

Requirement 11: Regularly Test Security Systems and Processes (Except 11.3 Penetration Tests)



John Elliott

PRIVACY, PAYMENTS, SECURITY AND RISK SPECIALIST

@withoutfire www.withoutfire.com



Requirement 11



Rogue wireless access points

Internal & external vulnerability scans

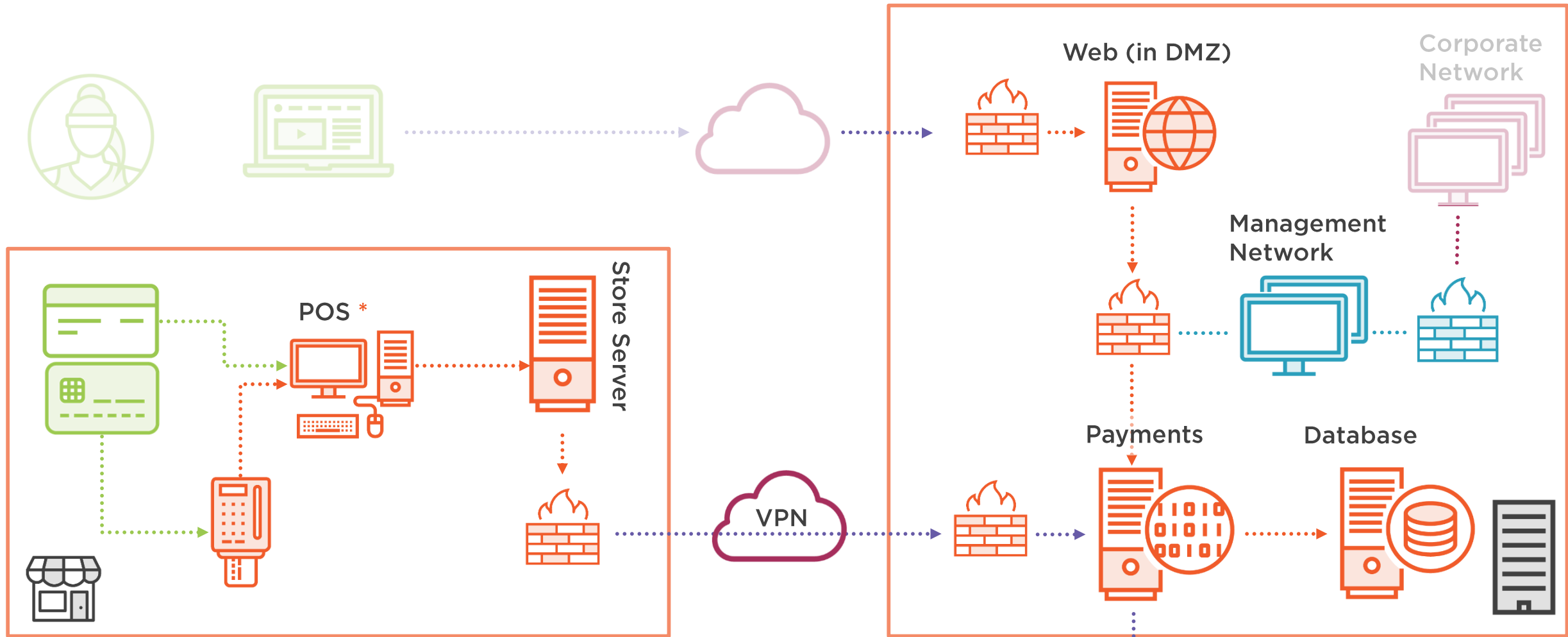
(Internal & external penetration tests)

Intruder detection / Intruder protection

Change-detection / file integrity
monitoring

Policies and procedures







Requirement 11.1

Rogue Wi-fi access points





Requirement 11.1

Implement processes to **test** for the presence of **wireless access points** (802.11), and **detect** and **identify** all **authorized and unauthorized** wireless access points on a **quarterly** basis.



Requirement Guidance

- Unauthorized wireless devices may be hidden within or attached to a computer or other system component, or be attached directly to a network port or device. Such a device could result in an unauthorized access point into the environment.
- Knowing which wireless devices are authorized helps quickly identify non-authorized wireless devices; responding to the identification of unauthorized access points helps to proactively minimize exposing CDE to malicious individuals.
- These processes must be performed even when a policy exists prohibiting the use of wireless technology because of the ease of adding them..

Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.

Note to requirement 11.1



11.1 Testing Procedures

Observe/examine systems and settings	-	
Examine documentation	Y	Policies and procedures
Examine records	Y	Recent wireless scans, automated monitoring
Interview people	-	





Requirement 11.1.1

Inventory of authorized wireless access points





Requirement 11.1.1

Maintain an **inventory** of **authorized** wireless access points including a **documented business justification**.



Requirement Guidance

- **For example:** In the case of a single standalone retail kiosk in a shopping mall, where all communication components are contained within tamper-resistant and tamper-evident casings, performing a detailed physical inspection of the kiosk itself may be sufficient to provide assurance that a rogue wireless access point has not been attached or installed. However, in an environment with multiple nodes, detailed physical inspection is difficult. In this case, multiple methods may be combined to meet the requirement, such as performing physical system inspections in conjunction with the results of a wireless analyzer.

1.1.1 Testing Procedures

Observe/examine systems and settings	-	
Examine documentation	-	
Examine records	Y	Inventory of access points
Interview people	-	





Requirement 11.1.2

Respond to the detection of an unauthorized access point





Requirement 11.1.2

Implement **incident response** procedures in the event **unauthorized** wireless **access points** are **detected**.



Requirement Guidance



1.1.2 Testing Procedures

Observe/examine systems and settings	-	
Examine documentation	Y	Incident response plan
Examine records	-	
Interview people	Y	People who would respond to the detection





Requirement 11.2

Quarterly vulnerability scans





Requirement 11.2

Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).



Requirement Guidance

- There are three types of vulnerability scanning required for PCI DSS:
- Internal quarterly vulnerability scanning by qualified personnel (use of a PCI SSC Approved Scanning Vendor (ASV) is not required)
- External quarterly vulnerability scanning, which must be performed by an ASV
- Internal and external scanning as needed after significant changes
- Once these weaknesses are identified, the entity corrects them and repeats the scan until all vulnerabilities have been corrected.

11.2 Testing Procedures

Observe/examine systems and settings	-	
Examine documentation	Y	Documentation supporting scan reports
Examine records	Y	Scan reports
Interview people	-	





Requirement 11.2.1

Perform **quarterly internal vulnerability scans**.

Address vulnerabilities and perform rescans to verify all “high risk” vulnerabilities are resolved in accordance with the entity’s vulnerability ranking (per Requirement 6.1).

Scans must be performed by qualified personnel.



Requirement Guidance

- An established process for identifying vulnerabilities on internal systems requires that vulnerability scans be conducted quarterly. Vulnerabilities posing the greatest risk to the environment (for example, ranked “High” per Requirement 6.1) should be resolved with the highest priority.
- Internal vulnerability scans can be performed by qualified, internal staff that are reasonably independent of the system component(s) being scanned, or an entity may choose to have internal vulnerability scans performed by a firm specializing in vulnerability scanning.



Requirement 11.2.1

Perform quarterly internal vulnerability scans.

Address vulnerabilities and perform rescans to verify all “high risk” vulnerabilities are resolved in accordance with the entity’s vulnerability ranking (per Requirement 6.1).

Scans must be performed by qualified personnel.



Requirement Guidance

- An established process for identifying vulnerabilities on internal systems requires that vulnerability scans be conducted quarterly. Vulnerabilities posing the greatest risk to the environment (for example, ranked “High” per Requirement 6.1) should be resolved with the highest priority.
- Internal vulnerability scans can be performed by qualified, internal staff that are reasonably independent of the system component(s) being scanned, or an entity may choose to have internal vulnerability scans performed by a firm specializing in vulnerability scanning.



Requirement 11.2.1

Perform quarterly internal vulnerability scans.

Address vulnerabilities and perform rescans to verify all “high risk” vulnerabilities are resolved in accordance with the entity’s vulnerability ranking (per Requirement 6.1).

Scans must be performed by qualified personnel.



Requirement Guidance

- An established process for identifying vulnerabilities on internal systems requires that vulnerability scans be conducted quarterly. Vulnerabilities posing the greatest risk to the environment (for example, ranked “High” per Requirement 6.1) should be resolved with the highest priority.
- Internal vulnerability scans can be performed by qualified, internal staff that are reasonably independent of the system component(s) being scanned, or an entity may choose to have internal vulnerability scans performed by a firm specializing in vulnerability scanning.

Qualified to Scan?



Trained / qualified in the use of the scanning tool

Does NOT have to be an ISA, QSA, ASV or PCIP

Can be internal or external

Must be independent of the people managing the infrastructure

11.2.1 Testing Procedures

Observe/examine systems and settings	-	
Examine documentation	-	
Examine records	Y	Scan reports
Interview people	Y	Responsible people





Requirement 11.2.2

Perform **quarterly external vulnerability scans**, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC).

Perform rescans as needed, until passing scans are achieved.



Requirement Guidance

- As external networks are at greater risk of compromise, quarterly external vulnerability scanning must be performed by a PCI SSC Approved Scanning Vendor (ASV).
- A robust scanning program ensures that scans are performed and vulnerabilities addressed in a timely manner.



APPROVED SCANNING VENDORS

An ASV is an organization with a set of security services and tools (“ASV scan solution”) to conduct external vulnerability scanning services to validate adherence with the external scanning requirements of PCI DSS Requirement 11.2.2. The scanning vendor’s ASV scan solution is tested and approved by PCI SSC before an ASV is added to PCI SSC’s List of Approved Scanning Vendors.





Requirement 11.2.2

Perform **quarterly external vulnerability scans**, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC).

Perform rescans as needed, until **passing scans** are achieved.



Requirement Guidance

- As external networks are at greater risk of compromise, quarterly external vulnerability scanning must be performed by a PCI SSC Approved Scanning Vendor (ASV).
- A robust scanning program ensures that scans are performed and vulnerabilities addressed in a timely manner.



11.2.2 Testing Procedures

Observe/examine systems and settings	-	
Examine documentation	-	
Examine records	Y	Output from four most recent ASVs
Interview people	-	





Requirement 11.2.3

Perform internal and external scans
after any significant change





Requirement 11.2.3

Perform **internal** and **external** scans, and rescans as needed, after **any significant change**. Scans must be performed by qualified personnel.



Requirement Guidance

- The determination of what constitutes a significant change is highly dependent on the configuration of a given environment. If an upgrade or modification could **allow access to cardholder data** or affect the **security of the cardholder data environment**, then it could be considered significant.
- Scanning an environment after any significant changes are made ensures that changes were completed appropriately such that the security of the environment was not compromised as a result of the change. All system components affected by the change will need to be scanned.

11.2.3 Testing Procedures

Observe/examine systems and settings	-	
Examine documentation	Y	Change control documentation
Examine records	Y	Scan reports Internal – nothing > medium External – nothing > CVSS 4.0
Interview people	-	



FAQs



pcisecuritystandards.org/faqs

1087: For vulnerability scans, what is meant by quarterly?

1152: Can an entity be PCI DSS compliant if they have performed quarterly scans, but do not have four “passing” scans?

1317: What is a “significant change” for PCI DSS Requirements 11.2 and 11.3?



11.3: Penetration Testing Is in the Next Module





Requirement 11.4

Implement intruder detection (IDS) and/or intruder prevention (IPS)





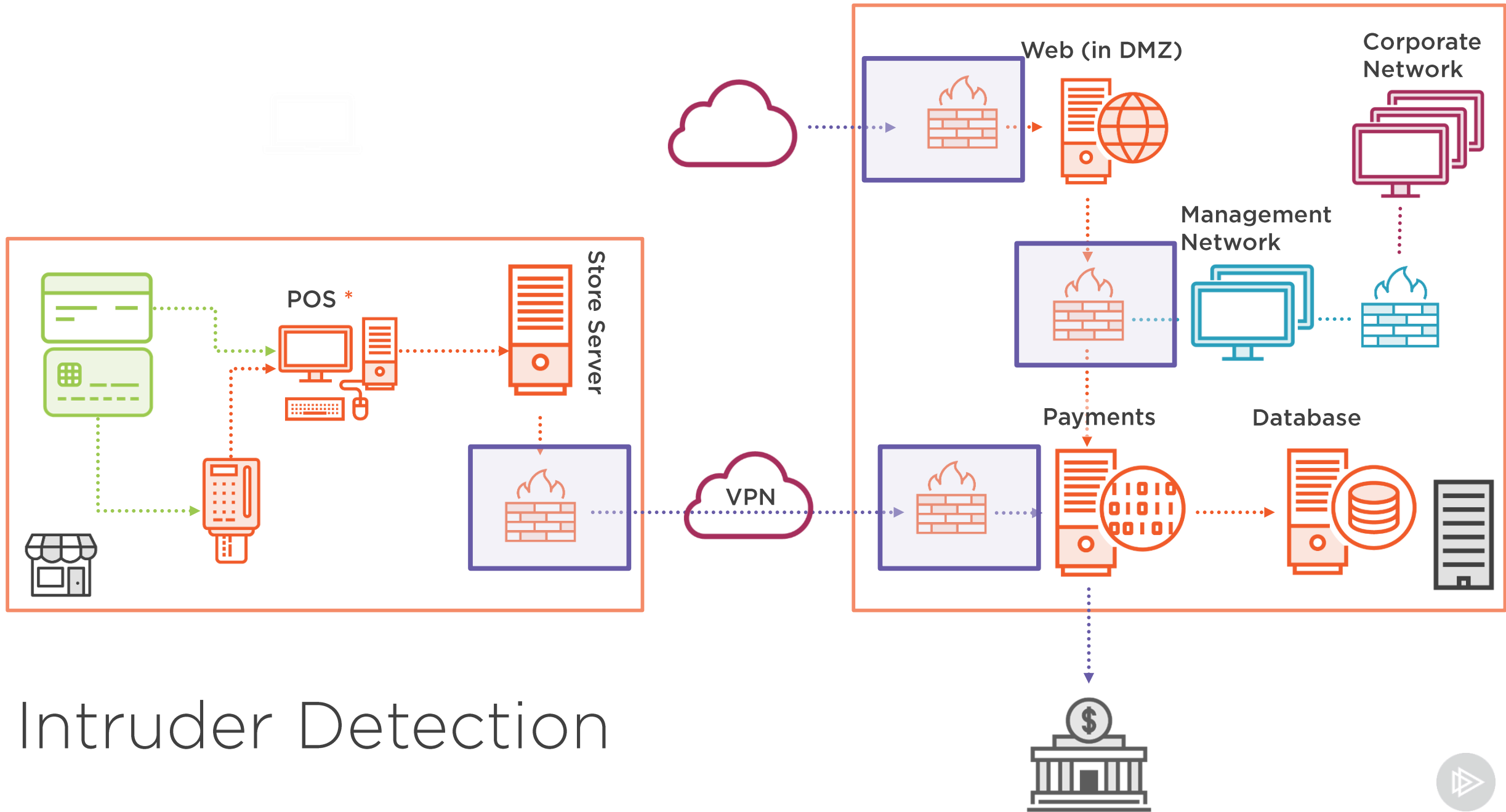
Requirement 11.4

Use **intrusion-detection** and/or **intrusion-prevention** techniques to detect and/or prevent intrusions into the network. **Monitor** all traffic at the **perimeter** of the CDE as well as at **critical points** in the CDE, and **alert personnel to suspected compromises**. **Keep** all intrusion-detection and prevention engines, baselines, and signatures **up to date**.



Requirement Guidance

- Intrusion detection and/or intrusion prevention techniques (such as IDS/IPS) compare the traffic coming into the network with known “signatures” and/or behaviors of thousands of compromise types (hacker tools, Trojans, and other malware), and send alerts and/or stop the attempt as it happens. Without a proactive approach to unauthorized activity detection, attacks on (or misuse of) computer resources could go unnoticed in real time. Security alerts generated by these techniques should be monitored so that the attempted intrusions can be stopped.



11.4 Testing Procedures

Observe/examine systems and settings	Y	System and configurations, IDS/IPS configurations
Examine documentation	Y	Vendor documentation
Examine records	Y	Network diagrams
Interview people	Y	Responsible people





Requirement 11.5

Use a change-detection mechanism such as file integrity monitoring (FIM)





Requirement 11.5

Deploy a **change-detection mechanism** (for example, file-integrity monitoring tools) to **alert personnel** to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and **configure** the software to perform **critical file comparisons at least weekly**.



Requirement Guidance

- Change-detection solutions such as file-integrity monitoring (FIM) tools check for changes, additions, and deletions to critical files, and notify when such changes are detected. If not implemented properly and the output of the change-detection solution monitored, a malicious individual could add, remove, or alter configuration file contents, operating system programs, or application executables. Unauthorized changes, if undetected, could render existing security controls ineffective and/or result in cardholder data being stolen with no perceptible impact to normal processing.



11.5 Testing Procedures

Observe/examine systems and settings	Y	System settings and monitored files, alerting mechanisms
Examine documentation	-	
Examine records	Y	Monitoring activity results
Interview people	-	





Requirement 11.5.1

Implement a process to respond to any alerts generated by the change-detection solution.



Requirement Guidance



11.5.1 Testing Procedures

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





Requirement 11.6

Policies and procedures





Requirement 11.6

Ensure that security policies and operational procedures for security monitoring and testing are **documented**, **in use**, and **known** to all affected parties.



Requirement Guidance

- Personnel need to be aware of and following security policies and operational procedures for security monitoring and testing on a continuous basis.

11.6 Testing Procedures

Observe/examine systems and settings	-	
Examine documentation	Y	Security policies, Operational procedures
Examine records	-	
Interview people	Y	Responsible people and people who need to know



That's Fine in Theory

