

Requirement 11.3: Penetration Testing

PRIVACY, PAYMENTS, SECURITY AND RISK SPECIALIST



John Elliott

@withoutfire www.withoutfire.com





Requirement 11.3

Implement a methodology
for penetration testing





Requirement 11.3

Implement a **methodology** for **penetration testing** that includes:

See list in 11.3 in PCI DSS



Requirement Guidance

- The intent of a penetration test is to simulate a real-world attack situation with a goal of identifying how far an attacker would be able to penetrate into an environment. This allows an entity to gain a better understanding of their potential exposure and develop a strategy to defend against attacks.
- A penetration test differs from a vulnerability scan, as a penetration test is an active process that may include exploiting identified vulnerabilities.

11.3 Testing Procedures

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





Requirement 11.3.1

External penetration testing





Requirement 11.3.1

Perform **external penetration** testing **at least annually** and after any **significant** infrastructure or application upgrade or modification [i.e. **change**] (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).



Requirement Guidance

- The determination of what constitutes a significant upgrade or modification 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. Performing penetration tests after network upgrades and modifications provides assurance that the controls assumed to be in place are still working effectively after the upgrade or modification.



11.3.1 Testing Procedures

Observe/examine systems and settings	-	
Examine documentation	Y	Change control Penetration test methodology
Examine records	Y	Penetration test methodology Most recent external penetration test
Interview people	-	





Requirement 11.3.2

Internal penetration testing





Requirement 11.3.2

Perform **internal penetration** testing **at least annually** and after any **significant** infrastructure or application upgrade or modification [i.e. **change**] (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).



Requirement Guidance

- The determination of what constitutes a significant upgrade or modification 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. Performing penetration tests after network upgrades and modifications provides assurance that the controls assumed to be in place are still working effectively after the upgrade or modification.



11.3.2 Testing Procedures

Observe/examine systems and settings	-	
Examine documentation	Y	Penetration test methodology
Examine records	Y	Penetration test methodology Most recent internal penetration test
Interview people	-	





Requirement 11.3.3

Fix the vulnerabilities found
by penetration testing





Requirement 11.3.3

Exploitable vulnerabilities found during penetration testing are **corrected**

and

testing is **repeated** to **verify the corrections**.



Requirement Guidance

- The determination of what constitutes a significant upgrade or modification 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. Performing penetration tests after network upgrades and modifications provides assurance that the controls assumed to be in place are still working effectively after the upgrade or modification.



11.3.3 Testing Procedures

Observe/examine systems and settings	-	
Examine documentation	-	
Examine records	-	Penetration testing results (Change control records)
Interview people	-	





Requirement 11.3.4

Test segmentation annually





Requirement 11.3.4

If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.



Requirement Guidance

- Penetration testing is an important tool to confirm that any segmentation in place to isolate the CDE from other networks is effective. The penetration testing should focus on the segmentation controls, both from outside the entity's network and from inside the network but outside of the CDE, to confirm that they are not able to get through the segmentation controls to access the CDE. For example, network testing and/or scanning for open ports, to verify no connectivity between in-scope and out-of-scope networks.

11.3.4 Testing Procedures

Observe/examine systems and settings	Y	Segmentation controls
Examine documentation	Y	Penetration-testing methodology
Examine records	Y	Most recent penetration test result
Interview people	-	





Requirement 11.3.4.1

Additional requirement for service providers only

If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every **six months** and after any changes to segmentation controls/methods.



Requirement Guidance

- For service providers, validation of PCI DSS scope should be performed as frequently as possible to ensure PCI DSS scope remains up to date and aligned with changing business objectives.



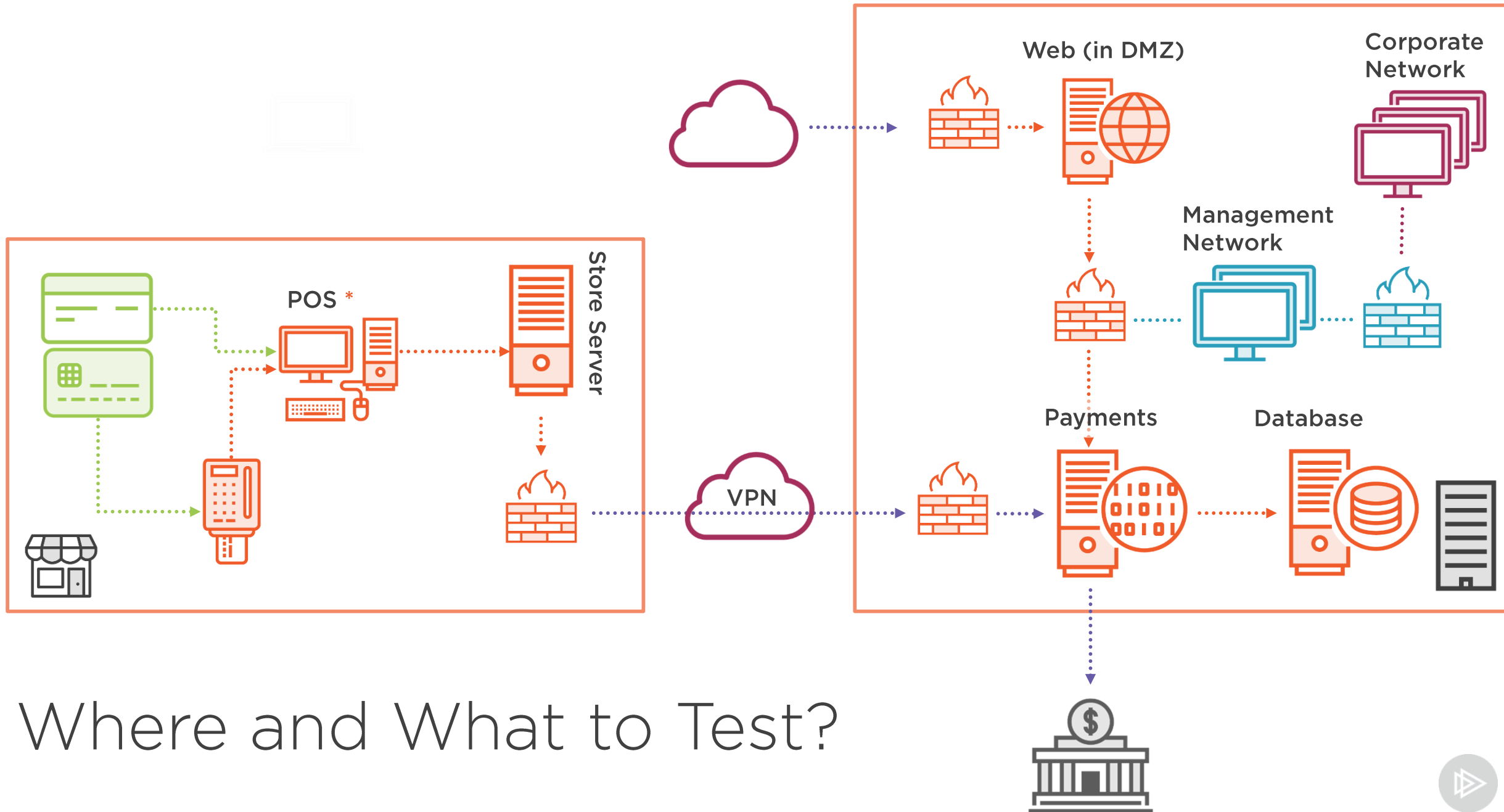
Why Test?



Security

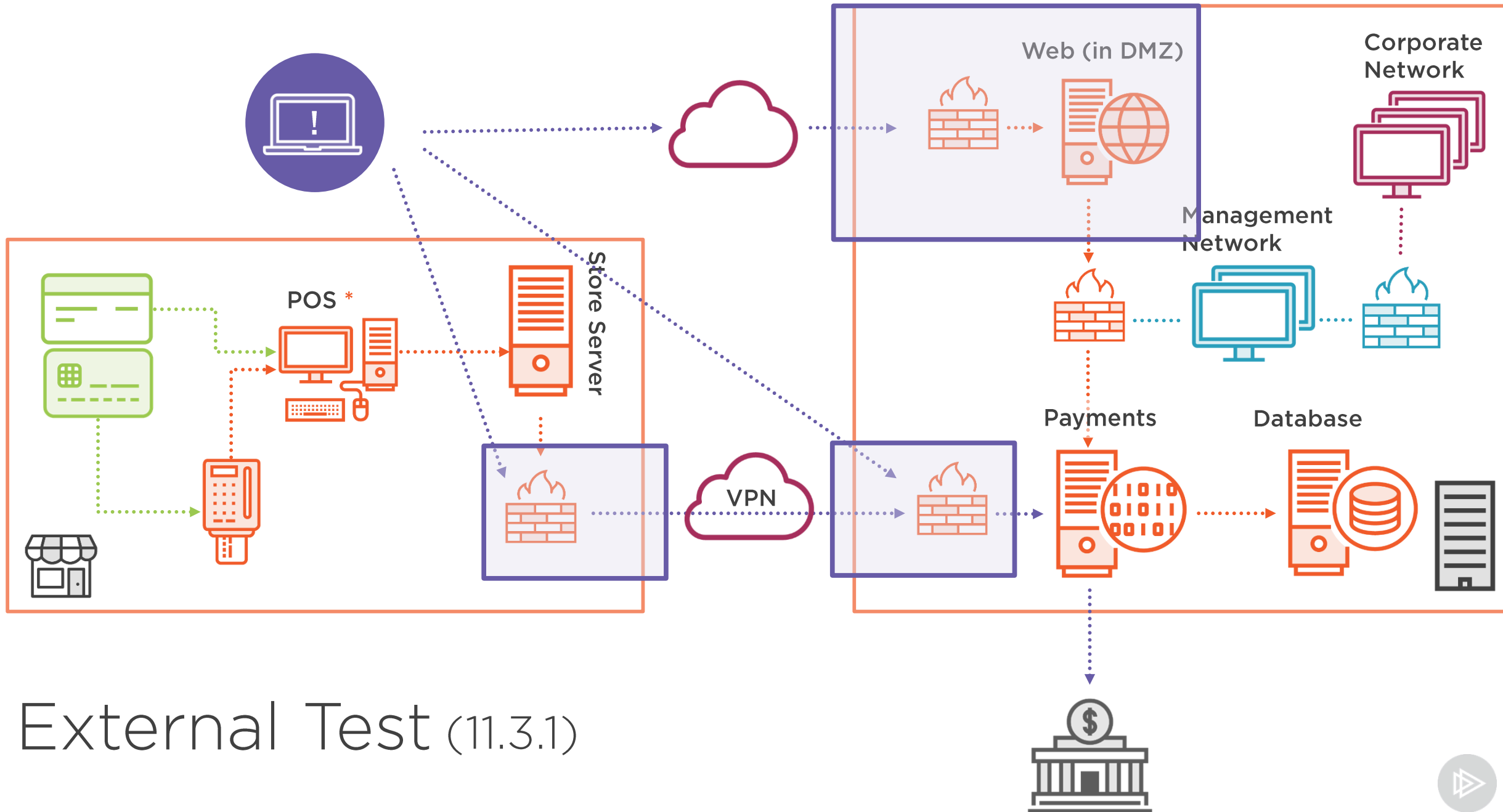


Compliance



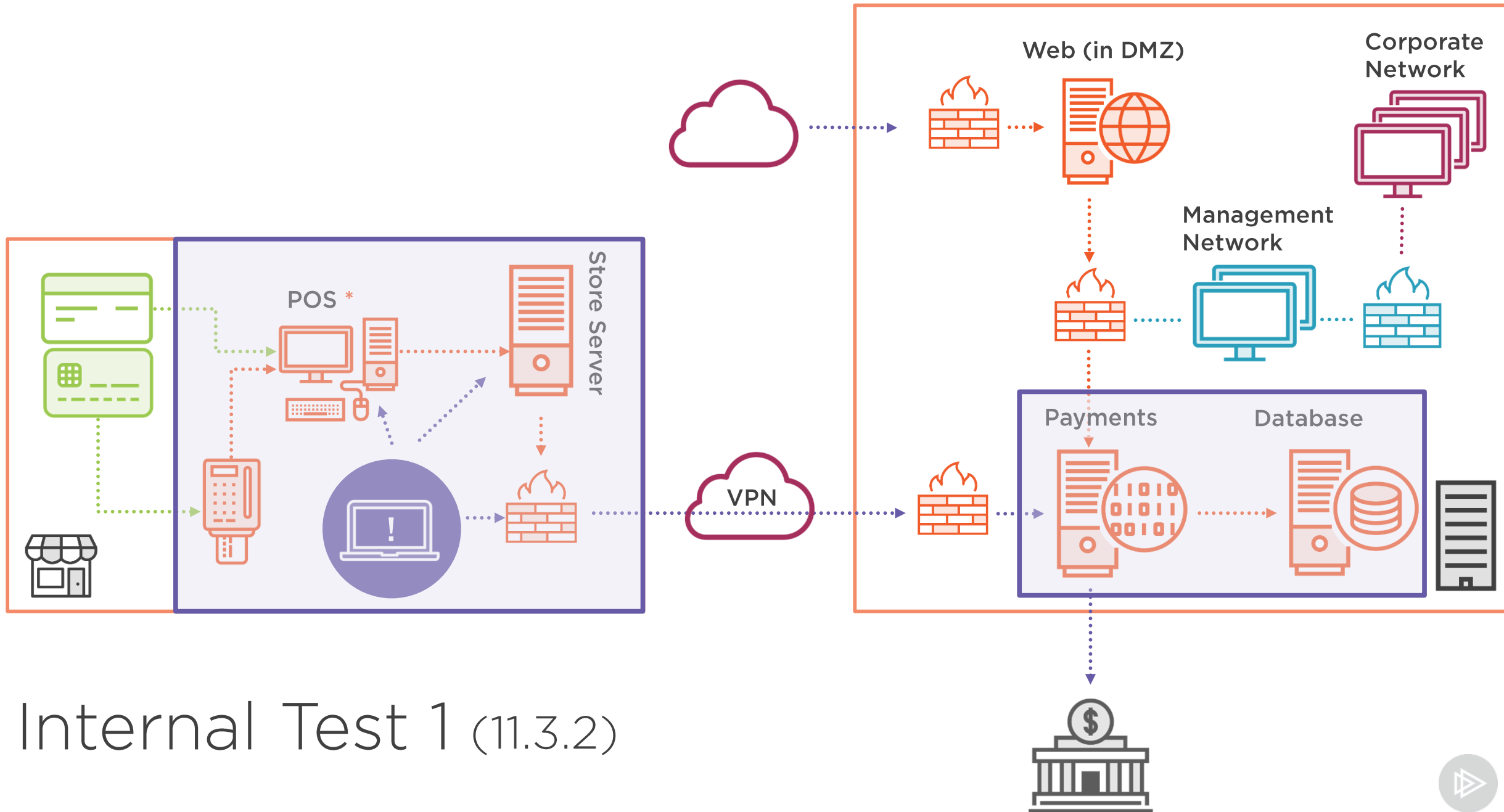
Where and What to Test?

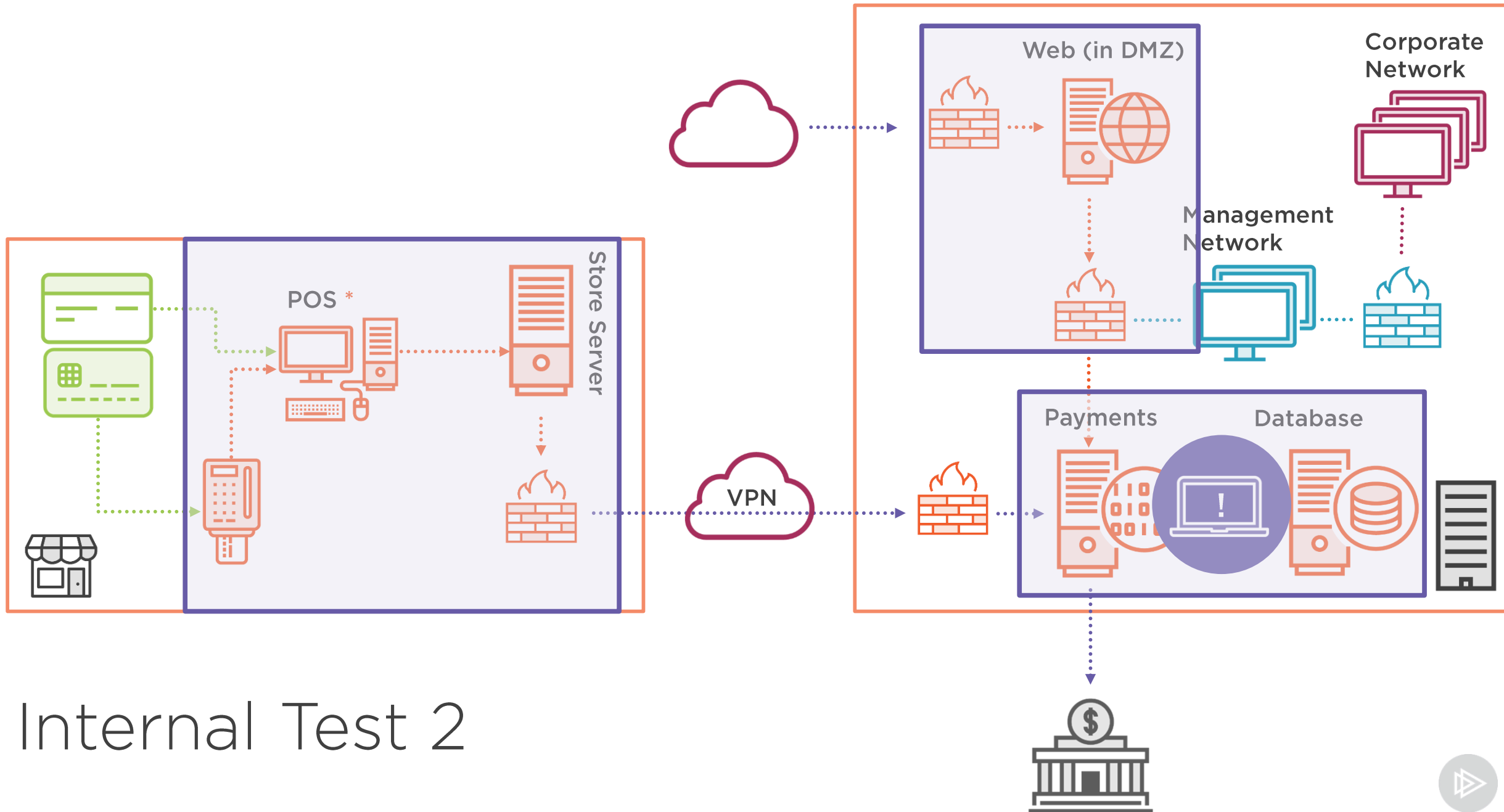


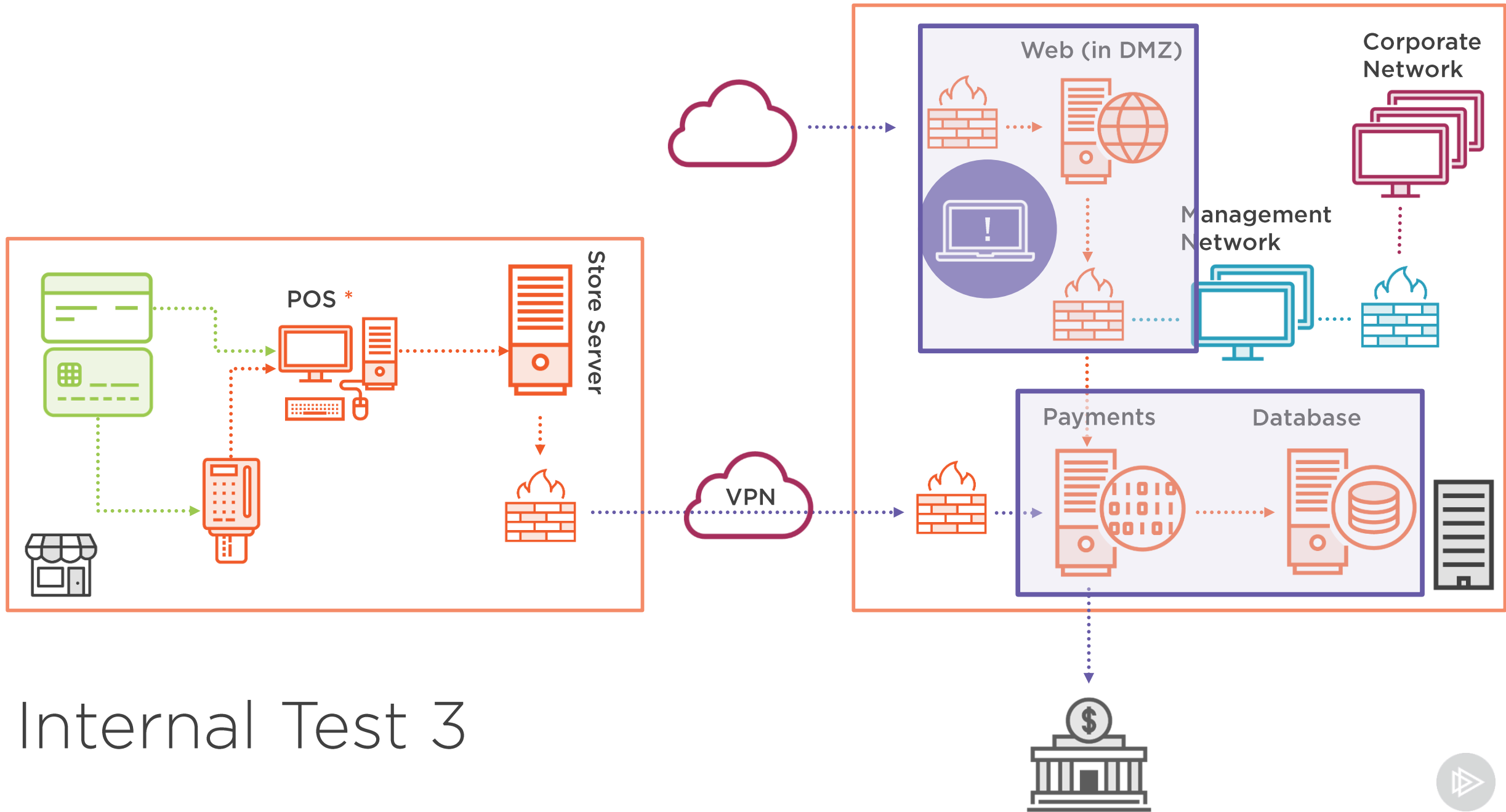


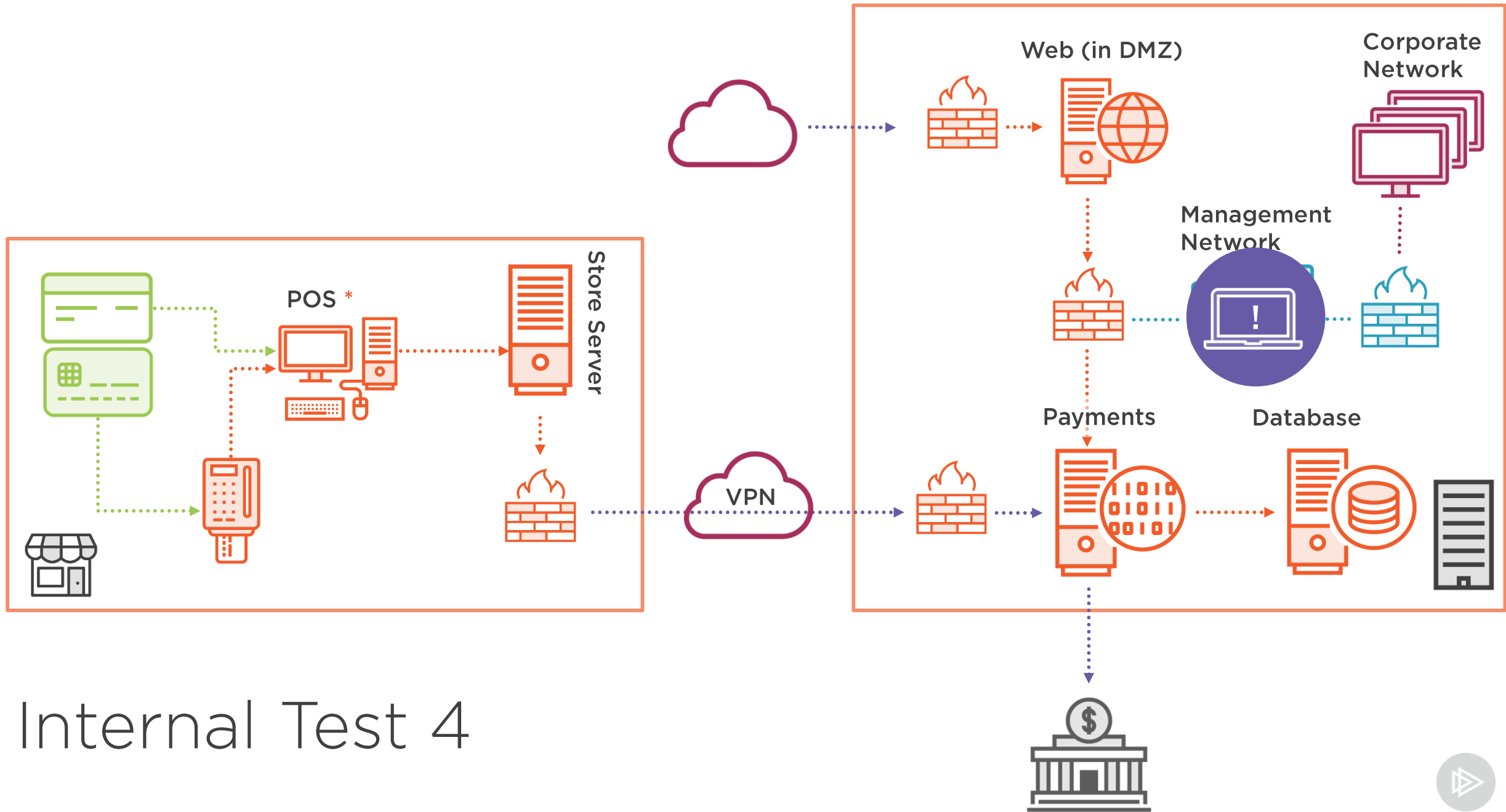
External Test (11.3.1)





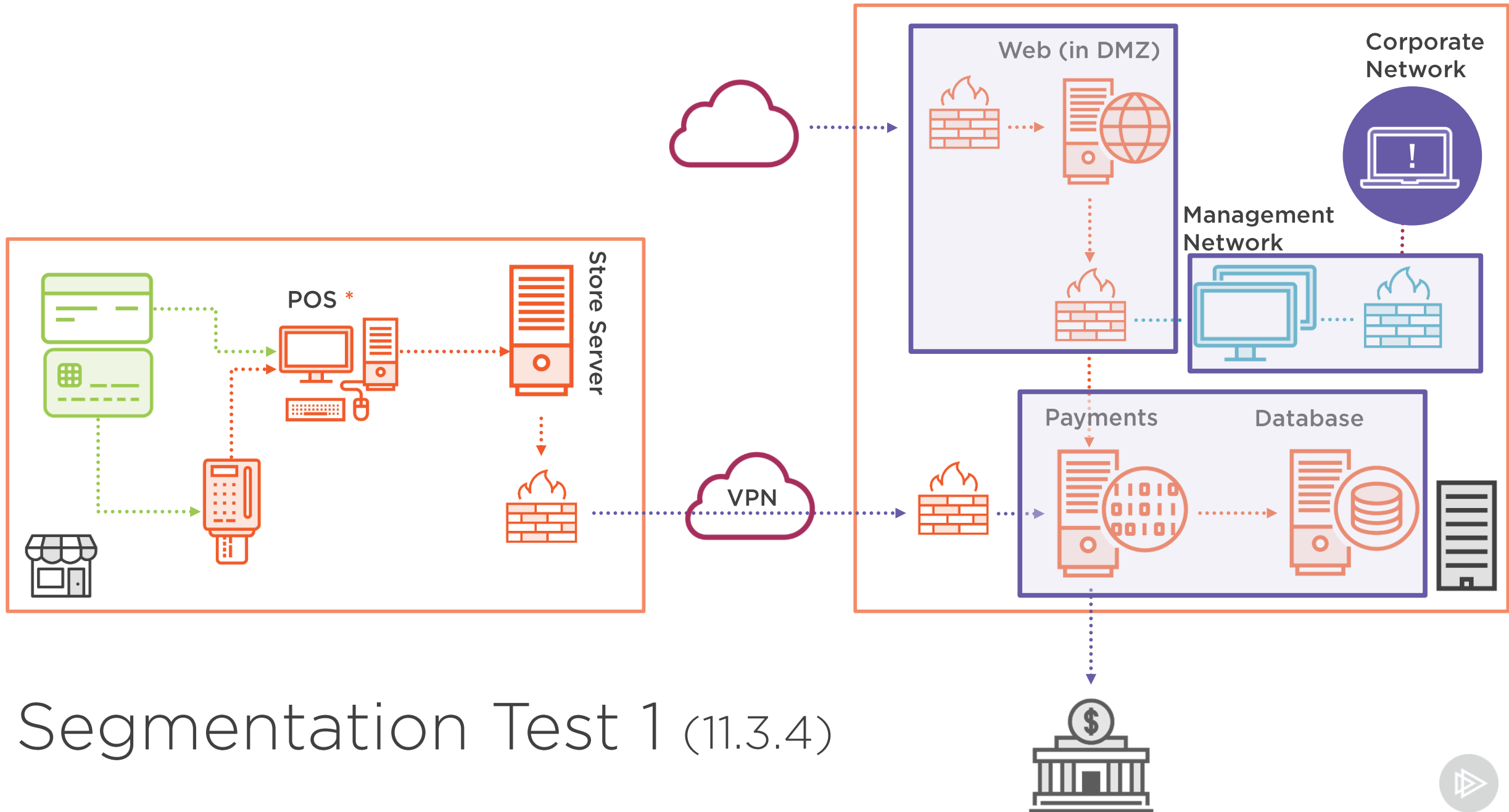






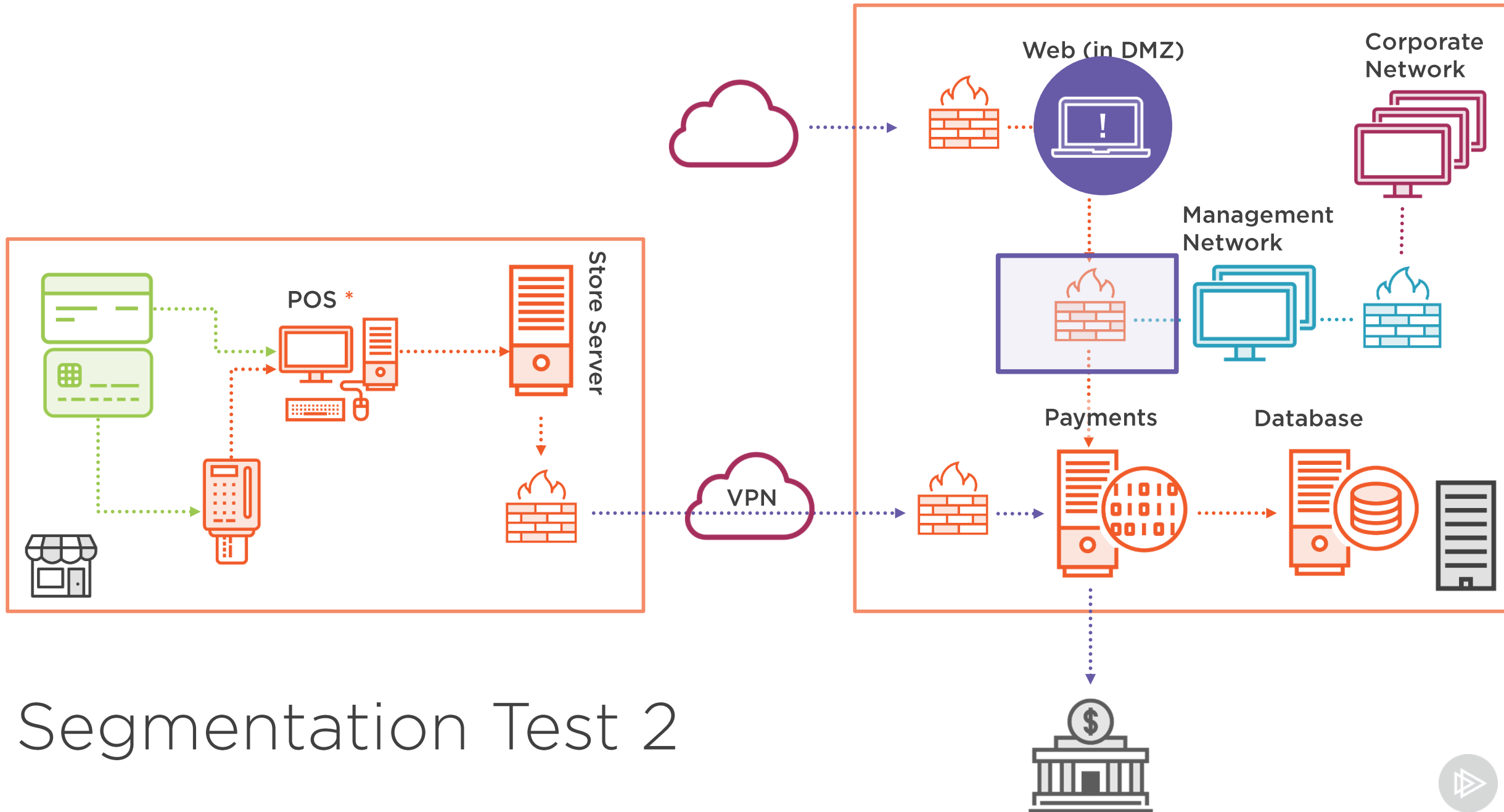
Internal Test 4





Segmentation Test 1 (11.3.4)





Segmentation Test 2





Standard: PCI Data Security Standard (PCI DSS)
Version: 1.1
Date: September 2017
Author: Penetration Test Guidance Special Interest Group
PCI Security Standards Council

**Information Supplement:
Penetration Testing Guidance**

[pcisecuritystandards.org/documents/
Penetration-Testing-Guidance-v1_1.pdf](https://pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf)



That's Fine in Theory

