
PCI
Security
Standards Council
What's New For SAQs

Lauren Holloway

Director, Data Security Standards

John Bloomfield

Manager, Data Security Standards

PCI Security Standards Council

What's New for PCI DSS v4.0 SAQs?

PCI Security Standards Council

General Changes for all SAQs

Response* (*Check one response for each requirement*)			
In Place	In Place with CCW	Not Applicable	Not In Place
☐	☐	☐	☐

PCI Security Standards Council

E-commerce Methods

E-commerce Method	SAQ Type for Eligible Merchants	How many PCI DSS v4.0 Requirements
Merchant has no access to own website	SAQ A Fully Outsourced	11
Merchant website redirects customers to a compliant TPSP (e.g., URL redirect)		27
Merchant website includes a compliant TPSP's embedded payment page/form (e.g., iframe)		29

PCI Security Standards Council

E-commerce Methods

E-commerce Method	SAQ Type for Eligible Merchants	How many PCI DSS v4.0 Requirements
Merchant has no access to own website. Merchant website redirects customers to a compliant TPSP	SAQ A	11
Merchant website creates the payment form, and payment data is delivered directly from the consumer browser to the TPSP (often called a "Direct Post")	SAQ A-EP Fully Outsourced..	27
Merchant website includes a compliant TPSP's embedded payment page/form (for example, an iframe).	Fully Outsourced..	139
Merchant website loads or delivers a script(s) that runs in the consumer browser (for example, JavaScript)	Except for the Payment Page	29
All other e-commerce methods and implementations	SAQ D for Merchants	All PCI DSS Requirements

PCI Security Standards Council

SAQ A – Why New Requirements?

- Many SAQ A merchant breaches…
- Requirement for ASV scanning & FAQ 1485
- New v4.0 requirements for payment page protection

PCI Security Standards Council

SAQ A – Why New Requirements?

- Many SAQ A merchant breaches…
- Requirement for ASV scanning & FAQ 1485
- New v4.0 requirements for payment page protection

PCI Security Standards Council

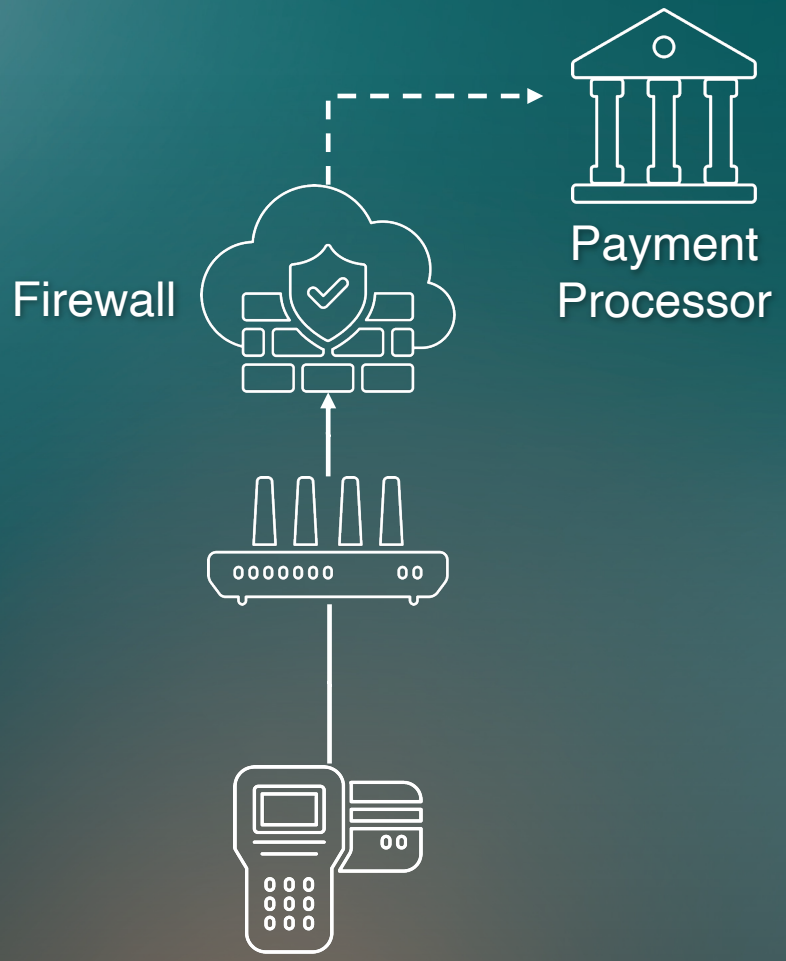
PCI Security Standards Council

SAQ B-IP

For approved PIN Transaction Security (PTS) Point-of-Interaction (POI) devices

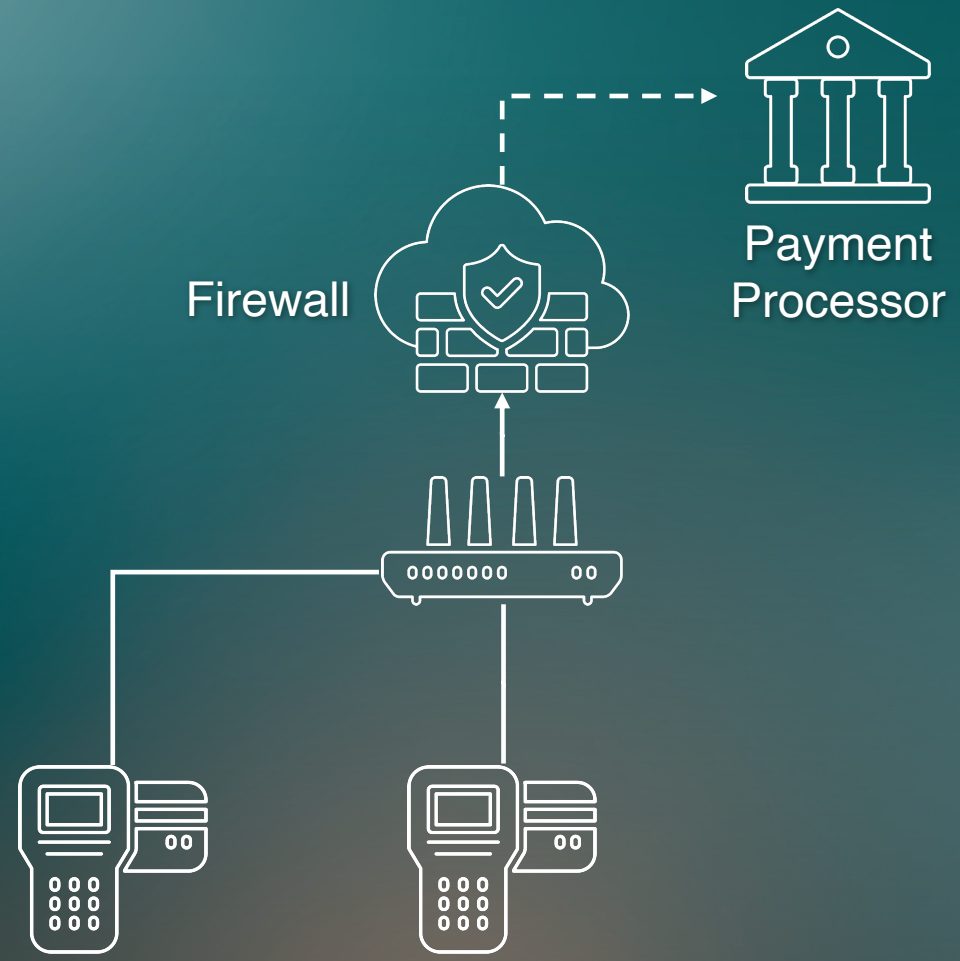
What does “devices are not connected” mean?

Connections Eligible for SAQ B-IP



PCI Security Standards Council

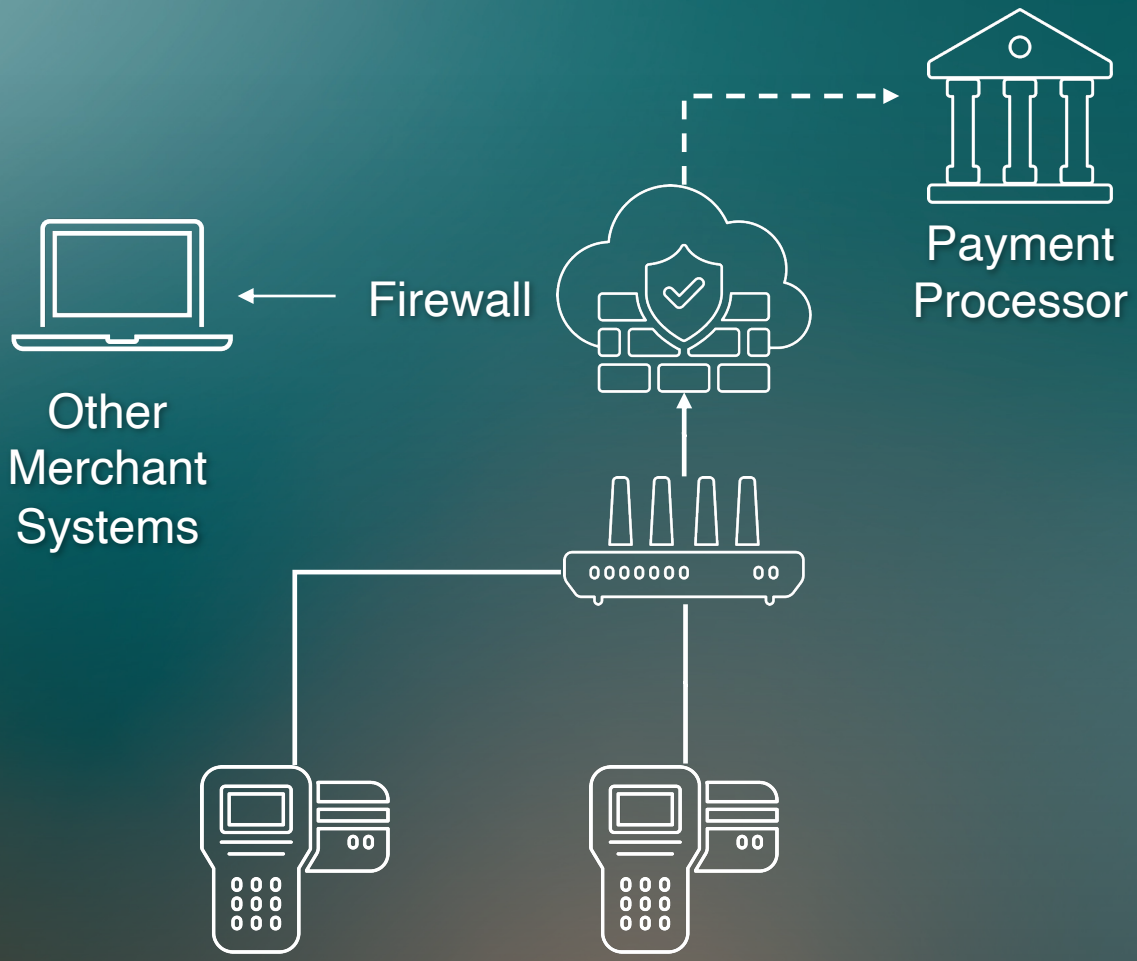
Connections Eligible for SAQ B-IP



Multiple IP-connected PTS-approved POI devices in same network zone

PCI Security Standards Council

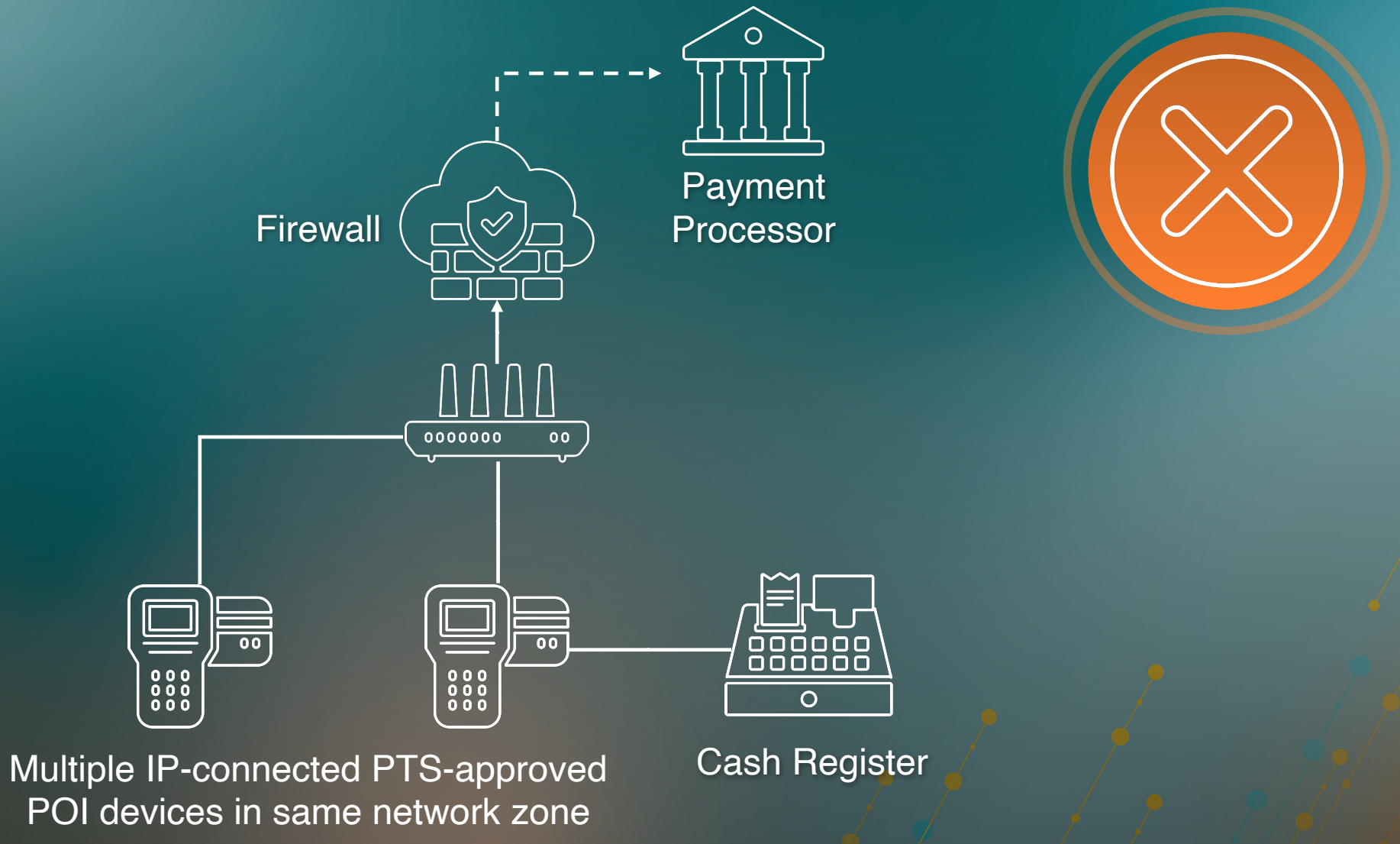
Connections Eligible for SAQ B-IP



Multiple IP-connected PTS-approved
POI devices in same network zone

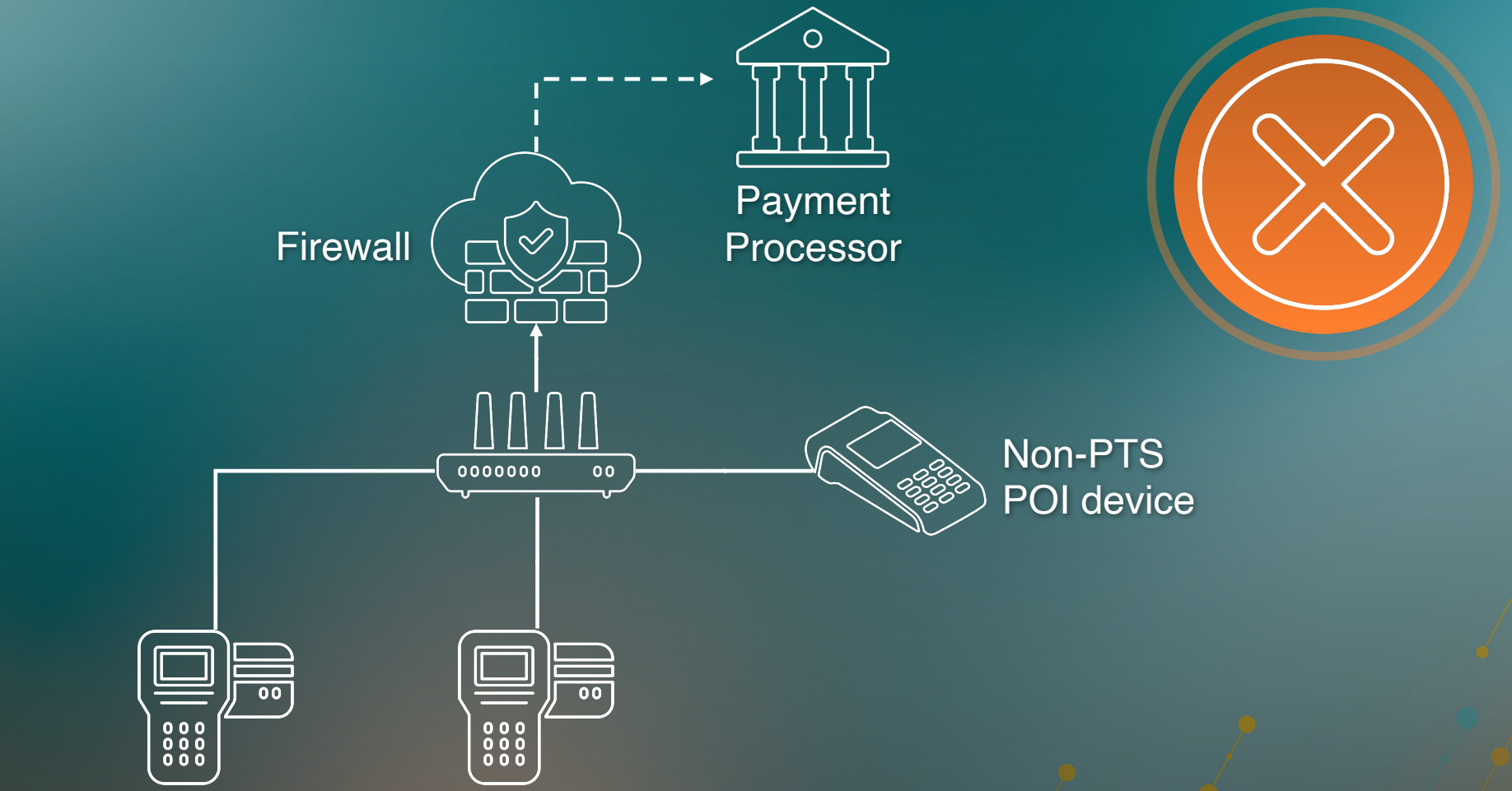
PCI Security Standards Council

Connections Not Eligible for SAQ B-IP



PCI Security Standards Council

Connections Not Eligible for SAQ B-IP



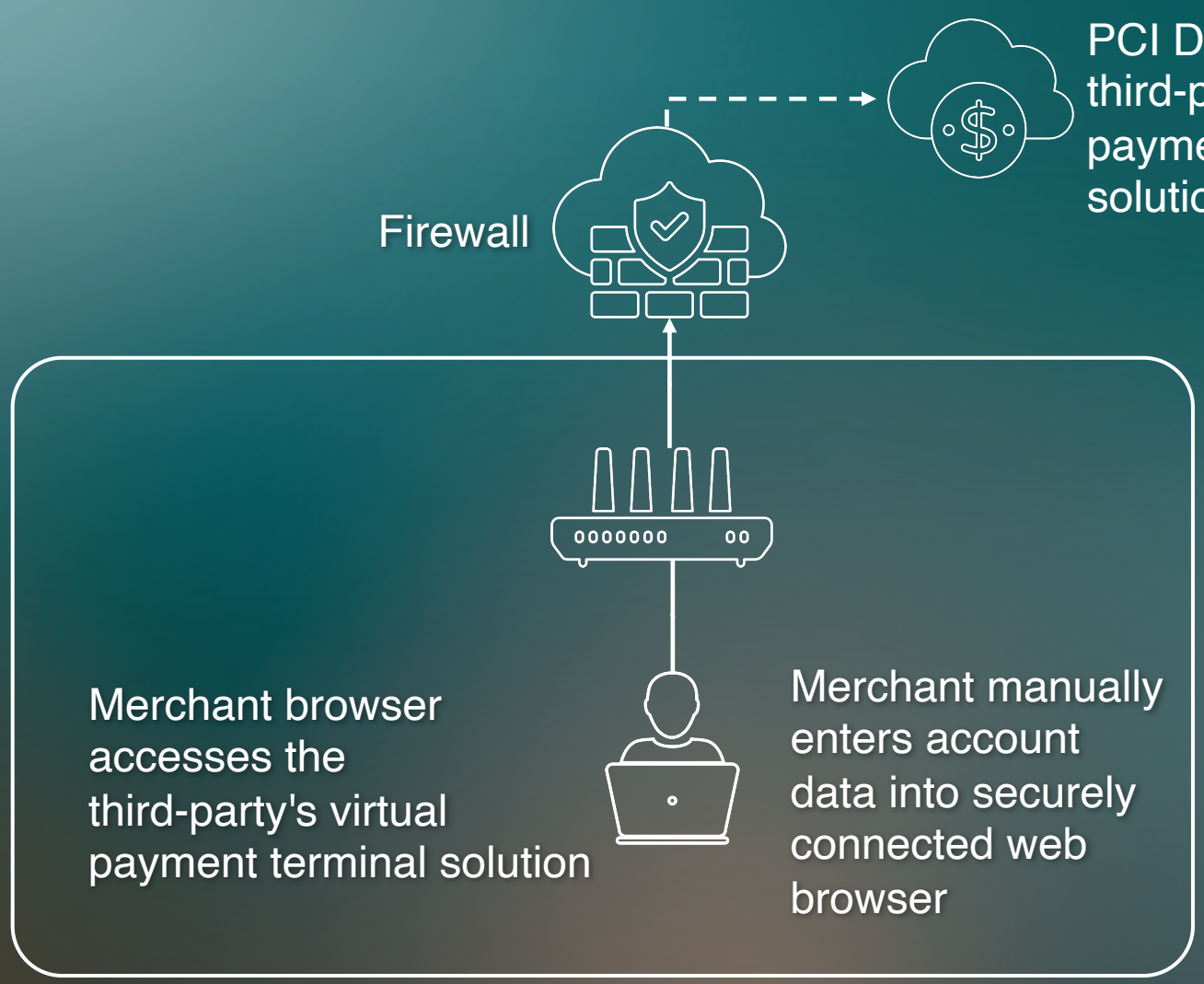
PCI Security Standards Council

PCI Security Standards Council

SAQ C-VT

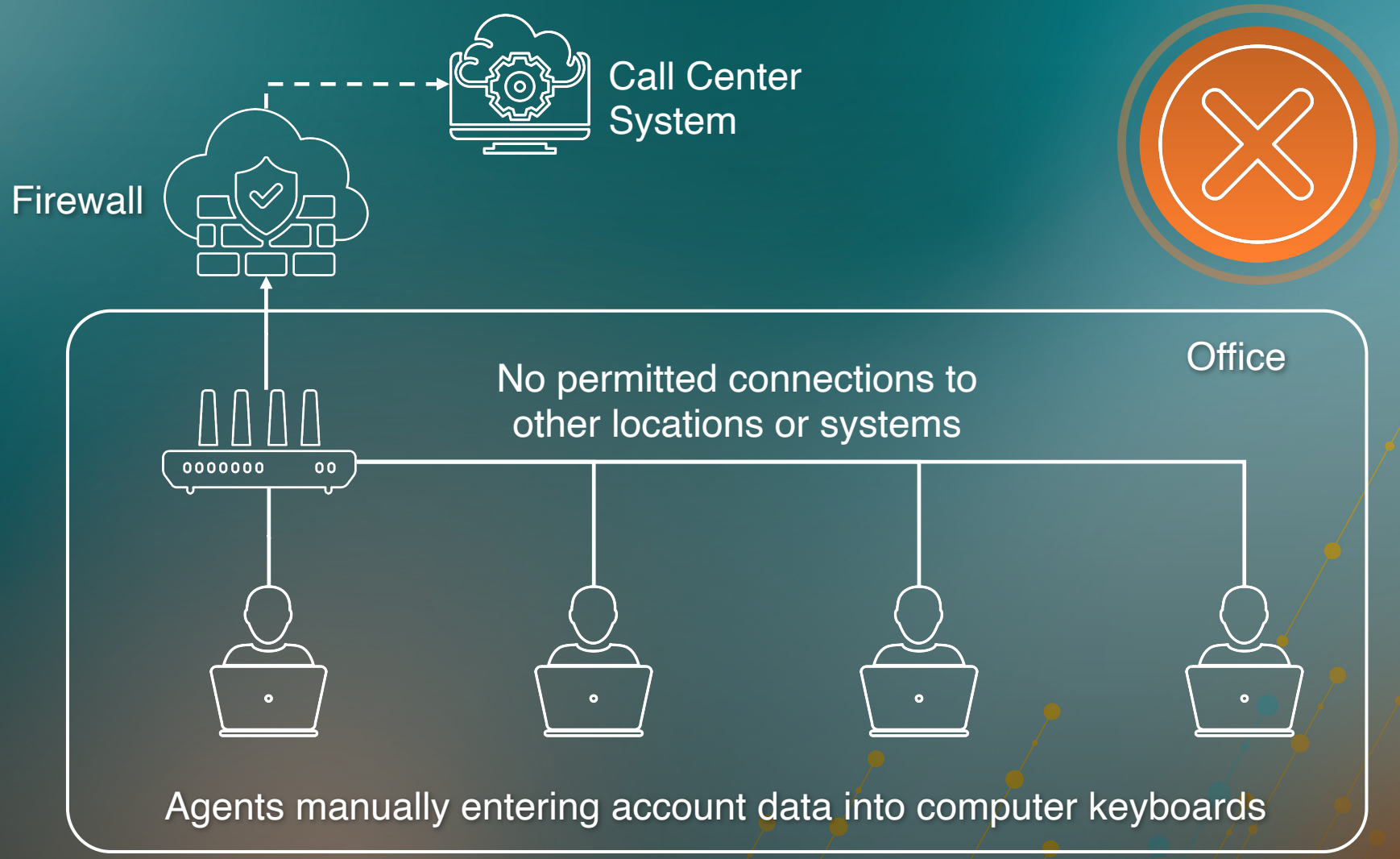
What does “no connections to other locations or systems” mean?

Connections Eligible for SAQ C-VT



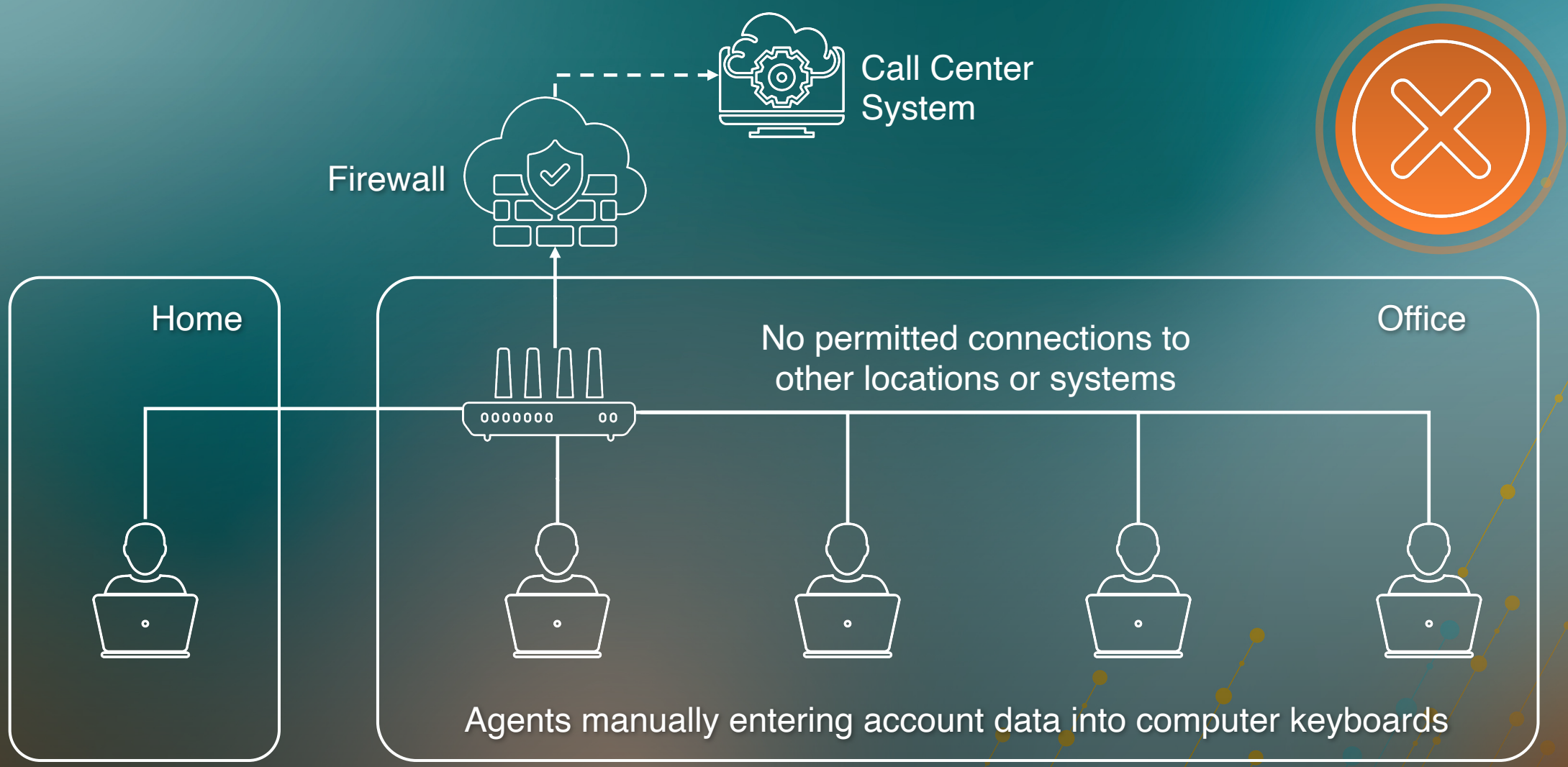
PCI Security Standards Council

Connections Not Eligible for SAQ C-VT



PCI Security Standards Council

Connections Not Eligible for SAQ C-VT



PCI Security Standards Council

Things That Don’t Exist…

SAQ A for Service Providers

PCI Security Standards Council

SAQ D for Service Providers

- The only SAQ for Service Providers
- Statement added to all SAQs

PCI Security Standards Council

SAQ D for Service Providers

- The only SAQ for Service Providers
- Statement added to all SAQs

PCI Security Standards Council

What Changed in SAQ D for Service Providers?

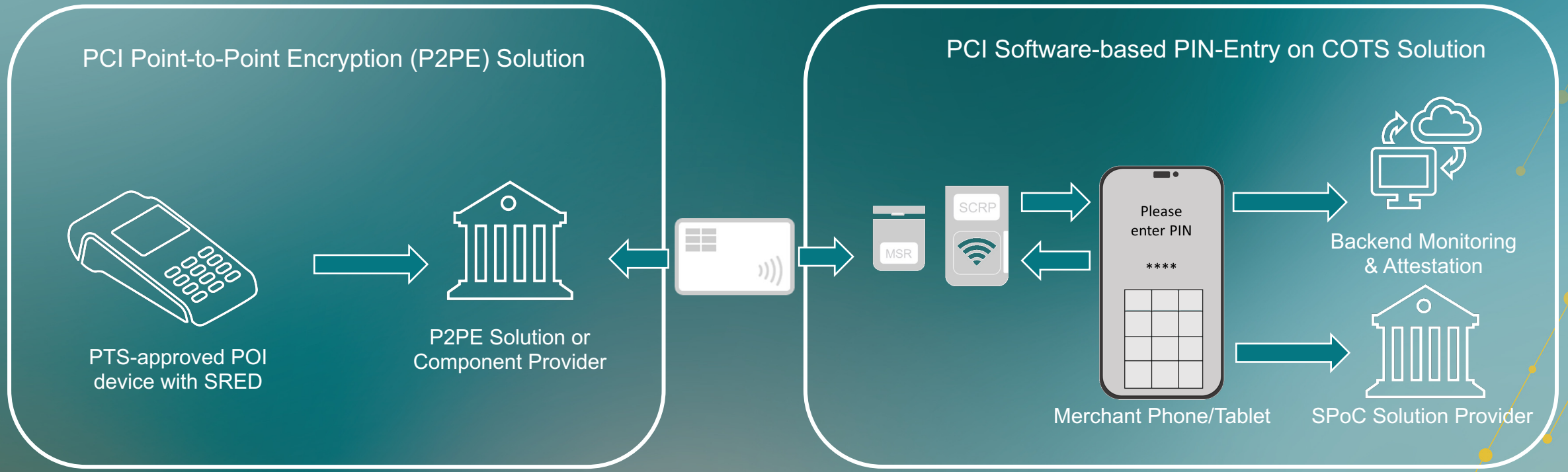
- Higher expectations for entities that provide services on behalf of others
- Additional documentation requirements in v4.0

PCI Security Standards Council

PCI Security Standards Council

SAQ Instructions and Guidelines v4.0 and a New SAQ

Difference Between P2PE and SPoC



PCI P2PE protects payment account data via encryption from the point it is captured in the merchant's payment device until it is decrypted in a P2PE solution or component provider's environment.

PCI SPoC facilitates mobile payment acceptance solutions that enable secure transactions with PIN on a merchant's commercial off-the-shelf (COTS) device (phone or tablet).

PCI Security Standards Council

Future SAQs?

PCI Security Standards Council

PCI Security Standards Council

Thank You!