to apply, and what "collateral damage" the rules would incur. If not, explain why not.

Possible solutions:

(1) If the flood uses a fixed number (not too large) of IP source addresses in its packets, then the target could install a number of firewall rules that deny traffic from those addresses. In this case, the collateral damage depends on how much legitimate traffic also comes from those addresses.

(2) If the flood uses a very large number of IP source addresses, either by employing a large number of different systems ("bots") to send the traffic, or by spoofing the IP source address in each SYN packet, it is not feasible to defend against the attack. The target cannot use a rule such as "drop any incoming TCP SYN sent to our web server" without enabling the attack to fully succeed, i.e., the collateral damage would be that no legitimate traffic can reach the server.

After a short while since the beginning of their operations, FreeMail's public web site comes under a massive **DDoS attack** that uses **SYN flooding**.

1. [2 points] Explain how the FreeMail service could itself be used to mount a DoS attack and how a victim can defend itself.

After a short while since the beginning of their operations, FreeMail's public web site comes under a massive **DDoS attack** that uses **SYN flooding**.

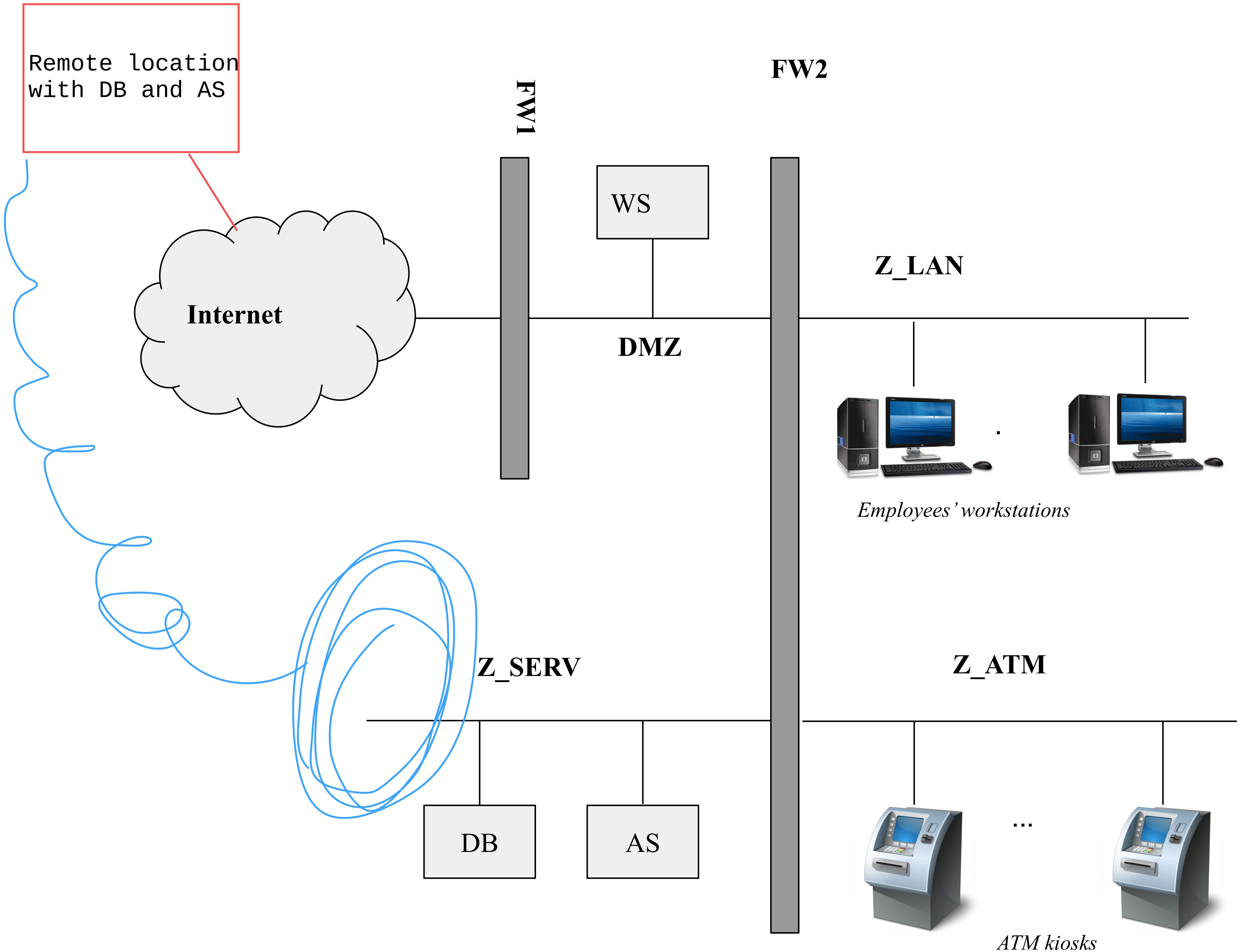
1. [2 points] Explain how the FreeMail service could itself be used to mount a DoS attack and how a victim can defend itself.

An attacker could send a large number of bogus spam reports to FreeMail, falsely indicating some victim site V has been sending spam. FreeMail's servers will then visit V to lodge complaints, overwhelming V in the process if the volume of visits is high enough. A victim can defend itself by blocking Freemail IP address.

Question

A small bank is in the process of setting up the network of their only, very small, branch. The branch employees, from their **desktop computers**, need to access the **Internet** for work purposes (e.g., accessing their web-based email) as well as use an **internal web application**, served from the branch web server over the **HTTP protocol**. The web server also hosts the customer-facing **online banking application**, available over the Internet and served over the **HTTPS protocol**. Furthermore, the web server is backed by (i.e., communicates with) an **application server**, which stores its data on a **relational database server**. As the information processed by the application server and stored in the database server is sensitive, there is a strong requirement to prevent the employees from directly accessing those servers.
Besides the employee computers, the branch has some **ATM kiosks** that allow self-service cash withdrawals and account balance inquiries. To process those transactions, ATMs communicate with the application server over a proprietary protocol. The ATMs do not have access to either the Internet or any other network.

The layout of this network is the following:


Remote location
with DB and AS
FW1
FW2
WS
Internet
DMZ
Z_LAN
Employees' workstations
Z_SERV
Z_ATM
DB
AS
...
ATM kiosks

Firewall	Src IP	Src PORT	Direction of the 1st packet	Dst IP	Dst PORT	Policy	Description
FW1 (example)	*10.0.0.1 (example)*	*ANY*	*zone 1 -> zone 2*	*192.168.0.2 (example)*	*443*	*DENY*	*(example: the X server in zone 1 cannot contact the Y server)*

Firewall	**Src IP**	**Src PORT**	**Direction of the 1st packet**	**Dst IP**	**Dst PORT**	**Policy**	**Description**
FW1 (example)	*10.0.0.1 (example)*	*ANY*	*zone 1 -> zone 2*	*192.168.0.2 (example)*	*443*	*DENY*	*(example: the X server in zone 1 cannot contact the Y server)*
FW1, FW2,	ANY	ANY	ANY	ANY	ANY	DENY	DENY ALL
FW1	ANY	ANT	Internet → DMZ	WS_IP	443	ALLOW	Online banking access
FW1	Any IP in Z_LAN	ANY	DMZ → Internet	ANY	80, 443	ALLOW	Internet access for employees
FW2	Any IP in Z_LAN	ANY	Z_LAN → DMZ	ANY	80, 443	ALLOW	Internet access for employees + internal webapp access
FW2	WS_IP	ANY	DMZ → Z_SERV	AS_IP	AS_PORT	ALLOW	Web server → application server
FW2	Any IP in Z_ATM	ANY	Z_ATM → Z_SERV	AS_IP	AS_PORT	ALLOW	ATM Kioks → application server

2. [1 point] Let's consider a more realistic scenario: the bank is now part of a larger banking group. While keeping its own web server locally, the application server and database server are now shared among various branches and kept in a central location, where they need to be made remotely accessible from each branch (and from the bank branches <u>only</u>).

How would you securely realize this architecture? Please state your assumption and detail any changes to the network diagram for this scenario.

2. [1 point] Let's consider a more realistic scenario: the bank is now part of a larger banking group. While keeping its own web server locally, the application server and database server are now shared among various branches and kept in a central location, where they need to be made remotely accessible from each branch (and from the bank branches <u>only</u>).

How would you securely realize this architecture? Please state your assumption and detail any changes to the network diagram for this scenario.

The AS and DB are now in a remote location. As we don't want to expose them over the Internet, we need to set up a VPN between our network and the central branch. Basically we can accomplish this by setting up a VPN between the remote location and placing the VPN client in Z_SERV to bridge the Z_SERV network with the remote network (or assuming to set up a firewall-to-firewall VPN with the appropriate policies). As the overall network structure is unchanged, except for the VPN tunnel, the firewall policies would be the same.

3. [1 point] The bank is worried that, as employees have full access to the Internet, their computer could become infected with malware. Thus, he decides to install a system to analyze the <u>content</u> of any HTTP response and scan it with an anti-virus for the presence of known malware. Assume we're interested in filtering traffic to HTTP pages only. What kind of packet filter should the bank put between the employees' LAN and the Internet zone? Why?

3. [1 point] The bank is worried that, as employees have full access to the Internet, their computer could become infected with malware. Thus, he decides to install a system to analyze the <u>content</u> of any HTTP response and scan it with an anti-virus for the presence of known malware. Assume we're interested in filtering traffic to HTTP pages only. What kind of packet filter should the bank put between the employees' LAN and the Internet zone? Why?

As we need to analyze the content, we need an application proxy (an HTTP proxy in particular).

4. [1 point] Is it possible to reach the same goal if the pages are served via HTTPS? How?

4. [1 point] Is it possible to reach the same goal if the pages are served via HTTPS? How?

…… HTTPS man in the middle ….. Trusted cert on employees computers …..

5. [4 points] Whoops! You discover that a network expert customer was able to enter the branch, locate a spare network outlet connected to the employees network (Z_LAN), connect his\her laptop and *intercept all the HTTP communication between the a bank employee and the branch web server exploiting the gateway*, with terrible consequences! Now the bank CISO wants a detailed report on what could have happened and on how we could prevent this to ever happen in the future. Please answer the following questions:

(a) Can you guess a technique that the customer could have used to reach this goal? State the name and briefly describe how it works *in general*.

5. [4 points] Whoops! You discover that a network expert customer was able to enter the branch, locate a spare network outlet connected to the employees network (Z_LAN), connect his\her laptop and *intercept all the HTTP communication between the a bank employee and the branch web server exploiting the gateway*, with terrible consequences! Now the bank CISO wants a detailed report on what could have happened and on how we could prevent this to ever happen in the future. Please answer the following questions:

(a) Can you guess a technique that the customer could have used to reach this goal? State the name and briefly describe how it works *in general*.

ARP spoofing, see slides

5. [4 points] Whoops! You discover that a network expert customer was able to enter the branch, locate a spare network outlet connected to the employees network (Z_LAN), connect his\her laptop and *intercept all the HTTP communication between the a bank employee and the branch web server exploiting the gateway*, with terrible consequences! Now the bank CISO wants a detailed report on what could have happened and on how we could prevent this to ever happen in the future. Please answer the following questions:

(b) Detail all the steps that the customer could have performed in order to intercept the communication between a bank employee's computer and the web server *in this specific scenario*.

5. [4 points] Whoops! You discover that a network expert customer was able to enter the branch, locate a spare network outlet connected to the employees network (Z_LAN), connect his\her laptop and *intercept all the HTTP communication between the a bank employee and the branch web server exploiting the gateway*, with terrible consequences! Now the bank CISO wants a detailed report on what could have happened and on how we could prevent this to ever happen in the future. Please answer the following questions:

(b) Detail all the steps that the customer could have performed in order to intercept the communication between a bank employee's computer and the web server *in this specific scenario*.

The customer uses ARP spoofing to pose as the network gateway and sniff all the communication between the employee's computer and the gateway, including the traffic to the WS.

1. The customer learns the IP address (e.g., by obtaining it via DHCP, or, if DHCP is not enabled, by passively sniffing the network broadcast traffic) and the real MAC address of the gateway (via ARP);

2. The customer broadcasts ARP messages with the gateway IP address and the customer's own MAC address;

3. If the spoofing succeeds, the traffic to the gateway is directed to the customer (the customer also forwards traffic to the real gateway). This, way, the customer is able to sniff all the information between the client and the gateway and, thus, between the client and the local web server.

5. [4 points] Whoops! You discover that a network expert customer was able to enter the branch, locate a spare network outlet connected to the employees network (Z_LAN), connect his\her laptop and *intercept all the HTTP communication between the a bank employee and the branch web server exploiting the gateway*, with terrible consequences! Now the bank CISO wants a detailed report on what could have happened and on how we could prevent this to ever happen in the future. Please answer the following questions:

(c) Describe a possible way for the branch to prevent, or mitigate, this type of attack *in this specific scenario, besides disabling/locking/damaging the* spare network outlet found by the customer.

5. [4 points] Whoops! You discover that a network expert customer was able to enter the branch, locate a spare network outlet connected to the employees network (Z_LAN), connect his\her laptop and *intercept all the HTTP communication between the a bank employee and the branch web server exploiting the gateway*, with terrible consequences! Now the bank CISO wants a detailed report on what could have happened and on how we could prevent this to ever happen in the future. Please answer the following questions:

(c) Describe a possible way for the branch to prevent, or mitigate, this type of attack *in this specific scenario, besides disabling/locking/damaging the* spare network outlet found by the customer.

From the application point of view: use HTTPS with a certificate trusted by the browsers of the employee computers (BONUS: in this case it is important also to enable HSTS to prevent the customer to try to downgrade the communication to unencrypted HTTP or to train the employees to always check whether the communication is encrypted). From the network point of view: various techniques; for example, 802.1x to authenticate clients connected to ethernet ports or attempt, ... (in general this approach is complementary to the use of HTTPS).

5. [4 points] Whoops! You discover that a network expert customer was able to enter the branch, locate a spare network outlet connected to the employees network (Z_LAN), connect his\her laptop and *intercept all the HTTP communication between the a bank employee and the branch web server exploiting the gateway*, with terrible consequences! Now the bank CISO wants a detailed report on what could have happened and on how we could prevent this to ever happen in the future. Please answer the following questions:

(d) Can the same attack be used to intercept communication between the web server and the application server?

5. [4 points] Whoops! You discover that a network expert customer was able to enter the branch, locate a spare network outlet connected to the employees network (Z_LAN), connect his\her laptop and *intercept all the HTTP communication between the a bank employee and the branch web server exploiting the gateway*, with terrible consequences! Now the bank CISO wants a detailed report on what could have happened and on how we could prevent this to ever happen in the future. Please answer the following questions:

(d) Can the same attack be used to intercept communication between the web server and the application server?

No, as they are on different networks.

Question

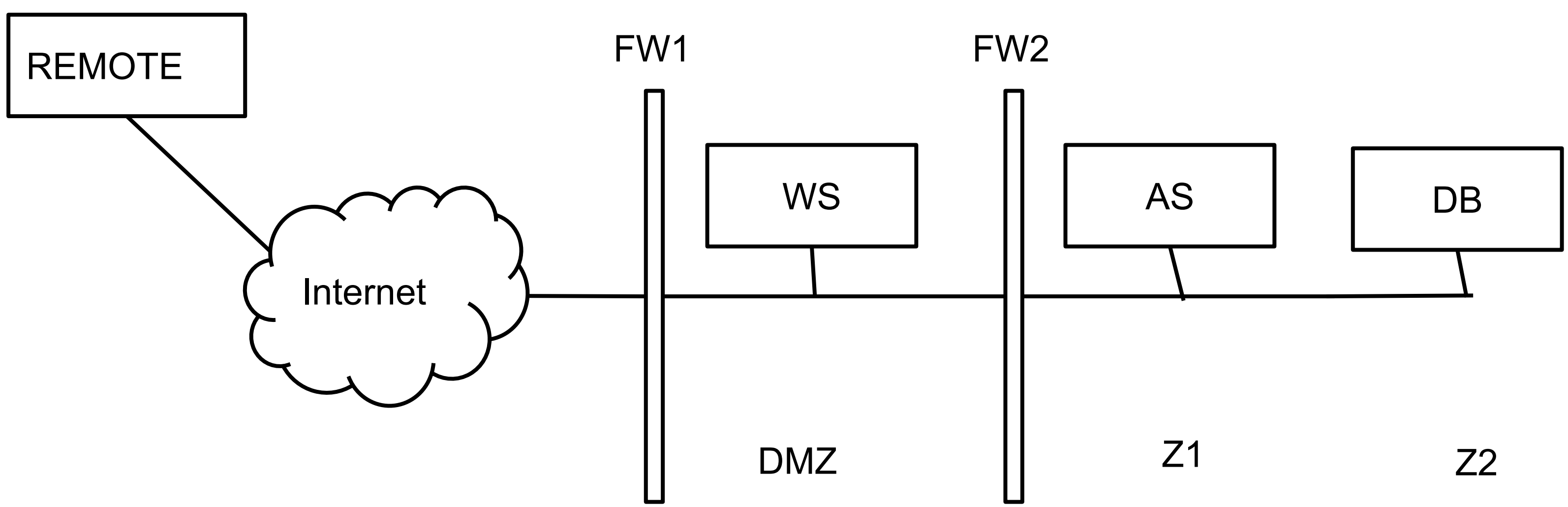
An online shop offers to its customers a **web application, publicly reachable from the Internet**, deployed on a **web server**. The web server uses application logic deployed on an **application server**. The application logic alone implements queries executed on a **database server**. The **application server** must be able to initiate a communication with a **remote web service** over HTTPS, and **receive the responses**, to perform payment transactions.

Read **all** the following questions and **then** answer one by one:

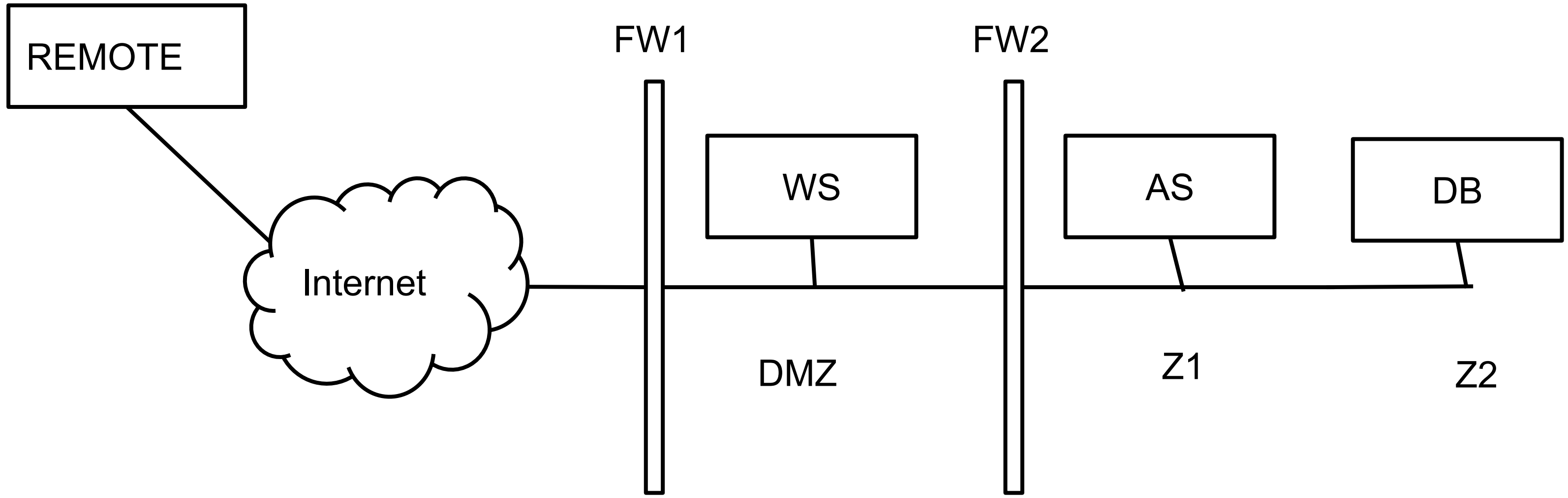
Draw the network layout and assign distinct names to any machine and zone.

Draw the network layout and assign distinct names to any machine and zone.

An online shop offers to its customers a web application, publicly reachable from the Internet, deployed on a web server. The web server uses application logic deployed on an application server. The application logic alone implements queries executed on a database server. The application server must be able to initiate a communication with a remote web service over HTTPS, and receive the responses, to perform payment transactions.

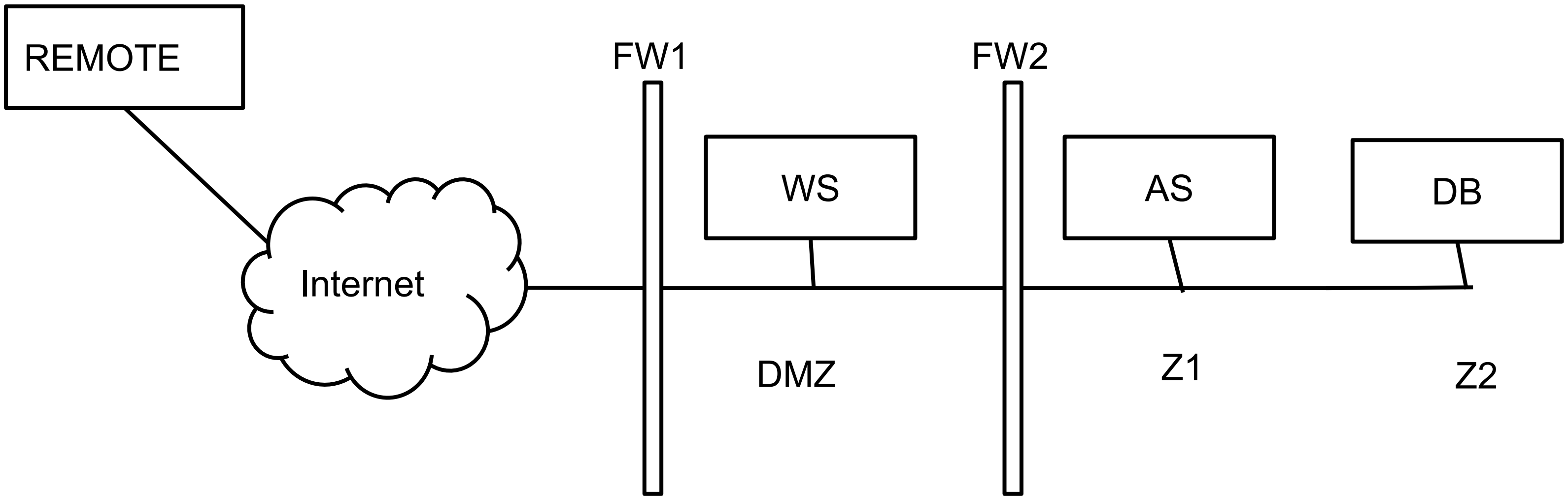


Write the firewall rules, assuming firewalls to be stateful packet filters (i.e. you can consider the response rules implicit)



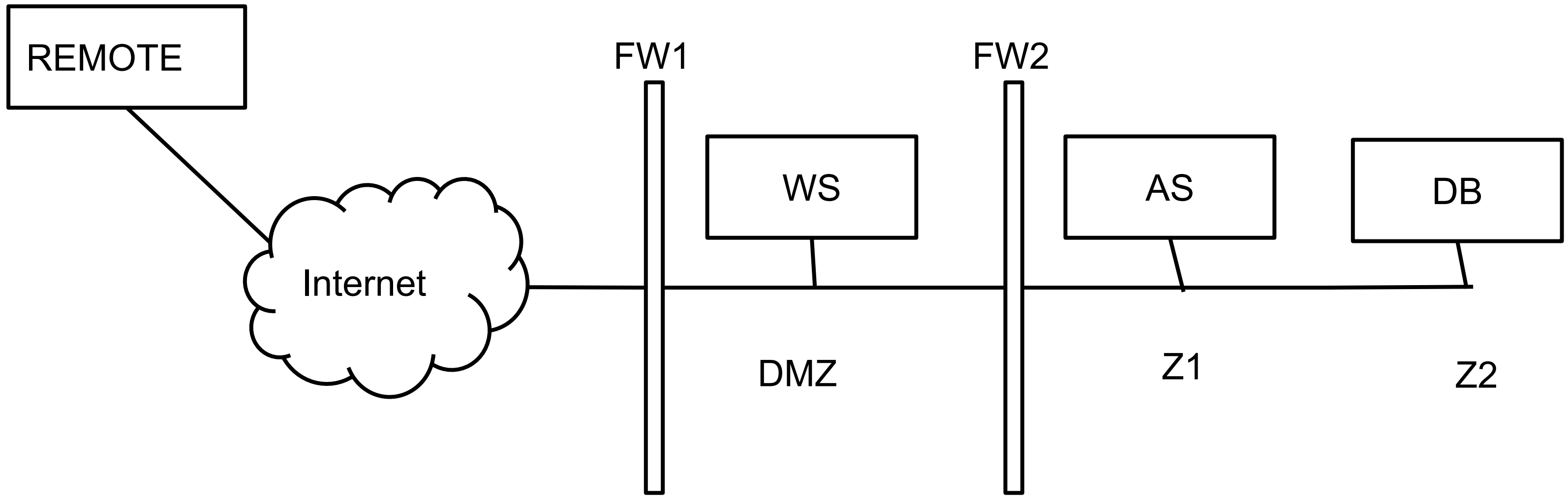
Firewall	Src IP	Src PORT	Direction of the 1st packet	Dst IP	Dst PORT	Policy	Description
FW1 (example)	10.0.0.1 (example)	ANY	zone 1 -> zone 2	192.168.0.2 (example)	443	DENY	(example: the X server in zone 1 cannot contact the Y server)

Write the firewall rules, assuming firewalls to be stateful packet filters (i.e. you can consider the response rules implicit)



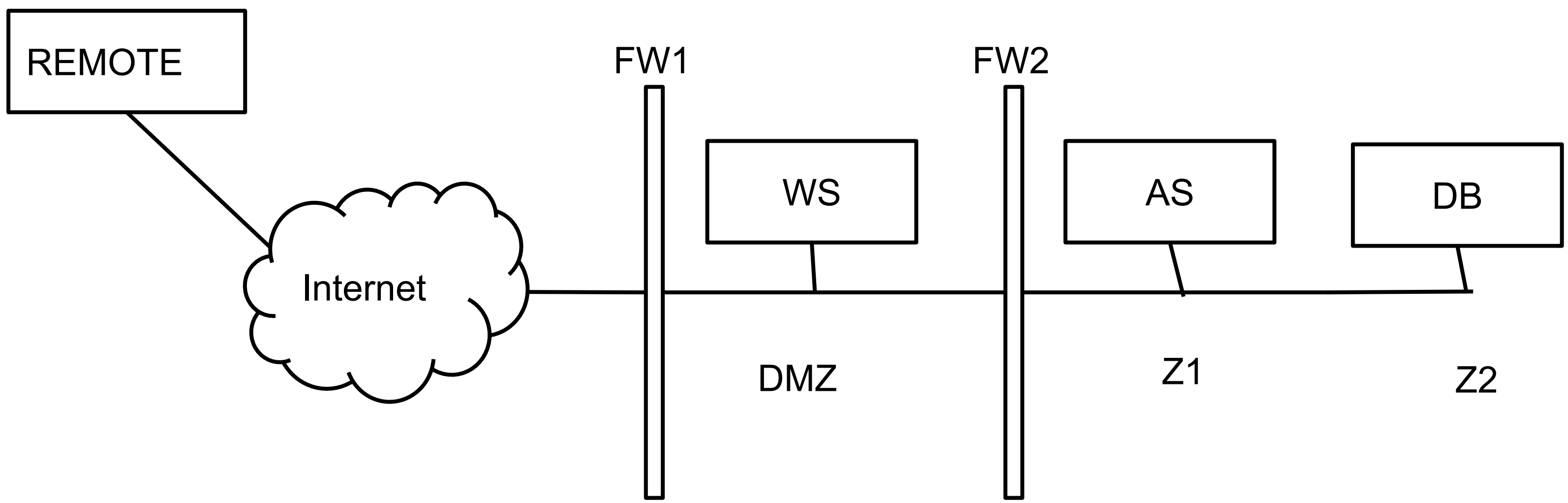
Firewall	Src IP	Src PORT	Direction of the 1st packet	Dst IP	Dst PORT	Policy	Description
FW1 (example)	**10.0.0.1 (example)**	**ANY**	**zone 1 -> zone 2**	**192.168.0.2 (example)**	**443**	**DENY**	**(example: the X server in zone 1 cannot contact the Y server)**
ALL	***ANY***	***ANY***	***ANY -> ANY***	***ANY***	***ANY***	***DENY***	***Default deny on all firewalls***

Write the firewall rules, assuming firewalls to be stateful packet filters (i.e. you can consider the response rules implicit)



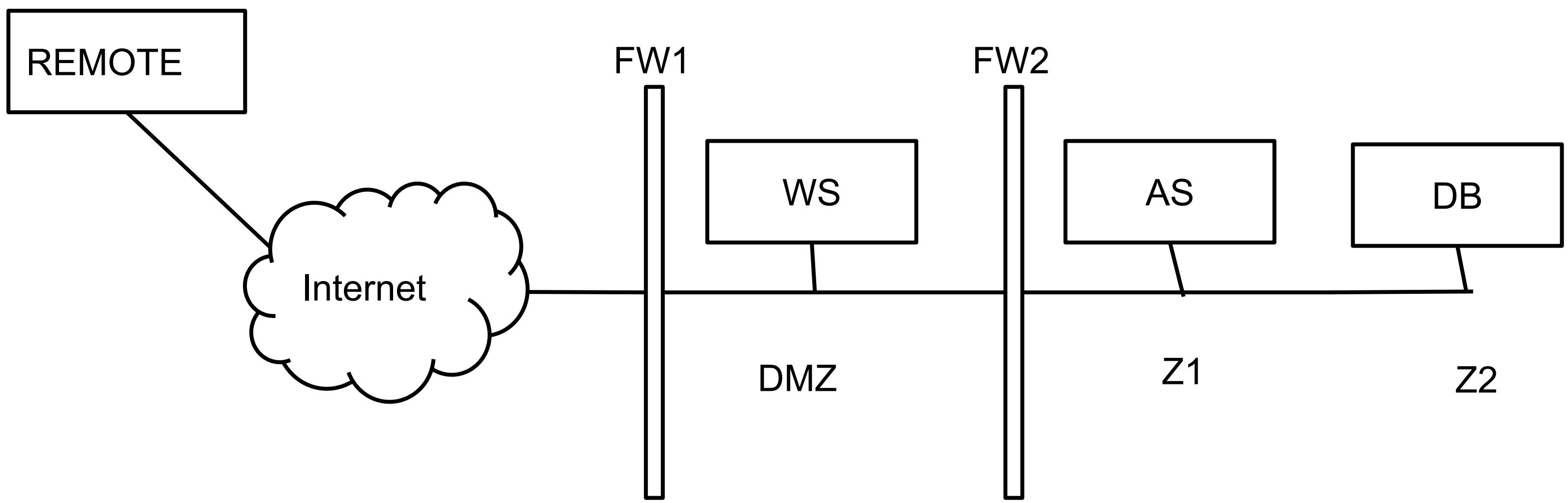
Firewall	Src IP	Src PORT	Direction of the 1st packet	Dst IP	Dst PORT	Policy	Description
FW1 (example)	**10.0.0.1 (example)**	**ANY**	**zone 1 -> zone 2**	**192.168.0.2 (example)**	**443**	**DENY**	**(example: the X server in zone 1 cannot contact the Y server)**
ALL	***ANY***	***ANY***	***ANY -> ANY***	***ANY***	***ANY***	***DENY***	***Default deny on all firewalls***
FW1	***ANY***	***ANY***	***PUB -> DMZ***	***WS_IP***	***80***	***ALLOW***	***The webserver is publicly reachable***

Write the firewall rules, assuming firewalls to be stateful packet filters (i.e. you can consider the response rules implicit)



Firewall	Src IP	Src PORT	Direction of the 1st packet	Dst IP	Dst PORT	Policy	Description
FW1 (example)	**10.0.0.1 (example)**	**ANY**	**zone 1 -> zone 2**	**192.168.0.2 (example)**	**443**	**DENY**	**(example: the X server in zone 1 cannot contact the Y server)**
ALL	***ANY***	***ANY***	***ANY -> ANY***	***ANY***	***ANY***	***DENY***	***Default deny on all firewalls***
FW1	***ANY***	***ANY***	***PUB -> DMZ***	***WS_IP***	***80***	***ALLOW***	***The webserver is publicly reachable***
FW2	***WS_IP***	***ANY***	***DMZ -> Z1***	***AS_IP***	***CUST***	***ALLOW***	***The webserver reaches the app server***

Write the firewall rules, assuming firewalls to be stateful packet filters (i.e. you can consider the response rules implicit)



Firewall	Src IP	Src PORT	Direction of the 1st packet	Dst IP	Dst PORT	Policy	Description
FW1 (example)	**10.0.0.1 (example)**	**ANY**	**zone 1 -> zone 2**	**192.168.0.2 (example)**	**443**	**DENY**	**(example: the X server in zone 1 cannot contact the Y server)**
ALL	*ANY*	*ANY*	*ANY -> ANY*	*ANY*	*ANY*	*DENY*	*Default deny on all firewalls*
FW1	*ANY*	*ANY*	*PUB -> DMZ*	*WS_IP*	*80*	*ALLOW*	*The webserver is publicly reachable*
FW2	*WS_IP*	*ANY*	*DMZ -> Z1*	*AS_IP*	*CUST*	*ALLOW*	*The webserver reaches the app server*
FW1	*AS_IP*	*ANY*	*DMZ -> PUB*	*REMOTE_IP*	*443*	*ALLOW*	*The app server reaches the remote server*
FW2	*AS_IP*	*ANY*	*Z1 -> DMZ*	*REMOTE_IP*	*443*	*ALLOW*	*The app server reaches the remote server*

Question

You are the network administrator of a small LAN and you're configuring the firewall. You want to allow the computers connected to the LAN to browse the Web (HTTP, port 80), but you want to avoid that they download known malware.

Read **all** the following questions and **then** answer one by one:

1. (2 points) What type of firewall do you need and why?

2. (1 points) What does the firewall need to do in order to prevent downloading known malware?

3. (3 points) Suppose now that you want to adapt the same solution to HTTPS (port 443). Explain how this can be done.

1. (2 points) What type of firewall do you need and why?

We need a firewall capable of decoding the application layer in order to trigger on HTTP responses corresponding to HTTP requests initiated from the internal network. In this specific case an HTTP proxy could be used.

2. (1 points) What does the firewall need to do in order to prevent downloading known malware?

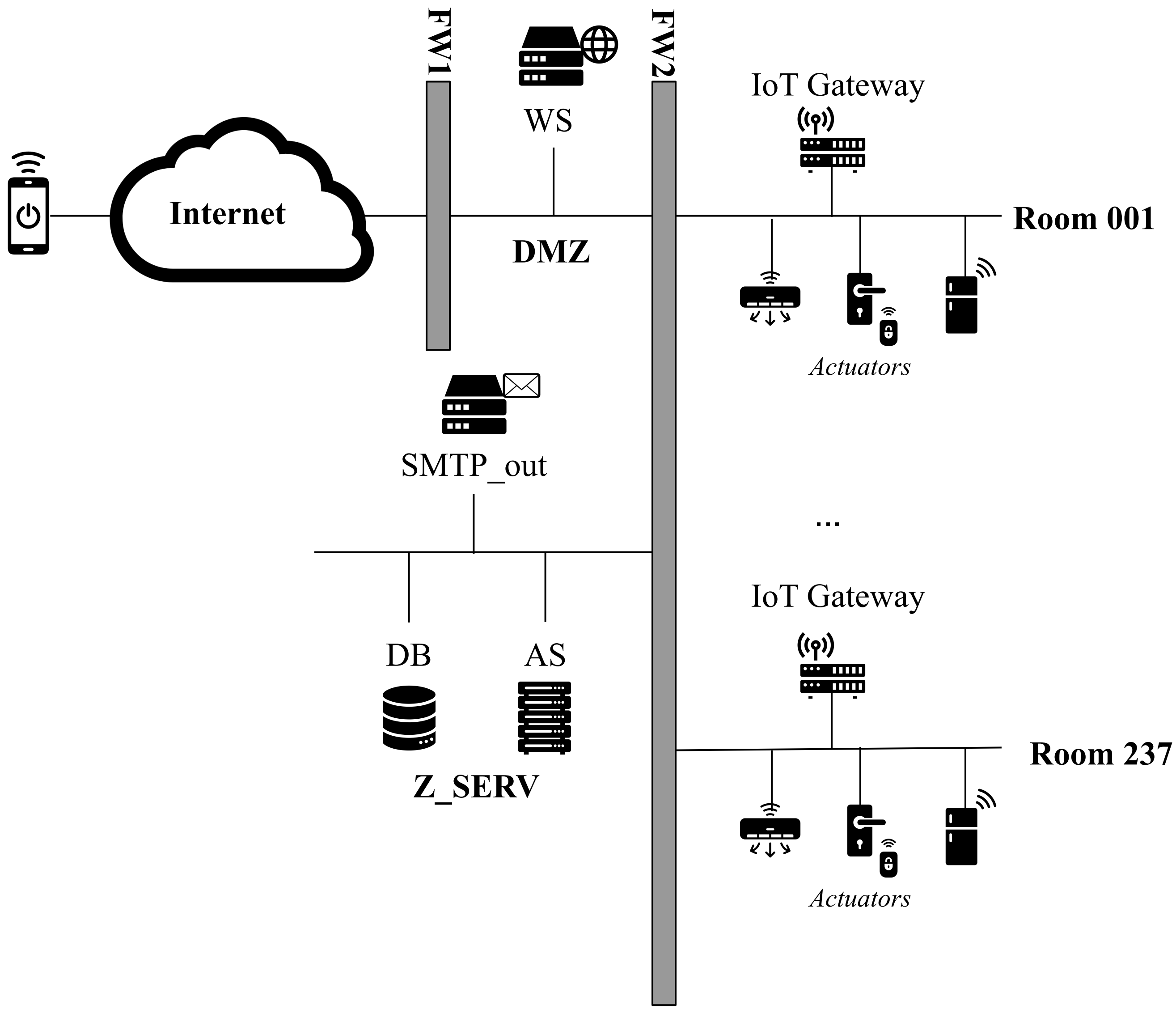
By parsing the HTTP response, the firewall extracts each file being downloaded and sends them to an AV for scanning.

3. (3 points) Suppose now that you want to adapt the same solution to HTTPS (port 443). Explain how this can be done.

Since the firewall needs to decrypt the application-level payload, it must become a MITM during the SSL handshake. To achieve this, we install another trusted CA in the certificate store of each client's browser.

Question

The Avengers Hotel has recently adopted a new domotic system that allows to control the appliances inside your hotel rooms (e.g., air conditioner, refrigerator, lights, door locks, gates) from your smartphone over the Internet. For example, you can turn on the air conditioner or open the door when you're approaching the room. The system is composed of a web server, which is connected to actuators (e.g., door lock, light on-off switch) over a local network. You can assume that the actuators are TCP/IP-based devices communicating on port 8080. You send commands to the web server over HTTP (on port 80) via Internet-connected smartphones. The web server forwards the commands on port 9060 towards a centralized Application Server that interprets each command received. The Application Server stores the data on a centralized DB on port 1433 and sends the commands on port 8080 to the respective Room IoT gateway that, in turn, activates or deactivates the actuators. The centralized application server communicates with a local email server to send daily reports to the room owner (on port 25) about the conditions of the room (e.g., temperature). Here is the network layout:


Internet
FW1
WS
DMZ
FW2
IoT Gateway
Room 001
Actuators
SMTP_out
DB
AS
Z_SERV
...
IoT Gateway
Room 237
Actuators

1. [2 points] Write the firewall rules, assuming firewalls to be stateful packet filters (i.e. you can consider the response rules implicit) and **considering only one room**.

Firewall	**Src IP**	**Src PORT**	**Direction of the 1st packet**	**Dst IP**	**Dst PORT**	**Policy**	**Description**
FW1 (example)	*10.0.0.1 (example)*	*ANY*	*zone 1 -> zone 2*	*192.168.0.2 (example)*	*443*	*DENY*	*(example: the X server in zone 1 cannot contact the Y server)*

1. **[2 points]** Write the firewall rules, assuming firewalls to be stateful packet filters (i.e. you can consider the response rules implicit) and **considering only one room**.

Firewall	Src IP	Src PORT	Direction of the 1st packet	Dst IP	Dst PORT	Policy	Description
FW1 (example)	*10.0.0.1 (example)*	*ANY*	*zone 1 -> zone 2*	*192.168.0.2 (example)*	*443*	*DENY*	*(example: the X server in zone 1 cannot contact the Y server)*
ALL	ANY	ANY	ANY	ANY	ANY	DENY	Default Deny
FW1	ANY	ANY	WWW->DMZ	WS_IP	80	ALLOW	Allow connection to WS
FW2	WS_IP	ANY	DMZ->Z_SERV	AS_IP	9060	ALLOW	Allow communication between WS and AS
FW2	AS_IP	ANY	Z_SERV->ROOMs	IoTGateway_IPs	8080	ALLOW	Allow communication between AS and IoTGateway
FW2	SMTPout_IP	ANY	Z_SERV->DMZ	ANY	25	ALLOW	Allow to send email
FW1	SMTPout_IP	ANY	DMZ->WWW	ANY	25	ALLOW	Allow to send email

2. [2 points] (1) Identify the most valuable asset and (2) describe a risk scenario against that asset, clarifying the (3) threats and the (4) vulnerabilities that cause it.

2. [2 points] (1) Identify the most valuable asset and (2) describe a risk scenario against that asset, clarifying the (3) threats and the (4) vulnerabilities that cause it.

The most valuable asset is the actuator of the door lock or gates. In a hypothetical risk scenario an attacker can open the door and break into the house. Specifically, a man in the middle attacker (threat agent) can read the commands and authentication session over the Internet. The vulnerability that caused this attack could be that the network traffic is not encrypted.

3. [1 point] Propose any network-level security mechanism or protocol to ensure that the above risk scenario is properly mitigated.

3. [1 point] Propose any network-level security mechanism or protocol to ensure that the above risk scenario is properly mitigated.

We propose to use HTTPS

4. After few days, the hotel was hit by a cyber attack: all clients were unable to connect to the web service to access their rooms by using the smartphone.

You are a computer security expert of the S.H.I.E.L.D. (Security Homeland Intervention, Enforcement and Logistics Division). You and your team have been assigned to solve this case and discover what happened. You have obtained the following network logs towards the company web server (with IP 10.133.17.10) through FW1:

Time [seconds]	source	destination	protocol	packet content
0.000	148.79.3.192	**10.133.17.10**	HTTP	GET / HTTP/1.1
0.002	131.75.7.123	**10.133.17.10**	HTTP	GET / HTTP/1.1
0.003	**10.133.17.10**	148.79.3.192	HTTP	200 OK
0.004	110.12.42.3	**10.133.17.10**	HTTP	GET / HTTP/1.1
0.004	87.15.22.9	**10.133.17.10**	HTTP	GET / HTTP/1.1
0.005	**10.133.17.10**	131.75.7.123	HTTP	200 OK
0.005	**10.133.17.10**	110.12.42.3	HTTP	200 OK
0.006	173.111.23.10	**10.133.17.10**	HTTP	GET / HTTP/1.1
0.008	**10.133.17.10**	87.15.22.9	HTTP	200 OK
0.009	141.12.113.33	**10.133.17.10**	HTTP	GET / HTTP/1.1
0.010	106.139.26.239	**10.133.17.10**	HTTP	GET / HTTP/1.1
0.011	**10.133.17.10**	173.111.23.10	HTTP	503 SERVER UNAVAILABLE
0.012	34.101.189.224	**10.133.17.10**	HTTP	GET / HTTP/1.1
0.012	160.91.121.205	**10.133.17.10**	HTTP	GET / HTTP/1.1
0.013	**10.133.17.10**	141.12.113.33	HTTP	503 SERVER UNAVAILABLE
0.014	**10.133.17.10**	106.139.26.239	HTTP	503 SERVER UNAVAILABLE
0.015	22.55.59.146	**10.133.17.10**	HTTP	GET / HTTP/1.1
0.016	37.216.29.160	**10.133.17.10**	HTTP	GET / HTTP/1.1

…

Tracking the IP addresses contacting the web server (148.79.3.192, 110.12.42.3, 173.111.23.10…), you were able to discover that the vast majority of them came from smart cameras, routers, smart fridges and other IoT devices.

4.1 [2 points] Which attack has been implemented? Give a brief explanation of how it works in general and in this specific case, focusing on what an attacker needs in order to implement them.

DDOS because many IPs are asking to retrieve data, though a botnet probably since the IoT devices...
see slides…

The attacker uses a network of (usually compromised) machines to flood the victim with large amounts of unrequested network packets. The attacker needs access to many machines with sizable internet connections.

Typically, trojans on compromised machines forming a botnet.

4.2 [1 points] Can you mitigate such attack? Motivate your answer.

Overall, there is no solution to this class of attacks. These attacks can only be mitigated by acting against botnets or by cleaning up infections on compromised machines.

The End

The End