Exercises
Secure Network Architectures

Computer Security

Question

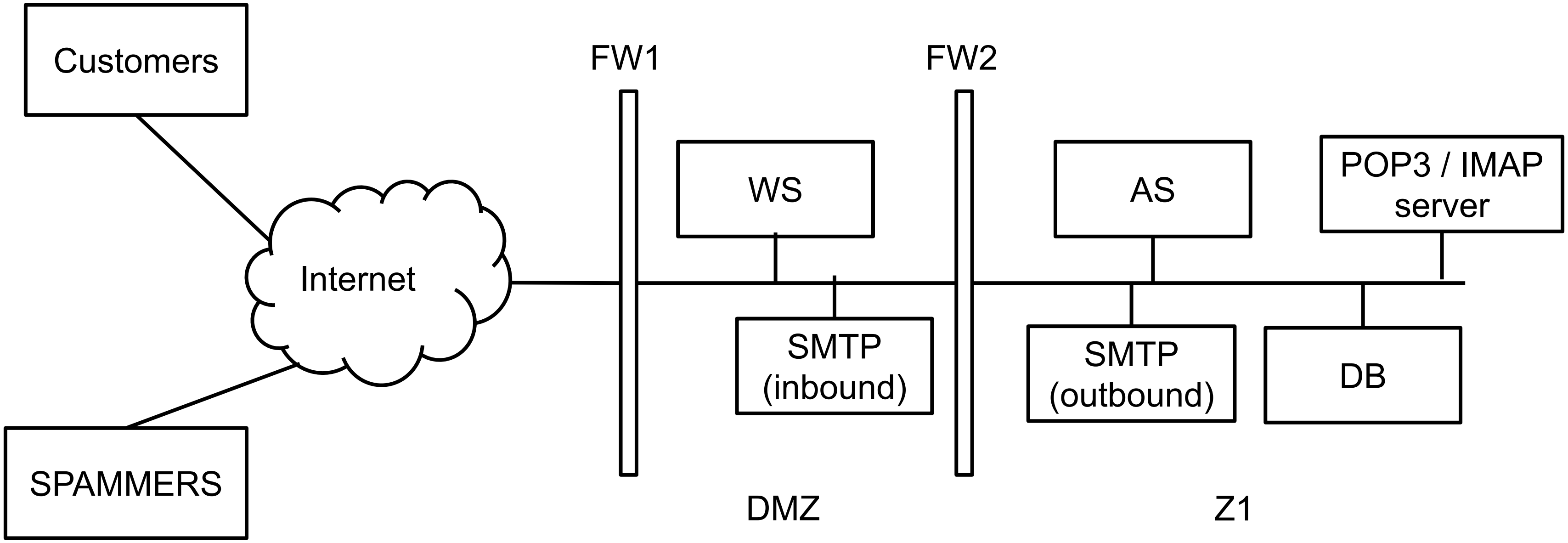
FreeMail is an anti-spam company that aims to fight spam using an innovative “vigilante” approach. FreeMail’s customers report their spam e-mails to FreeMail. Then, FreeMail leaves a generic complaint for each spam e-mail reported by users. FreeMail operates on the assumption that, as the community grows, 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.

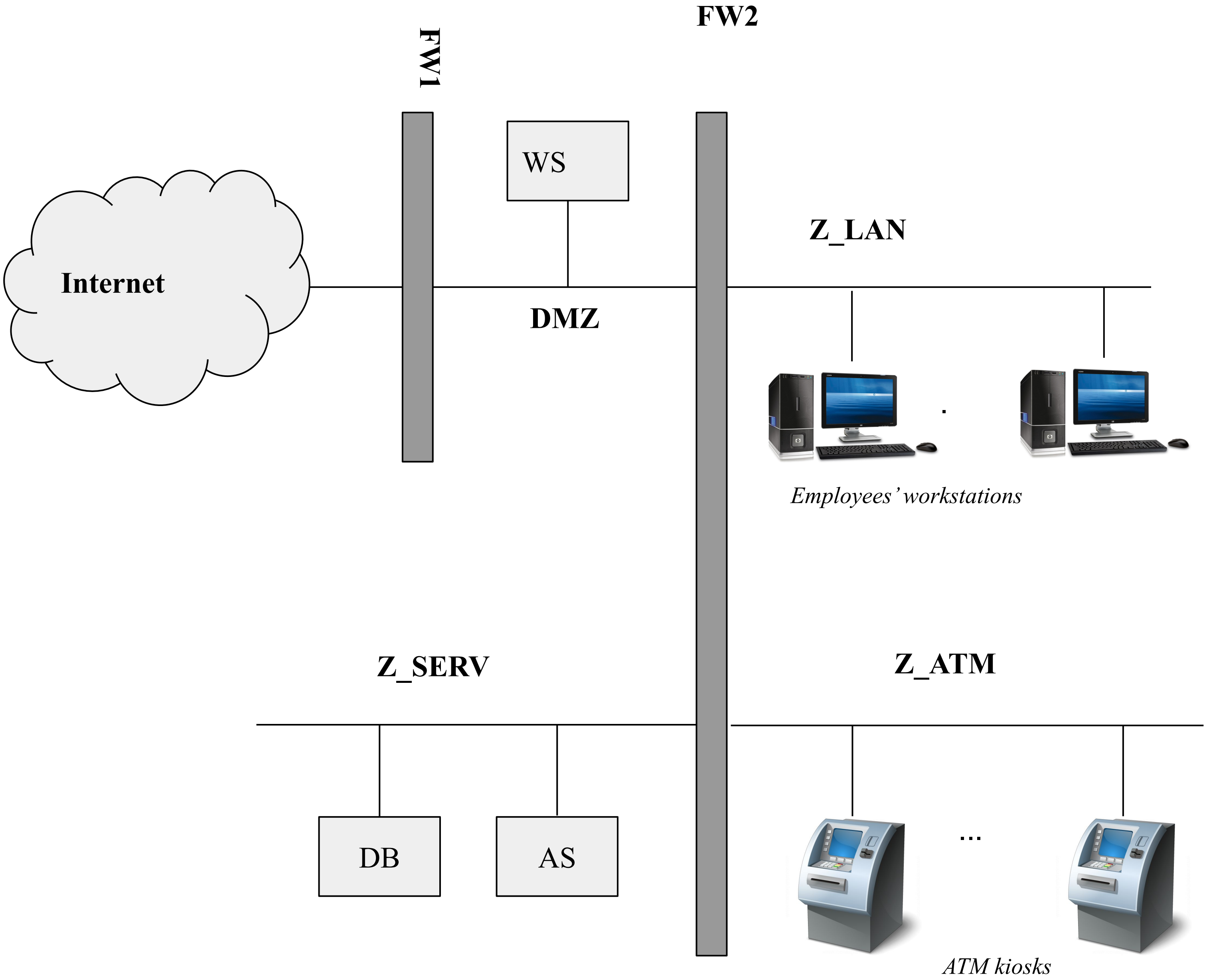
An attacker could send a large number of bogus spam reports to FreeMail, falsely indicating some victim site V has been sending spam. FreeMail's servers will then visit V to lodge complaints, overwhelming V in the process if the volume of visits is high enough. A victim can defend itself by blocking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


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

1. 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)*
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	Web server → 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 only).

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 only).

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 content 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 content 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

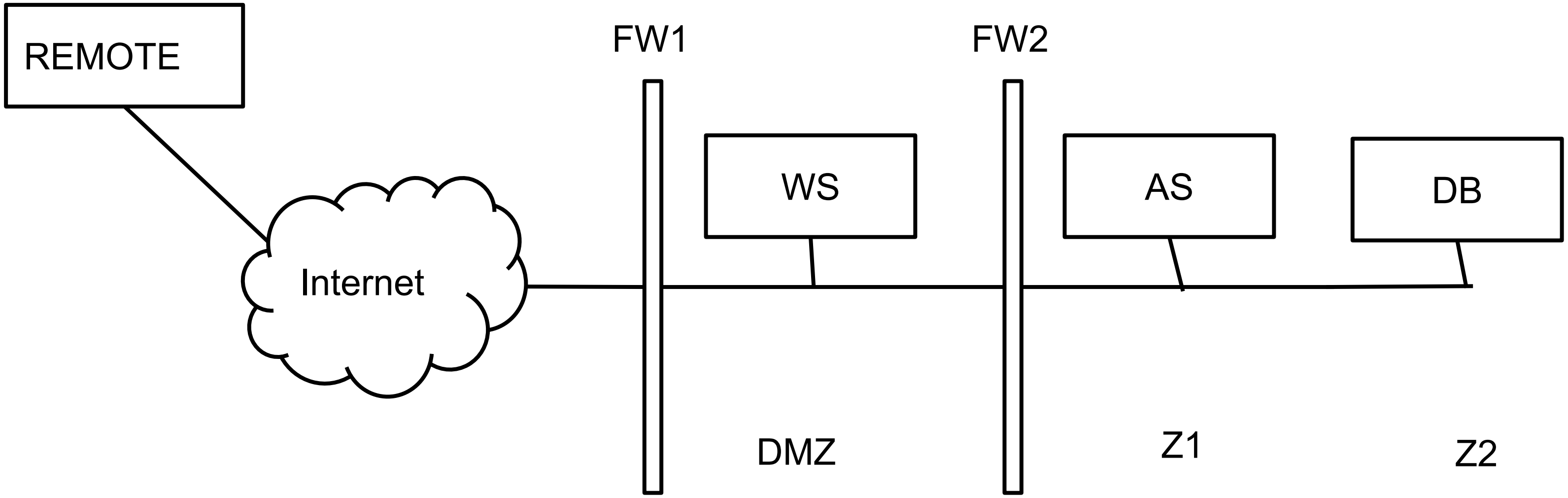
An online shop offers to its customers a **web application, publicly reachable from the Internet**, deployed on a **web server**. The web server uses application logic deployed on an **application server**. The application logic alone implements queries executed on a **database server**. The **application 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:

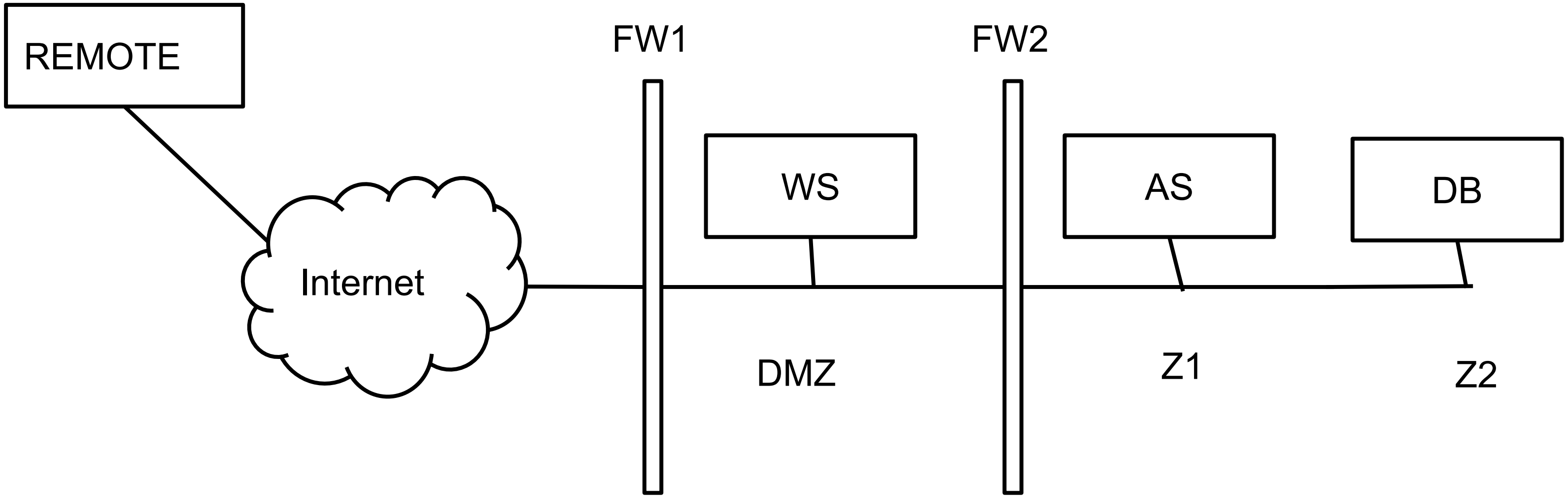
Draw the network layout and assign distinct names to any machine and zone.

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.

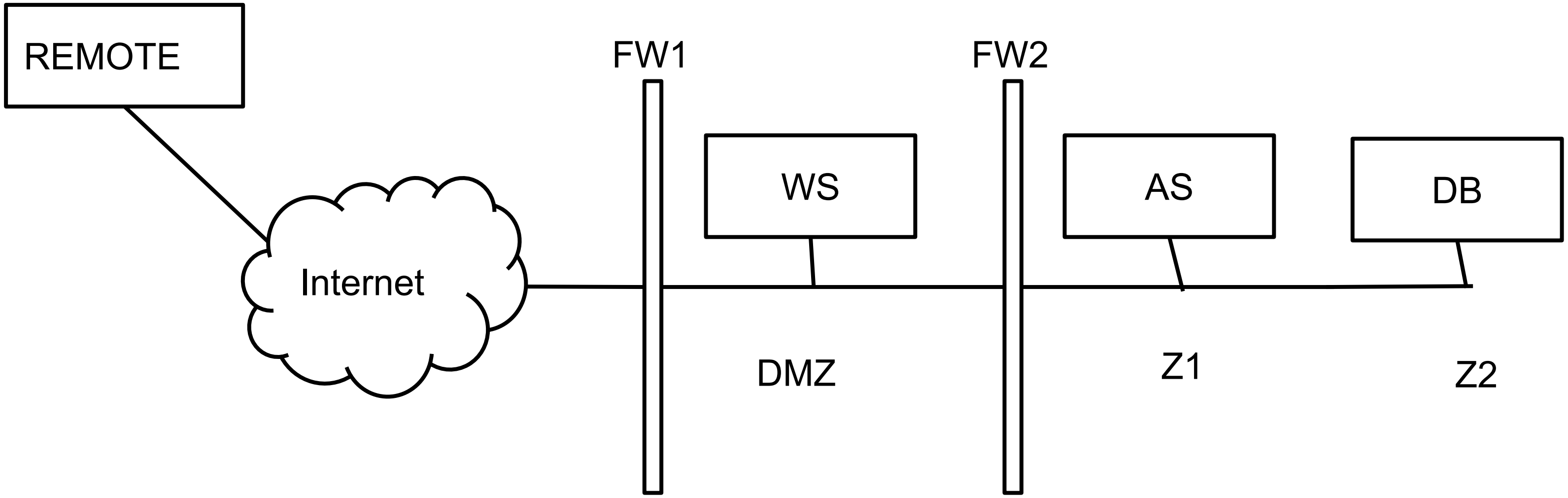


Write the firewall rules, assuming firewalls to be stateful packet filters (i.e. you can consider the response rules implicit)



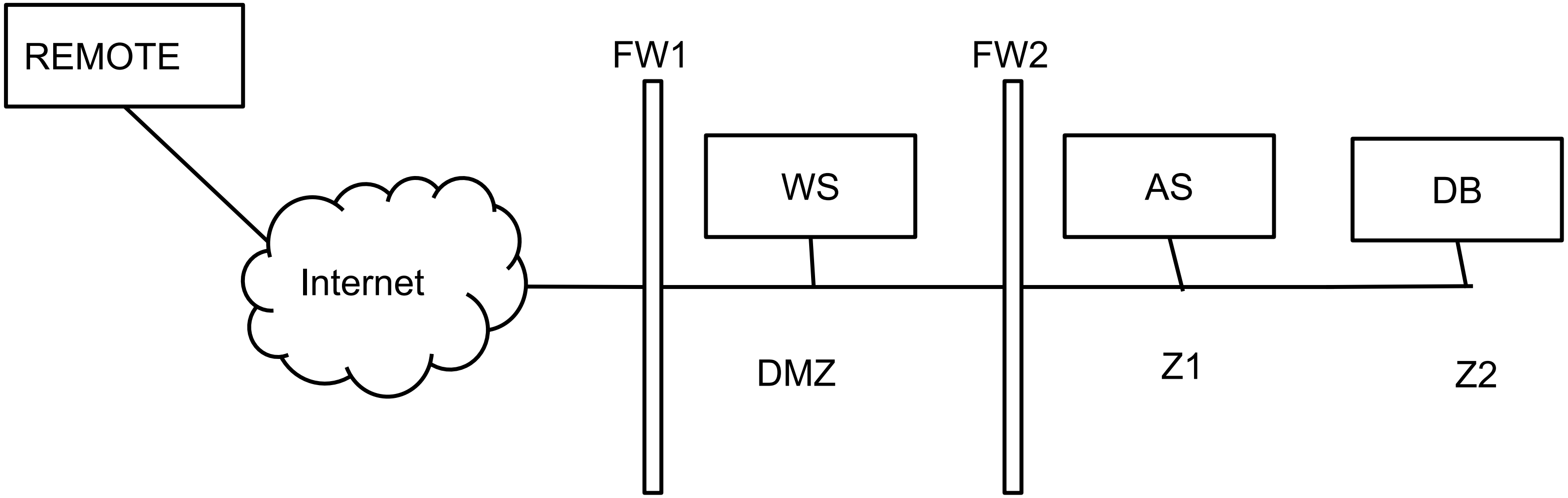
Firewall	Src IP	Src PORT	Direction of the 1st packet	Dst IP	Dst PORT	Policy	Description
FW1 (example)	10.0.0.1 (example)	ANY	zone 1 -> zone 2	192.168.0.2 (example)	443	DENY	(example: the X server in zone 1 cannot contact the Y server)

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



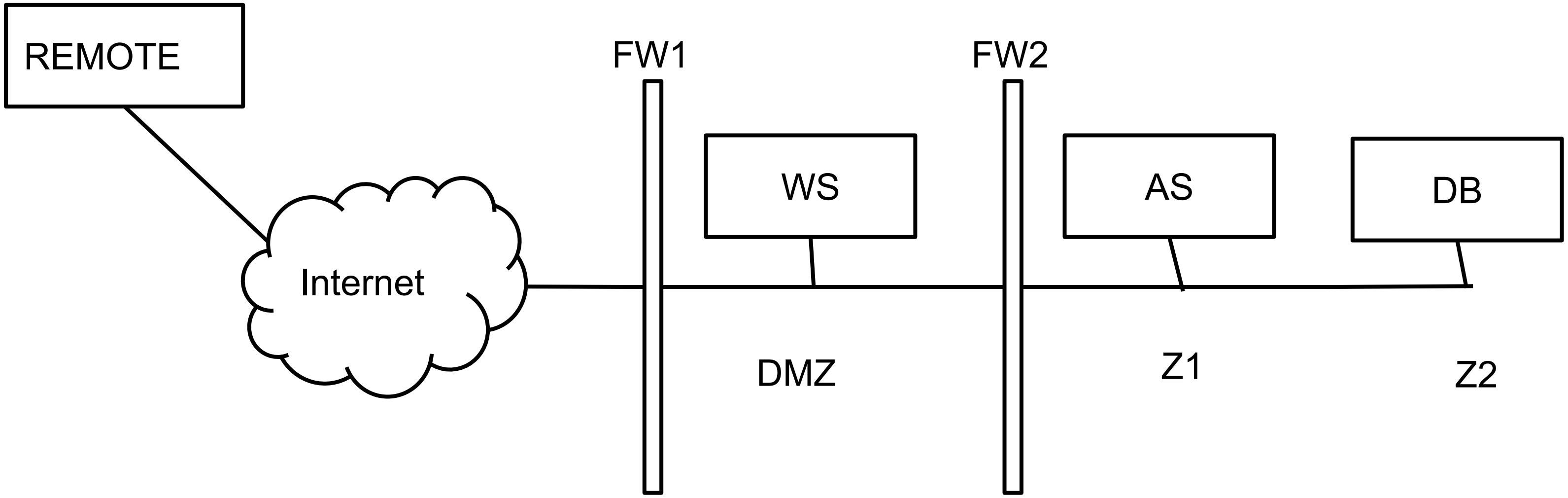
Firewall	Src IP	Src PORT	Direction of the 1st packet	Dst IP	Dst PORT	Policy	Description
FW1 (example)	**10.0.0.1 (example)**	**ANY**	**zone 1 -> zone 2**	**192.168.0.2 (example)**	**443**	**DENY**	**(example: the X server in zone 1 cannot contact the Y server)**
ALL	***ANY***	***ANY***	***ANY -> ANY***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



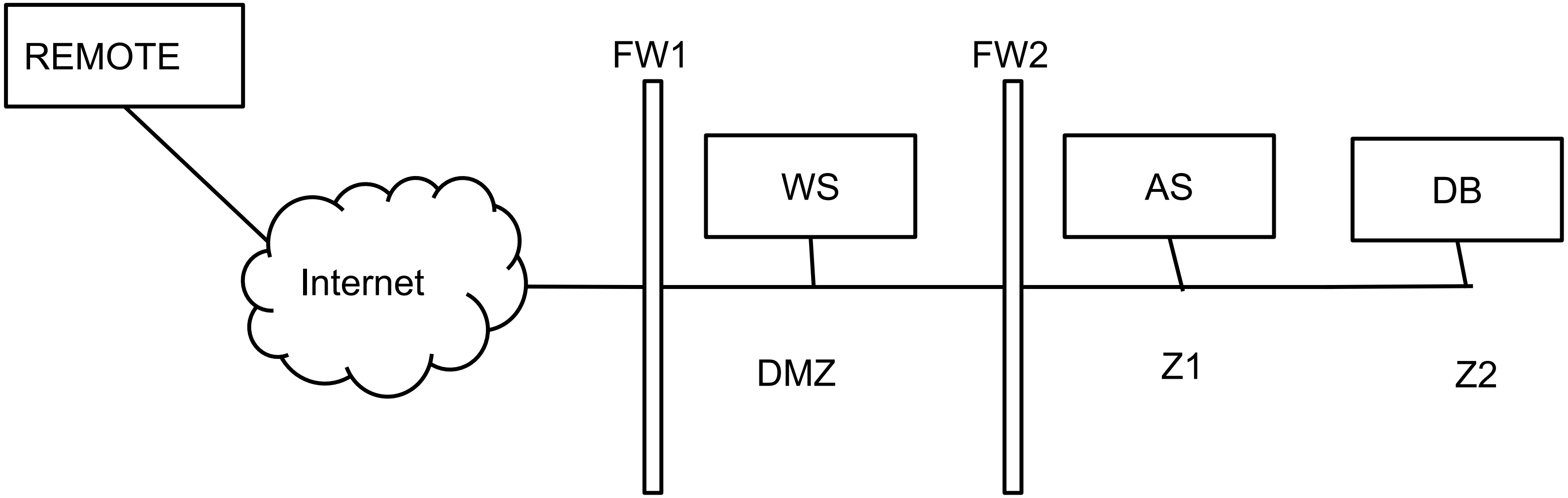
Firewall	Src IP	Src PORT	Direction of the 1st packet	Dst IP	Dst PORT	Policy	Description
FW1 (example)	10.0.0.1 (example)	ANY	zone 1 -> zone 2	192.168.0.2 (example)	443	DENY	(example: the X server in zone 1 cannot contact the Y server)
ALL	*ANY*	*ANY*	*ANY -> ANY*	*ANY*	*ANY*	*DENY*	*Default deny on all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

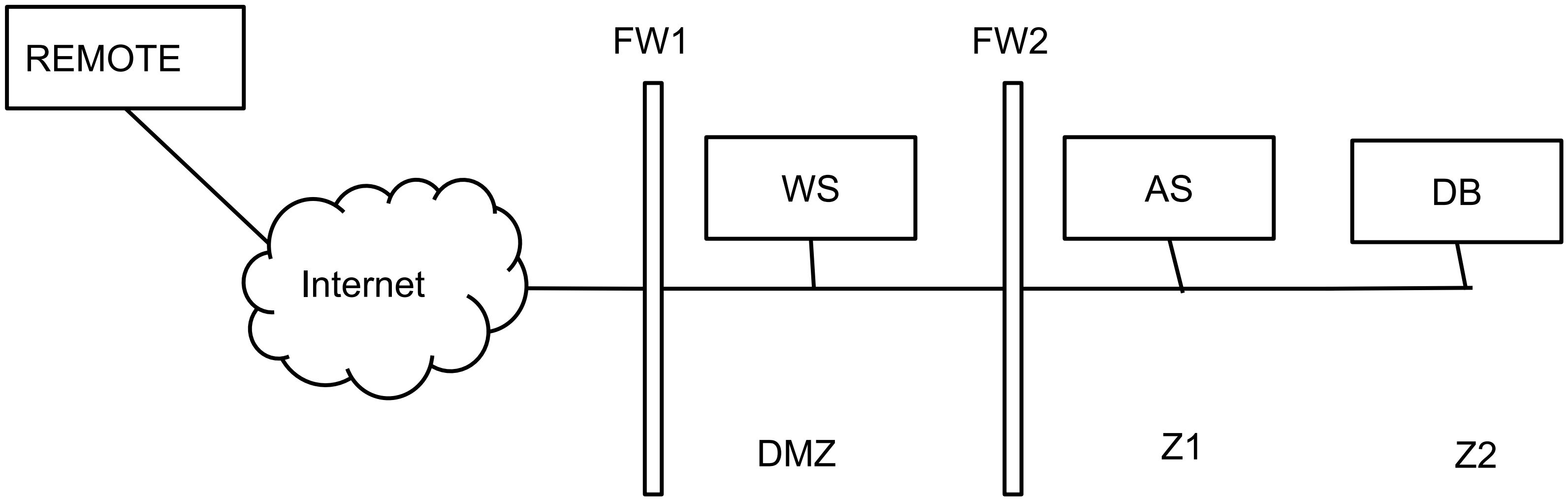
An online shop offers to its customers a **web application, publicly reachable from the Internet**, deployed on a **web server**. The web server uses application logic deployed on an **application server**. The application logic alone implements queries executed on a **database server**. The **application 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:

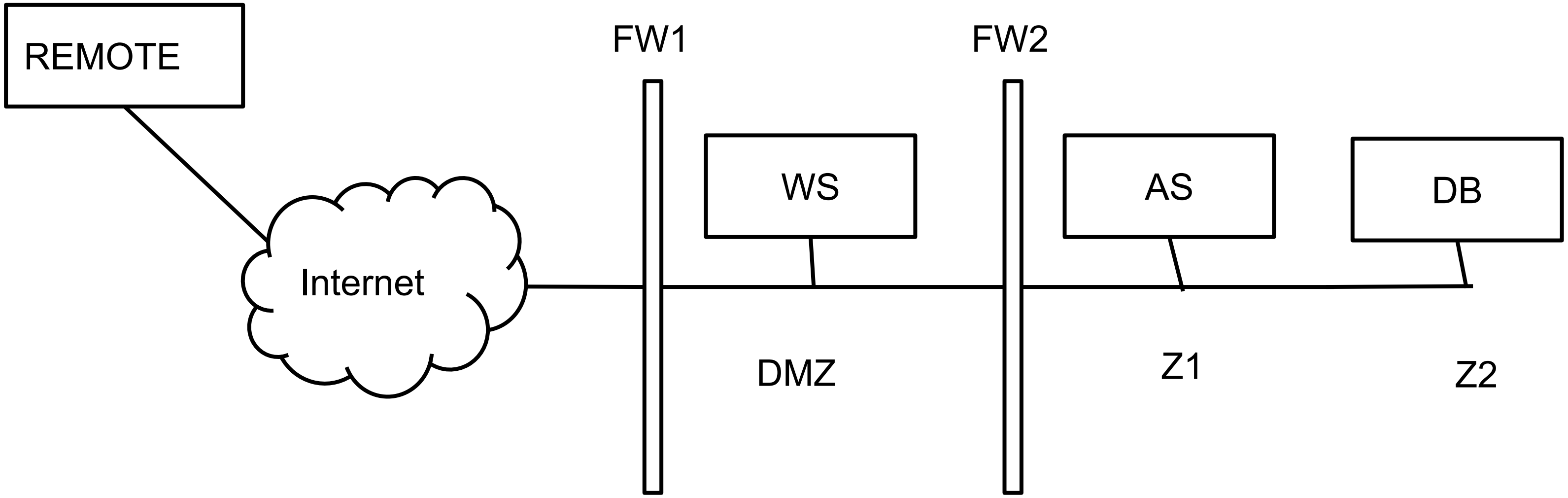
Draw the network layout and assign distinct names to any machine and zone.

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.

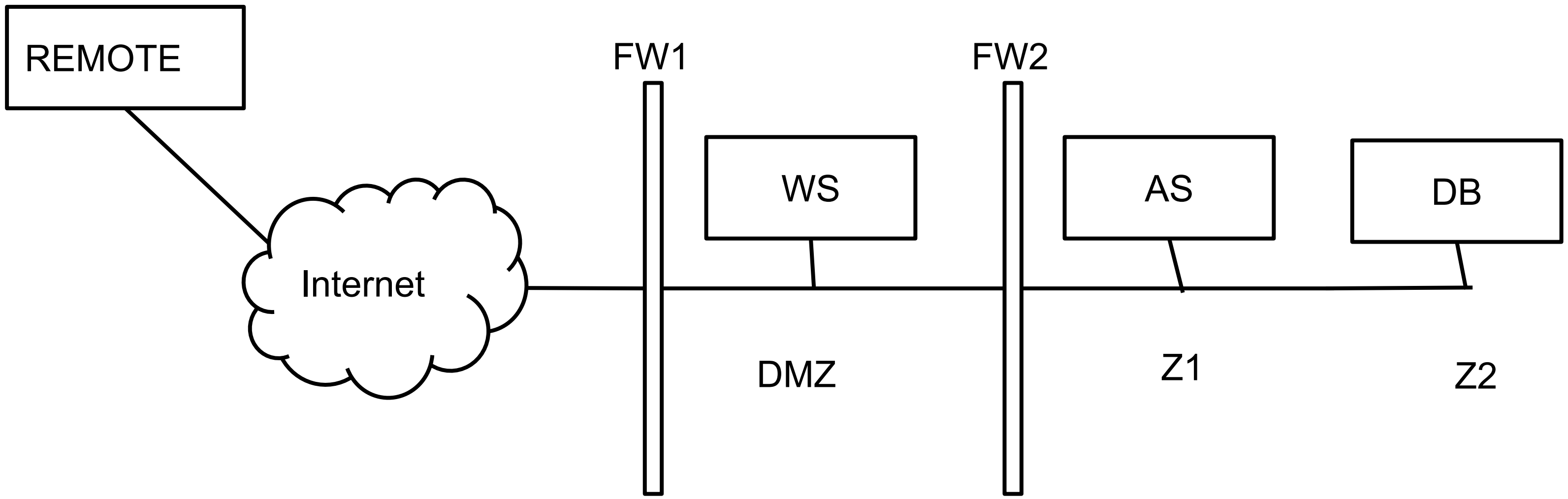


Write the firewall rules, assuming firewalls to be stateful packet filters (i.e. you can consider the response rules implicit)



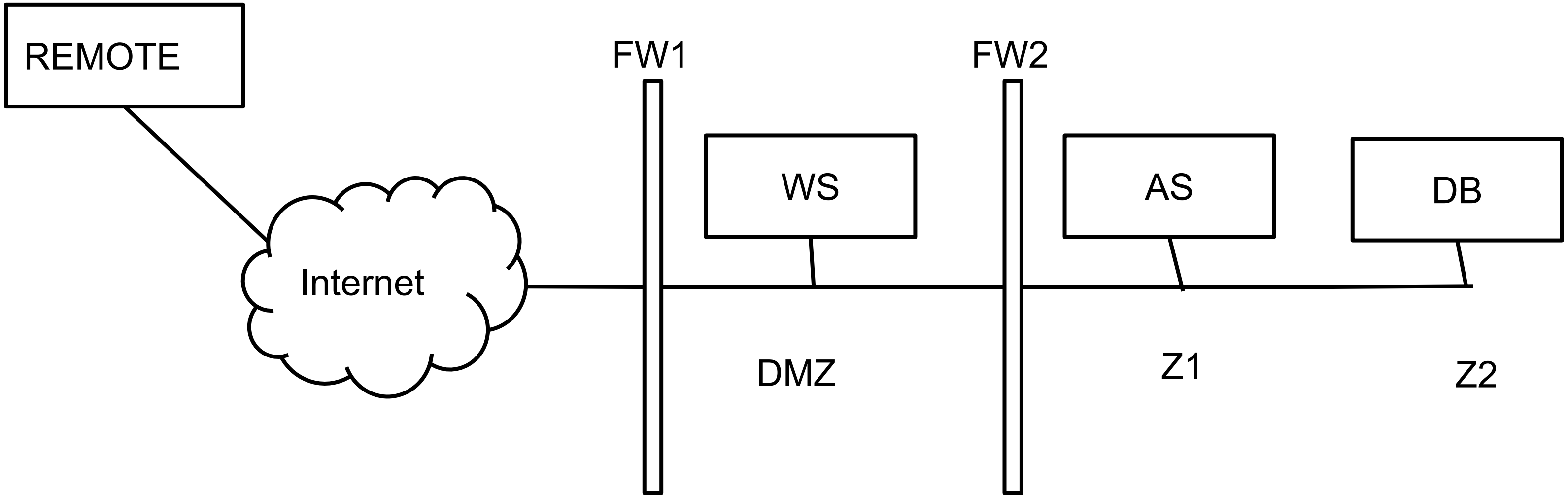
Firewall	Src IP	Src PORT	Direction of the 1st packet	Dst IP	Dst PORT	Policy	Description
FW1 (example)	10.0.0.1 (example)	ANY	zone 1 -> zone 2	192.168.0.2 (example)	443	DENY	(example: the X server in zone 1 cannot contact the Y server)

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



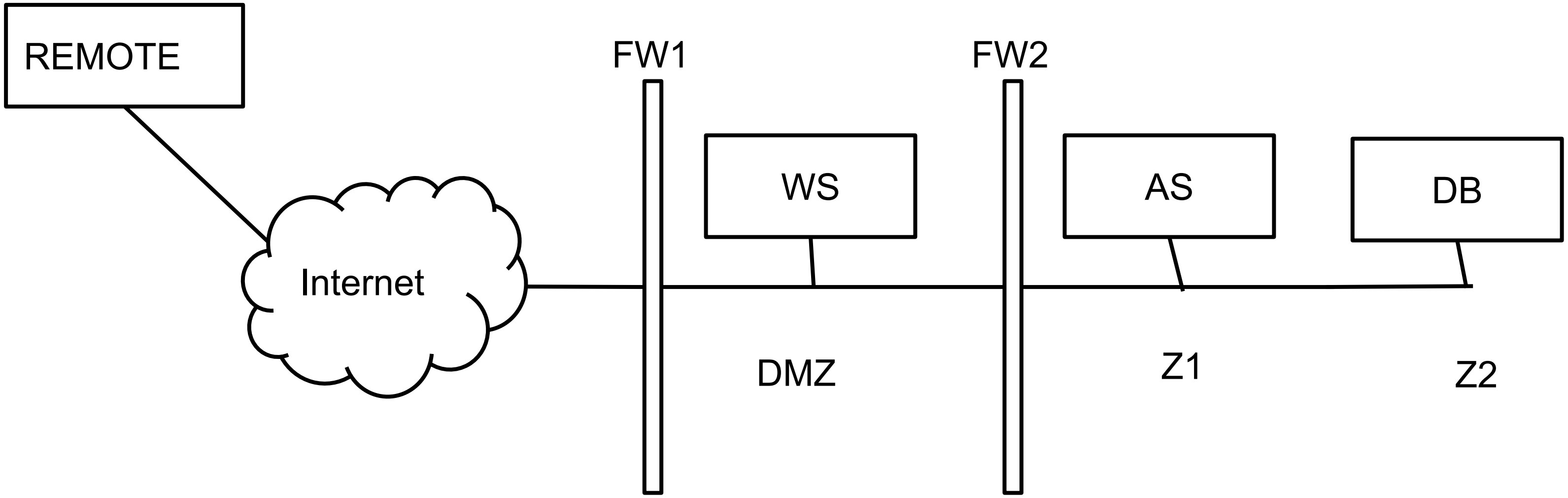
Firewall	Src IP	Src PORT	Direction of the 1st packet	Dst IP	Dst PORT	Policy	Description
FW1 (example)	**10.0.0.1 (example)**	**ANY**	**zone 1 -> zone 2**	**192.168.0.2 (example)**	**443**	**DENY**	**(example: the X server in zone 1 cannot contact the Y server)**
ALL	***ANY***	***ANY***	***ANY -> ANY***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



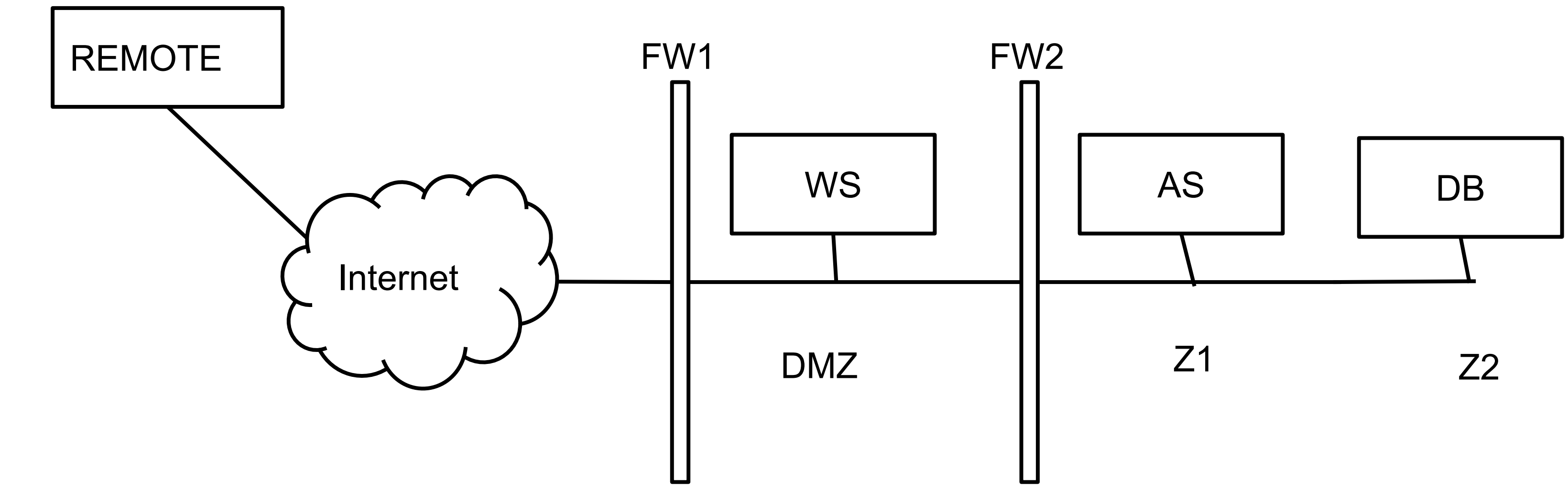
Firewall	Src IP	Src PORT	Direction of the 1st packet	Dst IP	Dst PORT	Policy	Description
FW1 (example)	**10.0.0.1 (example)**	**ANY**	**zone 1 -> zone 2**	**192.168.0.2 (example)**	**443**	**DENY**	**(example: the X server in zone 1 cannot contact the Y server)**
ALL	***ANY***	***ANY***	***ANY -> ANY***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

The End