Network Design and Emulation for a PCI-DSS Compliant Hadoop Cluster Infrastructure

Daniel Obi-Nwosu

0253187

COMM-1000 Technical Communications

Computer Networking Technology Program

Network Design and Emulation for a PCI-DSS Compliant Hadoop Cluster Infrastructure

Prepared by

Daniel Obi-Nwosu

0253187

Technical Communications

Computer Networking Technology Program

Holland College

April 10, 2025

Prepared for

Prosper Habada/ Robert Nicholson

Holland College

Executive Summary

The network architecture developed for Dancorp Analytics—a fintech company working with sensitive payment card data—provides a secure, scalable, and resilient foundation aligned with the requirements of PCI DSS version 4.0.1. It safeguards cardholder data while enabling advanced computing and analytics capabilities.

At its core, the infrastructure is built to support virtualized computing environment built on virtual and physical host computers, allowing flexible deployment of analytics workloads. High availability is ensured through clustering and failover mechanisms that maintain service continuity. The design incorporates multiple layers of network security, including firewalls, encrypted tunnels via Internet Protocol Security (IPSec), and defined routing protocols. Access to critical systems is tightly controlled through segmentation and dedicated zones for administration, monitoring, and compliance.

Key components were tested using Cisco Modelling Labs, validating the design's effectiveness within a simulated environment. Overall, this architecture ensures compliance, operational efficiency, and scalability to support Dancorp’s long-term growth.

List of Illustrations

Table of Contents

1.0 Introduction

1.1 Purpose

This report presents the architectural design of a secure, scalable, and resilient enterprise network tailored for Dancorp Analytics, a fintech organization engaged in the analysis of data containing sensitive payment card information. The network infrastructure is meticulously engineered to comply with the stringent requirements of the Payment Card Industry Data Security Standard (PCI DSS), as established by the Payment Card Industry Security Standards Council (PCI SSC). These standards offer a comprehensive baseline of technical and operational security measures to protect account data and reduce the risk of compromise (PCI SSC, 2024, p. 1).

Designed to support both the firm's current operational demands and anticipated future expansion, the network architecture promotes high availability for its Hadoop-based computing infrastructure, facilitates virtual machine mobility, and ensures secure interoperability with client systems and cloud service providers.

1.2 Background

As the fintech sector evolves, organisations handling electronic payment data are under growing pressure to implement secure, scalable infrastructures that not only meet regulatory compliance but also support data-driven services. Data analytics, central to such operations, involves extracting meaningful insights using mathematical, statistical, and computational techniques (Kte'pi, 2024).

Dancorp Analytics, acting as a service provider to fintech clients, processes significant volumes of data that fall within the scope of PCI compliance, with the goal of deriving actionable insights to support strategic decision-making and enhance operational performance for it clients. This function demands a robust infrastructure capable of balancing analytical efficiency with strict data protection requirements. To this end, the network design is aligned with the principles outlined in two publicly available and industry-recognised resources: the PCI DSS Scoping and Segmentation Guidance for Modern Network Architectures and the Payment Card Industry Data Security Standard (PCI DSS) v4.0.1: Requirements and Testing Procedures. These documents, published by the PCI Security Standards Council (PCI SSC), provide essential guidance for securing payment environments.

1.3 Scope

The network's computing layer is built on a high-performance spine-leaf topology, enabling low-latency, high-bandwidth communication, virtual machine mobility, and scalability. It supports real-time Hadoop analytics while maintaining segmentation and routing in line with PCI DSS requirements.

In accordance with PCI DSS guidance, the design will clearly separate the Cardholder Data Environment (CDE) from non-CDE systems through logical network segmentation and access controls. This approach minimises the PCI DSS scope, limits exposure, and secures all interactions between the CDE and external systems, ensuring that only authorised and controlled communication paths are permitted. The PCI DSS-scoped segment for this design has Cisco's Nexus Operating System (NX-OS) as the corner stone of its operations, selected for its advanced data centre capabilities, including east-west traffic optimisation, VM clustering, failover, application mobility, and both internal and client traffic isolation. With support for Virtual Extensible Local Area Network (VXLAN) and Border Gateway Protocol Ethernet Virtual Private Network (BGP EVPN), NX-OS and the Nexus 9000 platform are well-suited for secure, segmented, high-speed switching in scalable environments (Cisco, 2024).

The design also leverages PCI DSS's scope reduction flexibility, which permits the exclusion of components that cannot be securely managed, or the adoption of customised approaches—such as engaging a third-party service provider—to effectively meet specific control objectives. As Louthan (2024) explains, systems may be omitted when they present risk or complexity. In line with this principle, Dancorp excludes wireless infrastructure from its Cardholder Data Environment (CDE), as its inclusion would introduce unnecessary security overhead and operational risk without justified business value. The PCI DSS documentation advises entities to carefully evaluate the use of wireless technology due to its increased risk and difficulty in securing, even recommending limiting its use to non-sensitive data transmission where possible (PCI SSC, 2024, p. 14). Similarly, data at rest is excluded from the Cardholder Data Environment (CDE), with sensitive information streamed in real time to a simulated Azure endpoint. According to PCI DSS guidance, organisations may use third-party service providers to store encrypted data (PCI SSC, 2024, p. 15).

Due to the limitations of Cisco Modelling Labs (CML) Personal Edition—specifically the 20 virtual machine (VM) cap and host system resource constraints (Cisco, 2025)—the simulation

was scaled down accordingly. Although full enterprise modelling for this project would ideally require up to 45 VMs, the focus was placed on essential infrastructure components such as routers, switches, servers, and firewalls. These were emulated using Cisco virtual appliances to facilitate testing of secure traffic handling, with the design restricted to the 20-VM limit.

Dedicated network segments were provisioned to represent key support services, including Microsoft Active Directory, Lightweight Directory Access Protocol (LDAP), Security Information and Event Management (SIEM), Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access-Control System Plus (TACACS+), and Intrusion Detection and Prevention Systems (IDS/IPS). However, these services were not fully deployed, as the emulation environment lacks the capacity to support such resource-intensive applications. Instead, their network environments were created and segmented to reflect their intended placement in a production setting, enabling validation of routing, access control, and service integration without running the actual applications.

1.4 Methodology

Research for this study was conducted using Google Scholar, academic databases, and library resources from institutions offering networking and security programmes. Sources included textbooks, peer-reviewed papers, industry white papers, Original Equipment Manufacturer (OEM) documentation, standards documentation, and technical manuals. The Holland College library provided key academic support. Practical configuration skills were developed through online courses and tutorials from platforms like YouTube and LinkedIn Learning.

2.0 PCI DSS-Compliant Computing Cluster for Hadoop Infrastructure

2.1 Payment Card Industry Data Security Standard (PCI DSS)

Established in 2006 by the Payment Card Industry Security Standards Council (PCI SSC)—a collaborative effort by Visa, MasterCard, American Express, Discover, and JCB International—the Payment Card Industry Data Security Standard (PCI DSS) unified various card-brand security standards into a single, globally recognised framework. Regular updates reflect changes in technology and emerging threats, continually enhancing global payment security. The current version, formally titled Payment Card Industry Data Security Standard: Requirements and Testing Procedures, Version 4.0.1, is structured around twelve high-level requirements grouped into six control objectives, which together balance strategic intent with tactical implementation (PCI SSC, 2024, p. 1).

The first control objective—build and maintain secure systems and networks—is foundational to the protection of the Cardholder Data Environment (CDE) and is composed of two critical requirements. Requirement 1 mandates the installation and ongoing maintenance of Network Security Controls (NSCs), which serve as enforcement points for regulating traffic between different network segments. These controls—such as firewalls, routers, packet filters, deep packet inspection tools, and routing protocols—are used to monitor and control both incoming (ingress) and outgoing (egress) network traffic based on pre-defined policies. NSCs are strategically positioned between areas of differing trust or sensitivity and are essential for ensuring only authorised communications are permitted. Modern implementations may leverage virtualised network or compute environments, software-defined networking, or cloud-based technologies, in addition to traditional physical devices (PCI SSC, 2024, pp. 38-60). Requirement 2 complements this by ensuring the secure configuration of all system components. This entails the removal or disabling of default settings, unnecessary services, unused accounts, protocols, and open ports—elements commonly exploited by attackers. All systems, including operating systems, applications, databases, and network devices, must follow industry-accepted hardening standards (PCI SSC, 2024, pp. 61–73). Entities are required to define and apply secure configuration standards across all systems, using automated tools or manual reviews to ensure compliance. These practices may be guided by the National Institute of Standards and Technology Secure Software Development Framework (NIST SSDF) and the Defense Information Systems Agency Security Technical

Implementation Guides (DISA STIGs), both of which provide robust guidance that supports some of the core objectives related to PCI DSS (Malone, 2020).

The second control objective, protect account data, is addressed through Requirements 3 and 4, which focus on safeguarding sensitive information at rest and during transmission. Requirement 3 mandates the protection of stored account data—primarily the Primary Account Number (PAN)—through strong encryption, truncation, masking, or tokenization. The goal is to ensure that even if unauthorized access occurs, the data remains unreadable and unusable. For instance, full track data, card verification codes, and PIN blocks are explicitly prohibited from being stored after authorization, regardless of encryption (PCI SSC, 2024, pp. 74–93). Organizations are expected to apply key management controls and restrict access to encryption keys to minimize risk. Requirement 4 complements this by ensuring that cardholder data is protected with strong cryptographic protocols, for instance the use of Transport Layer Security (TLS) or Internet Protocol Security (IPSec) protocols during transmission over open or public networks. This prevents interception, tampering, or replay attacks that could compromise data integrity or confidentiality. Entities must identify all communication channels through which sensitive data travels—such as internet, wireless, or third-party links—and apply the necessary encryption mechanisms to secure those paths (PCI SSC, 2024, pp. 94–118).

The third control objective, maintain a vulnerability management program, is realized through Requirements 5 and 6. Requirement 5 emphasizes the importance of protecting systems and networks from malicious software. This includes deploying anti-malware solutions on all systems commonly affected by viruses and configuring them to automatically update and perform regular cyber security scans. Organizations must also document their approach to detecting and responding to malware, including in non-traditional environments such as cloud, containers, or custom applications (PCI SSC, 2024, pp. 119–133). Requirement 6 focuses on ensuring the secure development and maintenance of applications and systems. It requires organizations to establish and follow secure coding practices, conduct code reviews, and apply software patches in a timely manner. Regular vulnerability scans and risk assessments are also part of this process, and bespoke or custom software must adhere to secure development lifecycles. Features such as file integrity monitoring and logging must also be provisioned for to detect unauthorised changes or anomalies early (PCI SSC, 2024, pp. 134–160).

For fourth control objective, implement strong access control measures, is addressed through Requirements 7, 8, and 9, which together cover both logical and physical access control

mechanisms. Requirement 7 ensures that access to system components and cardholder data is limited strictly to individuals whose job roles require it—commonly known as the principle of least privilege—fulfilling the authorization component of AAA (Authentication, Authorization, and Accounting). Requirement 8 mandates the implementation of strong authentication methods to verify each user's identity before granting access. This includes the use of unique user IDs, secure passwords, multifactor authentication, and session management practices, directly satisfying the authentication requirement. Requirement 9 complements these controls by enforcing physical security to protect systems and data from unauthorized physical access. This may include the use of surveillance systems, badge access, visitor logs, and restricted access zones. The fourth control objective supports full implementation of the AAA model—Authentication, Authorization, and Accounting—by verifying user identities, restricting access based on roles, and enabling audit trails. These layered controls ensure that only authorized individuals can access sensitive systems, helping to reduce risk and protect the confidentiality, integrity, and availability of the CDE (PCI SSC, 2024, pp. 161-235).

The fifth objective—regularly monitor and test networks—includes Requirements 10 and 11, which mandate continuous logging, monitoring, and periodic security testing. Requirement 10 ensures that access to system components and cardholder data is logged and auditable, while Requirement 11 necessitates frequent vulnerability scanning, penetration testing, and detection of unauthorized wireless access points. Together, these controls create an adaptive security posture that is essential in detecting and responding to evolving threats (PCI SSC, 2024, pp. 236-289).

The final objective—maintain an information security policy—is encapsulated in Requirement 12, which demands a formalized, organization-wide information security policy and supporting governance mechanisms. This includes assigning roles, conducting risk assessments, and maintaining documentation on PCI DSS scope and segmentation strategies. Requirement 12 reinforces the principle that security is not just a technical discipline but also a governance and cultural imperative (PCI SSC, 2024, pp. 290-333).

PCI DSS outlines a set of security requirements that organisations must follow, each accompanied by specific validation checks to ensure proper implementation. The framework combines clear guidance with flexibility, allowing organisations to tailor controls to their specific environments. However, this flexibility is limited in certain areas—Requirement 3, for example, mandates strict methods for protecting stored cardholder data, leaving little room for alternative approaches (PCI SSC, 2024, pp. 74–75).

2.2 Cluster Computing and Hadoop-Based Analytics Infrastructure

A Hadoop cluster is a distributed computing system that relies on multiple interconnected machines to work together as a unified platform for large-scale data storage and processing. At the physical layer, this architecture consists of standard off-the-shelf servers—also known as commodity hardware—that are typically mounted in data center racks. Each rack accommodates several of these server nodes, and the entire system is organized into multiple racks to allow for fault isolation and horizontal expansion (HandsonERP, 2014).

A typical Hadoop cluster comprises one or more master nodes (see Figure 1), which oversee task coordination and metadata management, alongside multiple slave nodes responsible for data storage and computational execution. These components are physically deployed on computing host servers within a rack-based infrastructure, requiring careful consideration of power, cooling, and spatial provisioning to ensure optimal performance, scalability, and operational reliability.

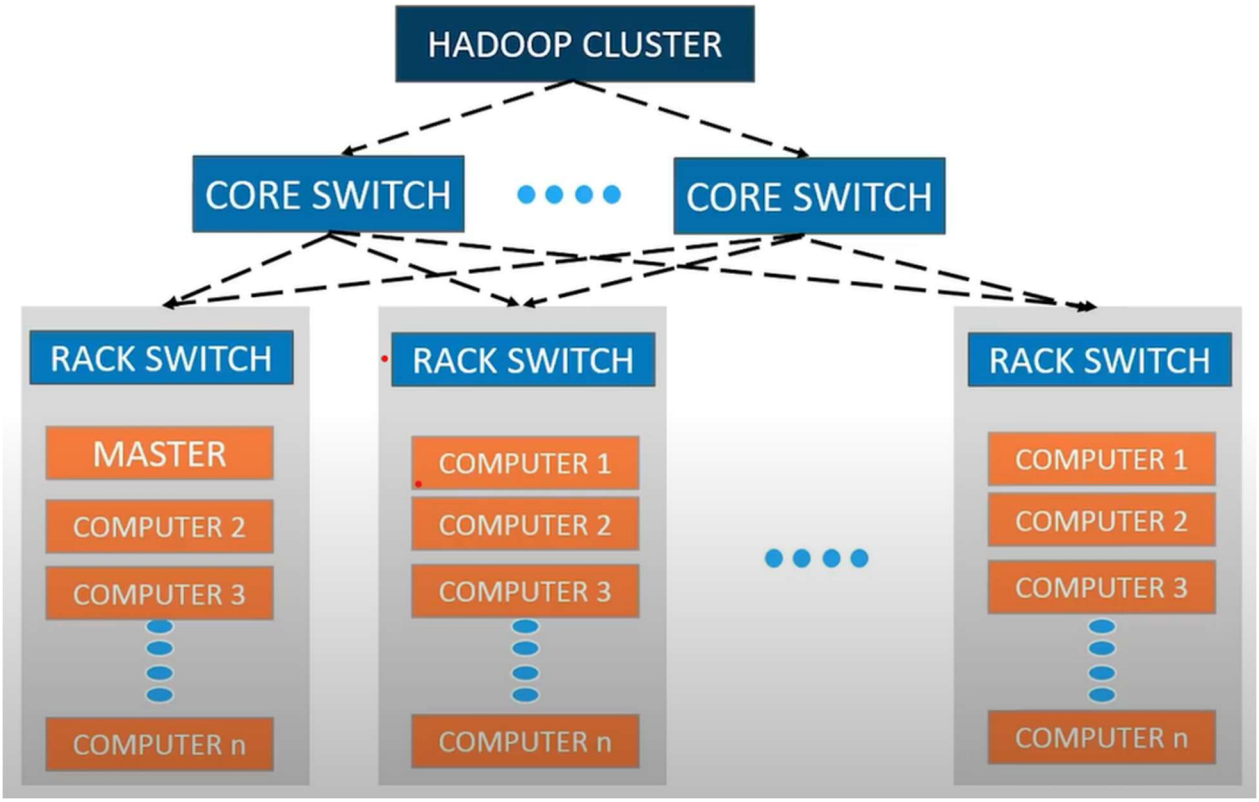

Figure 1- Hadoop Cluster Architecture

The master and slave nodes are connected using high-speed networking infrastructure, such as core and top-of-rack switches, to support low-latency communication and high throughput.

Rack interconnects play a critical role in ensuring east-west data flow and handling traffic between nodes across the cluster (Edureka, 2020).

High availability in such infrastructure is achieved through replicated computing redundancy and rack-aware placement, ensuring fault tolerance even in the presence of application, hardware, or rack-level failures. A rack-aware architecture, functions in a way that ensures data computing replicas are distributed across different racks rather than being confined to a single failure domain. This design mitigates the risk of data loss or service interruption if an entire rack becomes unavailable (Venkataramanachary, Reveron, & Shi, 2020).

Hadoop uses this rack awareness algorithm to distribute data computing replicas across nodes in different racks. For example, the first replica of a data block is stored on a local rack, while subsequent replicas are placed on different racks to ensure redundancy and resilience in the event of node or rack failure (Edureka, 2020).

In high scale hadoop environments, virtualization significantly improves scalability by allowing Hadoop nodes to function as virtual machines (VMs) distributed across diverse physical infrastructure. This abstraction from hardware enables more flexible resource management, efficient load distribution, and enhanced system resilience. Research indicates that scaling virtual nodes across multiple hosts leads to improved data analytics performance and overall throughput, particularly when integrated with rack-aware scheduling mechanisms and optimized cluster configurations (Ahamed, Venkatesh, & Samanta, 2018).

Networking is integral to such Hadoop performance. Each node must be assigned an IP address and mapped hostname to allow seamless communication.

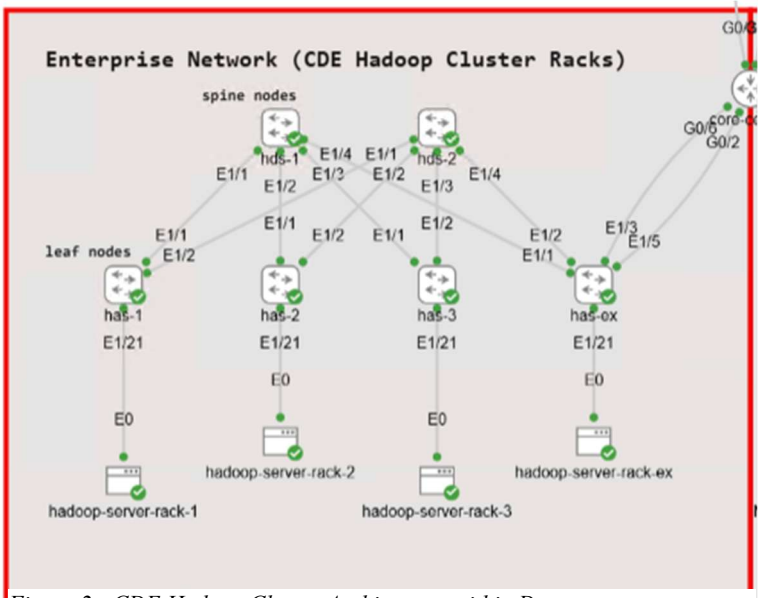

Figure 2 - CDE Hadoop Cluster Architecture within Dancorp

Dancorp's network houses a distributed Hadoop cluster composed of multiple server racks (See Figure 2), each connected via dedicated Layer 2 switches (has-1, has-2, has-3, and has-ex) and aggregated through Layer 3 distribution switches (hds-1 and hds-2). This rack-aware topology is a

foundational design choice for orchestrating large-scale Hadoop deployments across both virtual and physical infrastructures.

By distributing compute workloads across dedicated servers on the racks for such high-volume data processes—each independently connected to access-layer switches (has-1, has-2, has-3 and has-ex)—and interconnecting them through high-bandwidth spine switches (hds-1, hds-2), the architecture supports horizontal scalability, optimized workload placement, and fault isolation. Each rack operates autonomously while remaining part of a cohesive analytics cluster, enabling balanced job scheduling, consistent throughput, and rapid recovery from localized hardware or virtual machine failures. The high-capacity east-west data paths further enhance performance by distributing loads efficiently across the fabric, ensuring resiliency and responsiveness in dynamic workload environments.

For the Dancorp enterprise network topology, the core-central (See Fig 3) router functions as the principal control boundary responsible for regulating routing exchanges across various segments of the infrastructure. Its primary role is to ensure that each operational area—such as Hadoop CDE segment, management, and service delivery—remains logically isolated and secured. This is achieved through the deployment of a Virtual Routing and Forwarding (VRF) instance, which enable the creation of independent routing domains on the same physical router. These VRFs prevent accidental route leaks between sensitive zones and enforce controlled communication where explicitly required.

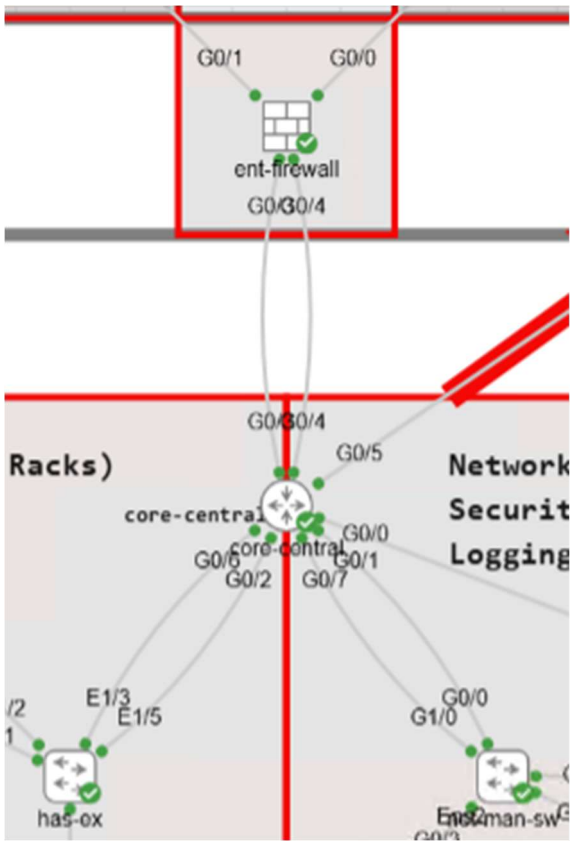

Figure 3 - Core-central Router

This router maintains two main routing contexts. The global routing table (See Figure 4) contains all routes associated with the underlay infrastructure— these includes the OSPF-learned paths from core subnets, directly connected loopbacks, and uplinks to the perimeter firewalls. The default routing namespace supports essential network services and infrastructure management, forming the backbone for administrative operations.

```
core-central#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 9 subnets, 4 masks
S        10.20.1.0/24 [1/0] via 101.101.101.2
S        10.30.1.0/24 [1/0] via 10.168.150.10
S        10.168.0.0/16 [1/0] via 10.168.150.5
C        10.168.3.1/32 is directly connected, Loopback0
C        10.168.150.0/30 is directly connected, GigabitEthernet0/1
L        10.168.150.1/32 is directly connected, GigabitEthernet0/1
C        10.168.150.4/30 is directly connected, GigabitEthernet0/6
L        10.168.150.6/32 is directly connected, GigabitEthernet0/6
S        10.168.200.0/24 [1/0] via 10.168.150.2
      101.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        101.101.101.0/30 is directly connected, GigabitEthernet0/5
L        101.101.101.1/32 is directly connected, GigabitEthernet0/5
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.1.0/30 is directly connected, GigabitEthernet0/0
L        172.16.1.1/32 is directly connected, GigabitEthernet0/0
core-central#
```

Figure 4 - Global Routing Table Overview

In contrast, the VRF-specific routing table (see Figure 5) for the hadoop_cluster environment is entirely separate from the global routing table. It includes routes dedicated to the analytics fabric, such as subnets for Hadoop worker racks (e.g., 10.10.1.1/24, 10.10.1.2/24 and 10.10.1.3/24 and 10.10.1.64/24) and transport paths established over VXLAN overlays.

To support this segmentation, the network employs IEEE 802.1Q encapsulation tags using sub-interface technology, allowing multiple VLANs to coexist over trunk links while maintaining strict traffic separation at Layer 2. By operating within this isolated VRF, data analytics workloads are shielded from general network traffic, improving throughput, and significantly reducing the lateral attack surface. Only predefined inter-VRF interactions are permitted, governed by route-maps and prefix lists that strictly control which routes are exchanged between domains.

```
core-central#show ip route vrf hadoop_cluster

Routing Table: hadoop_cluster
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 11 subnets, 3 masks
B        10.10.1.0/24 [20/0] via 10.168.4.1, 5d12h
B        10.10.1.1/32 [20/0] via 10.168.4.1, 5d12h
B        10.10.1.2/32 [20/0] via 10.168.4.1, 5d12h
B        10.10.1.3/32 [20/0] via 10.168.4.1, 5d12h
S        10.30.1.0/24 [1/0] via 10.168.150.10
C        10.168.4.0/30 is directly connected, GigabitEthernet0/2.101
L        10.168.4.2/32 is directly connected, GigabitEthernet0/2.101
C        10.168.5.0/24 is directly connected, GigabitEthernet0/1.101
L        10.168.5.254/32 is directly connected, GigabitEthernet0/1.101
C        10.168.150.8/30 is directly connected, GigabitEthernet0/7
L        10.168.150.9/32 is directly connected, GigabitEthernet0/7
core-central#
```

Figure 5 - VRF Routing Table (hadoop_cluster)

To support secure hybrid cloud integration, specific traffic originating from the hadoop_cluster VRF—such as data bound for cloud-based analytics pipelines or storage—is selectively routed through the dedicated perimeter firewall (See Figure 6). The firewall is stationed to performs deep packet inspection, enforces access control policies, and establishes secure connections to the designated Azure VPN endpoints. This ensures that traffic leaving the analytics zone does so via encrypted, policy-compliant channels. The firewall validates the source-destination combinations based on configure NSC and forwarding only vetted packets into the Azure ecosystem.

Figure 6 - Enterprise Firewall

This design approach ensures end-to-end encryption, operational compartmentalization, and the safe bridging of on-premises data infrastructure with external cloud services such as Azure Blob Storage or Synapse Analytics.

```
hds-1# show ip route
IP Route Table for VRF "default"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

1.2.3.4/32, ubest/mbest: 2/0, attached
    *via 1.2.3.4, Lo1, [0/0], 2w6d, local
    *via 1.2.3.4, Lo1, [0/0], 2w6d, direct
10.168.0.1/32, ubest/mbest: 2/0, attached
    *via 10.168.0.1, Lo0, [0/0], 2w6d, local
    *via 10.168.0.1, Lo0, [0/0], 2w6d, direct
10.168.0.2/32, ubest/mbest: 4/0
    *via 10.168.1.1, Eth1/1, [110/81], 2w4d, ospf-CSPF_UNDERLAY_NET, intra
    *via 10.168.1.2, Eth1/2, [110/81], 2w4d, ospf-CSPF_UNDERLAY_NET, intra
    *via 10.168.1.3, Eth1/3, [110/81], 2w4d, ospf-CSPF_UNDERLAY_NET, intra
    *via 10.168.1.64, Eth1/4, [110/81], 2w4d, ospf-OSPF_UNDERLAY_NET, intra
10.168.1.1/32, ubest/mbest: 1/0
    *via 10.168.1.1, Eth1/1, [110/41], 2w6d, ospf-CSPF_UNDERLAY_NET, intra
10.168.1.2/32, ubest/mbest: 1/0
    *via 10.168.1.2, Eth1/2, [110/41], 2w4d, ospf-CSPF_UNDERLAY_NET, intra
10.168.1.3/32, ubest/mbest: 1/0
    *via 10.168.1.3, Eth1/3, [110/41], 2w5d, ospf-CSPF_UNDERLAY_NET, intra
10.168.1.64/32, ubest/mbest: 1/0
    *via 10.168.1.64, Eth1/4, [110/41], 2w4d, ospf-OSPF_UNDERLAY_NET, intra
10.168.200.0/24, ubest/mbest: 1/0
    *via 10.168.1.64, Eth1/4, [110/20], 1w0d, ospf-OSPF_UNDERLAY_NET, type-2

hds-1#
```

Figure 7 - hds-1 OSPF underlay routes via spine switch.

```
hds-2# show ip route
IP Route Table for VRF "default"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

1.2.3.4/32, ubest/mbest: 2/0, attached
    *via 1.2.3.4, Lo1, [0/0], 2w4d, local
    *via 1.2.3.4, Lo1, [0/0], 2w4d, direct
10.168.0.1/32, ubest/mbest: 4/0
    *via 10.168.1.1, Eth1/1, [110/81], 2w4d, ospf-CSPF_UNDERLAY_NET, intra
    *via 10.168.1.2, Eth1/2, [110/81], 2w4d, ospf-CSPF_UNDERLAY_NET, intra
    *via 10.168.1.3, Eth1/3, [110/81], 2w4d, ospf-CSPF_UNDERLAY_NET, intra
    *via 10.168.1.64, Eth1/4, [110/81], 2w4d, ospf-OSPF_UNDERLAY_NET, intra
10.168.0.2/32, ubest/mbest: 2/0, attached
    *via 10.168.0.2, Lo0, [0/0], 2w4d, local
    *via 10.168.0.2, Lo0, [0/0], 2w4d, direct
10.168.1.1/32, ubest/mbest: 1/0
    *via 10.168.1.1, Eth1/1, [110/41], 2w4d, ospf-CSPF_UNDERLAY_NET, intra
10.168.1.2/32, ubest/mbest: 1/0
    *via 10.168.1.2, Eth1/2, [110/41], 2w4d, ospf-CSPF_UNDERLAY_NET, intra
10.168.1.3/32, ubest/mbest: 1/0
    *via 10.168.1.3, Eth1/3, [110/41], 2w4d, ospf-CSPF_UNDERLAY_NET, intra
10.168.1.64/32, ubest/mbest: 1/0
    *via 10.168.1.64, Eth1/4, [110/41], 2w4d, ospf-OSPF_UNDERLAY_NET, intra
10.168.200.0/24, ubest/mbest: 1/0
    *via 10.168.1.64, Eth1/4, [110/20], 1w0d, ospf-OSPF_UNDERLAY_NET, type-2
192.168.99.4/32, ubest/mbest: 2/0, attached
    *via 192.168.99.4, Lo99, [0/0], 2w2d, local
    *via 192.168.99.4, Lo99, [0/0], 2w2d, direct

hds-2#
```

Figure 8 - hds-2 OSPF underlay routes via spine switch.

The spine-leaf architecture implemented by Dancorp Analytics inherently supports scalability through its modular design, particularly via the high-performance spine switches (hds-1 and hds-2). These spine nodes provide high port-density, which ensures ample capacity to accommodate increasing numbers of leaf switches as network growth demands. This capability enables seamless expansion, allowing new racks or entire clusters to be integrated effortlessly into the existing fabric without significant reconfiguration or downtime.

Moreover, as the enterprise continues to scale, additional spine switches can be integrated into the existing topology. This modular approach enables horizontal growth—spine nodes can be incrementally added to enhance overall throughput and resilience, ensuring the network remains robust and efficient despite rising workloads and complexity. This design often utilizes the spine switches (hds-1 and hds-2) to provide route reflector functionality for the control plane (using BGP EVPN).

```
hds-1# show bgp l2vpn evpn summary
BGP summary information for VRF default, address family L2VPN EVPN
BGP router identifier 10.168.0.1, local AS number 64520
BGP table version is 1243, L2VPN EVPN config peers 4, capable peers 4
16 network entries and 16 paths using 4672 bytes of memory
BGP attribute entries [11/4048], BGP AS path entries [1/6]
BGP community entries [0/0], BGP clusterlist entries [0/0]

Neighbor        V    AS    MsgRcvd    MsgSent   TblVer  InQ OutQ Up/Down  State/
PfxRcd
10.168.1.1      4 64520      27319      27048     1243    0    0     2w4d 3

10.168.1.2      4 64520      26797      27062     1243    0    0     2w2d 3

10.168.1.3      4 64520      25508      25781     1243    0    0     2w3d 3

10.168.1.64     4 64520      24347      24056     1243    0    0     2w1d 7


Neighbor        T    AS PfxRcd     Type-2     Type-3     Type-4     Type-5     T
ype-12
10.168.1.1      I 64520 3          2          0          0          1          0

10.168.1.2      I 64520 3          2          0          0          1          0

10.168.1.3      I 64520 3          2          0          0          1          0

10.168.1.64     I 64520 7          2          0          0          5          0

hds-1#
```

Figure 9 - hds-1 BGP EVPN peer summary

```
hds-2# show bgp l2vpn evpn summary
BGP summary information for VRF default, address family L2VPN EVPN
BGP router identifier 10.168.0.2, local AS number 64520
BGP table version is 1114, L2VPN EVPN config peers 4, capable peers 4
16 network entries and 16 paths using 4672 bytes of memory
BGP attribute entries [11/4048], BGP AS path entries [1/6]
BGP community entries [0/0], BGP clusterlist entries [0/0]

Neighbor        V    AS    MsgRcvd    MsgSent   TblVer  InQ OutQ Up/Down  State/
PfxRcd
10.168.1.1      4 64520      23955      23706     1114    0    0     2w2d 3

10.168.1.2      4 64520      23471      23731     1114    0    0     2w2d 3

10.168.1.3      4 64520      23466      23732     1114    0    0     2w2d 3

10.168.1.64     4 64520      24017      23713     1114    0    0     2w1d 7


Neighbor        T    AS PfxRcd     Type-2     Type-3     Type-4     Type-5     T
ype-12
10.168.1.1      I 64520 3          2          0          0          1          0

10.168.1.2      I 64520 3          2          0          0          1          0

10.168.1.3      I 64520 3          2          0          0          1          0

10.168.1.64     I 64520 7          2          0          0          5          0

hds-2#
```

Figure 10 - hds-2 BGP EVPN peer summary

In this role, they efficiently distribute reachability information for the overlay network across the fabric. Crucially, while the leaf nodes operate within this overlay and maintain awareness of specific Virtual Routing and Forwarding instances (VRFs) for network segmentation, the spine switches function primarily within the underlay network. As route reflectors and core transport nodes, they are typically not aware of the overlay VRFs themselves. Instead, their focus is on high-speed IP forwarding, which includes processing the UDP encapsulation commonly used by overlay protocols like VXLAN to tunnel traffic between leaf switches. This separation of concerns between the overlay intelligence at the leaves and the efficient underlay transport at the spines is key to the architecture's scalability.

Each leaf switch connects directly to each spine nodes, expanding the spine layer also increases available bandwidth, reduces latency, and further reinforces redundancy.

The spine layer's modularity and extensive port capacity, therefore, provide Dancorp Analytics with a future-proof networking foundation. It guarantees that operational requirements can always be met by dynamically adapting to evolving business and technology demands, maintaining seamless performance, and ensuring uninterrupted service availability even as the Hadoop cluster environment scales substantially over time.

This architectural model ensures that traffic within Dancorp's analytics cluster—particularly east–west communication between server racks—is consistently high-performing, fault-tolerant, and easy to scale. As the business grows, new leaf switches can be added to the fabric simply by up linking them to existing spine switches. The spine's route reflector role automatically propagates routing information across the network, ensuring immediate visibility and reachability of new nodes with no disruption to ongoing operations.

The spine does not host any Virtual Routing and Forwarding (VRF) instances, it remains free of the complexity tied to tenant specific (VRF specific) routing tables. This separation of concerns enhances security and manageability by confining segmentation logic to the leaf layer, where each VXLAN Network Identifier (VNI) is bound to a specific VRF. The spines facilitate this design by forwarding encapsulated packets based solely on outer IP headers, using equal-cost multipath routing to maximize throughput.

Together, these characteristics establish the spine layer as the transport backbone of Dancorp's virtualized, multi-tenant environment. The design accommodates PCI DSS-aligned segmentation and supports the demands of a dynamic analytics workload. By combining route reflection, stateless forwarding, and port-dense scalability, the spine switches empower Dancorp to evolve its infrastructure confidently while preserving both performance and compliance integrity.

The leaf layer in Dancorp Analytics' enterprise architecture forms the access tier of the network, where servers, storage systems, and other compute resources are physically connected.

```
has-1# show bgp l2vpn evpn summary
BGP summary information for VRF default, address family L2VPN EVPN
BGP router identifier 10.168.1.1, local AS number 64520
BGP table version is 2728, L2VPN EVPN config peers 2, capable peers 2
29 network entries and 45 paths using 8468 bytes of memory
BGP attribute entries [39/14352], BGP AS path entries [1/6]
BGP community entries [0/0], BGP clusterlist entries [6/24]

Neighbor        V    AS    MsgRcvd    MsgSent   TblVer  InQ OutQ Up/Down  State/
PfxRcd
10.168.0.1      4 64520      27387      27055     2728    0    0     2w4d 13

10.168.0.2      4 64520      26927      26593     2728    0    0     2w2d 13


Neighbor        T    AS PfxRcd     Type-2     Type-3     Type-4     Type-5     T
ype-12
10.168.0.1      I 64520 13         6          0          0          7          0

10.168.0.2      I 64520 13         6          0          0          7          0

has-1#
```

```
has-2# show bgp l2vpn evpn summary
BGP summary information for VRF default, address family L2VPN EVPN
BGP router identifier 10.168.1.2, local AS number 64520
BGP table version is 3493, L2VPN EVPN config peers 2, capable peers 2
29 network entries and 45 paths using 8468 bytes of memory
BGP attribute entries [39/14352], BGP AS path entries [1/6]
BGP community entries [0/0], BGP clusterlist entries [6/24]

Neighbor        V    AS    MsgRcvd    MsgSent   TblVer  InQ OutQ Up/Down  State/
PfxRcd
10.168.0.1      4 64520      24690      23867     3493    0    0     2w2d 13

10.168.0.2      4 64520      24282      23472     3493    0    0     2w2d 13


Neighbor        T    AS PfxRcd     Type-2     Type-3     Type-4     Type-5     T
ype-12
10.168.0.1      I 64520 13         6          0          0          7          0

10.168.0.2      I 64520 13         6          0          0          7          0

has-2#
```

```
has-3# show bgp l2vpn evpn summary
BGP summary information for VRF default, address family L2VPN EVPN
BGP router identifier 10.168.1.3, local AS number 64520
BGP table version is 3708, L2VPN EVPN config peers 2, capable peers 2
29 network entries and 45 paths using 8468 bytes of memory
BGP attribute entries [39/14352], BGP AS path entries [1/6]
BGP community entries [0/0], BGP clusterlist entries [6/24]

Neighbor        V    AS    MsgRcvd    MsgSent   TblVer  InQ OutQ Up/Down  State/
PfxRcd
10.168.0.1      4 64520      25468      24607     3708    0    0     2w3d 13

10.168.0.2      4 64520      24994      24150     3708    0    0     2w2d 13


Neighbor        T    AS PfxRcd     Type-2     Type-3     Type-4     Type-5     T
ype-12
10.168.0.1      I 64520 13         6          0          0          7          0

10.168.0.2      I 64520 13         6          0          0          7          0

has-3#
```

```
has-ex# show bgp l2vpn evpn summary
BGP summary information for VRF default, address family L2VPN EVPN
BGP router identifier 10.168.1.64, local AS number 64520
BGP table version is 2169, L2VPN EVPN config peers 2, capable peers 2
25 network entries and 37 paths using 7300 bytes of memory
BGP attribute entries [35/12880], BGP AS path entries [1/6]
BGP community entries [0/0], BGP clusterlist entries [6/24]

Neighbor        V    AS    MsgRcvd    MsgSent   TblVer  InQ OutQ Up/Down  State/
PfxRcd
10.168.0.1      4 64520      24359      24070     2169    0    0     2w1d 9

10.168.0.2      4 64520      24010      23735     2169    0    0     2w1d 9


Neighbor        T    AS PfxRcd     Type-2     Type-3     Type-4     Type-5     T
ype-12
10.168.0.1      I 64520 9          6          0          0          3          0

10.168.0.2      I 64520 9          6          0          0          3          0

has-ex#
```

Figure 11 - EVPN BGP Summary Between Leaf Nodes

The BGP EVPN summaries from all leaf switches shown in Figure 11 (has-1, has-2, has-3, and has-ex) confirm stable and synchronized control plane operations across Dancorp Analytics' VXLAN fabric. Each leaf maintains active BGP sessions with both spine switches (10.168.0.1 and 10.168.0.2), with no message backlog and consistent uptime, indicating healthy peering. Each leaf receives the EVPN routes, Type-2 (MAC/IP advertisements) and Type-5 (IP prefixes)—ensuring full endpoint visibility for both Layer 2 and Layer 3 services within the hadoop_cluster VRF. This confirms successful route reflection by the spines and proper route propagation across the overlay. Overall, the this reflects a functioning and scalable EVPN control plane, enabling dynamic VXLAN connectivity between all racks.

The routing structure observed across the leaf switches (has-1, has-2, has-3, and has-ex) illustrates the core principles of Dancorp Analytics' segmented VXLAN-EVPN architecture. The design leverages a clear separation

between the underlay and overlay networks, enabling scalable, secure communication across the data center environment.

The underlay network serves as the IP-based transport fabric, built on traditional BGP routing with Autonomous System Number (ASN) 64520.

This underlay facilitates IP connectivity among all spine and leaf nodes, ensuring that VXLAN-encapsulated packets can traverse the infrastructure without awareness of the encapsulated (tenant) content.

It provides the physical reachability necessary for overlay operations and is entirely agnostic of any virtual routing and forwarding (VRF) constructs. The overlay network, in contrast, operates at the logical level, utilizing EVPN as the control plane and VXLAN as the encapsulation mechanism for tenant or service-specific traffic. Each leaf node functions as a VXLAN Tunnel Endpoint (VTEP), responsible for encapsulating and decapsulating tenant traffic as it enters and exits the overlay fabric.

Within this design, segmentation is achieved through the instantiation of separate VRFs at each leaf switch, notably the hadoop_cluster VRF. These VRFs maintain

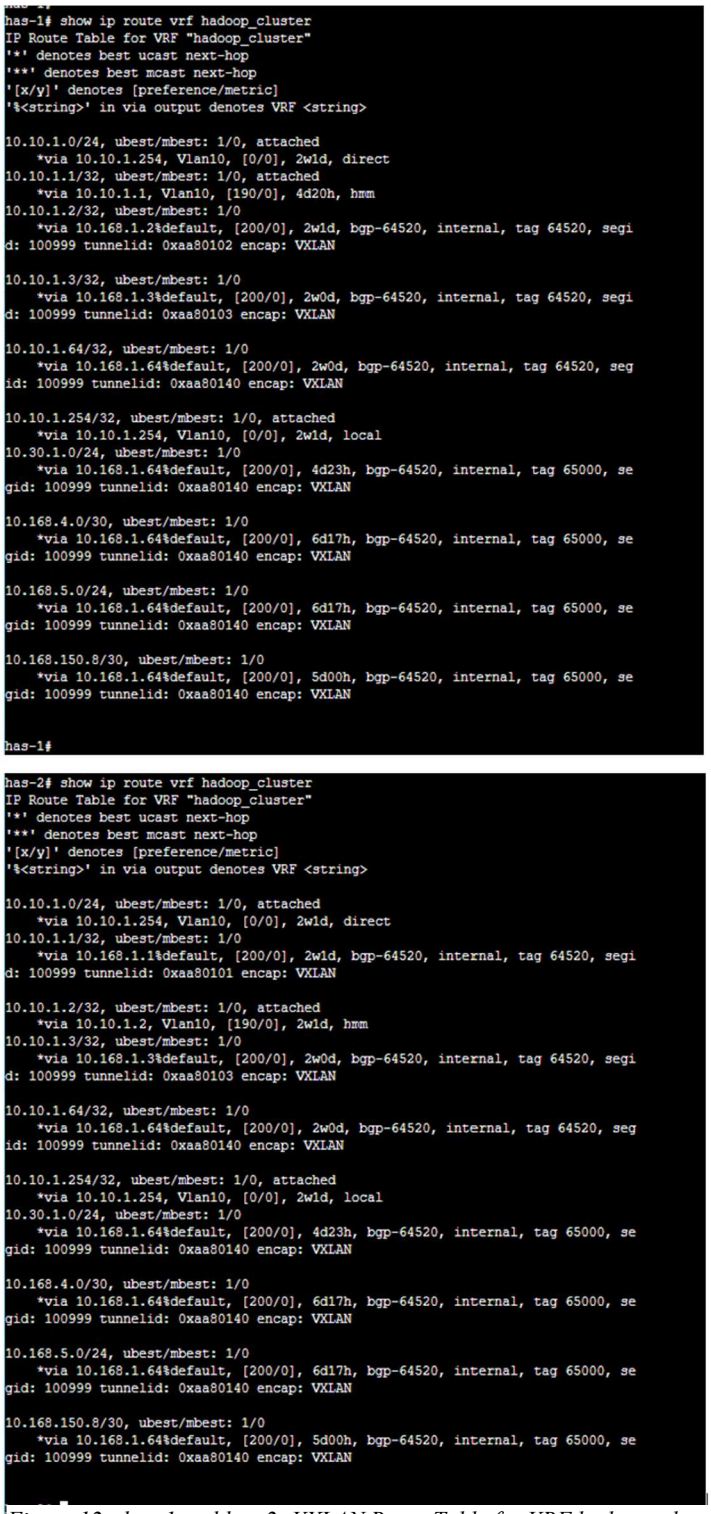

Figure 12 - has-1 and has-2: VXLAN Route Table for VRF hadoop_cluster

independent forwarding tables and are bound to unique VXLAN Network Identifiers (VNIs), ensuring strict traffic isolation between services or tenants, for when Dancorp takes on more clients, the traffic from each operation can co-exist with traffic from another organisation in different VRFs and NSC.

```
has-3# show ip route vrf hadoop_cluster
IP Route Table for VRF "hadoop_cluster"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

10.10.1.0/24, ubest/mbest: 1/0, attached
    *via 10.10.1.254, Vlan10, [0/0], 2w1d, direct
10.10.1.1/32, ubest/mbest: 1/0
    *via 10.168.1.1%default, [200/0], 2w1d, bgp-64520, internal, tag 64520, segi
d: 100999 tunnelid: 0xaa80101 encap: VXLAN

10.10.1.2/32, ubest/mbest: 1/0
    *via 10.168.1.2%default, [200/0], 2w1d, bgp-64520, internal, tag 64520, segi
d: 100999 tunnelid: 0xaa80102 encap: VXLAN

10.10.1.3/32, ubest/mbest: 1/0, attached
    *via 10.10.1.3, Vlan10, [190/0], 2w0d, hmm
10.10.1.64/32, ubest/mbest: 1/0
    *via 10.168.1.64%default, [200/0], 2w0d, bgp-64520, internal, tag 64520, seg
id: 100999 tunnelid: 0xaa80140 encap: VXLAN

10.10.1.254/32, ubest/mbest: 1/0, attached
    *via 10.10.1.254, Vlan10, [0/0], 2w1d, local
10.30.1.0/24, ubest/mbest: 1/0
    *via 10.168.1.64%default, [200/0], 4d23h, bgp-64520, internal, tag 65000, se
gid: 100999 tunnelid: 0xaa80140 encap: VXLAN

10.168.4.0/30, ubest/mbest: 1/0
    *via 10.168.1.64%default, [200/0], 6d17h, bgp-64520, internal, tag 65000, se
gid: 100999 tunnelid: 0xaa80140 encap: VXLAN

10.168.5.0/24, ubest/mbest: 1/0
    *via 10.168.1.64%default, [200/0], 6d17h, bgp-64520, internal, tag 65000, se
gid: 100999 tunnelid: 0xaa80140 encap: VXLAN

10.168.150.8/30, ubest/mbest: 1/0
    *via 10.168.1.64%default, [200/0], 5d00h, bgp-64520, internal, tag 65000, se
gid: 100999 tunnelid: 0xaa80140 encap: VXLAN

has-3#
```

```
has-ex# show ip route vrf hadoop_cluster
IP Route Table for VRF "hadoop_cluster"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

10.10.1.0/24, ubest/mbest: 1/0, attached
    *via 10.10.1.254, Vlan10, [0/0], 2w1d, direct
10.10.1.1/32, ubest/mbest: 1/0
    *via 10.168.1.1%default, [200/0], 2w1d, bgp-64520, internal, tag 64520, segi
d: 100999 tunnelid: 0xaa80101 encap: VXLAN

10.10.1.2/32, ubest/mbest: 1/0
    *via 10.168.1.2%default, [200/0], 2w1d, bgp-64520, internal, tag 64520, segi
d: 100999 tunnelid: 0xaa80102 encap: VXLAN

10.10.1.3/32, ubest/mbest: 1/0
    *via 10.168.1.3%default, [200/0], 2w0d, bgp-64520, internal, tag 64520, segi
d: 100999 tunnelid: 0xaa80103 encap: VXLAN

10.10.1.64/32, ubest/mbest: 1/0, attached
    *via 10.10.1.64, Vlan10, [190/0], 4d20h, hmm
10.10.1.254/32, ubest/mbest: 1/0, attached
    *via 10.10.1.254, Vlan10, [0/0], 2w1d, local
10.30.1.0/24, ubest/mbest: 1/0
    *via 10.168.4.2, [20/0], 4d23h, bgp-64520, external, tag 65000
10.168.4.0/30, ubest/mbest: 1/0, attached
    *via 10.168.4.1, Eth1/5.101, [0/0], 2w0d, direct
10.168.4.1/32, ubest/mbest: 1/0, attached
    *via 10.168.4.1, Eth1/5.101, [0/0], 2w0d, local
10.168.5.0/24, ubest/mbest: 1/0
    *via 10.168.4.2, [20/0], 6d18h, bgp-64520, external, tag 65000
10.168.150.8/30, ubest/mbest: 1/0
    *via 10.168.4.2, [20/0], 5d00h, bgp-64520, external, tag 65000

has-ex#
```

Figure 13 - has-3 and has-ex: VXLAN Route Table for VRF hadoop_cluster

Route visibility within the VRF confirms that BGP EVPN is used to advertise host and subnet reachability information across the fabric. These advertisements include tags and tunnel IDs indicating that the associated traffic is encapsulated and routed using VXLAN over the underlay. Importantly, the spine switches do not host any VRFs themselves. Instead, they function purely as route reflectors in the control plane, relaying EVPN updates between leaves without participating in tenant-specific routing. This simplifies the spine configuration while maintaining full isolation and reachability within the overlay.

This architecture enforces segmentation through a layered routing model, where the underlay guarantees transport reliability, and the overlay ensures tenant isolation. The VRF-based segmentation strategy, combined with EVPN route propagation and

stateless VXLAN forwarding, supports Dancorp's objectives for secure, scalable, and PCI-compliant network operations.

```
line vty
router ospf OSPF_UNDERLAY_NET
  redistribute static route-map REDIST_STATIC
  log-adjacency-changes
router bgp 64520
  router-id 10.168.1.64
  log-neighbor-changes
  address-family ipv4 unicast
  address-family l2vpn evpn
  template peer VXLAN_SPINE
    remote-as 64520
    update-source loopback0
    address-family ipv4 unicast
      send-community extended
      soft-reconfiguration inbound
    address-family l2vpn evpn
      send-community
      send-community extended
  neighbor 10.168.0.1
    inherit peer VXLAN_SPINE
  neighbor 10.168.0.2
    inherit peer VXLAN_SPINE
  neighbor 10.168.4.5
    remote-as 65000
  vrf hadoop_cluster
    timers bgp 7 21
    log-neighbor-changes
    address-family ipv4 unicast
      network 10.10.1.0/24
      advertise l2vpn evpn
      maximum-paths 2
      maximum-paths ibgp 2
    neighbor 10.168.4.2
      remote-as 65000
      address-family ipv4 unicast
        send-community
        send-community extended
    neighbor 10.168.4.6
      remote-as 65000
      address-family ipv4 unicast
        send-community
        send-community extended
evpn
  vni 100010 l2
    rd auto
    route-target import auto
    route-target export auto


has-ex#
```

Figure 14 - has-ex Route Leak Configuration

Also, within Dancorp's VXLAN EVPN fabric, the has-ex node is strategically deployed as a border leaf, facilitating interconnection between the internal analytics infrastructure and external routing domains. This deployment aligns with Cisco's validated VXLAN EVPN design model, wherein external connectivity is achieved through VRF-lite–enabled border gateways. These border leaf nodes support both overlay control plane participation via EVPN and route exchange with external autonomous systems through eBGP peering. In Dancorp's case, has-ex bridges the hadoop_cluster VRF with external AS 65000, enabling selective route leaking and seamless integration with upstream environments (Cisco, n.d). Through its iBGP EVPN peering with spines (hds-1 and hds-2), has-ex ensures consistent distribution of MAC/IP prefixes via Route Type 2 and Route Type 5 advertisements. These routes are injected into the local VRF and exported to the WAN edge using eBGP, with associated labels and route targets for proper encapsulation and segmentation. The device supports automatic RD and route-target propagation, VNI alignment (e.g., VNI 100010), and ECMP load balancing, making it scalable and resilient. The captured BGP outputs confirm propagation of loopbacks and tenant subnet routes across the fabric, reflecting tight control-plane convergence and route visibility.

Cisco recommends that only relevant VRF instances be extended outside the fabric and mapped to 802.1Q-tagged sub interfaces, ensuring precise route control (Cisco, 2024, p. 2). In the has-ex configuration, this model is adhered to by defining sub interfaces tied to WAN-facing peers, enabling a clean Layer-3 data traffic handoff. Traffic received from external networks is matched to the correct VRF and then encapsulated into VXLAN for east-west forwarding through the fabric.

By enabling Layer-3 peering and BGP route exchange at a designated border node, has-ex supports secure and scalable data flow between cloud services, partner sites, or firewalls, and the analytics environment. This approach simplifies domain segmentation while preserving operational integrity—essential for analytics environments that demand performance and policy enforcement across boundaries. This interconnection is what enables security scans, Authentication, Authorization, and Accounting (AAA) service integration, and the foundation for implementing Role-Based Access Control (RBAC) within the internal cluster. It also facilitates access to essential enterprise services such as Active Directory for identity management, internal email services, automated computer imaging, system backup and restoration, and broader business continuity operations (eg DHCP and DNS). Without this gateway-level connectivity, these foundational IT services would be siloed, compromising both manageability and security in the data-centric enterprise environment.

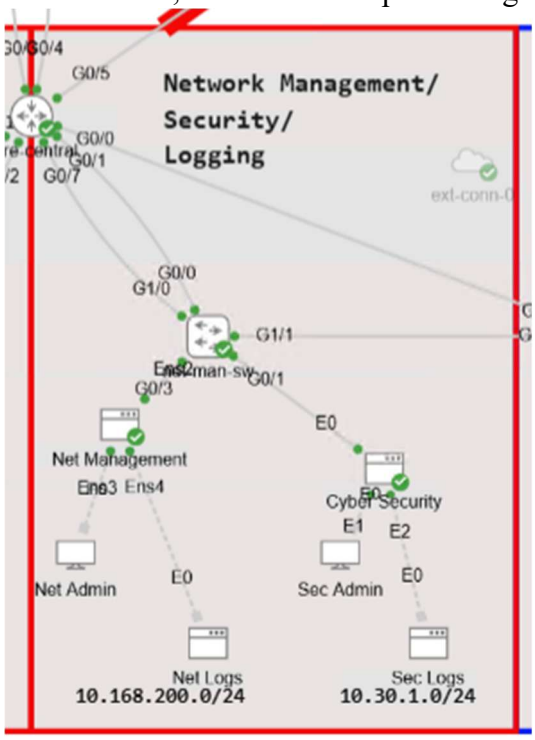

Figure 15 - Network Management, Security, and Logging (NMSL) zone

The Network Management, Security, and Logging (NMSL) zone is a provisioned segment in Dancorp Analytics' network design, intended to deliver centralized control, visibility, and enforcement across the enterprise. While full deployment is constrained by current emulation limits, the architecture accounts for future integration of these critical services. As shown in Figure 15, the NMSL zone spans two logically separated subnets: 10.168.200.0/24 for administrative access and network events logging, and 10.30.1.0/24 for cybersecurity operations and security event monitoring performed by IDP/IDS systems. Its design components include Net Admin and Cyber Security servers, along with placeholders for a Security Information and Event Management

(SIEM) platform and log servers. AAA (Authentication, Authorization, and Accounting) integration is factored into the design through RADIUS and TACACS+, while Microsoft Active Directory (AD) is positioned as the central identity provider for enforcing role-based access control.

The enterprise network (non-CDE) segment is designed to support internal business operations that do not interact with sensitive or regulated data. As shown in Figure 11, this zone operates within the 172.16.0.0/16 address space and is routed through the Business Access Switch (BAS), which provides Layer 2 and Layer 3 capabilities for departmental connectivity and user access. This segment is physically and logically isolated from the Cardholder Data Environment (CDE) through both infrastructure design and strict routing policies.

The routing configuration, detailed in Figure 11, shows that the BAS uses only static routing to manage all traffic within the enterprise zone. No dynamic routing protocols such as BGP, OSPF, or EIGRP are present.

This design choice ensures predictable routing behavior and prevents the risk of route advertisement or leakage into more sensitive network areas. A single static default route is configured via 172.16.1.1 for upstream traffic, while another static route to 10.168.200.0/24 via 192.168.100.1 provides controlled access to the Network Management segment under restricted policies.

```
bas#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 172.16.1.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.1.1
      10.0.0.0/24 is subnetted, 1 subnets
S        10.168.200.0 [1/0] via 192.168.100.1
      172.16.0.0/16 is variably subnetted, 19 subnets, 3 masks
C        172.16.1.0/30 is directly connected, GigabitEthernet0/0
L        172.16.1.2/32 is directly connected, GigabitEthernet0/0
C        172.16.20.0/24 is directly connected, Vlan20
L        172.16.20.1/32 is directly connected, Vlan20
C        172.16.30.0/24 is directly connected, Vlan30
L        172.16.30.1/32 is directly connected, Vlan30
C        172.16.40.0/24 is directly connected, Vlan40
L        172.16.40.1/32 is directly connected, Vlan40
C        172.16.50.0/24 is directly connected, Vlan50
L        172.16.50.1/32 is directly connected, Vlan50
C        172.16.60.0/24 is directly connected, Vlan60
L        172.16.60.1/32 is directly connected, Vlan60
C        172.16.70.0/24 is directly connected, Vlan70
L        172.16.70.1/32 is directly connected, Vlan70
C        172.16.80.0/24 is directly connected, Vlan80
L        172.16.80.1/32 is directly connected, Vlan80
C        172.16.90.0/24 is directly connected, Vlan90
L        172.16.90.1/32 is directly connected, Vlan90
C        172.16.100.1/32 is directly connected, Loopback0
      192.168.100.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.100.0/30 is directly connected, GigabitEthernet1/1
L        192.168.100.2/32 is directly connected, GigabitEthernet1/1
bas#
```

Figure 16- BAS Routing Overview

Departmental segmentation is achieved using dedicated VLANs on the BAS, as illustrated in Figure 12. Each business unit—including finance, human resources, sales and marketing, IT administration, development, legal, executive management, and customer support—is assigned its own VLAN and corresponding subnet within the 172.16.x.0/24 range.

These VLANs are directly connected and locally routed through the BAS, enabling internal access while maintaining operational boundaries. Additionally, VLAN 192 is designated for logging and monitoring, further reinforcing administrative oversight. To maintain strict isolation from the CDE and other high-security segments, access control lists (ACLs) are applied to restrict both inter-VLAN communication and any outbound traffic that could compromise the integrity of isolated zones. These ACLs are typically enforced at both the switch and firewall levels, explicitly denying unauthorized IP ranges and protocols. This ensures that even if traffic reaches the routing layer, it cannot traverse into restricted environments. Overall, the Enterprise Network (Non-CDE) segment is a self-contained and compartmentalized zone, designed with static routing, VLAN segmentation, and access control policies that collectively enforce strong isolation. This provides a clear boundary between general enterprise operations and sensitive network functions, supporting a layered, structured approach to infrastructure security.

```
bas#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/1, Gi0/2, Gi0/3
20   interface_finance                active
30   interface_HR                     active    Gi1/2
40   interface_sales_marketing        active    Gi1/3
50   interface_IT_admin               active    Gi2/0
60   interface_dev                    active    Gi2/1
70   interface_exec_senior_management active    Gi2/2
80   interface_legal_compliance       active    Gi2/3
90   interface_customer_support       active    Gi3/0
192  interface_logging_monitoring_VI  active    Gi3/1
419  used_ports                       active    Gi1/0, Gi3/2, Gi3/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Figure 17 - Operational Segmentation Vlans (Non-CDE)

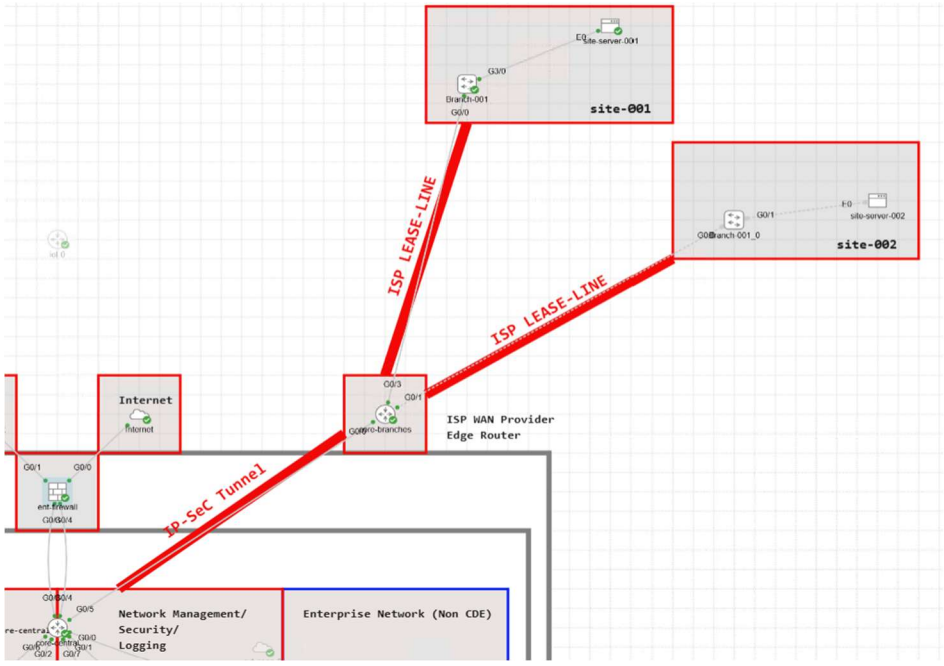

Figure 18 - Remote Site WAN Topology

The diagram in Figure 18 illustrates the wide area network (WAN) topology used to connect Dancorp Analytics' central infrastructure to its remote client sites which transmit data from client sites for processing in the Hadoop cluster. The connectivity model combines IPSec tunneling and

leased-line circuits to deliver secure, reliable communication between the core data center and geographically distributed sites.

A dedicated router labeled core-branches serves as the aggregation point for branch and site connectivity. This router is connected to the central infrastructure via an IPSec tunnel, ensuring that all traffic between the core (e.g., core-central) and remote locations is encrypted and securely routed through an untrusted ISP path. The use of an IPSec VPN enables the organization to securely extend its private network over a public medium while maintaining confidentiality, integrity, and authentication of transmitted data.

The core-branches router connects to remote sites Site-001 and Site-002 via ISP partners' leased lines, ensuring reliable, low-latency communication. Each site operates as a separate Layer 3 domain using static routing, avoiding dynamic protocols to maintain tight control and reduce exposure. ACLs are applied to restrict traffic to only permitted services, such as server synchronization. An IPSec tunnel is also available to encrypt interesting traffic across untrusted networks. This design ensures secure, isolated communication between the central network and remote locations, combining the stability of leased lines with the confidentiality of encrypted tunnels.

The core-central router is connected to core-branches over a secured IPSec tunnel (See Figure 14), which encrypts all incoming traffic from remote sites such as Site-001 and Site-002. Upon arrival, the traffic is decrypted and routed through the global routing table of core central. From there, it is forwarded to the enterprise firewall, where security policies and ACLs are applied. If permitted, the traffic is then rerouted into the Hadoop analytics cluster via the appropriate VRF instance. This layered routing path ensures encrypted transmission, centralized policy enforcement, and controlled access to sensitive resources within the analytics environment.

```
core-central#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
101.101.101.1   101.101.101.2   QM_IDLE           1007 ACTIVE

IPv6 Crypto ISAKMP SA

core-central#
core-central#
core-central#show run | section crypto
crypto isakmp policy 10
 encr aes
 hash sha256
 authentication pre-share
 group 14
crypto isakmp key vpnuser address 101.101.101.2
crypto ipsec transform-set MYSET esp-aes esp-sha256-hmac
 mode tunnel
crypto map VPN-MAP 10 ipsec-isakmp
 set peer 101.101.101.2
 set transform-set MYSET
 match address 100
 crypto map VPN-MAP
core-central#
```

Figure 19 - Core-central IPSec Status with ISP WAN Edge

2.3 Design Analysis for PCI DSS Compliance and Dancorp' Business Objectives

PCI DSS v4.0 introduces two implementation paths: the Defined Approach, which follows prescribed controls and validation procedures, and the Customized Approach, which allows organisations with mature security programs to adopt alternative controls tailored to their environment. While this flexibility supports innovation and scalability, it demands thorough risk analysis, documentation, and proof of effectiveness. Critically, some core requirements—like the ban on storing Sensitive Authentication Data (SAD)—remain ineligible for customization. This model demonstrates that PCI DSS is flexible, permitting organisations to implement controls that align with their capabilities, so long as they meet audit expectations and uphold the standard's security intent (PCI Security Standards Council, 2024, pp. 28–29).

Dancorp Analytics' enterprise network has been strategically designed to meet the twelve core requirements of the Payment Card Industry Data Security Standard (PCI DSS) v4.0.1, while also supporting operational flexibility and future scalability. The PCI DSS framework outlines six principal objectives that form a foundation for securing cardholder data and shaping robust organisational security policies (PCI SSC, 2024, p. 1).

2.3.1 *Build and Maintain a Secure Network and Systems.*

In PCI DSS v4.0.1, Build and Maintain a Secure Network and Systems forms the first of six principal requirement groups, comprising Requirements 1 and 2. These focus on implementing Network Security Controls (NSCs) and enforcing secure system configurations to defend against internal and external threats to cardholder data environments (PCI DSS, 2024, p. 38). Together, these requirements ensure that strong security is embedded in both the design and operation of systems. By incorporating routing as a core component of NSCs, organisations reinforce their network segmentation strategies and control traffic at a granular level. These measures establish a baseline for preventing misconfigurations, reducing attack surfaces, and promoting a proactive, compliance-driven security culture (PCI SSC, 2024, p. 38).

The architecture adopts a three-zone segmentation model—Untrusted, Demilitarised (DMZ), and Trusted—to enforce strict traffic control and reduce risk. At the heart of the Trusted Zone is the Cardholder Data Environment (CDE), which hosts Dancorp's Hadoop-based analytics cluster and is tightly segmented from all non-PCI systems. Key infrastructure components and

communication paths that handle CDE-related data are marked by red boundaries in the topology diagram. These include the Hadoop Access Switches (has), Hadoop Distribution Switches (hds), and core/segment routing and security devices.

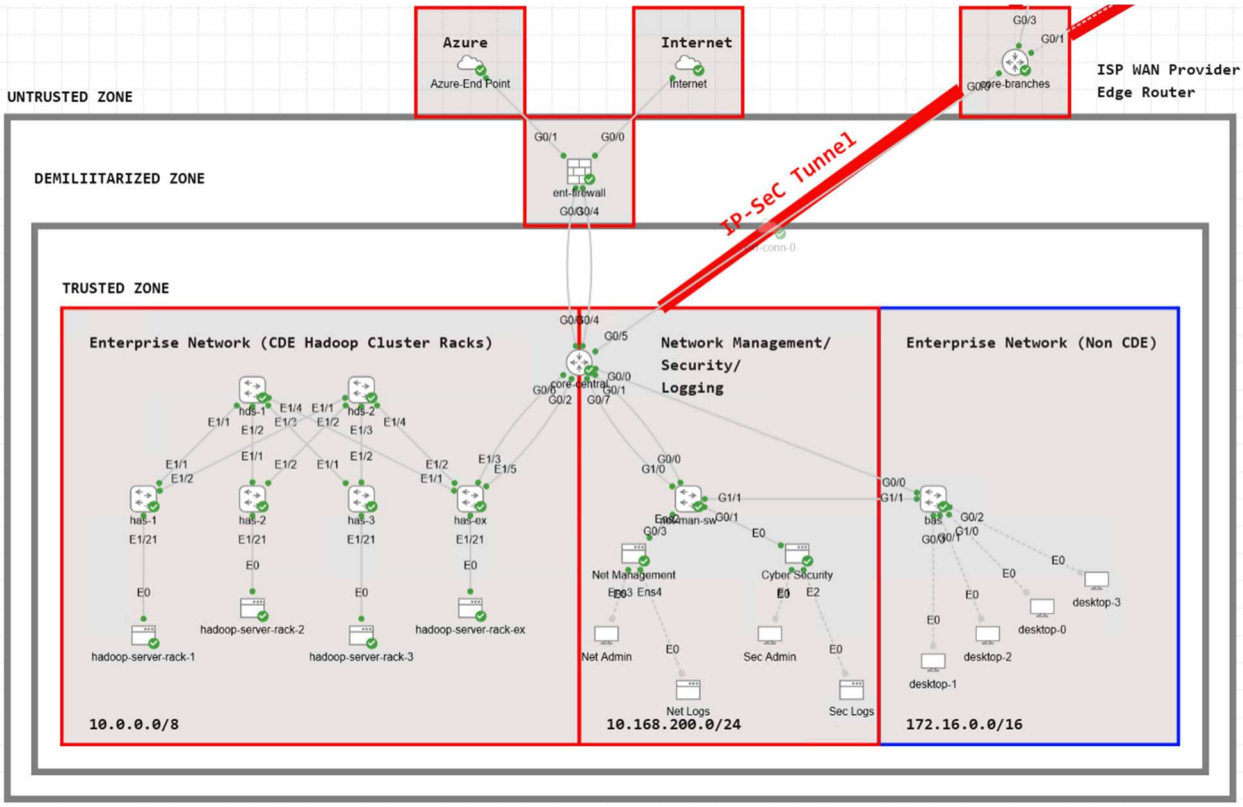

Figure 20 - Dancorp Enterprise Network Security Zones and Architecture

For Dancorp to meet these requirements, the environment is segmented into untrusted, dmz, and trusted zones, with a central enterprise firewall enforcing strict access controls between zones—meeting key objectives of Requirement 1 related to Network Security Controls (PCI SSC, 2024, pp. 19–25).

In the non CDE segment, the Business Access Switch (BAS), used for general user access, is deliberately isolated from the CDE, with only a controlled tap line for network administration, linking it to the management segment of the topology.

The Non-CDE section of Dancorp's enterprise network is isolated from the Cardholder Data Environment (CDE) and operates independently under the 172.16.0.0/16 IP block.

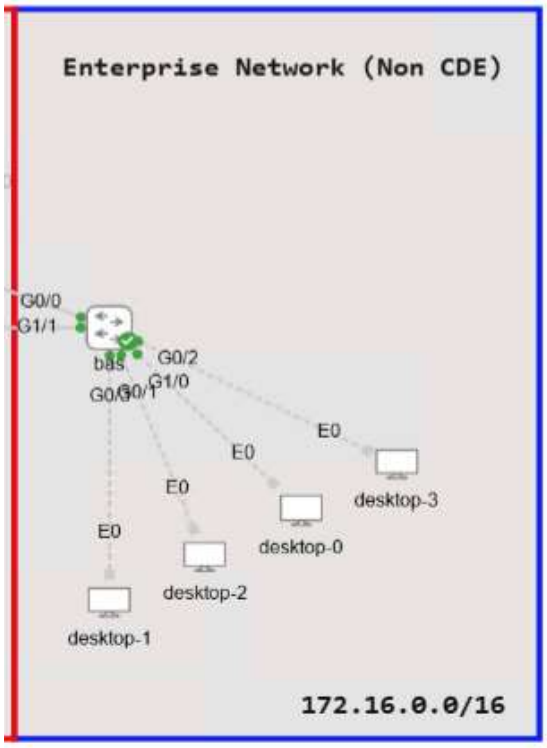

Figure 22 - Enterprise Non CDE Segment

It is anchored by a Layer 3 Business Access Switch (BAS), which provides routed access to general corporate users across multiple VLANs. Each business unit—such as Finance, HR, Sales, Legal, Development, and Executive Management—is segmented into its own VLAN, as reflected in the show vlan brief output. This segmentation enhances security, visibility, and performance within the general-purpose enterprise zone.

Routing on the BAS confirms that each VLAN is directly connected and reachable, with a default route forwarding traffic to the upstream firewall. The BAS handles internal routing within the 172.16.x.x range and maintains reachability to external networks, including 192.168.100.0/30 and 192.168.200.0/24. A dedicated link connects the BAS to the core management zone, enabling administrative visibility without granting direct access to the Cardholder Data Environment (CDE). To mitigate the risk of lateral movement in the event of a device compromise within the non-CDE network, an Access Control List is applied on the BAS uplinks. This ACL explicitly blocks all traffic destined for the 10.0.0.0/8 range—where PCI-scoped

```
bas#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 172.16.1.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.1.1
      10.0.0.0/24 is subnetted, 1 subnets
S        10.168.200.0 [1/0] via 192.168.100.1
      172.16.0.0/16 is variably subnetted, 19 subnets, 3 masks
C        172.16.1.0/30 is directly connected, GigabitEthernet0/0
L        172.16.1.2/32 is directly connected, GigabitEthernet0/0
C        172.16.20.0/24 is directly connected, Vlan20
L        172.16.20.1/32 is directly connected, Vlan20
C        172.16.30.0/24 is directly connected, Vlan30
L        172.16.30.1/32 is directly connected, Vlan30
C        172.16.40.0/24 is directly connected, Vlan40
L        172.16.40.1/32 is directly connected, Vlan40
C        172.16.50.0/24 is directly connected, Vlan50
L        172.16.50.1/32 is directly connected, Vlan50
C        172.16.60.0/24 is directly connected, Vlan60
L        172.16.60.1/32 is directly connected, Vlan60
C        172.16.70.0/24 is directly connected, Vlan70
L        172.16.70.1/32 is directly connected, Vlan70
C        172.16.80.0/24 is directly connected, Vlan80
L        172.16.80.1/32 is directly connected, Vlan80
C        172.16.90.0/24 is directly connected, Vlan90
L        172.16.90.1/32 is directly connected, Vlan90
C        172.16.100.1/32 is directly connected, Loopback0
      192.168.100.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.100.0/30 is directly connected, GigabitEthernet1/1
L        192.168.100.2/32 is directly connected, GigabitEthernet1/1
```

Figure 21 - BAS L3 Switch Route Table

systems reside—while permitting communication from the trusted management subnet (10.168.200.0/24), as well as allowing legitimate enterprise traffic such as internet access and inter-VLAN communication.

This architecture ensures PCI DSS segmentation by clearly isolating user and departmental traffic from sensitive processing zones. It also supports policy enforcement, traffic control, and monitoring, enabling the network to maintain a secure and compliant state while serving the broader enterprise user base efficiently.

```
core-central#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 9 subnets, 4 masks
S        10.20.1.0/24 [1/0] via 101.101.101.2
S        10.30.1.0/24 [1/0] via 10.168.150.10
S        10.168.0.0/16 [1/0] via 10.168.150.5
C        10.168.3.1/32 is directly connected, Loopback0
C        10.168.150.0/30 is directly connected, GigabitEthernet0/1
L        10.168.150.1/32 is directly connected, GigabitEthernet0/1
C        10.168.150.4/30 is directly connected, GigabitEthernet0/6
L        10.168.150.6/32 is directly connected, GigabitEthernet0/6
S        10.168.200.0/24 [1/0] via 10.168.150.2
      101.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        101.101.101.0/30 is directly connected, GigabitEthernet0/5
L        101.101.101.1/32 is directly connected, GigabitEthernet0/5
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.1.0/30 is directly connected, GigabitEthernet0/0
L        172.16.1.1/32 is directly connected, GigabitEthernet0/0
```

```
core-central#show ip route vrf hadoop_cluster

Routing Table: hadoop_cluster
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 11 subnets, 3 masks
B        10.10.1.0/24 [20/0] via 10.168.4.1, 2d21h
B        10.10.1.1/32 [20/0] via 10.168.4.1, 2d21h
B        10.10.1.2/32 [20/0] via 10.168.4.1, 2d21h
B        10.10.1.3/32 [20/0] via 10.168.4.1, 2d21h
S        10.30.1.0/24 [1/0] via 10.168.150.10
C        10.168.4.0/30 is directly connected, GigabitEthernet0/2.101
L        10.168.4.2/32 is directly connected, GigabitEthernet0/2.101
C        10.168.5.0/24 is directly connected, GigabitEthernet0/1.101
L        10.168.5.254/32 is directly connected, GigabitEthernet0/1.101
C        10.168.150.8/30 is directly connected, GigabitEthernet0/7
L        10.168.150.9/32 is directly connected, GigabitEthernet0/7
core-central#
```

Figure 23 - Routing Table Views on Core-Central Router (Global And VRF)

Within the trusted zone, the Cardholder Data Environment (CDE)—which hosts the Hadoop cluster racks—is operational designed to operate in the the 10.0.0.0/8 subnet block and operates within a strictly controlled and segmented routing domain. This segmentation is engineered using a multi-protocol routing strategy that includes Border Gateway Protocol (BGP), static routing, and Open Shortest Path First (OSPF)—specifically, OSPF Area 10.10.10.10—to achieve both granular control and high availability. BGP is employed to facilitate inter-zone communication and remote site integration, such as the IPsec tunnel to external branch networks. BGP's policy-based routing capabilities ensure that only explicitly permitted prefixes are advertised and received, fulfilling PCI DSS Requirement 1.3 by preventing

unauthorised access paths and maintaining full administrative control over advertised and learned routes (PCI SSC, 2024, p. 22).

Static routing is implemented within the core-central router of the trusted zone to define deterministic paths between the CDE, management, and security networks. This eliminates ambiguity in route resolution and prevents dynamic propagation of potentially unvetted routes. The use of these deterministic routes enhances compliance with Requirements 1.4 and 2.2, which mandate secure, controlled network access and hardened configurations (PCI SSC, 2024, pp. 23, 28). OSPF, configured within Area 10.10.10.10, serves as the internal dynamic routing protocol, distributing reachability underlay network information between routers and spine leaf switches within the CDE and its supporting infrastructure. This ensures fast convergence, scalability, and efficient routing updates while maintaining domain isolation.

To support logical separation at scale, the design further incorporates Virtual Routing and Forwarding (VRF) instances, enabling multiple isolated routing tables on the same physical infrastructure. This supports tenant-like separation between CDE, management, and non-CDE environments, aligning with segmentation mandates in PCI DSS.

On the Hadoop computing rack's segment of the enterprise network, VXLAN (Virtual Extensible LAN) is used to extend Layer 2 segments across Layer 3 boundaries, supporting virtual machine mobility and service chaining without breaching the CDE boundary. EVPN (Ethernet VPN) combined with VXLAN ensures control plane learning for MAC and IP routes, improving scalability and security by reducing flooding and supporting endpoint authentication. Furthermore, L2VPN

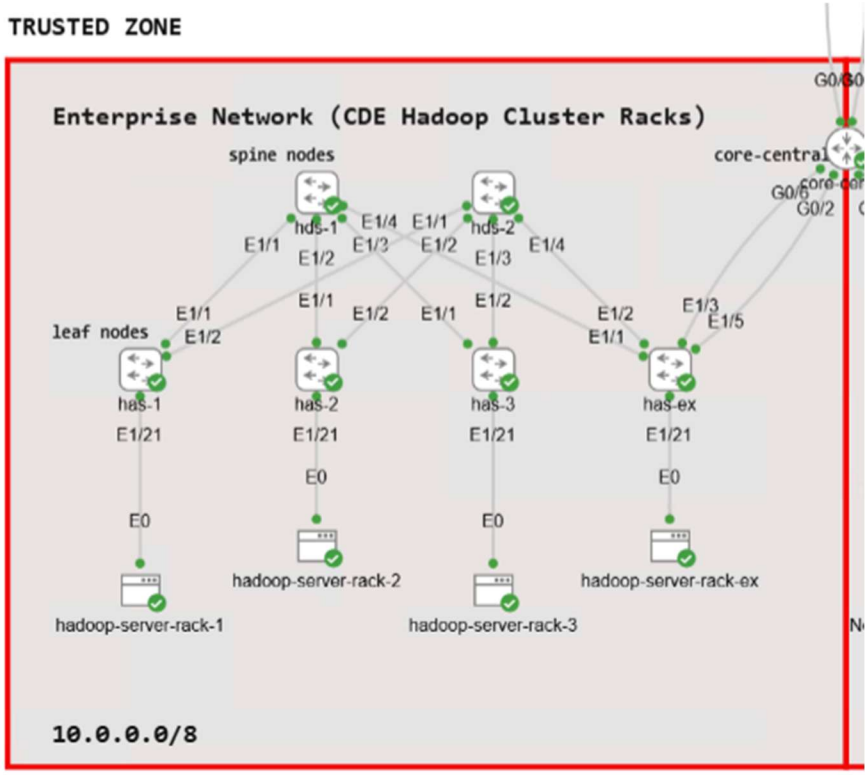

Figure 24 - Enterprise Hadoop CDE Segment

(Layer 2 VPN) technologies are leveraged in limited, policy-enforced instances to extend secure Layer 2 domains between data centre zones where required, such as synchronising Hadoop racks without compromising network segmentation. The integration of BGP, OSPF, static routing, VRF, VXLAN, EVPN, and L2VPN forms a resilient, segmented, and PCI DSS-aligned routing and forwarding architecture—ensuring that the CDE remains isolated, protected, and auditable within Dancorp Analytics' broader infrastructure.

This routing design ensures that all traffic destined to or from the Cardholder Data Environment (CDE) is governed by deterministic, pre-defined paths, reinforcing both perimeter control and internal segmentation in alignment with PCI DSS best practices.

The Non-CDE Enterprise Network (172.16.0.0/16), which is connected via the BAS switch, has no Layer 3 route into the CDE and shares no Layer 2 adjacency. The BAS device is intentionally excluded from all forwarding paths and has no direct visibility into the Hadoop cluster network. However, there is a dedicated tap line provides the sole connection to the network management infrastructure (route to 10.168.200.0/24 management network) this connection is carefully controlled to ensure that no route exists which would enable or allow any interaction with the CDE.

As shown in the topology diagram, the CDE is entirely contained within the enterpris's hadoop cluster network section. It is supported by dedicated top spine switches (hds-1, hds-2) and access switches (has-1 through has-ex), which collectively facilitate low-latency, high-throughput communication for sensitive cardholder data and large-scale analytical workloads. This infrastructure is subject to stringent access controls and both physical and logical isolation, ensuring compliance with PCI DSS Requirement 1.3 (PCI SSC, 2024, p. 22).

Adjacent to the CDE, the Management and Security zone is further segmented to enforce functional isolation and role-based access control. It includes components such as Net Management, Cyber Security, Net Logs, and Sec Logs, each confined to separate subnets and VLANs. These systems are explicitly denied direct Layer 2 connectivity and unrestricted Layer 3 access to the CDE. Within the trusted zone, the network management, security, and logging segment has been strategically provisioned to satisfy the rigorous demands of Requirement 2, which mandates the secure configuration and continuous hardening of all system components (PCI SSC, 2024, pp. 24–27). This segment of the architecture is designed as a centralised control and observability plane. The inclusion of dedicated servers for network administration, cybersecurity management, and security log retention illustrates an intentional approach to enforcing secure defaults and minimising vulnerabilities at the system level. Upon deployment to production, systems within the network management and security zone will be aligned with industry-recognised hardening standards, including the National Institute of Standards and Technology (NIST), Center for Internet Security (CIS) Benchmarks, Payment Card Industry Data Security Standard (PCI DSS), and Security Technical Implementation Guides (STIG). These collectively define best practices for secure configurations, access control, and system integrity. Incorporating these benchmarks—alongside directory services such as Active Directory for centralised authentication and role-based access—ensures that PCI DSS Requirement 2 is fully addressed. This combination enforces the elimination of default credentials, secures administrative interfaces, and upholds consistent policy enforcement across all system components.

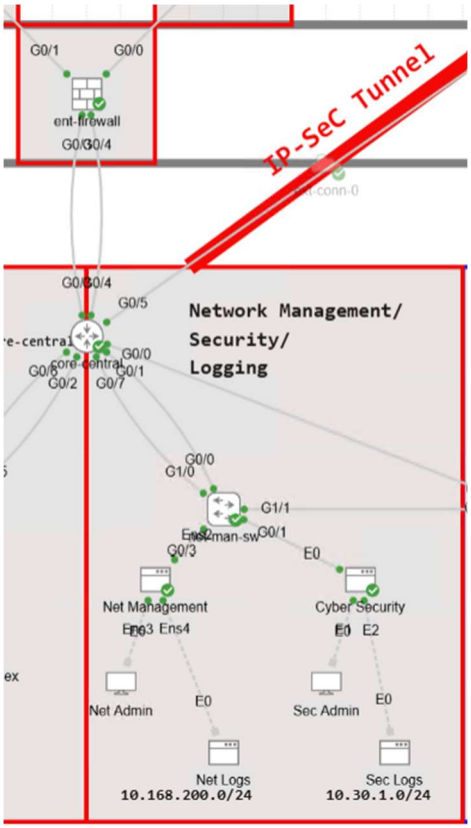

Figure 25 - Network Management, Security, and Logging Network

In addition, this zone is configured to host critical security services such as intrusion detection systems (IDS), anti-malware solutions, and SIEM tools for continuous monitoring and alerting. These components are instrumental in identifying anomalous behaviours, generating real-time alerts, and maintaining forensic visibility across the enterprise environment. This proactive monitoring ecosystem reinforces Dancorp's commitment to maintaining a hardened operational

state, ensuring all systems are subject to ongoing security evaluation, and that threats are mitigated before they materialise into breaches (PCI SSC, 2024, pp. 26–30).

Further augmenting the boundary defences, the proposed deployment includes a next-generation ASA firewall placed at the DMZ, which plays a dual role in external threat filtration and internal policy enforcement. This firewall, equipped with deep packet inspection and application-aware filtering capabilities, not only inspects packet headers but also examines payloads for malicious content. Functioning as a boundary monitoring system, the firewall has both a topological and logical vantage point—serving as the network's primary gatekeeper between the untrusted external domains (e.g., Azure, Internet, and ISP WAN) and the critical internal infrastructure. This strategic placement allows it to enforce high-confidence threat prevention while logging all ingress and egress traffic for compliance review.

Altogether, these provisions were consciously integrated into the design to uphold the integrity, availability, and confidentiality of system components, as mandated by Requirement 2 of the PCI DSS v4.0.1 standard. Through this layered security model—anchored in routing policies, hardened configurations, and intelligent boundary monitoring—Dancorp establishes a resilient, compliant, and security-conscious network architecture capable of withstanding both known and emergent threats (PCI SSC, 2024, pp. 13–30).

2.3.2 *Protect Stored Account Data*

The protection of cardholder data (CHD) represents the cornerstone of the PCI DSS framework, permeating not only Requirement 3 but influencing the rationale behind every other control within the standard. From network segmentation to access control and audit logging, the ultimate objective remains the same: to ensure that CHD—especially sensitive elements such as the Primary Account Number (PAN)—is never exposed, mishandled, or retained unnecessarily. This poses some of the strictest PCI DSS controls, especially for Sensitive Authentication Data (SAD) and Primary Account Number (PAN). Storing SAD post-authorisation is prohibited, and PAN must be encrypted—both must follow the defined approach and cannot be customised due to the high risk involved (PCI SSC, 2024, pp. 77–82).

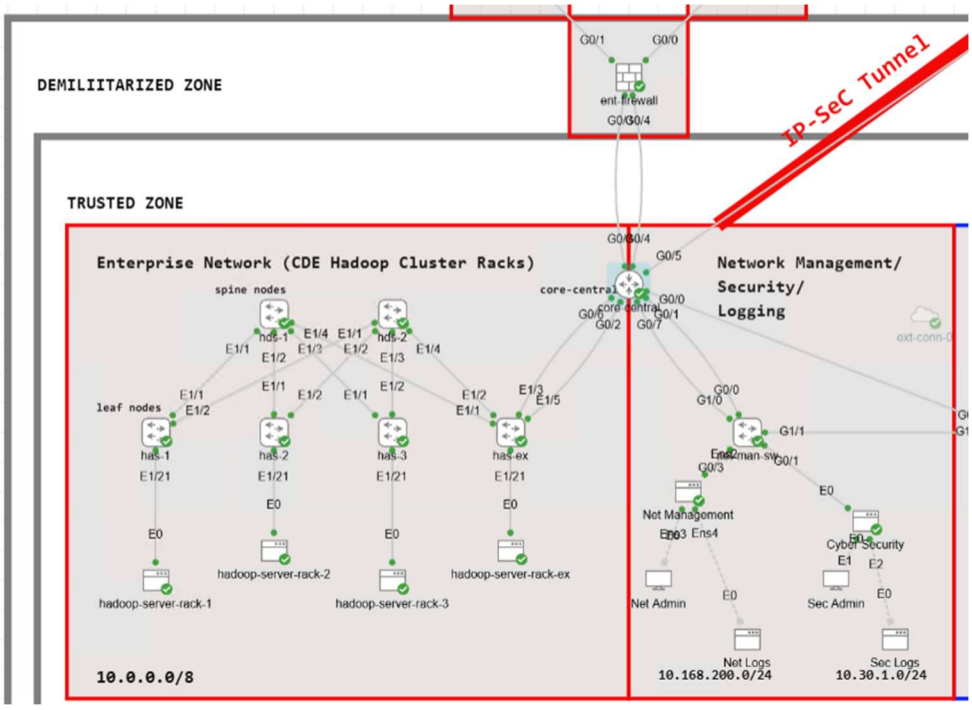

Figure 26 - Internal Data Protection Scope for PCI DSS

To meet this challenge, Dancorp Analytics incorporates account data protection as a foundational element of its network and system design. Rather than retaining sensitive data within the local infrastructure, Dancorp employs a hybrid architecture that offloads CHD to a simulated Azure endpoint for long-term storage and further processing. Within this design, data generated in the Cardholder Data Environment (CDE) is routed using a dedicated VRF instance (hadoop_cluster). This traffic is securely channelled to the core network, then inspected and processed through the organisation's ASA firewall, which serves as both a deep-packet inspection system and a security boundary. From there, authorised traffic is securely forwarded to Azure over an encrypted tunnel, ensuring end-to-end confidentiality and compliance enforcement.

This offloading strategy directly aligns with Requirement 3.1, which emphasises minimising data retention, and is further reinforced by Azure's own adherence to PCI DSS (Microsoft, 2024). As a PCI DSS-certified cloud service provider, Azure undergoes rigorous and regular audits, making it a suitable partner for storing CHD and managing sensitive cryptographic operations. Azure's infrastructure includes built-in controls for encryption at rest, access governance, file system isolation, and key lifecycle management—each of which addresses specific mandates under Requirements 3.5 and 3.6.

By integrating with Azure's compliance ecosystem, Dancorp effectively delegates the responsibility for storing and securing data at rest to a platform that exceeds its own operational capabilities, as permitted under PCI DSS guidelines. Nevertheless, the company retains full accountability by enforcing structured access control pathways, role-based permissions, audit trails, and continuous monitoring—all of which ensure that CHD remains protected, traceable, and only accessible under strict conditions.

This hybrid architecture not only supports scalable analytics and secure cloud storage, but also reinforces Dancorp's compliance strategy by reducing its local audit footprint and aligning operational decisions with best-practice security standards such as NIST SP 800-57, ISO 11568, and the broader principles of PCI DSS. In essence, the protection of account data permeates Dancorp's entire infrastructure design—from the VRF-based routing of CHD to the cryptographic guarantees provided by Azure—reflecting a security-first ethos designed to meet both the spirit and letter of PCI DSS in a dynamic fintech environment.

This also has another requirement. To meet the objectives of PCI DSS Requirement 4, Dancorp Analytics has designed its network to encrypt all incoming data originating from client environments before it enters the Cardholder Data Environment (CDE). These environments—such as remote customer sites or third-party partners—are not directly part of Dancorp's trusted internal infrastructure. However, they transmit sensitive analytics and cardholder data (CHD) for real-time processing within Dancorp's internal systems. As this information traverses' networks

not under Dancorp's exclusive administrative control, the company treats these paths as public or untrusted networks, regardless of the presence of private leasing agreements.

To validate compliance with PCI DSS Requirement 4.2, Dancorp conducted a Wireshark-based packet capture analysis on traffic entering through the leased-line router. The results confirm that all data transmissions between 101.101.101.2 and 101.101.101.1 are encapsulated using the Encapsulating Security Payload (ESP) protocol, part of the IPSec suite.

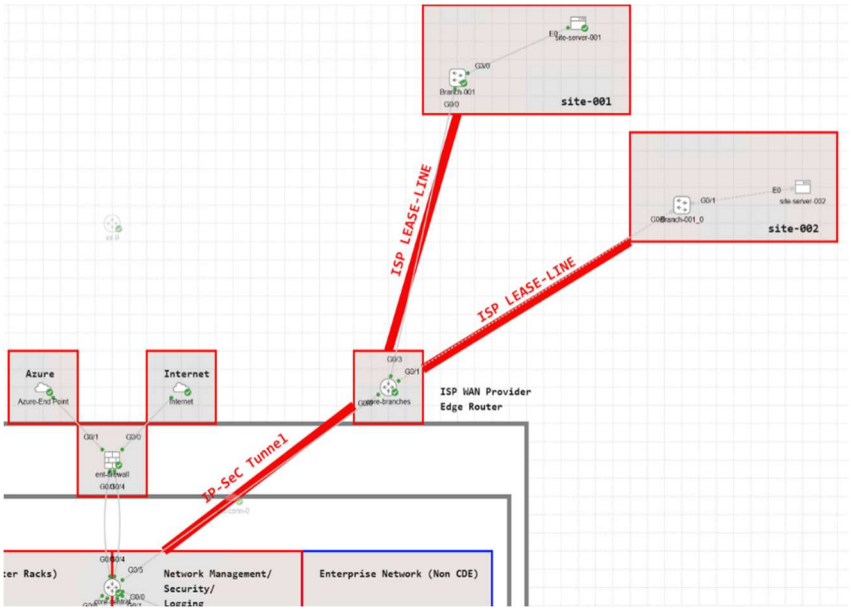

Figure 28 - External Data Protection Scope for PCI DSS

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Lengtl	Info
1	0.000000	101.101.101.2	101.101.101.1	ESP	314	ESP (SPI=0x6c5751cf)
2	0.027543	101.101.101.1	101.101.101.2	ESP	314	ESP (SPI=0x05d190b9)
3	0.999818	101.101.101.2	101.101.101.1	ESP	314	ESP (SPI=0x6c5751cf)
4	1.027831	101.101.101.1	101.101.101.2	ESP	314	ESP (SPI=0x05d190b9)
5	2.002382	101.101.101.2	101.101.101.1	ESP	314	ESP (SPI=0x6c5751cf)
6	2.033069	101.101.101.1	101.101.101.2	ESP	314	ESP (SPI=0x05d190b9)
7	2.994347	101.101.101.2	101.101.101.1	ESP	314	ESP (SPI=0x6c5751cf)
8	3.023086	101.101.101.1	101.101.101.2	ESP	314	ESP (SPI=0x05d190b9)
9	3.269545	52:54:00:1f:11:e3	CDP/VTP/DTP/PAgP/UD…	CDP	417	Device ID: core-central.dancorp.local Port ID: GigabitEthernet0/5
10	3.918534	52:54:00:0a:16:7b	CDP/VTP/DTP/PAgP/UD…	CDP	404	Device ID: core-branches Port ID: GigabitEthernet0/0
11	4.000818	101.101.101.2	101.101.101.1	ESP	314	ESP (SPI=0x6c5751cf)
12	4.028581	101.101.101.1	101.101.101.2	ESP	314	ESP (SPI=0x05d190b9)
13	4.995175	101.101.101.2	101.101.101.1	ESP	314	ESP (SPI=0x6c5751cf)
14	5.028369	101.101.101.1	101.101.101.2	ESP	314	ESP (SPI=0x05d190b9)
15	5.348738	52:54:00:1f:11:e3	52:54:00:1f:11:e3	LOOP	60	Reply
16	6.005414	101.101.101.2	101.101.101.1	ESP	314	ESP (SPI=0x6c5751cf)
17	6.037381	101.101.101.1	101.101.101.2	ESP	314	ESP (SPI=0x05d190b9)
18	6.087367	52:54:00:0a:16:7b	52:54:00:0a:16:7b	LOOP	60	Reply
19	6.244520	101.101.101.2	101.101.101.1	BGP	73	KEEPALIVE Message
20	6.507151	101.101.101.1	101.101.101.2	TCP	60	179 → 55005 [ACK] Seq=1 Ack=20 Win=15282 Len=0
21	7.011077	101.101.101.2	101.101.101.1	ESP	314	ESP (SPI=0x6c5751cf)
22	7.037693	101.101.101.1	101.101.101.2	ESP	314	ESP (SPI=0x05d190b9)
23	7.993295	101.101.101.2	101.101.101.1	ESP	314	ESP (SPI=0x6c5751cf)
24	8.025526	101.101.101.1	101.101.101.2	ESP	314	ESP (SPI=0x05d190b9)

Figure 29 - Wireshark Capture Showing Encrypted Data-in-Transit over IPSec

A packet capture analysis conducted on a tap on the connection of Dancorp's leased-line router reveals consistent use of the Encapsulating Security Payload (ESP) protocol, validating the operational enforcement of IPSec encryption as required under PCI DSS Requirement 4.2. The capture (See Figure 21) shows traffic between source 101.101.101.2 and destination 101.101.101.1 using ESP. This snapshot demonstrates that encryption-in-transit is actively implemented and

verifiable, further supporting Dancorp's layered compliance posture and real-time security monitoring strategy. Although the leased lines facilitating this communication are managed by regulated transmission providers who themselves are subject to PCI DSS compliance audits as per Requirement 12.8 and 12.9 (PCI SSC, 2024, pp. 291–292), Dancorp does not assume compliance by association. Instead, it applies a defense-in-depth approach, treating the ISP as an external entity and reinforcing the transmission path with its own encryption, sanitisation, and security protocols.

In operational terms, the CHD received over the leased lines is routed through a dedicated VRF (hadoop_cluster), this is to ensure that it is isolated from general traffic and securely forwarded to the ASA firewall. There, the firewall decrypts the traffic, applies policy enforcement, and passes it to the internal Hadoop cluster for real-time analytics processing. This process creates an end-to-end protected data flow, where both transit and post-transit states are continuously monitored, logged, and hardened against attack.

By adopting this approach, Dancorp fulfils not only the letter of Requirement 4, but also the broader PCI DSS goal of ensuring confidentiality, integrity, and accountability in environments exposed to network-based threats. The encryption algorithms employed conform to the definitions of "strong cryptography" as outlined in Appendix G of the standard (PCI SSC, 2024, p. 380. This hybrid architecture underscores Dancorp's overarching commitment to architectural resilience, regulatory alignment, and trustworthy data handling, and reaffirms its position as a security-conscious fintech enterprise operating in strict alignment with the principles of PCI DSS.

2.3.3 ***Security Operations and Compliance Controls***

The Security Operations and Compliance Controls zone has been architecturally provisioned to support critical components of enterprise security governance: maintaining a vulnerability management program, enforcing strong access control measures, and enabling continuous monitoring and testing of network infrastructure. This dedicated segment ensures centralized oversight of threats, access, and system behavior, enhancing Dancorp's operational resilience.

In line with PCI DSS Requirements 5 and 6, the infrastructure supports an effective vulnerability management program by incorporating controls designed to protect systems and networks against malicious software and ensuring secure systems and software development. The planned integration of Security Information and Event Management (SIEM) systems, vulnerability scanners, and endpoint monitoring platforms allows proactive identification and mitigation of vulnerabilities. Administrative workstations, such as Sec Admin, manage regular patch cycles and enforce industry-standard secure configuration baselines, including DISA STIGs, reducing potential threats and limiting security exposure (PCI-DSS-v4_0_1.pdf, p. 119).

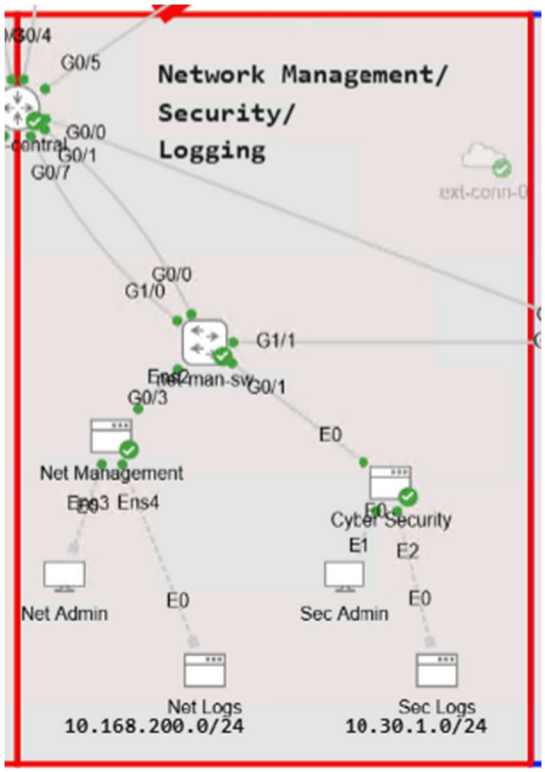

Figure 30 - Provision Block for Security Operations and Compliance Controls

To implement strong access control measures as outlined in PCI DSS Requirements 7 and 8, the environment leverages robust Authentication, Authorization, and Accounting (AAA) frameworks through RADIUS, TACACS+, and centralized identity management via Microsoft Active Directory. These measures restrict system component and data access based strictly on business needs, utilizing granular role-based access control (RBAC). Operational duties are segregated through separate administrative zones (Net Admin and Sec Admin), thus significantly reducing risks associated with privilege misuse or unintended access (PCI-DSS-v4_0_1.pdf, p. 161).

Lastly, consistent with PCI DSS Requirements 10 and 11, the architecture provisions dedicated logging servers (Net Logs and Sec Logs) designed for systematic logging and monitoring of all access to system components and data. These logs provide real-time event analysis and comprehensive historical records, supporting forensic investigation and continuous security validation. Regular internal assessments, vulnerability scans, and event correlation through SIEM integration ensure accurate monitoring, timely detection, and prompt incident response (PCI-DSS-v4_0_1.pdf, p. 236).

2.3.4 Maintain an information security policy

Maintaining an information security policy, as mandated by PCI DSS Requirement 12, is a critical operational step for Dancorp Analytics, which involves the development, documentation, and dissemination of a comprehensive policy framework tailored to its enterprise environment. This policy framework explicitly defines the organization's security objectives and clearly communicates roles and responsibilities concerning information security to all personnel, including employees, contractors, and third-party stakeholders (PCI DSS v4.0.1, p. 290).

While the primary focus of Requirement 12 is on an already running enterprise, within this design framework, provisions have been made to ensure seamless integration and effective adoption of these policies at the operational deployment stage. The policy mandates regular reviews and updates—at least annually or whenever significant infrastructure or operational changes occur—to proactively address emerging security threats and evolving business risks. This continual review cycle ensures the policy accurately reflects the dynamic operational landscape of the fintech sector, providing robust governance while accommodating growth and technological innovation.

3.0 Conclusion

The comprehensive network design presented in this thesis effectively demonstrates how rigorous adherence to PCI DSS v4.0.1 can be practically achieved within a fintech operational context. By methodically addressing each of the twelve PCI DSS requirements through meticulous segmentation, secure routing policies, robust encryption strategies, and comprehensive security operations planning, the architecture achieves robust protection of sensitive cardholder data. Also, the detailed provision for centralized management, proactive monitoring, and stringent access controls ensures compliance readiness and enhances overall security posture. Though limited by current emulation capabilities, the design successfully establishes a clear roadmap for Dancorp Analytics' operational resilience, compliance alignment, and future growth.

References

Ahamed, M. T., Venkatesh, B., & Samanta, D. (2018). Impact of virtual hadoop cluster scalability on the performance of big data. *International Journal of Computer Applications,* 182(38), 25–32. https://doi.org/10.5120/ijca2018917204

BitsPlease. (2020, August 25). *VXLAN BGP EVPN- L2VNI (Episode 1)* [Video]. YouTube. https://www.youtube.com/watch?v=faUd0vcRzI8&t

BitsPlease. (2020, August 25). *VXLAN BGP EVPN- L3VNI (Episode 2)* [Video]. YouTube. https://www.youtube.com/watch?v=pu21qr3b1GA&list=PLgnrksnL_Rn2GO1RX1-9T497iDFFwccnb&index

BitsPlease. (2021, February 1). *VXLAN BGP EVPN- External connectivity via VRF-LITE (Episode4)* [Video]. YouTube. https://www.youtube.com/watch?v=VJGucCOHvCQ&list=PLgnrksnL_Rn2GO1RX1-9T497iDFFwccnb&index

Canadian Centre for Cyber Security. (2024, June 14). Top 10 IT security actions: Number 4 - Harden operating systems and applications (ITSM.10.090). Government of Canada. https://www.cyber.gc.ca/en/guidance/top-10-security-actions-number-4-harden-operating-systems-and-applications-itsm10090

Cisco Systems. (2022). *External connectivity—VRF lite. In Cisco VXLAN BGP EVPN Fabric Configuration Guide.* https://www.cisco.com/c/en/us/td/docs/switches/datacenter/pf/configuration/guide/b-pf-configuration/External-Connectivity-VRF-Lite.pdf

Cisco Systems. (2024). *VXLAN BGP EVPN: Design and implementation guide.* https://www.cisco.com/c/en/us/td/docs/dcn/whitepapers/cisco-vxlan-bgp-evpn-design-and-implementation-guide.html

Cisco. (2025). *Cisco modeling labs - personal. Cisco Learning Network Store.* https://learningnetworkstore.cisco.com/cisco-modeling-labs-personal/cisco-modeling-labs-personal/CML-PERSONAL.html

Edureka. (2020, August 25). *What is hadoop cluster? Hadoop cluster setup and architecture Hadoop training* [Video]. YouTube. https://www.youtube.com/watch?v=g4E5kO7ykcE

Gurutech Networking Training. (2022, June 4). *Bank network design & implementation part 3 – Banking network system, enterprise network project 5* [Video]. YouTube. https://www.youtube.com/watch?v=NLMqmaBvD8Q&t

HandsonERP. (2014, February 15). *What is a Hadoop cluster?* [Video]. YouTube. https://www.youtube.com/watch?v=xd9hLHQrjnM

Jeremy's IT Lab. (2019, October 13). *Free CCNA: Network devices, day 1, CCNA 200-301 complete course* [Video]. YouTube. https://www.youtube.com/watch?v=H8W9oMNSuwo&list=PLxbwE86jKRgMpuZuLBivzlM8s2Dk5lXBQ

Kte'pi, B. (2024). Data analytics. In *Salem Press Encyclopedia of Science*. Grey House Publishing.

Louthan, L. (2024, October 21). *Working with the PCI DSS 4.0 compliance requirements.* [Video]. LinkedIn Learning. https://www.linkedin.com/learning/working-with-the-pci-dss-4-0-compliance-requirements/secure-configurations-building-hardening-standards-18928079

Malone, A. (2020, September 10*).* NIST and PCI SSC find common ground in development of software frameworks*.* PCI Perspectives Blog. *PCI Security Standards Council*. https://blog.pcisecuritystandards.org/nist-and-pci-ssc-find-common-ground-in-development-of-software-frameworks

Microsoft. (2024). *PCI DSS compliance in Azure.* https://learn.microsoft.com/en-us/azure/compliance/offerings/offering-pci-dss

PCI Security Standards Council. (2024). *Information supplement: PCI DSS Scoping and Segmentation Guidance for Modern Network Architectures* https://docs-prv.pcisecuritystandards.org/Guidance%20Document/PCI%20DSS%20General/PCI-DSS-Scoping-and-Segmentation-Guidance-for-Modern-Network-Architectures.pdf

PCI Security Standards Council. (2024). *Payment card industry data security standard: Requirements and testing procedures, v4.0.1.* https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf

Syafrizal, M., Selamat, S. R., & Zakaria, N. A. (2020). Analysis of cybersecurity standard and framework components. *International Journal of Communication Networks and Information Security (IJCNIS)*, 12(3). Retrieved February 02, 2025, from https://www.academia.edu/download/78607584/426.pdf

Venkataramanachary, V., Reveron, E., & Shi, W. (2020). Storage and rack sensitive replica placement algorithm for distributed platform with data as files. In *2020 12th International Conference on Communication Systems & Networks (COMSNETS)* (pp. 535–538). IEEE. https://doi.org/10.1109/COMSNETS48256.2020.9027415

Image References

Cover Image (1): - https://stockcake.com/i/network-server-cables_1297966_236778

Cover Image (2): - https://www.pexels.com/photo/a-woman-scanning-her-card-8834116/

Figure 1: Hadoop Cluster Architecture - https://www.youtube.com/watch?v=aBCDy-dJE0Y&t