Network Segmentation Strategy

Moderator Name:

Pramod Deshmane, *ControlCase*

Panelists Names:

Colin McGuire, *Coactive Technology Solutions*
Chet Patel, *Walt Disney Swan & Dolphin Resort*

What is Network Segmentation

- In IT World, Network Segmentation means, logical segregations of systems based on their security levels.

- In PCI DSS world, Network Segmentation is process where you isolate the CDE systems (Systems storing, processing & transmitting the CHD) from Non-CDE systems in order to reduce the scope. To be considered out of scope for PCI DSS, Non-CDE systems must be properly isolated (segmented) from the CDE, such that even if the out-of-scope system component was compromised it could not impact the security of the CDE.

- Key thing to Note: Network Segmentation is not mandatory requirement.

ControlCase

Compliance as a Service

Network Segmentation & Scoping Guidelines

What should be considered in PCI scope?
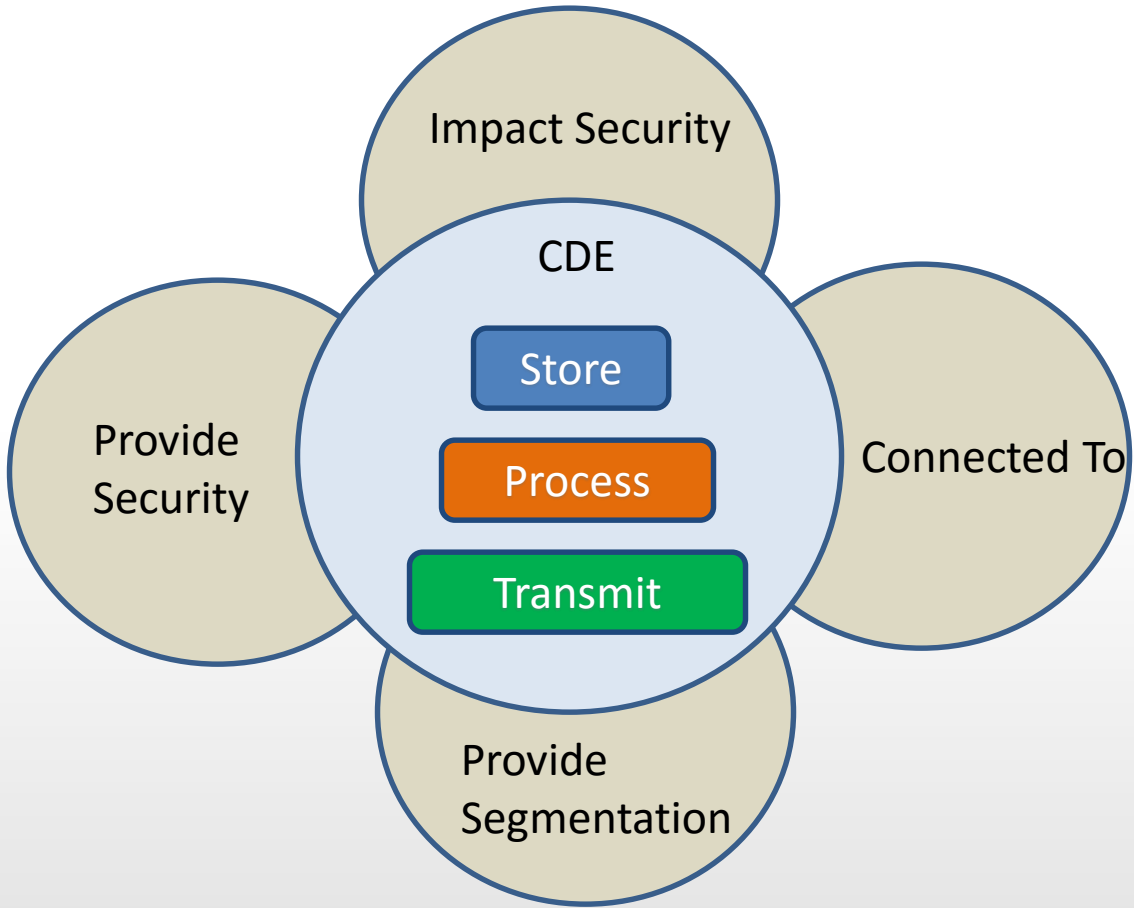
Flat Network Example

Since there is no segmentation done all the Systems will fall in PCI DSS scope

Users

Cardholder Data Servers

Infrastructure support servers

Non-cardholder data Servers

ControlCase
Compliance as a Service
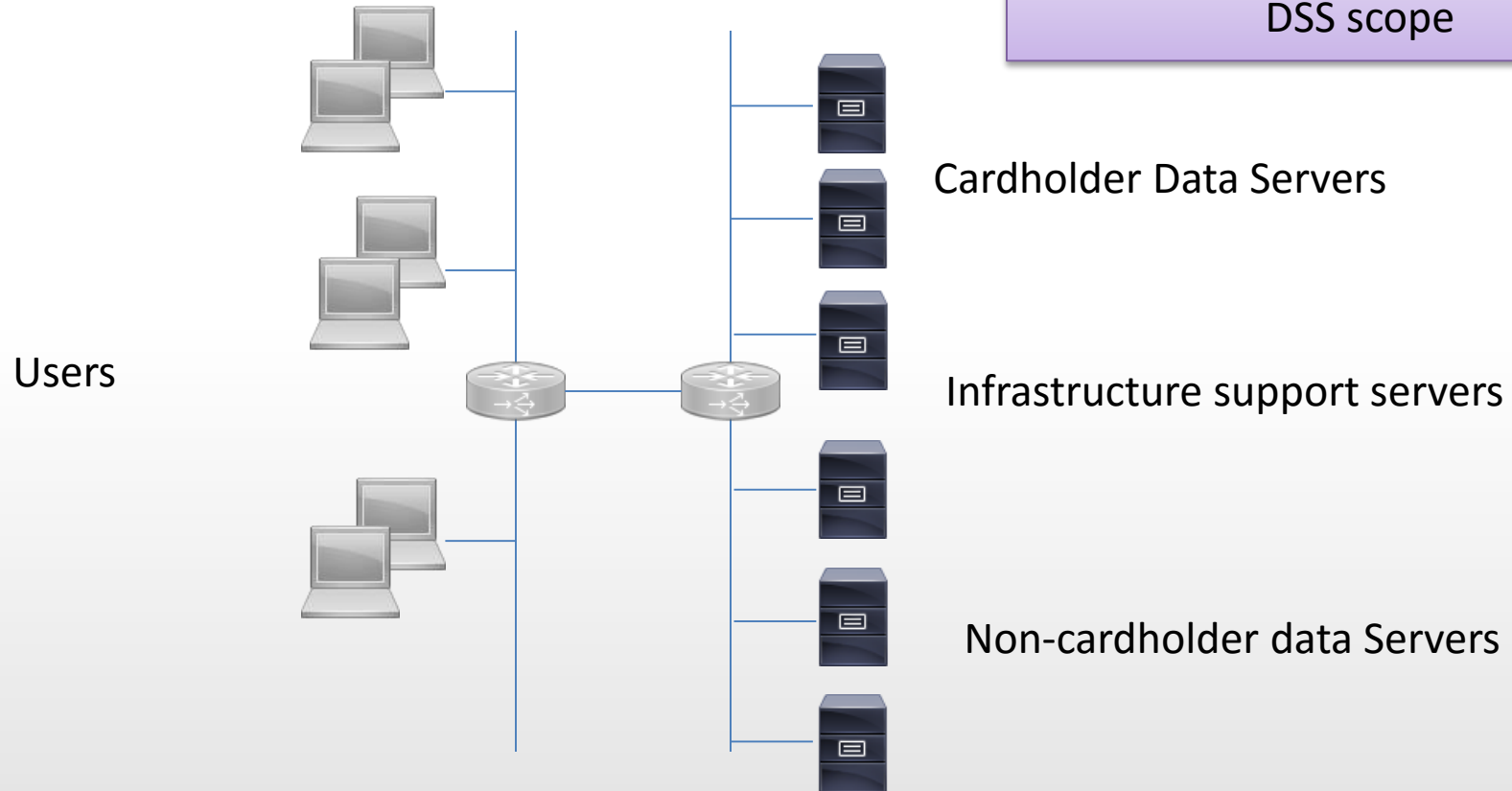
Segmented Network Example

Finance Users

Other Users

Firewall/Core Switch

Cardholder Data Servers

Infrastructure Support servers

Non-Cardholder data Servers
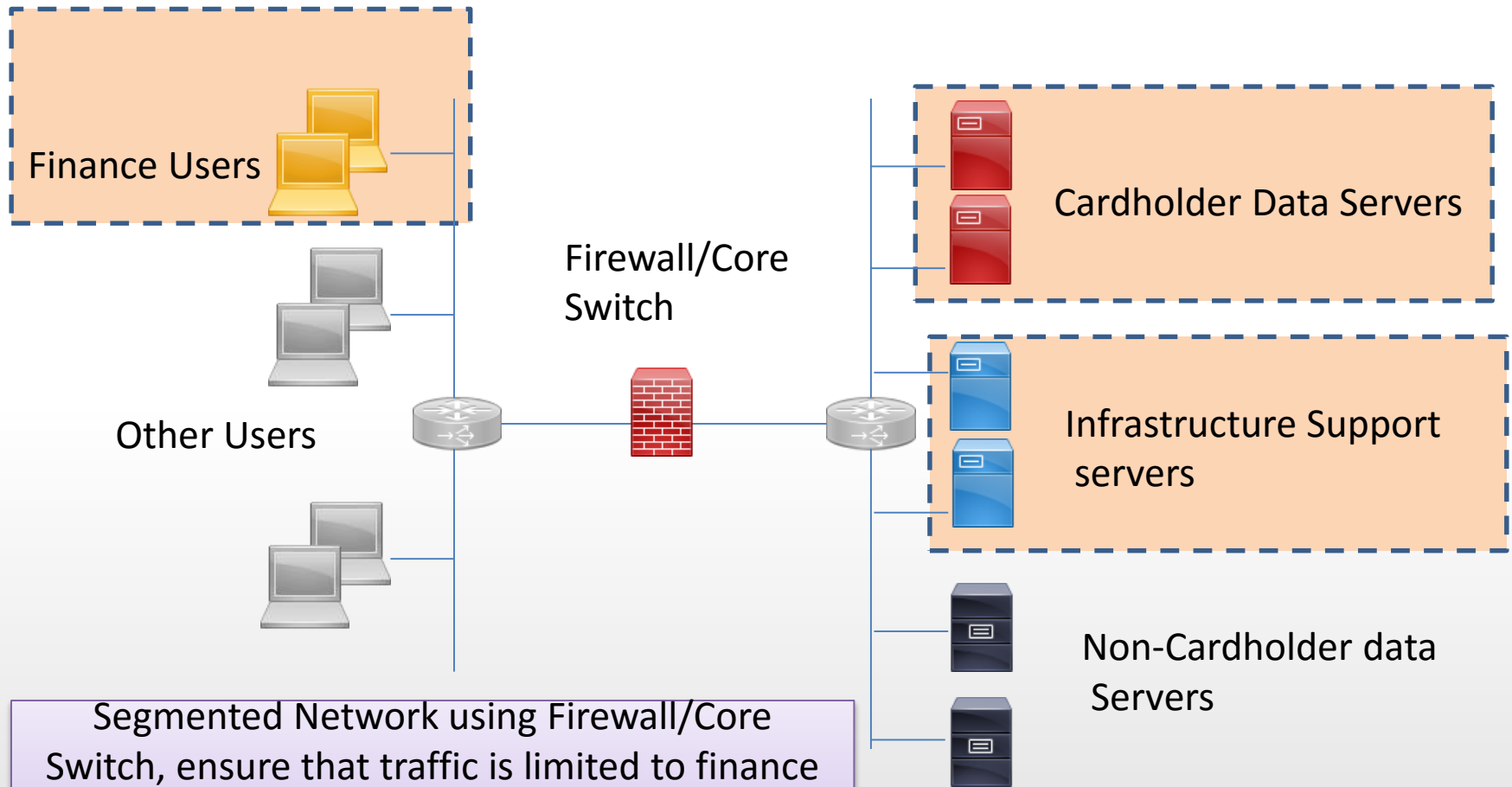
Segmented Network using Firewall/Core Switch, ensure that traffic is limited to finance users and scope is reduces to only finance users, Cardholder data servers and infrastructure support servers

ControlCase
Compliance as a Service

Questions and Answers