

PCI DSS: Infrastructure Security



John Elliott

PRIVACY, PAYMENTS, SECURITY AND RISK SPECIALIST

@withoutfire www.withoutfire.com



Requirement 1



Have (and implement) firewall configuration standards

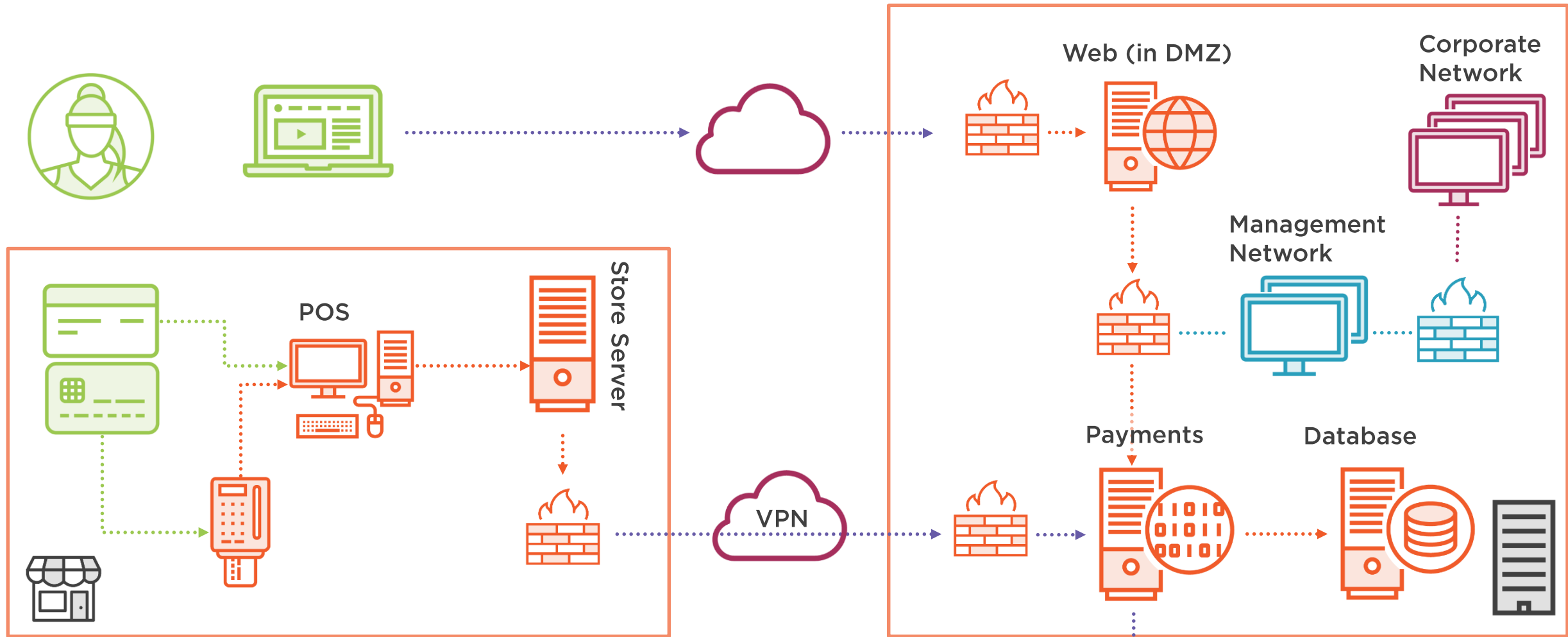
Restrict connections between the cardholder data environment and other networks

Control inbound internet traffic

Personal firewalls

Policies and procedures

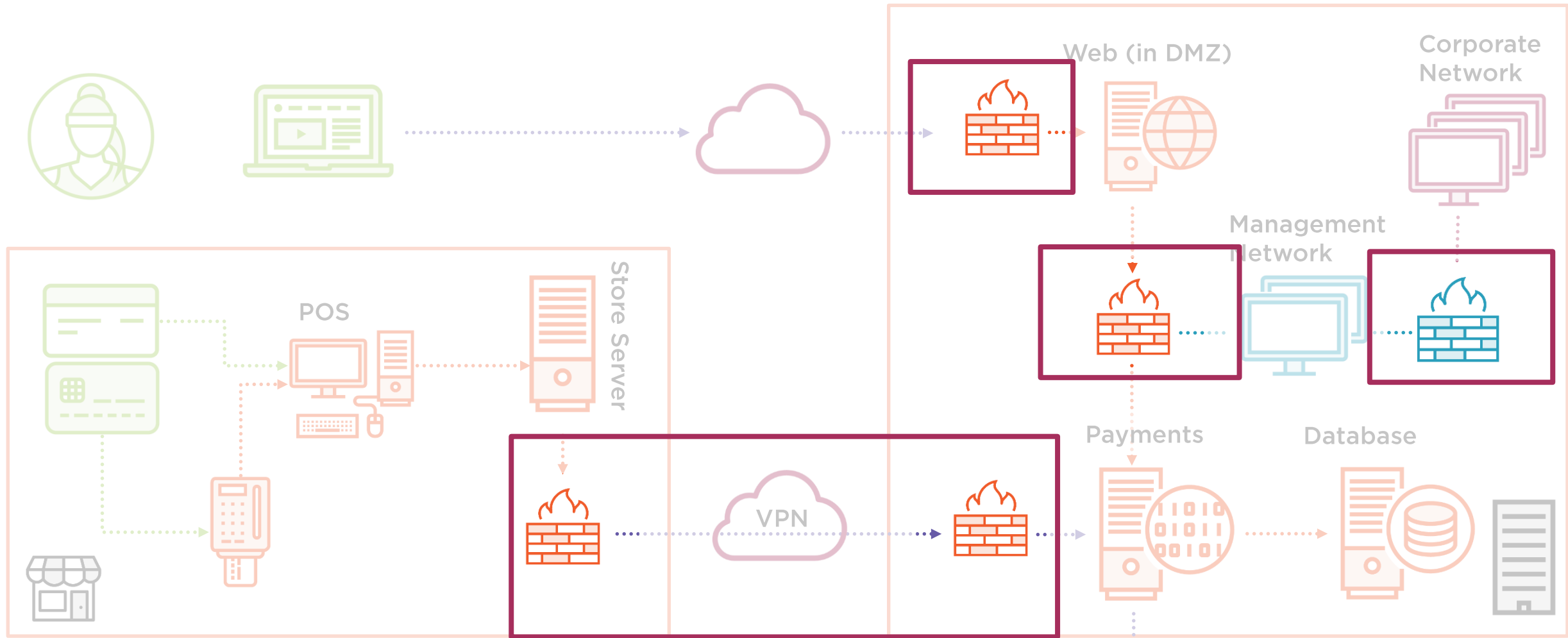




- Cardholder's card and systems
- Stores, processes or transmits
- Connected to or security affecting
- Out of scope of PCI DSS

- Unencrypted cardholder data
- Encrypted cardholder data
- Physical card read
- Management network
- Corporate network







Requirement 1.1

Have and implement configuration and management standards





Requirement 1.1

Establish and **implement** firewall and router **configuration standards** that include the following (1.1.1 thru 1.1.7):



Requirement Guidance

- Firewalls and routers are key components of the architecture that controls entry to and exit from the network. These devices are software or hardware devices that block unwanted access and manage authorized access into and out of the network.
- Configuration standards and procedures will help to ensure that the organization's first line of defense in the protection of its data remains strong.

1.1 Testing Procedures

Observe/examine systems and settings	Y	Implementation of standards
Examine documentation	Y	Policies and procedures
Examine records	Y	Evidence
Interview people	!	Responsible people

Requirement 1 | Install and maintain a firewall configuration to protect cardholder data





Requirement 1.1.1

Firewall change management

There's a documented reason for every network connection in and out of the cardholder data environment

Someone approved it





Requirement 1.1.1

A **formal process** for **approving** and **testing** all network connections and changes to the firewall and router configurations.



Requirement Guidance

- A documented and implemented process for approving and testing all connections and changes to the firewalls and routers will help prevent security problems caused by misconfiguration of the network, router, or firewall.
- Without formal approval and testing of changes, records of the changes might not be updated, which could lead to inconsistencies between network documentation and the actual configuration.

1.1.1 Testing Procedures

Observe/examine systems and settings	-	
Examine documentation	Y	Policies and procedures
Examine records	Y	Firewall change logs and change control records
Interview people	Y	Responsible people

Requirement 1 | Install and maintain a firewall configuration to protect cardholder data





Requirement 1.1.2

A **current** network diagram exists and that it documents all connections to cardholder data

Did I say it must be kept **current**?



Requirement 1.1.2

Current network diagram that identifies **all connections** between the cardholder data environment and other networks, including any wireless networks.



Requirement Guidance

- Network diagrams describe how networks are configured, and identify the location of all network devices.
- Without current network diagrams, devices could be overlooked and be unknowingly left out of the security controls implemented for PCI DSS and thus be vulnerable to compromise.



1.1.2 Testing Procedures

Observe/examine systems and settings	Y	Network configurations
Examine documentation	-	
Examine records	Y	Network diagrams
Interview people	Y	People responsible for the network

Requirement 1 | Install and maintain a firewall configuration to protect cardholder data





Requirement 1.1.3

There is a **current** data-flow diagram showing cardholder data flows across systems and networks



Requirement 1.1.3

Current diagram that shows all cardholder data flows across systems and networks.



Requirement Guidance

- Cardholder data-flow diagrams identify the location of all cardholder data that is stored, processed, or transmitted within the network.
- Network and cardholder data-flow diagrams help an organization to understand and keep track of the scope of their environment, by showing how cardholder data flows across networks and between individual systems and devices.

1.1.3 Testing Procedures

Observe/examine systems and settings	-	
Examine documentation	-	
Examine records	Y	Data-flow diagram
Interview people	Y	Responsible people

Requirement 1 | Install and maintain a firewall configuration to protect cardholder data





Requirement 1.1.4

Your policy must require firewalls protecting the internal network



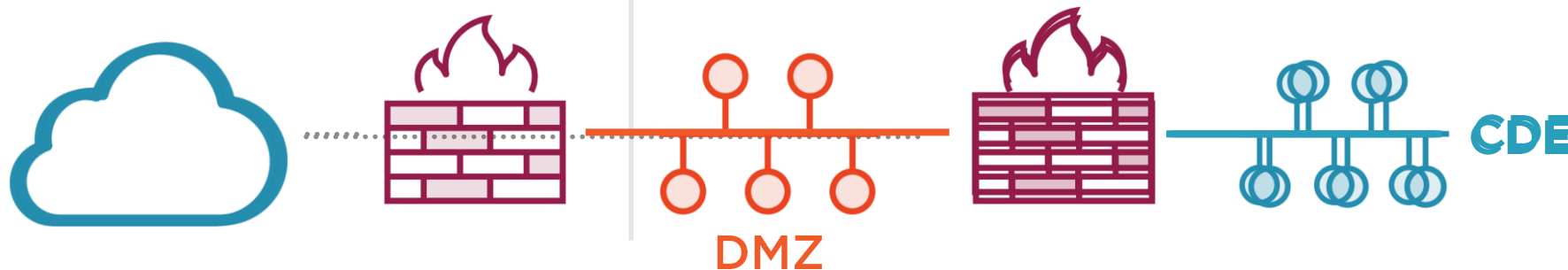
Requirement 1.1.4

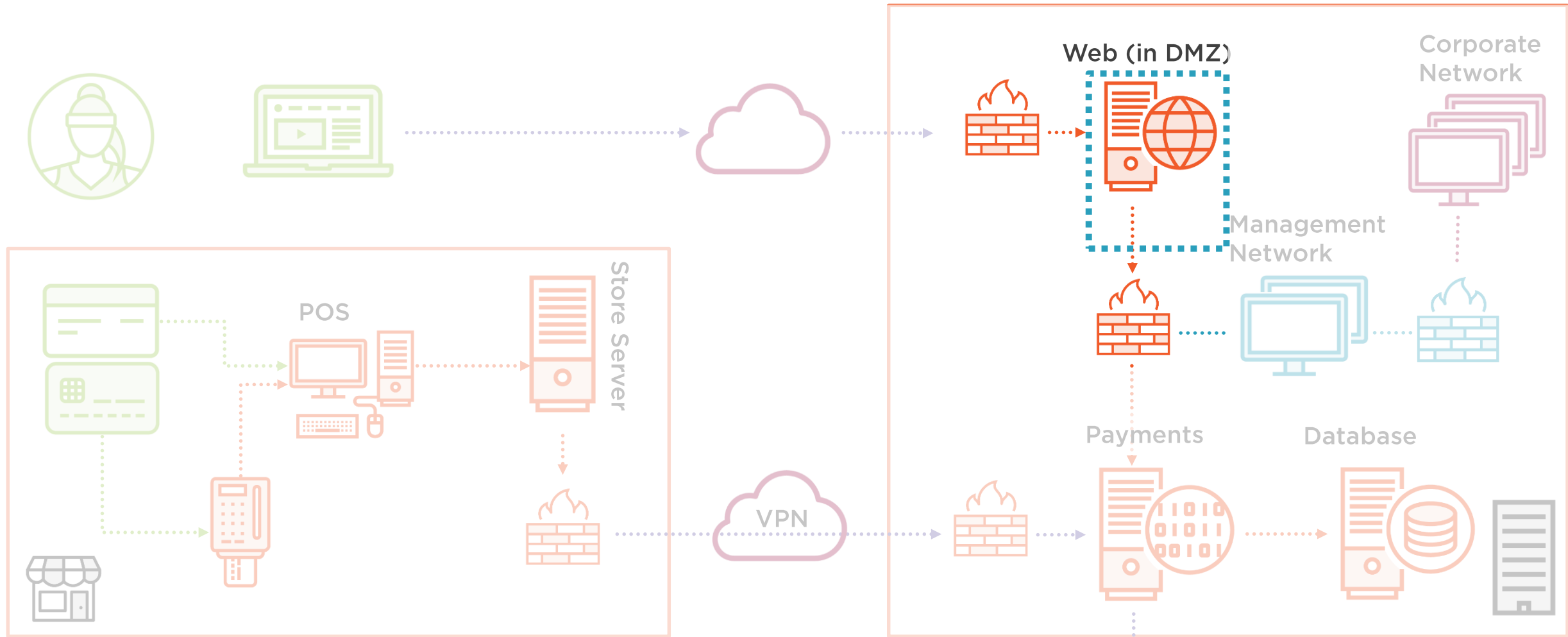
Requirements for a firewall at **each Internet connection** and between any **demilitarized zone (DMZ)** and the **internal network zone**.

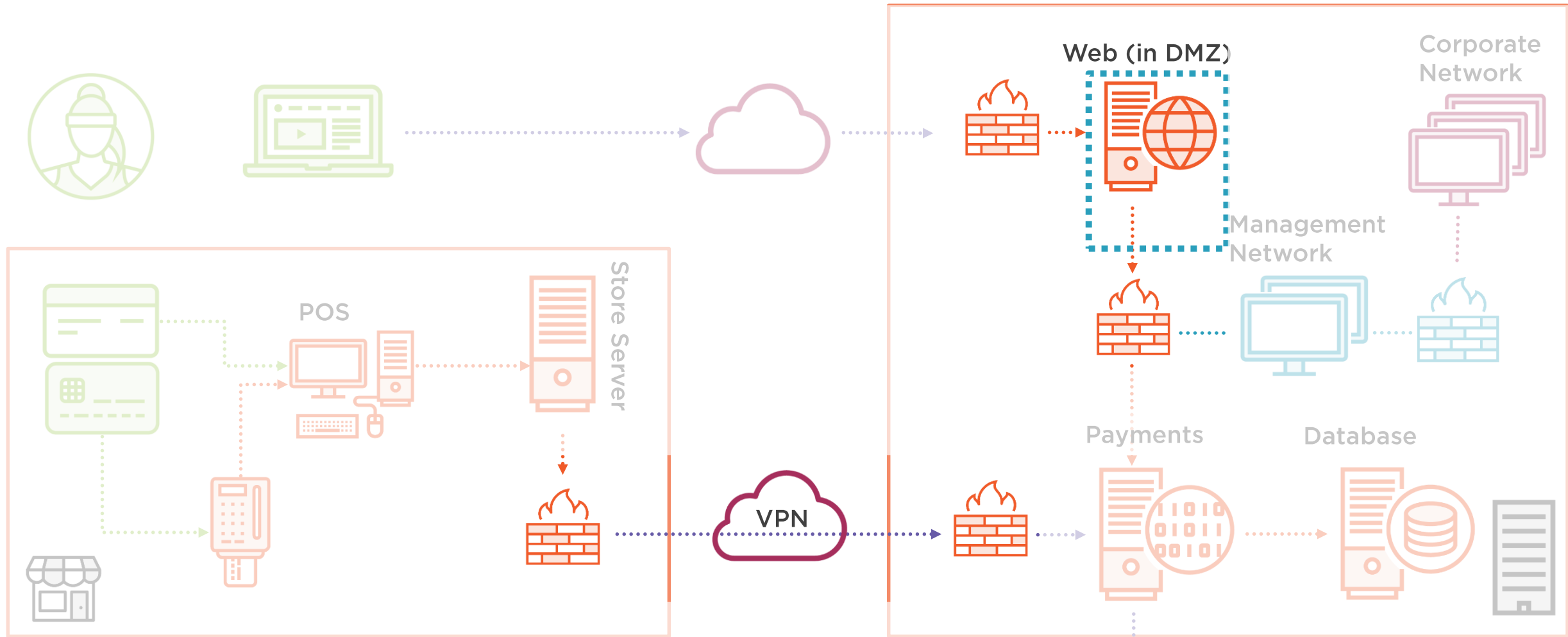


Requirement Guidance

- Using a firewall on every Internet connection coming into (and out of) the network, and between any DMZ and the internal network, allows the organization to monitor and control access and minimizes the chances of a malicious individual obtaining access to the internal network via an unprotected connection.







- Cardholder's card and systems
- Stores, processes or transmits
- Connected to or security affecting
- Out of scope of PCI DSS

- Unencrypted cardholder data
- Encrypted cardholder data
- Physical card read
- Management network
- Corporate network



1.1.4 Testing Procedures

Observe/examine systems and settings	Y	Network configurations
Examine documentation	Y	Firewall configuration standards
Examine records	Y	Network diagram
Interview people	-	

Requirement 1 | Install and maintain a firewall configuration to protect cardholder data





Requirement 1.1.5

Role-based access for firewalls

Requirement 1 | Install and maintain a firewall configuration to protect cardholder data





Requirement 1.1.5

Description of **groups**, **roles**, and **responsibilities** for management of network components.



Requirement Guidance

- This description of roles and assignment of responsibilities ensures that personnel are aware of who is responsible for the security of all network components, and that those assigned to manage components are aware of their responsibilities. If roles and responsibilities are not formally assigned, devices could be left unmanaged.

1.1.5 Testing Procedures

Observe/examine systems and settings	!	Firewalls and directory servers
Examine documentation	Y	Firewall and router configuration standards
Examine records	!	Members of management groups
Interview people	Y	Responsible people

Requirement 1 | Install and maintain a firewall configuration to protect cardholder data





Requirement 1.1.6

Every firewall rule is documented with the business need AND there's a record that each one has been approved.



Requirement 1.1.6

Documentation of **business justification** and **approval** for use of **all** services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.



Requirement Guidance

- ... By clearly defining and documenting the services, protocols, and ports that are necessary for business, organizations can ensure that all other services etc are disabled or removed.
- Approvals should be granted by personnel independent of the personnel managing the configuration.
- If insecure services etc are necessary for business, the risk posed ...should be clearly understood and accepted by the organization ... the security features that allow these protocols to be used securely should be documented and implemented.

1.1.6 Testing Procedures

Observe/examine systems and settings	Y	Firewall and router configurations
Examine documentation	Y	Firewall and router configuration standards
Examine records	Y	List of connections and business rules
Interview people	-	

Requirement 1 | Install and maintain a firewall configuration to protect cardholder data





Requirement 1.1.7

Review firewall (and router) rules every six months.

Most people use tools





Requirement 1.1.7

Requirement to **review** firewall and router rule sets **at least** every **six months**



Requirement Guidance

- This review gives the organization an opportunity at least every six months to clean up any unneeded, outdated, or incorrect rules, and ensure that all rule sets allow only authorized services and ports that match the documented business justifications.
- Organizations with a high volume of changes to firewall and router rule sets may wish to consider performing reviews more frequently, to ensure that the rule sets continue to meet the needs of the business.



1.1.7 Testing Procedures

Observe/examine systems and settings	-	
Examine documentation	Y	Firewall and router configuration standards
Examine records	Y	Rule set reviews
Interview people	Y	Responsible people

Requirement 1 | Install and maintain a firewall configuration to protect cardholder data





Requirement 1.2

Manage (restrict) connections between untrusted networks and the CDE





Requirement 1.2

Build firewall and router **configurations** that **restrict connections** between **untrusted networks** and any system components in the **cardholder data environment**.

***Note:** An “untrusted network” is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity’s ability to control or manage.*



Requirement Guidance

- It is essential to install network protection between the internal, trusted network and any untrusted network that is external and/or out of the entity’s ability to control or manage. Failure to implement this measure correctly results in the entity being vulnerable to unauthorized access by malicious individuals or software.
- For firewall functionality to be effective, it must be properly configured to control and/or limit traffic into and out of the entity’s network.



1.2 Testing Procedures

Observe/examine systems and settings	Y	Firewall and router configurations
Examine documentation	!	Standards
Examine records	-	
Interview people	-	

Requirement 1 | Install and maintain a firewall configuration to protect cardholder data





Requirement 1.2.1

Start with a deny all rule

Only allow traffic that is **necessary**
for the CDE



Requirement 1.2.1

Restrict **inbound** and **outbound** traffic to that which is **necessary** for the cardholder data environment, and specifically **deny all other** traffic.



Requirement Guidance

- Examination of all inbound and outbound connections allows for inspection and restriction of traffic based on the source and/or destination address, thus preventing unfiltered access between untrusted and trusted environments. This prevents malicious individuals from accessing the entity's network via unauthorized IP addresses or from using services, in an unauthorized manner.
- Implementing a rule that denies all inbound and outbound traffic that is not specifically needed helps to prevent inadvertent holes that would allow unintended and potentially harmful traffic in or out.



1.2.1 Testing Procedures

Observe/examine systems and settings	Y	Firewall and router configurations
Examine documentation	Y	Firewall and router standards
Examine records	Y	Documented firewall rules – including the “necessity” of the rule
Interview people	-	





Requirement 1.2.2

Secure and synchronize
router configuration files

(if this is a thing for you)





Requirement 1.2.2

Secure and **synchronize**
router configuration files.



Requirement Guidance

- While the running (or active) router configuration files include the current, secure settings, the start-up files (which are used when routers are re-started or booted) must be updated with the same secure settings to ensure these settings are applied when the start-up configuration is run.
- Because they only run occasionally, start-up configuration files are often forgotten and are not updated. When a router re-starts and loads a start-up configuration that has not been updated with the same secure settings as those in the running configuration, it may result in weaker rules that allow malicious individuals into the network.



1.2.2 Testing Procedures

Observe/examine systems and settings	Y	Router configurations Router configuration files
Examine documentation	-	
Examine records	-	
Interview people	-	





Requirement 1.2.3

Segment wireless networks from the CDE
Only allow authorized traffic





Requirement 1.2.3

Install **perimeter firewalls** between all **wireless networks** and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, **permit only authorized traffic** between the wireless environment and the cardholder data environment.



Requirement Guidance

- ...If a wireless device or network is installed without the entity's knowledge, a malicious individual could easily and "invisibly" enter the network. If firewalls do not restrict access from wireless networks into the CDE, malicious individuals that gain unauthorized access to the wireless network can easily connect to the CDE and compromise account information.
- Firewalls must be installed between all wireless networks and the CDE, regardless of the purpose of the environment to which the wireless network is connected. This may include, but is not limited to, corporate networks, retail stores, guest networks, warehouse environments, etc.



1.2.3 Testing Procedures

Observe/examine systems and settings	Y	Firewall and router configurations
Examine documentation	-	
Examine records	!	Documentation of “business purposes” Network diagrams
Interview people	-	

Requirement 1 | Install and maintain a firewall configuration to protect cardholder data





Requirement 1.3

No public access between the internet and anything in the cardholder data environment





Requirement 1.3

Prohibit direct public **access** between the **Internet** and any system component in the **cardholder data environment**.



Requirement Guidance

- While there may be legitimate reasons for untrusted connections to be permitted to DMZ systems (e.g., to allow public access to a web server), such connections should never be granted to systems in the internal network. A firewall's intent is to manage and control all connections between public systems and internal systems, especially those that store, process or transmit cardholder data. If direct access is allowed between public systems and the CDE, the protections offered by the firewall are bypassed, and system components storing cardholder data may be exposed to compromise.



1.3 Testing Procedures

Observe/examine systems and settings	Y	Firewall and router configurations
Examine documentation	-	
Examine records	!	Network and card data flow diagrams
Interview people	-	

Requirement 1 | Install and maintain a firewall configuration to protect cardholder data





Requirement 1.3.1

Put publicly accessible services in a DMZ





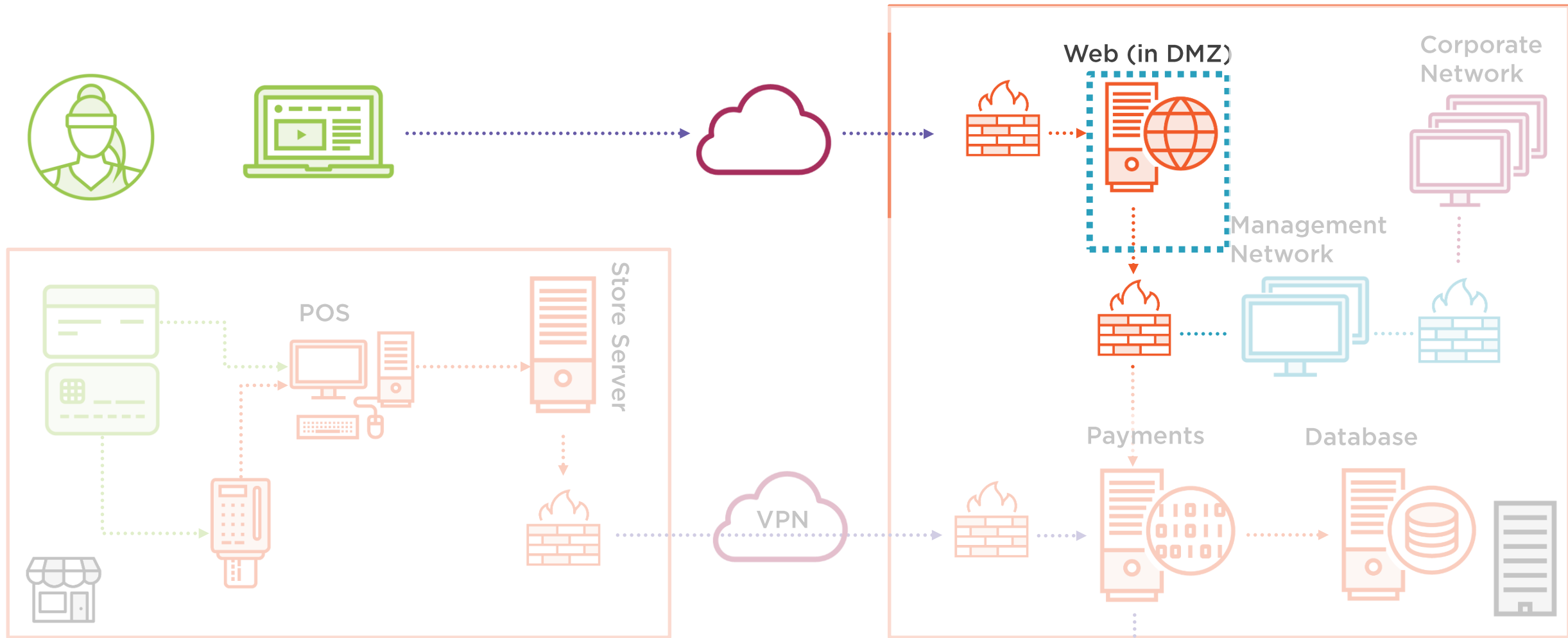
Requirement 1.3.1

Implement a **DMZ** to **limit inbound traffic** to only system components that provide **authorized** publicly accessible **services**, protocols, and ports.



Requirement Guidance

- The DMZ is that part of the network that manages connections between the Internet (or other untrusted networks), and services that an organization needs to have available to the public (like a web server).



1.3.1 Testing Procedures

Observe/examine systems and settings	Y	Firewall and router configurations
Examine documentation	-	
Examine records	!	Where to find authorization?
Interview people	-	

Requirement 1 | Install and maintain a firewall configuration to protect cardholder data





Requirement 1.3.2

Inbound internet traffic stops in the DMZ –
i.e. use the DMZ required in 1.3.1





Requirement 1.3.2

Limit inbound **Internet** traffic to IP addresses within the DMZ.



Requirement Guidance

- This functionality is intended to prevent malicious individuals from accessing the organization's internal network from the Internet, or from using services, protocols, or ports in an unauthorized manner.



1.3.2 Testing Procedures

Observe/examine systems and settings	Y	Firewall and router configurations
Examine documentation	-	
Examine records	-	
Interview people	-	

Requirement 1 | Install and maintain a firewall configuration to protect cardholder data





Requirement 1.3.3

Protect against packet spoofing



Requirement 1.3.3

Implement **anti-spoofing** measures to detect and block **forged source IP addresses** from entering the network.

(For example, block traffic originating from the Internet with an internal source address.)



Requirement Guidance

- Normally a packet contains the IP address of the computer that originally sent it so other computers in the network know where the packet came from. Malicious individuals will often try to spoof (or imitate) the sending IP address so that the target system believes the packet is from a trusted source.
- Filtering packets coming into the network helps to, among other things, ensure packets are not “spoofed” to look like they are coming from an organization’s own internal network.

1.3.3 Testing Procedures

Observe/examine systems and settings	Y	Firewall and router configurations
Examine documentation	-	
Examine records	-	
Interview people	-	

Requirement 1 | Install and maintain a firewall configuration to protect cardholder data





Requirement 1.3.4

Ensure all outbound traffic is deliberate





Requirement 1.3.4

Do **not** allow **unauthorized outbound traffic** from the cardholder data environment to the Internet.



Requirement Guidance

- All traffic outbound from the cardholder data environment should be evaluated to ensure that it follows established, authorized rules. Connections should be inspected to restrict traffic to only authorized communications (for example by restricting source/destination addresses/ports, and/or blocking of content).



1.3.4 Testing Procedures

Observe/examine systems and settings	Y	Firewall and router configurations
Examine documentation	-	
Examine records	!	Records of authorization
Interview people	-	

Requirement 1 | Install and maintain a firewall configuration to protect cardholder data





Requirement 1.3.5

Use stateful firewalls





Requirement 1.3.5

Permit only “**established**” **connections** into the network.



Requirement Guidance

- A firewall that maintains the “state” (or the status) for each connection through the firewall knows whether an apparent response to a previous connection is actually a valid, authorized response (since it retains each connection’s status) or is malicious traffic trying to trick the firewall into allowing the connection.

1.3.5 Testing Procedures

Observe/examine systems and settings	Y	Firewall and router configurations
Examine documentation	-	
Examine records	-	
Interview people	-	

Requirement 1 | Install and maintain a firewall configuration to protect cardholder data





Requirement 1.3.6

Don't store cardholder data in a DMZ





Requirement 1.3.6

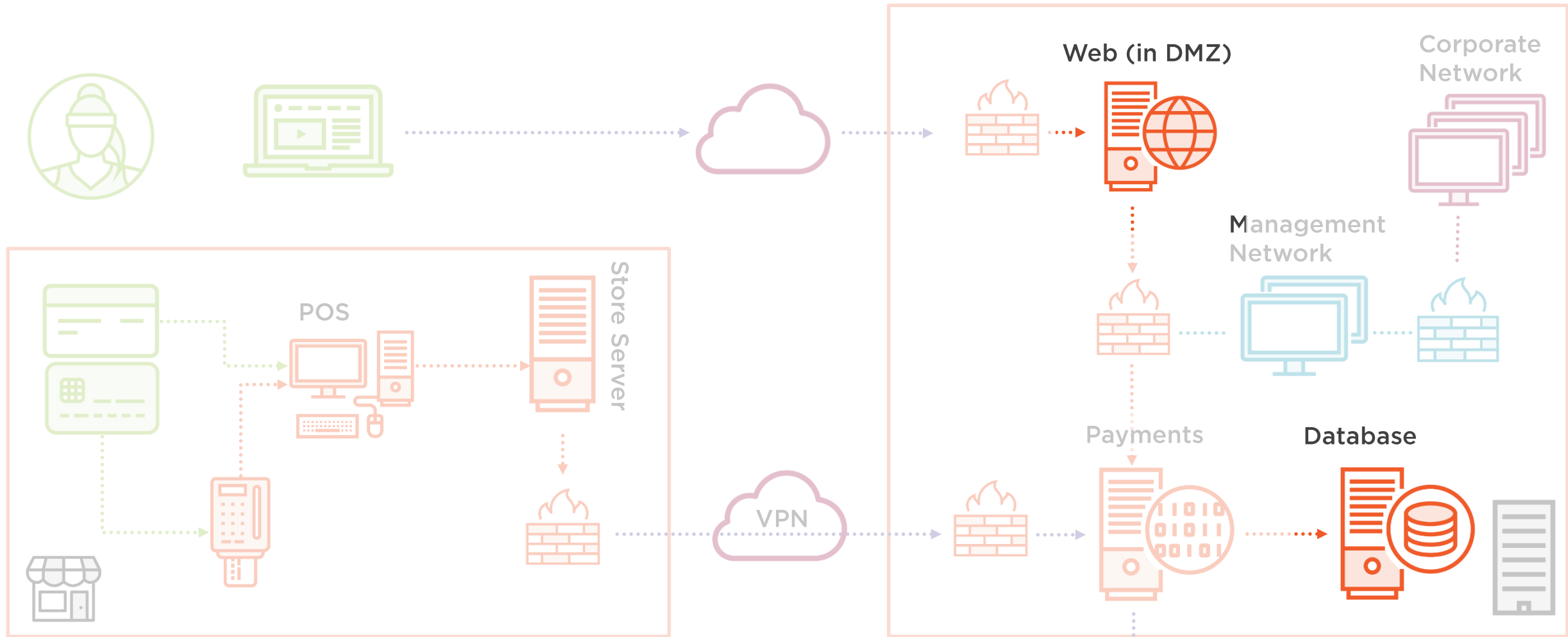
Place **system components** that **store cardholder data** (such as a database) in an **internal network zone**, segregated from the DMZ and other untrusted networks.



Requirement Guidance

- If cardholder data is located within the DMZ, it is easier for an external attacker to access this information, since there are fewer layers to penetrate. Securing system components that store cardholder data in an internal network zone that is segregated from the DMZ and other untrusted networks by a firewall can prevent unauthorized network traffic from reaching the system component.
- ***Note:** This requirement is not intended to apply to temporary storage of cardholder data in volatile memory.*





1.3.6 Testing Procedures

Observe/examine systems and settings	Y	Firewall and router configurations
Examine documentation	-	
Examine records	!	Network and data flow diagrams
Interview people	-	

Requirement 1 | Install and maintain a firewall configuration to protect cardholder data





Requirement 1.3.7

Keep internal IP address ranges a secret





Requirement 1.3.7

Do **not** disclose **private IP** addresses and routing information to unauthorized parties.

Note: Methods to obscure IP addressing may include, but are not limited to:

- Network Address Translation (NAT)
- Placing servers containing cardholder data behind proxy servers/firewalls,
- Removal or filtering of route advertisements for private networks that employ registered addressing,
- Internal use of RFC1918 address space instead of registered addresses.



Requirement Guidance

- Restricting the disclosure of internal or private IP addresses is essential to prevent a hacker “learning” the IP addresses of the internal network, and using that information to access the network.
- Methods used to meet the intent of this requirement may vary depending on the specific networking technology being used. For example, the controls used to meet this requirement may be different for IPv4 networks than for IPv6 networks.



1.3.7 Testing Procedures

Observe/examine systems and settings	Y	Firewall and router configurations
Examine documentation	Y	Firewall and router information
Examine records	-	
Interview people	Y	Responsible people

Requirement 1 | Install and maintain a firewall configuration to protect cardholder data



That's Fine in Theory

