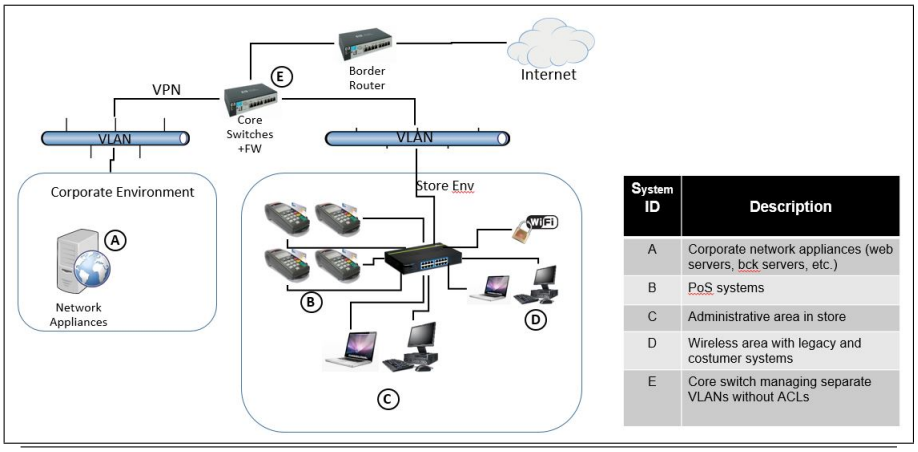
Segmented network

Network Description

Figure 1 describes the scenario which was also complemented by textual description from the book.

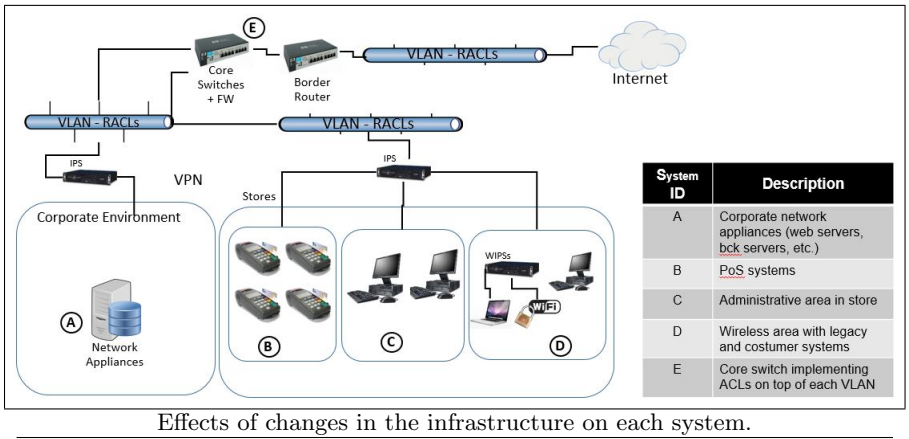


ID	Description
A	Servers systems to attend the requirements of the services of network environment.
B	POS are used by vendors to handle payment for purchases made by customers.
C	PCs that are used by the manager and assistant manager of each store to browse the WEB, check e-mail, and access the order fulfillment screens from the online store.
D	Wi-Fi for use with authenticated users.
E	Managed Ethernet switch to segment the traffic of network.

Fig. 1: Segmented Network – Before Compliance with PCI DSS

"Christines company has recently become a Level 1 merchant, it discovers that its internal assessors have underestimated the scope of PCI due to their flat corporate network. There are legacy system not involved in card processing on its corporate network, and many of those are no longer maintained and cannot meet PCI DSS requirements. There are core switches that run its corporate infrastructure simply due to capacity limitations. The IT staff have several VLANs defined in the core switching infrastructure and they have the ability to place ACLs on some of the switching interfaces or directly on VLANs. The cardholder environment is isolate across ACLs such that her legacy computing systems are not included in the scope of the assessment. The firewall blades will be purchase to boost the security and efficiency of her switching network." [2, p. 77].

Figure 2 describes the scenario which was also complemented by textual description from the book.



Effects of changes in the infrastructure on each system.

ID	Description of changes to meet compliance requirements
A	Access to server systems now controlled by remote ACLs that enforce access mechanisms from other systems in the network. This enforces segmentation.
B	POS are in their own VLAN and segmentation is enforced by the RACLs.
C	The administrative computers are also segmented out thanks to the RACLs on the VLAN.
D	Wi-fi is now logically separate from the wired network. Customers' devices and other systems on the wifi can not access any other system in the network.
E	Managed Ethernet switch creates the VLAN and enforces the RACLs on both.

Fig. 2: Segmented Network – After Compliance with PCI DSS

"After compliance:
The cardholder environment will be segmented form the rest of the core network; IT and Management staff requiring access to those systems (both internally and remotely) are provided two-factor authentication tokens and have VPN software installed on their laptops; Christine creates segmented areas inside her store locations. IT staff to place RACLs in the stores to segment the POS environment from the administrative and wireless areas in the stores; Will introduce additional controls on the wireless network with more stringent RACLs and deploys wireless intrusion prevention system (WIPSs) to further bolster the security around her wireless network; Christine has her security staff review the overall architecture of her network and design additional enclaves to boost the security of the network and increase its overall resistance to worms, viruses, and other malware that propagates via weak network access controls." [2, p. 77].

References

1. CVSS-SIG. Common vulnerability scoring system v3.0: Specification document. Technical report, First.org, 2015.
2. B. R. Williams and A. Chuvakin. *PCI compliance: understand and implement effective PCI data security standard compliance*. Syngress, 2014.