Segmentation, Compensating Controls and P2PE Summary

Segmentation

Reducing PCI Scope

ControlCase
Compliance as a Service

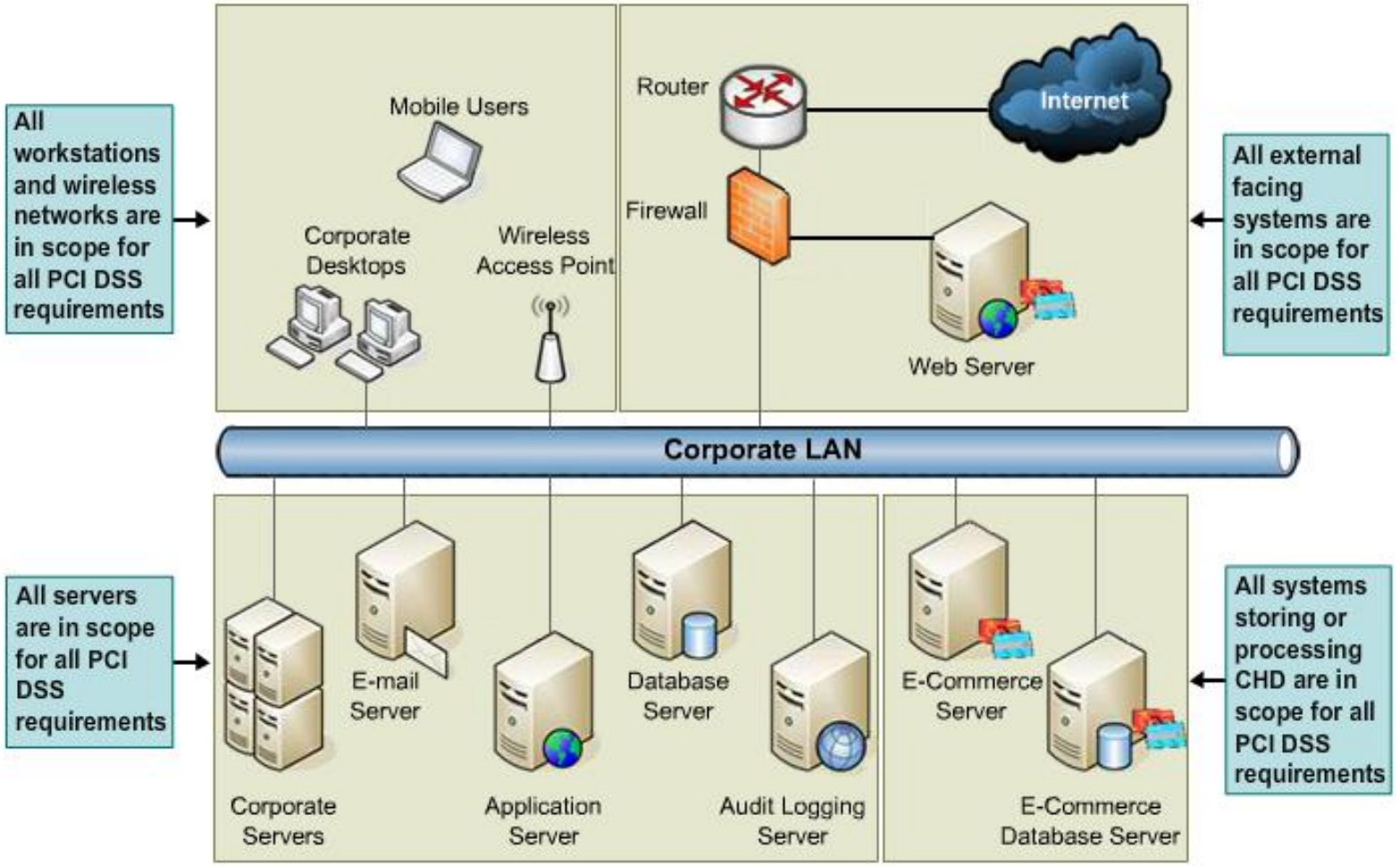
PCI Scoping

Network segments fall into 3 classifications within PCI DSS:

- Networks that store, process and/or transmit CHD
- Networks that do not store, process and/or transmit CHD, but are still in scope (e.g., connected to the CDE or provide management functions to the CDE)
- Networks confirmed to be out of scope

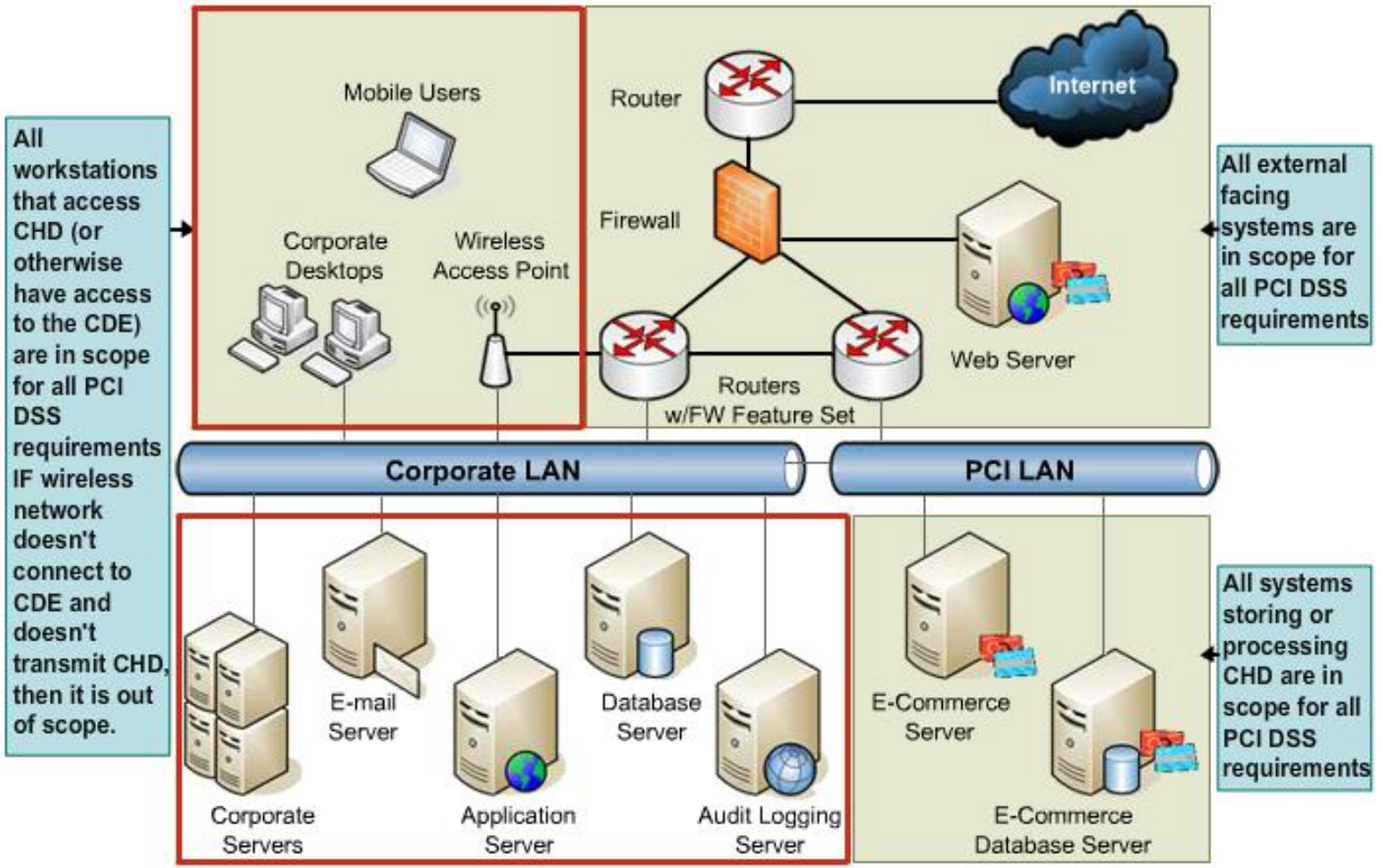
ControlCase
Compliance as a Service

No Segmentation



ControlCase
Compliance as a Service

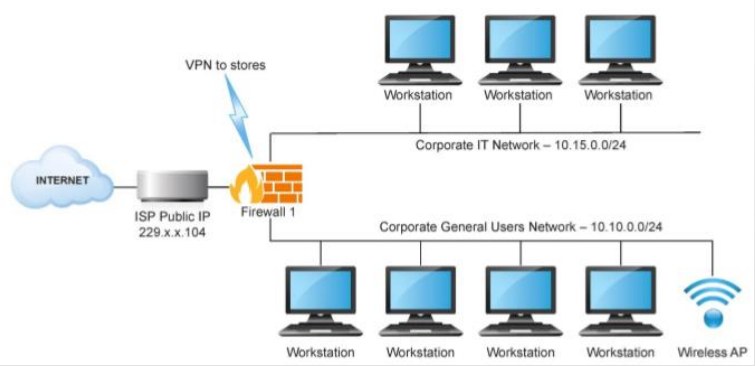
Proper Segmentation



ControlCase
Compliance as a Service

Segmentation Testing

- PCI DSS requires that segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems
- Certification must include review of all segmentation technologies
- Must include penetration testing:
  - against CDE systems from outside CDE
  - against out-of-scope systems within the CDE



ControlCase
Compliance as a Service

Compensating Controls

Above and Beyond

ControlCase
Compliance as a Service

Definition

Compensating Controls may be considered for most PCI DSS requirements when you cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but you have sufficiently mitigated the risk associated with the requirement through implementation of compensating controls.

- All compensating controls cannot already be required by PCI DSS and must be reviewed by your QSA.
- The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the con figuration of the control.
- A particular compensating control will not be effective in all environments.

ControlCase
Compliance as a Service

Misconceptions

- A compensating control accepted for another organization is acceptable in my organization.
- Once validated by a QSA, a compensating control does not need to be reassessed.
- A compensating control can only be used once.
- Compensating controls only cover technical PCI DSS requirements.

ControlCase
Compliance as a Service

Compensating Control Example

- **Constraint** - Organization uses a legacy payment transaction switch which does not support encryption for storage of cardholder data stored in the backend database.

- **Requirement 3.4** - Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs)

- **Identified Risk** – Cardholder data can be compromised since it is stored in clear text format.

ControlCase
Compliance as a Service

Valid Compensating Control

- Ensure the transaction switch database is segmented in a separate segment from other in-scope systems with access control filtering.
- Ensure two factor authentication for access to the database.
- Ensure monthly vulnerability assessment for the database servers.
- Ensure administrative access to the server from limited network segments/systems.

ControlCase
Compliance as a Service

P2PE

Basic Understanding

ControlCase
Compliance as a Service

Definition of Account Data

Account Data consists of cardholder data and/or sensitive authentication data, all information printed on the physical card and data on the magnetic strip and chip.

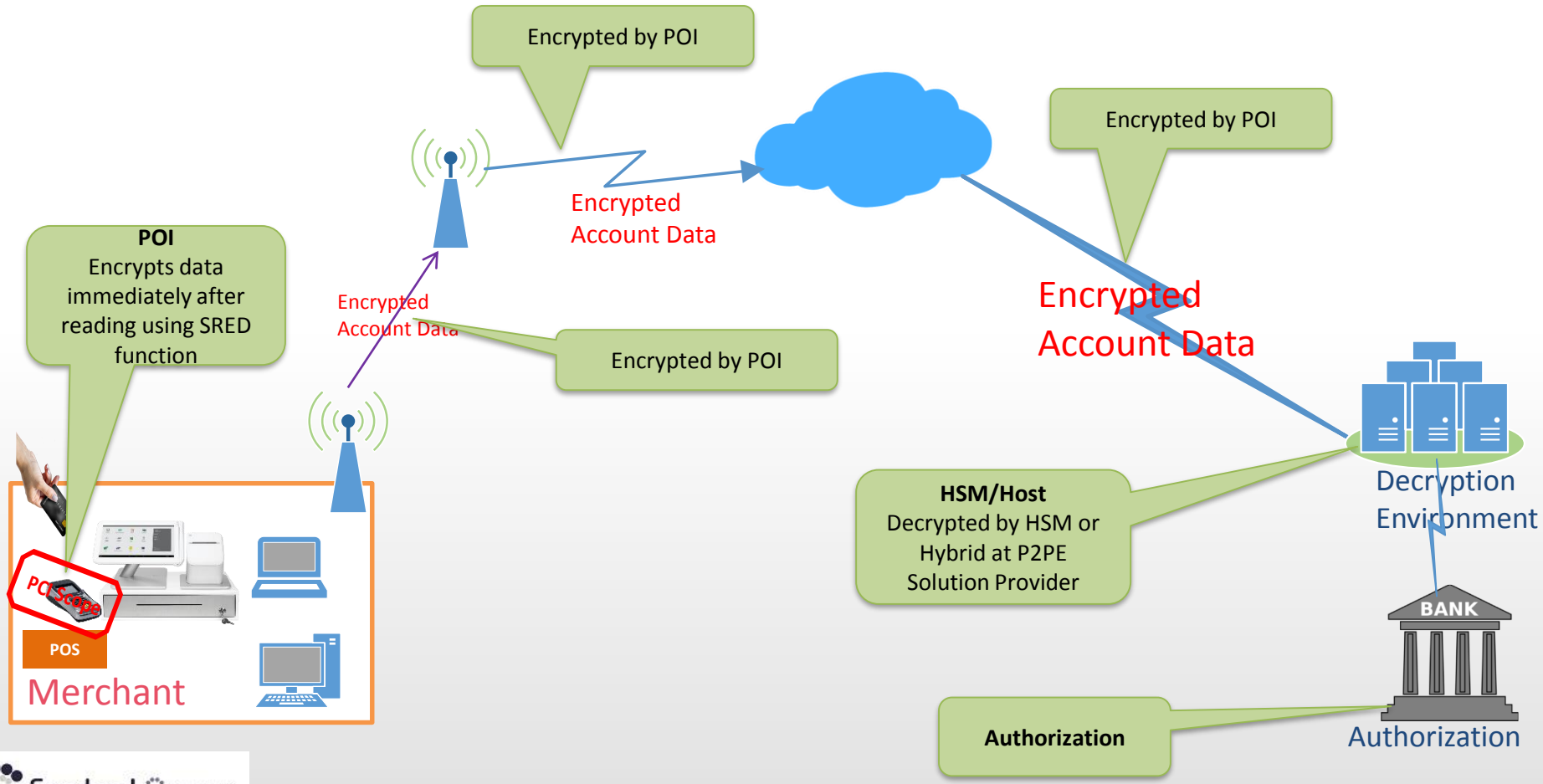
Account Data	
Cardholder Data includes:	**Sensitive Authentication Data includes:**
Primary Account Number (PAN)	Full Magnetic Stripe Data
Cardholder Name	or Equivalent on a Chip
Expiration Date	CAV2/CVC2/CVV2/CID
Service Code	PINs/PIN block

ControlCase
Compliance as a Service

What is P2PE?

- A point-to-point encryption (P2PE) solution cryptographically protects account data from the point where a merchant accepts the payment card to the secure point of decryption.

Payment Method in P2PE



P2PE Solution overview

Typical data-flow:

Benefits of P2PE

- Offers a powerful, flexible solution for all stakeholders
- Makes account data unreadable by unauthorized parties
- Reduces fraud and theft
- Protects customer data and client reputation
- Simplifies compliance with PCI DSS
- Recognized by all Participating Payment Brands

ControlCase
Compliance as a Service

Thank You !

ControlCase
Compliance as a Service