REDSEAL

CDE SEGMENTATION VALIDATION

THE MEASURE OF RESILIENCE

BACKGROUND

PCI 3.0 added a number of significant new requirements for securing cardholder data when compared to the preceding 2.0 standard. One of these new controls relates to validation of segmentation. "Segmentation" refers to the general requirement to isolate the cardholder data environment (CDE) from the rest of the network and unrelated systems.[1]

Previously, there was no requirement to test that segmentation was actually working correctly between annual audits. This is no longer the case, and this new requirement creates a challenge for organizations to implement in a manner that is operationally efficient.

SEGMENTATION VALIDATION

The requirement to validate segmentation appears in section 11.3.4 and is specified as follows:
"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 in-scope systems."

The testing procedures are further clarified in sections 11.3.4a and b, and include the following initial testing step:[2]
"Examine segmentation controls and review penetration-testing methodology to verify that penetration-testing procedures are defined to test all segmentation methods to confirm they are operational and effective, and isolate all out-of-scope systems from in-scope systems."

Furthermore, the Guidance section of 11.3.4 clarifies segmentation to apply to everything outside the CDE:
"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."

As of this writing, a consensus of how exactly to implement a valid control for segmentation validation is still a work in progress. But it is clear that the control needs to be as easy to perform as possible, as it needs to be done every time there's a change to the segmentation systems (for example, after any firewall rule change) and because there may be dozens or hundreds of devices that form the segmentation boundary. Unfortunately, the DSS Guidance for 11.3 states that "Penetration testing is generally a highly manual process", and manual processes do not scale well nor are particularly cost effective. Finally, the procedures and guidance sections make it clear that prior to doing actual penetration testing, there needs to be a systematic review of how and where segmentation is implemented, in order to know where the testing needs to occur. Clearly this approach can be used to scope down the manual effort.

CDE SEGMENTATION VALIDATION

REDSEAL SUPPORT FOR PCI SEGMENTATION VALIDATION

RedSeal was specifically designed to validate segmentation policies such as those required to secure the CDE for PCI DSS. RedSeal leverages network configuration details to map segmentation boundaries, test policies against those boundaries, and conduct multi-depth vulnerability assessments against them.

The following table describes the specific RedSeal capabilities that pertain to implementing PCI DSS 11.3.4 segmentation validation.

FUNCTION	ROLE IN SUPPORTING 11.3.4
PCI zone policy	Defines hosts and subnets within CDE and tests access into CDE. Provides the basis for continuous auditing of segmentation boundary policy. The PCI policy definition is locked down to ensure compliance.
Policy dashboard	Provides "at a glance" view of integrity of segmentation boundary, updated daily.
PCI policy report	Daily segmentation testing: Provides report-based view of any access across segmentation boundary. Null output indicates no boundary degradation.
Tracked query	Provides vulnerability risk report: If access is opened across a segmentation boundary, this report details which CDE vulnerabilities have been exposed and how high the threat is.
Topology inventory	Provides "centralized PCI DSS security and operational processes and controls" as defined in Sampling guidelines (DSS page 15) for auditor to reduce test sample size and therefore cost of compliance.

CONTROL METHODOLOGY

A suggested control activity methodology for segmentation validation would rely on RedSeal as the key control technology, augmented by spot testing using either scanning or manual penetration testing:

1. Any change to firewall rule or router access control list (ACL) on a device that participates in segmentation triggers control activity.
2. Check PCI policy reports for segmentation access violations (unauthorized access across the segmentation boundary).
3. If any access violations are found, check a tracked query report to see if there are any high risk threats exposed by the violations.
4. As a compensating control, periodically conduct vulnerability scans against sample portions of the segmentation boundary to verify boundary integrity consistent with RedSeal reports. Alternatively, more comprehensive penetration testing (e.g. based on NIST 800- 115 recommendations) could be conducted, but the scope should be limited given the primary control.

[1] PCI DSS 3.0, page 10

[2] 11.3.4a

CDE SEGMENTATION VALIDATION

SUMMARY

PCI DSS 3.0 introduced a requirement (11.3.4) to validate segmentation boundaries anytime a change is made to a boundary element. Although this could be a very time consuming task, a control that isn't implemented at all times is not effective. RedSeal was designed to continuously validate network segmentation. By using it as part of a control activity set for segmentation validation, organizations can meet the new requirement as efficiently as possible without compromising the security of cardholder data.