ControlCase
Compliance as a Service

Penetration Testing and PCI DSS 3.1

Erik Winkler, ControlCase

Agenda

- What is a Penetration Test?
- Why is it important?
- What should we include in the test?
- What's new in PCI DSS 3.1
- How the methodology is defined?
- Is a segmentation test different than a pen test?
- Pre-requisites for segmentation
- Case Study
- Best Practices to pass a segmentation pen test

ControlCase
Compliance as a Service

What is a Penetration Test?

- A method of evaluating the security of a computer system, network or application by simulating an attack by a malicious hacker.
- Involves an active analysis of the system for any weaknesses, technical flaws or vulnerabilities.
- Carried out from the position of a potential attacker, and involves an active exploitation of security vulnerabilities.
- Performed from outside the external security perimeter or internal to the internal security perimeter.

ControlCase
Compliance as a Service

Why is it important?

- To determine whether and how a malicious user can gain unauthorized access to assets and eventually sensitive data

- To confirm that the applicable controls, such as scope, vulnerability management, methodology, and segmentation, required in PCI DSS are in place.

ControlCase
Compliance as a Service

What should we include in the test?

- Entire CDE perimeter
- Any critical systems that may impact the security of the CDE
- External perimeter (public-facing attack surfaces)
- Internal perimeter of the CDE (LAN-LAN attack surfaces)
- Validate segmentation and scope-reduction controls

ControlCase
Compliance as a Service

What's new in PCI DSS 3.1

- 11.3.4 - CDE Segmentation Verification
  - Applicable if segmentation is used to isolate CDE from other networks
  - Verifies that segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems
  - Must provide tester documentation of segmentation technologies
  - Testing against CDE systems from outside CDE
  - Testing against out-of-scope systems within the CDE

ControlCase
Compliance as a Service

How the methodology is defined?

- Based on the best practices from Open-Source Security Testing Methodology Manual (OSSTMM), Open Web Application Security Project (OWASP) and NIST SP800-115
- Includes coverage for the entire CDE perimeter and critical systems
- Includes testing from both inside and outside the network
- Includes testing to validate any segmentation and scope-reduction controls
- Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5
- Defines network-layer penetration tests to include components that support network functions as well as operating systems
- Includes review and consideration of threats and vulnerabilities experienced in the last 12 months
- Specifies retention of penetration testing results and remediation activities results

ControlCase
Compliance as a Service

What is the difference between tests?

Penetration Testing	Segmentation Penetration Testing
Mandatory as per the requirement 11.3	Applicable only if segmentation is in place
Can be done on Application and Network Layer as well	Can be done on Network Layer only as a start point
Done from inside of CDE network	Done from outside of CDE network
Identify ways to exploit vulnerabilities to circumvent or defeat the security features of system components.	Validate any segmentation and scope-reduction controls

ControlCase
Compliance as a Service

Pre-requisites for segmentation

- Detailed network diagram showing CDE and Non-CDE segments
- Network Zone/VLAN information for CDE and Non-CDE
- Ability to move a source system from one network/VLAN to other in case of multiple Non-CDE segments
- No changes are required w.r.t configuration on the network devices

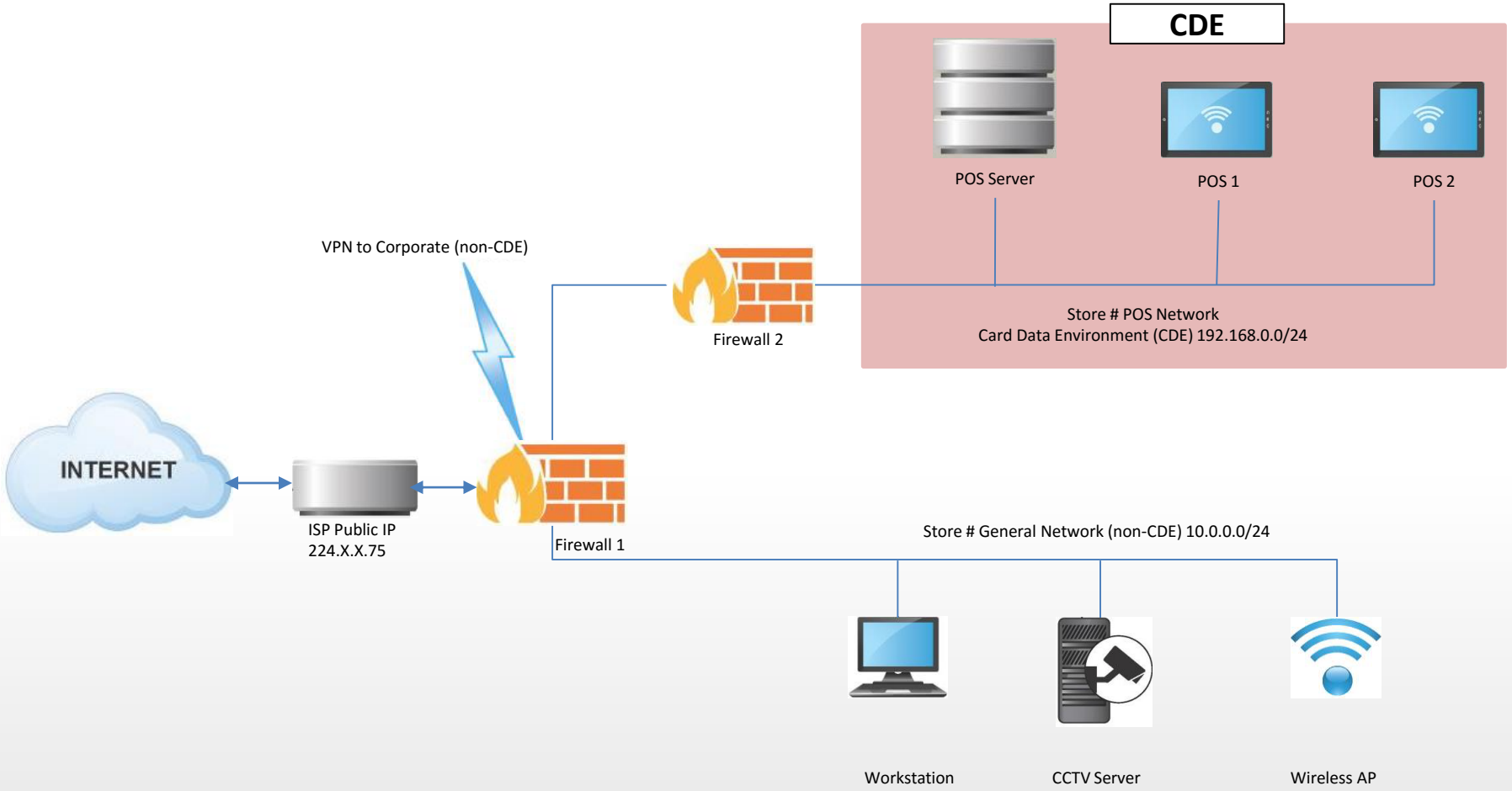
ControlCase
Compliance as a Service

Case Study

For **Retail Merchant**

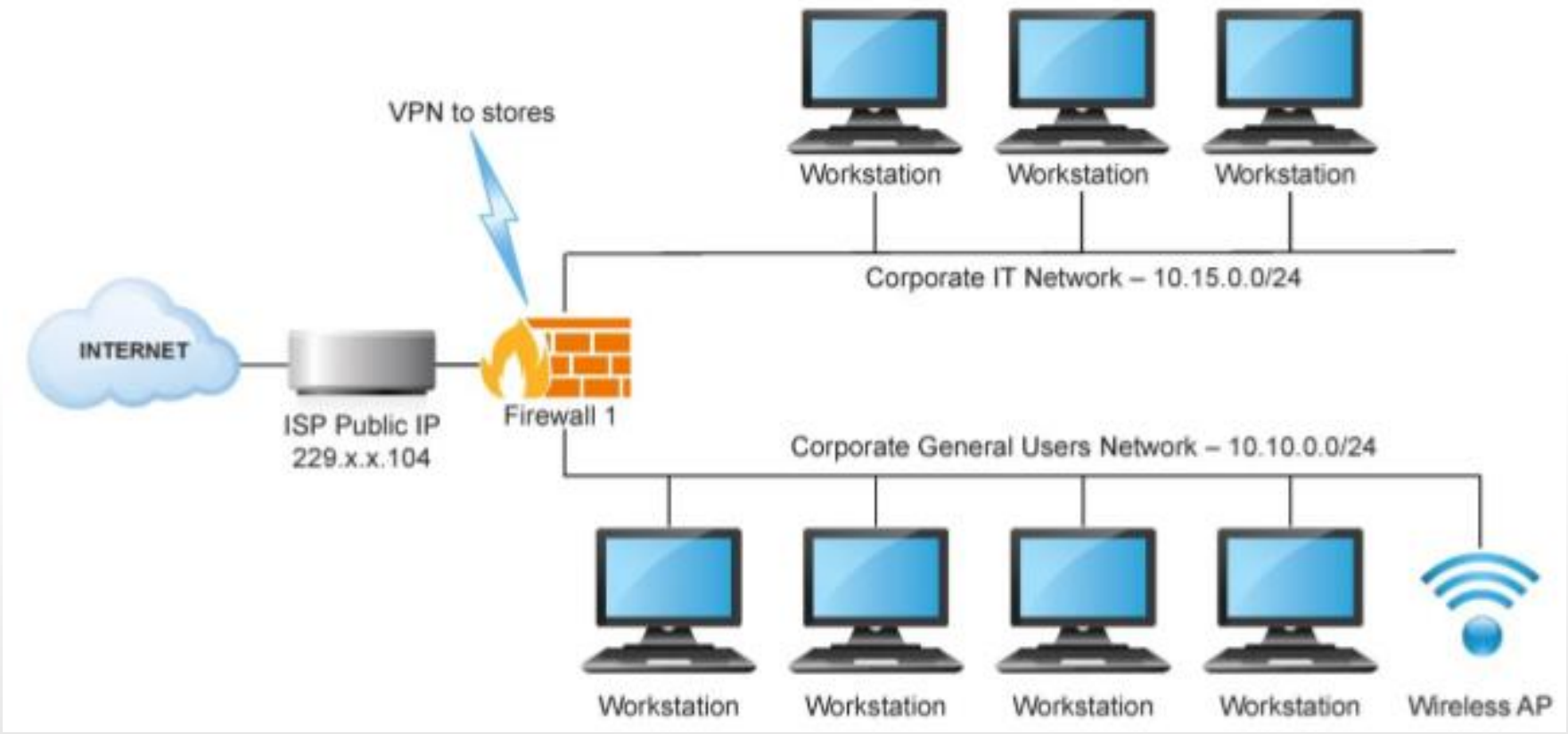
ControlCase
Compliance as a Service

Example Store Network Diagram



ControlCase
Compliance as a Service

Example Corporate Network Diagram



ControlCase
Compliance as a Service

Description of Access

Description of Access

The table below outlines the access from all non-CDE networks into the CDE.

Source Network (Non CDE)	Destination Network (CDE)	Access
Corporate General User Network	Store POS Network	None – Segmented
Corporate IT Management Network	Store POS Network	SSH to POS server
Store General Network	Store POS Network	None – Segmented

The “success criteria” for the penetration test were defined as getting access to the CDE environment and accessing cardholder data.

- Based on the defined scope, the following different attack scenarios can be evaluated:
  - External attacker without knowledge of the environment
  - Internal attacker with no CDE access (guest, contractor, etc.) in the store/corporate general network

ControlCase
Compliance as a Service

Segmentation PT Result

- Segmentation Failed
  - If we note that firewall #2 (CDE firewall) is configured to allow unrestricted access (any ports and services) from the store/corporate General Network (10.0.0.0/24) into the store POS Network (192.168.0.0/24).

- Segmentation Passed
  - If there is no access detected for any of the ports and services from the store General Network (10.0.0.0/24) into the store POS Network (192.168.0.0/24). In short, if the access is as per the table mentioned in earlier slide.

ControlCase
Compliance as a Service

Best Practices to Pass Segmentation PT

- Rule-set review shall be done to verify the rules against the business requirements.
- All unused rules shall be removed
- All ACLs shall be configured in a way that they do not allow access to Non-CDE to CDE and vice versa.
- All changes in network shall be done through change management process only by following Network segmentation policy and procedure.
- If Non-CDE segments have access into the CDE, either the organization needs to restrict that access or a full network-layer penetration test should be performed to characterize the access.

ControlCase
Compliance as a Service

Questions?

Thank you

ControlCase
Compliance as a Service