FANSHAWE

Integrating a Corporate Merger Network (NAWI) | INFO6033 Fall 2024 – Group 6

Student Name	Student Number	Project tasks completed	Approved
(PM) Sunshine Cotejo	1140357	Project Manager Headed the Visio diagram submission 1. SD-WAN design 2. NAWI High level overview 3. GCWC & GAWC Environment Assisted with the overall documentation 1. Network Management Implementation 2. VPN Design for Offices and Remote Personnel 3. OpenDaylight SDN 4. Conclusion	Yes
Aashish KC	1164325	Assisted the Visio diagram submission 1. Regional Office Design 2. Dallas Head office Headed the overall documentation Assisted with Research and Documentation: 1. Failover Design 2. How the connectivity will function, between countries, sites, and SD-WAN 3. Network Management Implementation 4. OpenDaylight SDN 5. How Zero Trust Provide Additional Security	Yes
Saiganesh Jeyapandi	1154547	Headed the Presentation Slides Assisted the Visio design 1. Markham Data Centre Assisted with Research and Documentation 1. Executive Summary 2. GCWC & GAWC Environment 3. Modularized Branch, Regional and Data Centers 4. Benefits and Drawbacks of the Solution 5. SDN Datacenter design and its Benefits to NAWI 6. How Zero Trust Provide Additional Security	Yes
Ahmad Malkawi	1171774	Headed the Change Request Form Assisted the Visio design 1. Public Cloud Assisted with Research and Documentation 1. Tiered Hierarchical Design in Canada 2. Purpose and ROI for the Network Management module (SNMP) 3. Network Changes in Both Countries 4. How Networks will be Integrated 5. Public and Private Clouds for Canada and the US	Yes

Table of Contents

I. Executive Summary

Following the merging of Great Canadian Widget Company (GCWC) and Great American Widget Company (GAWC), there are overlapping customer bases and complementary products under one banner: North American Widget Inc. The acquisition is expected to increase revenue by 30%. Operations will be divided into Northern, Eastern, Western, Central, and Southern regions. Canadian operations will remain intact, capitalizing on their strong sales team and expanded product lines across North America.

The Board of NAWI expects to realize substantial cost savings and operational efficiency from the integration of IT systems and the migration from Frame Relay to an OpenDaylight SD-WAN architecture. Furthermore, a Zero Trust framework will be implemented to enhance security across the organization. The IT integration will make sure both companies are operating on one uniform and upgraded network design. The initial focus is to align GAWC's U.S. network with this design, while further assessments will be conducted for Canadian network modifications.

The merger also entails the use of Software Defined Networking, allowing the smoothing of IT operations to further increase agility and scalability. Application and database consolidation will take as high as two years, whereas the integration of the network has been one of the priorities to ensure fluent operations from all regions. Canadian Regional Offices will be re-organized as Districts under Toronto, Northern Region, within the organizational framework of NAWI. This project may not only increase the sales revenue, but also establish groundwork for NAWI's future expansion in Europe Region.

II. GCWC Environment

The Great Canadian Widget Company (GCWC) employs a tiered hierarchical structure, with its headquarters located in Toronto, which serves as the central office connecting various regions throughout Canada. The Toronto data center is situated at the head office, while the backup data center is in Markham. Regional offices are set up in the consolidated Southwestern Region, Montreal for the Central Region, Calgary for the Western Region, and Halifax for the Atlantic Region. Furthermore, each regional office supports branch offices in every city. GCWC has just implemented SD-WAN by configuring the Cisco router in the Toronto Head office. The preexisting VLANS are being utilized to isolate traffic flow.

Please refer to Figure 1 for the GCWC environment:

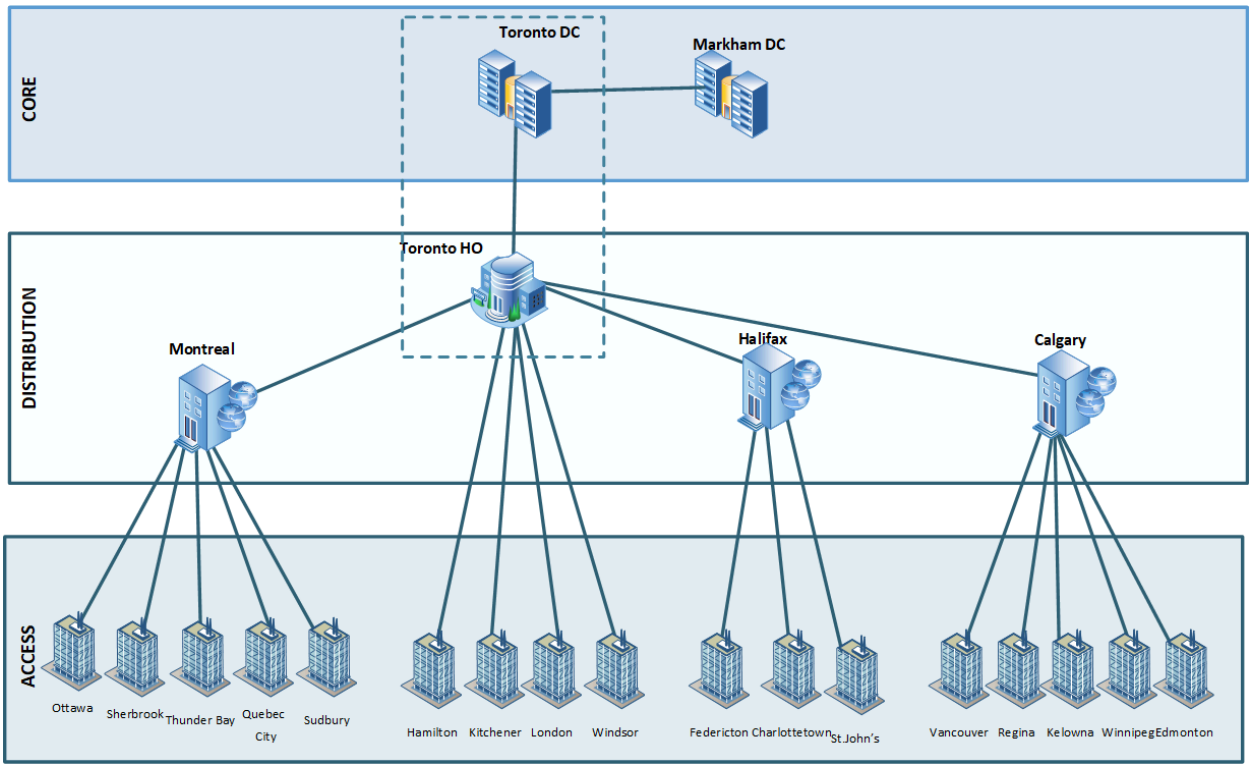

Figure 1GCWC Environment High Level Overview

III. GAWC Environment

Great American Widget Company (GAWC) manages the connecting networks in the US namely Dallas head office as well as the collapsed Southern Region, Boston for the Eastern

Region, Chicago for the Central Region, and San Francisco for the Western Region. They are currently in Frame Relay and will transition to SD WAN architecture like the GCWC. Please refer to Figure 2 for the GAWC environment:

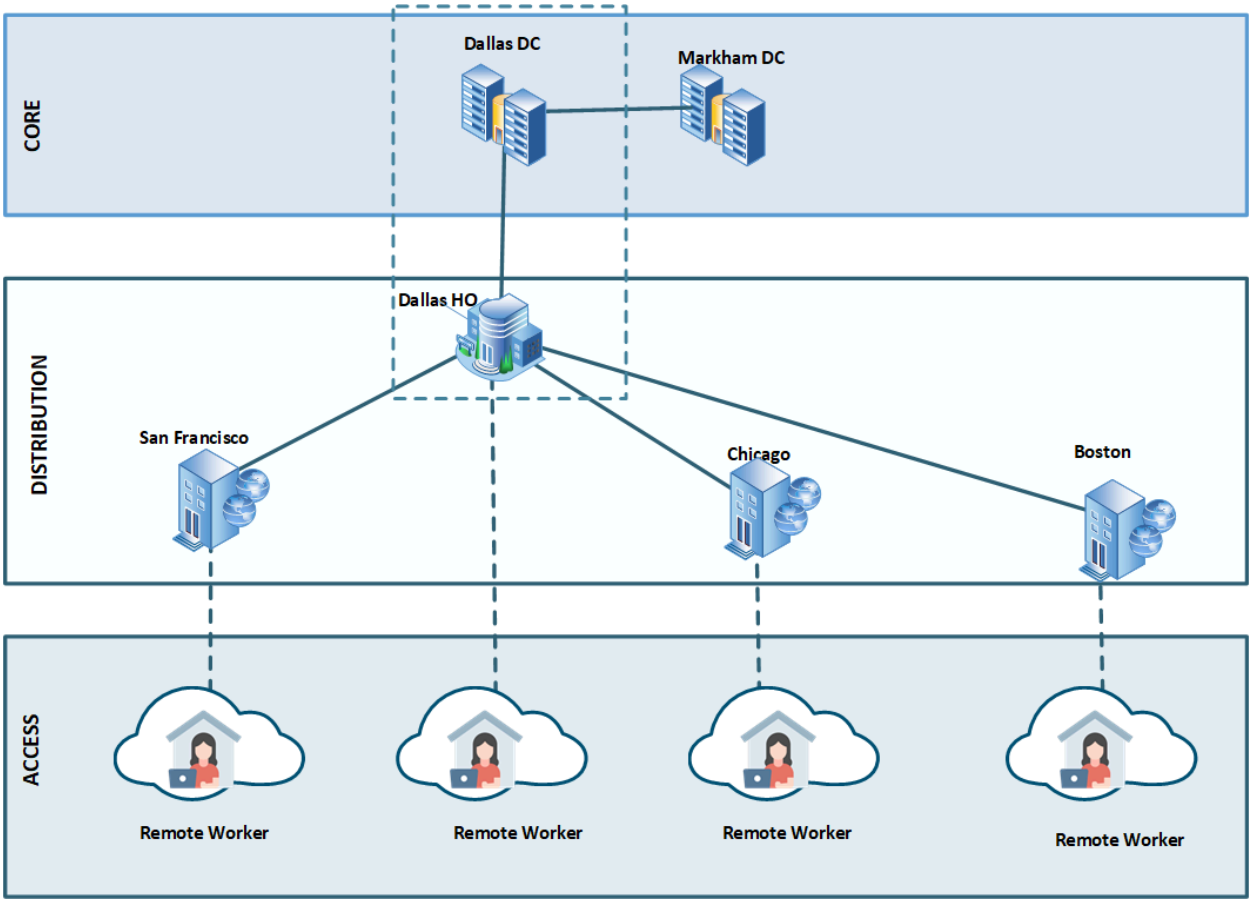

Figure 2 GAWC Environment High-Level Overview

IV. Current Environment

A. Modularized Branch, Regional and Datacenters

The current network infrastructure for the Great Canadian Widget Company (GCWC) and the Great American Widget Company (GAWC) follows a modularized design across their branch offices, regional sites, and datacenters. This segregation of the network into distinct modules allows for easier management, consistent application of policies, and enhanced scalability across all locations. By dividing the network into smaller, manageable segments, the organization can more efficiently monitor and maintain its operations. The modular design also allows for seamless scalability, enabling the network to expand as the company grows without compromising performance or security. This approach ensures that resources are allocated

optimally, and network management can be simplified, reducing the complexity of handling larger, more diverse environments.

B. Tiered Hierarchical Design in Canada

GCWC is structured using a tiered hierarchical design, which promotes efficient traffic management, effective troubleshooting, and robust security zoning. The tiered approach organizes the network into layers that serve different functions, such as the core, distribution, and access layers. Each layer has specific responsibilities, making it easier to manage and troubleshoot the network.

The GCWC core layer ensures high-speed data transfer and connectivity across Toronto data center and Markham backup datacenter. The distribution layer handles the routing and traffic control between different regional offices – Montreal for Central Region, Halifax for Atlantic Region, Calgary for Western Region and Toronto Head Office Finally, the access layer connects end devices to the branch network, with stringent security policies applied to ensure only authorized access.

C. Purpose and ROI for the Network Management module (SNMP)

OpenDaylight SDN leverages the SNMP protocol (in southbound traffic) to monitor and control routers, switches, and servers among other network devices (NetworkLessons.com, n.d.). It basically helps in viewing the real-time performance of networks by proactively identifying and resolving issues, thereby minimizing downtime and reducing the risk of costly outages. SNMP, through automated monitoring and alerts, reduces human effort and manually intensive tasks, freeing IT staff to focus on more strategic tasks. Looking from an SNMP ROI perspective, it enhances network reliability by optimizing resource use, avoiding pointless hardware costs, and boosting user satisfaction-all extremely cost-effective investments to help the maintenance of a robust IT infrastructure.

V. Proposed Solution

A. Network Changes in Both Countries

To optimize the network infrastructure for the NAWI, we are moving from full-mesh Frame Relay to OpenDaylight SD-WAN and Zero Trust solution. According to Dr Mukherjee (n.d.), one of the major drawbacks is a lack of flexibility and scalability; Frame Relay operates using static circuits, thus making it highly difficult for the network to adapt to ever-changing network demands or cloud services integration. With Frame Relay, there is also limited bandwidth efficiency since over-provisioning could be required to handle peak loads, and this

means increased costs. Lack of centralized management makes monitoring and optimizing network performance very hard, especially across multiple sites. Contrasting with this, SD-WAN provides dynamic bandwidth allocation, has centralized control, and better cloud integration, making it more cost-efficient and agile for modern networks.

Below are the modifications triggered by SD-WAN update at the Markham and Dallas data centers:

1. Deployment of SDN (OpenDaylight SDN Controller)
    - Integrate an OpenDaylight SDN controller to centralize network management, allowing for fine-grained control over traffic flows and automated policy enforcement across both data centers.
2. SDN Underlay Network
    - Enable dynamic routing and traffic optimization by using SDN protocols with NETCONF in the Southbound Interface, ensuring seamless communication and configuration management across the network.
    - The RESTCONF on the NBI side can be integrated with different scripting languages e.g. Python, Java to automate network operations.
3. SDN Overlay Network
    - We deployed network configurations to Azure Public Cloud through Azure ExpressRoute circuit over the Internet.
4. Spine-Leaf Architecture Implementation
    - Replace the traditional network topology with a spine-leaf topology in both data centers, regional and head offices. This architecture supports low-latency, high-bandwidth communication and redundancy (Kumar et al., 2023).
    - Set up two (2) spine switches and four (4) leaf switches in the regional office for cost efficiency
    - Set up four (4) spine switches and six (6) leaf switches in head office and data center due to their heavy-duty activities
5. Cisco 8000 Series Routers and Cisco® Catalyst Switches
    - We are using Cisco 8000 Series Routers and Cisco® Catalyst Switches to facilitate dynamic traffic forwarding and easier management of routing policies.
    - We also implement standby switches in data centers in case the primary switch fails
6. Cross-Data Center Mirroring
    - Add on-premises servers and private cloud in Markham data center to act as backup for the Dallas data center
    - Use BGP to route to Markham DC in the event that Dallas data center fails
7. Add additional connection of preexisting Public Cloud Infrastructure

- Implement Azure ExpressRoute for a high-bandwidth private connection to Azure Cloud infrastructure to connect Dallas US to Markham DC
- Set up IPSec VPN tunnel for automatic failover in case of connectivity to Azure ExpressRoute is down

8. Uninstall the Frame relay infrastructure

Additionally, Regional offices in Canada, the branch offices, and the Toronto datacenter will not be changed. The Toronto Head Office will be re-named as NAWI Northern Region. NAWI has moved to incorporate SDN into its refreshed architecture. The Markham data center will be the main backup site for the Dallas data center.

B. How Networks will be Integrated

To ensure seamless integration between the networks across both countries (Canada and the US) and the global sites, we will implement a Software Defined Networking (SDN) architecture utilizing OpenDaylight as the central controller. Integration will involve the following key steps:

1. **OpenDaylight SDN**
   a. The OpenDaylight SDN will connect to the network devices, Cisco 8000 Series Routers and Cisco® Catalyst Switches, by leveraging RESTCONF in northbound and NETCONF in southbound. Cisco routers will use OpenDaylight by configuring NETCONF on the routers for secure communication via SSH.
2. **Azure Express Route**
   a. We utilize Azure ExpressRoute to establish a high-speed, private connection directly to the Azure Public Cloud infrastructure. This ensures a reliable and secure connection for our operations.
3. **IPSec VPN Tunnel**
   a. In case the Azure Express Route private connection to Azure public cloud fails, we set up an IPSec VPN Tunnel as a backup.

C. SDN Datacenter design and its Benefits to NAWI

In a Software-Defined Network (SDN) data center design, the spine-and-leaf architecture creates a non-blocking, high-performance network fabric. Each leaf switch connects to every spine switch in the network. The data center has four (4) spine switches and six (6) leaf switches, each leaf switch will have connections to all 4 spine switches. Typically, 10G, 25G, 40G, or 100G links are used for these connections, depending on bandwidth requirements. The

connections are north-south, meaning data travels from the leaf (access layer) to the spine (core) and vice versa. The leaf switches will be connected to servers. Deploying a spine-leaf topology can maintain connections by ensuring low latency and high bandwidth (ServerSimply, 2024). This supports dynamic routing and traffic optimization that can be easily managed by OpenDaylight.

Spine Layer	Use the Cisco Catalyst 9500 series for their modular, high-bandwidth capabilities (Cisco, n.d.)
Leaf Layer	Use the Cisco Catalyst 9300 series depending on the performance and port requirements (Cisco, n.d.).

OpenDaylight SDN introduces centralized network management, protocol support and network automation. It helps us manage all network configuration, policies and traffic control flows across all Markham and Dallas data centers.

The benefits of OpenDaylight SDN Data Center design to NAWI are the following:

1. ODL's vendor-neutral approach will support different kinds of network devices, thus protecting the investment of NAWI in existing hardware. This also prevents vendors' lock-in, enabling data centers to select the best devices that meet their specific needs and ensuring their flexibility in future upgrades (OpenDaylight, n.d.).
2. OpenDaylight SDN solution enables centralized management of the entire data center network by providing a single view and tap into control of all the network devices. Complexity because of large-scale environments is reduced, hence streamlined network operations (OpenDaylight, n.d.).
3. OpenDaylight SDN can thus automate the routinary network tasks of SDN data center such as configuration changes, provisioning, and updates while reducing manual interventions and minimizing errors. This leads to faster deployments, quicker responses to changing requirements, and more consistent configurations across the network.
4. OpenDaylight architecture is modular and scalable, making it appropriate for data centers of any size. As these data centers expand, the OpenDaylight architecture can easily scale to accommodate increasing devices and services without a complete network overhaul to support dynamic expansion.
5. Centralized security policies could be enforced with OpenDaylight to make the implementation of consistent security measures easier within the network. Integration with third party security solutions can enhance security by controlling access based on the context of users and devices.
6. OpenDaylight Project has strong community support. Their founders are Cisco, Citrix, Ericsson, and Big Switch Networks (SDXCentral, n.d.)

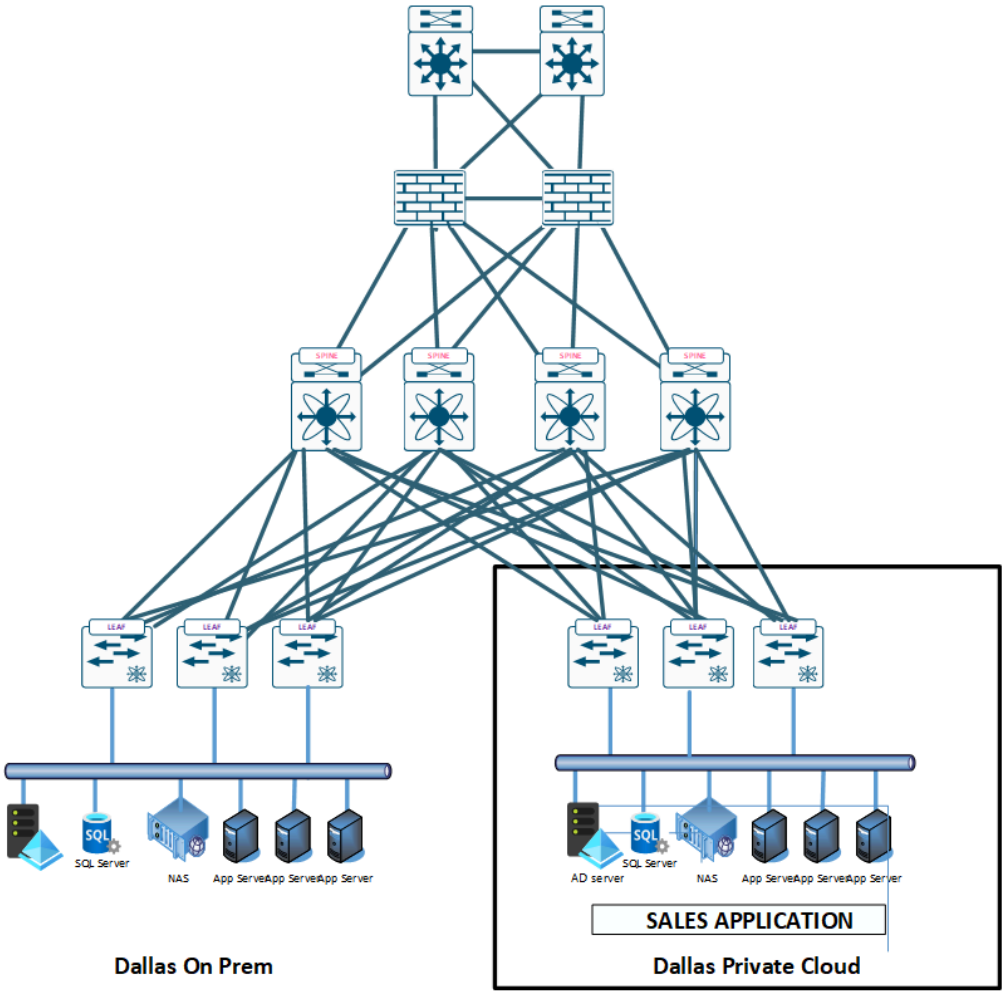

Figure 3 NAWI SDN DataCenter Design

D. Public and Private Clouds for Canada and the US

Private cloud infrastructure in Dallas Center will be maintained by the US Sales employees. They will have complete control of the files and documents stored in the private cloud. Private cloud infrastructure in Toronto Data center will remain as is.

NAWI deploys Azure public cloud infrastructure of the Dallas Data center for scalability and reliability. However, we will follow strict data security and regulatory compliance. Microsoft Azure (n.d.) needs to follow the rules and regulation on data residency requiring data to be stored in a specific geographic location to allow them to choose data centers in the US or Canada. In short, Canada-specific data remains in Toronto. U.S.-specific data is managed in Dallas.

E. How the connectivity will function, between countries, sites, and SD-WAN

The connection between different network infrastructure, i.e., regional sites, head offices and SD-WAN is ensured with the help of different combined planes within the SD-WAN. This makes sure that the connection is seamless across different locations globally.

Data Plane

This plane basically takes control over the flow of data between different sites such as Chicago, Dallas, San Francisco, Toronto, Boston, and Markham via NETCONF. This ensures that there is redundancy and flexibility in the network. Each site is connected to the SD-WAN via the edge routers, this will form a mesh network for direct site-to-site like connection reducing the latency. OpenDaylight implements Azure ExpressRoute and IPSec VPN tunneling as backup to Azure Public Cloud where the traffic takes the low-latency path and secure encrypted path.

Control Plane

Within OpenDaylight SDN the control plane is the brain of the whole network. This plane can communicate with all the networking devices within the data plane like routers, switches and even the edge nodes with the help of northbound API (RESTCONF) and southbound API (NETCONF). This controller can also work dynamically as well by determining the best path for traffic flow by calculating different types of factors such as latency, bandwidth, link health, etc.

We will be using BGP for managing the east west traffic as we should consider scalability routings, managing data traffic based on the policies and also mainly integrating the new network with the old one. BGP also supports the efficient distribution of routes between the controllers and other sites (Cloudflare, 2018).

Application Plane

OpenDaylight also integrates an orchestration layer with the help of northbound APIs. This makes it easier to apply SDN policies for QoS and security to align with business needs. This application layer also helps to route traffic between VLANs in an isolated or prioritized manner in OpenDaylight policies (Medeiros et al., 2015).

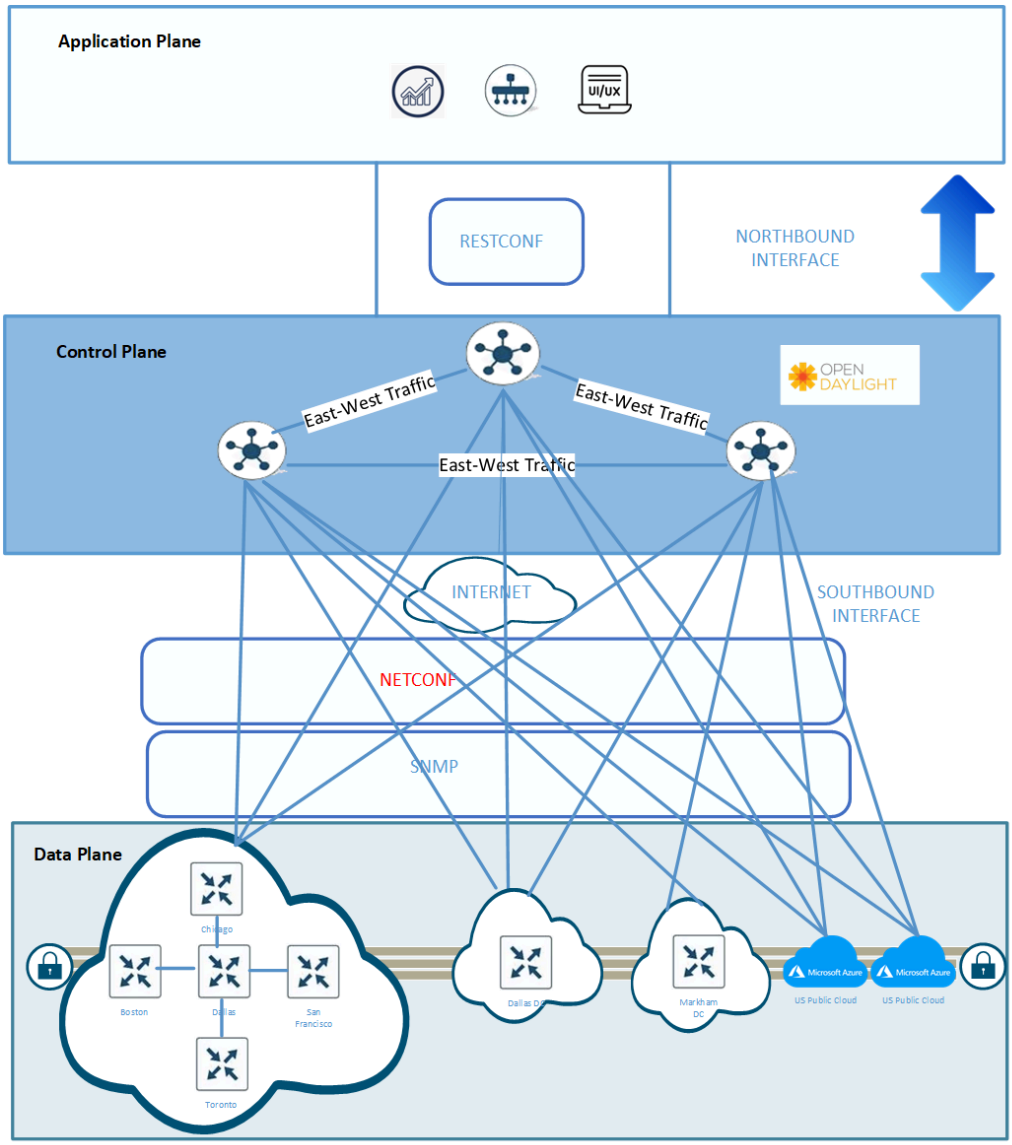

Figure 4NAWI SD-WAN Architecture Design

F. How Zero trust provide additional Security

A zero-trust environment always follows these two principles. *"Never Trust, Always Verify"* and *"Always give Least Privilege Access"*. Every device, users and applications should have limited access to resources based upon the role and must be authenticated and authorized in the company.

Identity and Access Management (IAM)

MFA, RBAC, and least privilege access may be enabled by Azure Active Directory (now, Microsoft EntraID) through Conditional Access Policies in such a way that a variety of

verification factors can be demanded for security of authentication. Roles based on user/group responsibilities using built-in or custom roles for data handling will be defined via RBAC. Also, it may implement the least access required with a one-time-only administrative level by granting users and resources the minimum levels necessary for accomplishing their needs through Privilege Identity Management (PIM). Further, set up Conditional Access policies to block access based on risk or location and monitor user activity with Azure AD Identity Protection to make sure Zero Trust principles are followed (Microsoft, 2024).

Policy Enforcement

Palo Alto NGFW serves as a critical Policy Enforcement Point (PEP) within the SDN architecture. It inspects both north-south and east-west traffic and enforces security policies that restrict access to only those users or devices that have been authenticated and authorized for the requested NAWI resources.

Microsegmentation

Palo Alto NGFW divides the NAWI networks into smaller, isolated environments to limit lateral movement. For example, we only allow HTTPS over HTTP, SFTP over FTP.

Data Protection

In Azure public cloud, we will encrypt data at rest with AES and data in transit with TLS to ensure Personal Identifiable Information (PII) data is protected.

Network Security

IPSec VPN tunnel ensures a secure connection between data centers, i.e., Dallas and Markham, and regional offices. We use Palo Alto firewalls for site-to-site connections. OpenDaylight can manage and configure Palo Alto firewalls through supported protocols like NETCONF or REST API.

Continuous Monitoring

We will set up Grafana for monitoring by collecting telemetry data from OpenDaylight or other tools like Prometheus and use it to create dashboards for visualizing network activity, flow statistics, and policy enforcement. We configure alerts in Grafana for anomalies, unauthorized access, or policy violations to ensure real-time Zero Trust monitoring and response User guide: Time series data repository (TSDR), (n.d.).

G. Failover Design

Firstly, we plan to set up OpenDaylight controllers in a cluster manner for the maximum redundancy and high availability of the network. It will use an alternate SDN controller if the

primary controller fails, the same data flow table and policies synchronized over all its controllers (Pioth, 2023).

Secondly, the Dallas Data center will have a mirror backup data center, Markham Datacenter. This failover design provides active/active configuration to ensure simultaneous update in network configurations. Moreover, for the automated failover path from regional and head office to the Markham backup data center it will be managed by the Border Gateway Protocol (BGP). We will be using BGP on all edge routers and SD-WAN for external connections. With BGP, if the connection to the Dallas DC fails it will first withdraw the routes (advertised prefixes). After that it will search for the alternative path to the Markham DC with the help of predefined alternate routes while configuring the SD-WAN. Here, BGP can help update the new SD-WAN policies for making; now Markham as the primary DC (Gerend, 2021).

Lastly, our SDN solution has added the spine-leaf architecture – four (4) Cisco Catalyst 9500 Series Spine switches and six (6) Cisco Catalyst 9300 Series Leaf switches that will be connected in full mesh topology. This spine-leaf architecture inherently supports an active-active configuration which means that the traffic always has the same number of hops from its next destination, so latency is lower and predictable (ServerSimply, 2024).

H. Network Management Implementation

We opted OpenDaylight (ODL) as our SDN solution where the control and management of the network are centralized in an SDN controller. OpenDaylight provides a robust platform to manage, configure, and monitor network devices through a unified and programmable interface.

Both GCWC and GAWC will use Cisco 8000 Series Routers and Cisco® Catalyst Switches. The Cisco devices can be integrated into OpenDaylight through the following protocols:

A. NETCONF/YANG

Cisco 8000 Series Routers and Cisco® Catalyst Switches support NETCONF protocol. YANG models describe the configuration and operational data structures, making programmability possible in the network elements. OpenDaylight can leverage NETCONF to connect with Cisco devices for configuration management, state information retrieval, and updating.

B. RESTCONF

According to Singh (2021), RESTCONF uses the HTTP protocol for transport while supporting XML and JSON data encoding. RESTCONF retrieves and pushes network configuration using the YANG data model structure.

C. SNMP

We utilize the SNMP (Simple Network Management Protocol) for device configuration and monitoring.

D. OpenDaylight Group Based Policy

This will allow the network devices to be grouped together according to their purpose like web group or database group (Oswalt, 2014).

E. **Prometheus and Grafana**

Prometheus collects metrics data from OpenDaylight Calcium and Grafana will import those to visualize in a graphical manner.

I. VPN Design for Offices and Remote Personnel

NAWI will have the remote users who will initiate a VPN connection using the Palo Alto Global Protect VPN client to the Dallas head office's VPN Gateway. The VPN Gateway authenticates the user, and once approved, grants access to resources available in the corporate network. OpenDaylight does not inherently provide an IPSec tunnel, so we need to configure the Palo Alto NGFW to create a VPN tunnel. The regional offices communicate directly with the Dallas head office over site-to-site VPN tunnels. Traffic is encrypted end-to-end using IPsec, ensuring confidentiality and integrity. Dallas datacenter connects to the Dallas head office using secure, redundant VPN tunnels.

Lastly, we implement a VPN tunnel in the edge router of the head office failure domain to perform data hiding and isolate the traffic of the northern region. We leverage the Palo Alto Panorama for centralized management and visibility of Palo Alto Networks firewalls and VPN tunnels.

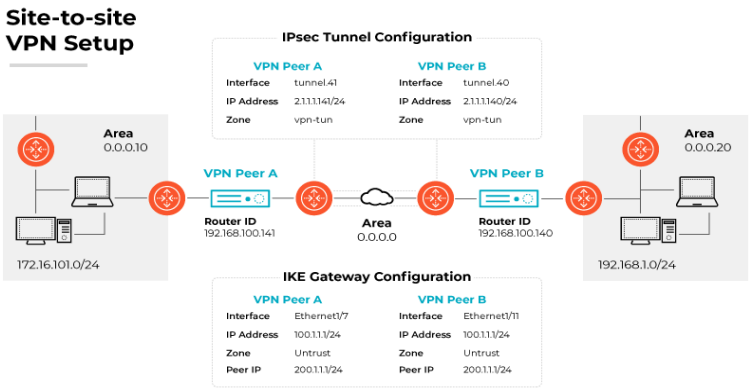

Figure 5 Site to Site VPN Setup (Palo Alto Networks, n.d.)

J. Ability for Future Expansion

As per our current network we have shown the future expansion feature as the different WAN edge router to expect the upcoming expansion to Europe region. These WAN edge routers will be deployed in Dallas and Markham data centers will be managed by OpenDaylight SDN Controller. SD WAN provides features like plug and play for centralized policy management. The new devices that are being added to the SD-WAN can be pre-configured so that when connected to the network, those network devices will get the configurations automatically and will be ready to use. Similarly, with the help of centralized policy management, all the new devices from a new site once connected will automatically get the pre-configured policy once admins define it (Casey, 2021). We will be using NETCONF API for easier configuration of the newly added devices from the new sites. This protocol will automatically add the predefined policies and configuration required for the connection with the existing infrastructure which reduces the load of the manual input.

VI. Conclusion

The proposed solution provides the most flexible and modular architecture that can fit diverse networking needs, thus being quite economical for NAWI. Moving from full-mesh Frame Relay, the SDN architecture brings scalability and agility to the merged companies. Also, the spine-leaf architecture introduces redundant paths and consequently reduces latency and increases high performance.

While the transition to SD-WAN and Zero Trust architecture has a number of benefits related to network performance, security, cost savings, and scalability, there are challenges associated with implementation that an organization should be prepared for. These include but are not limited to potential integration complexities, hardware compatibility, company cultural resistance, costs, and ensuring user experience does not suffer.

To implement these technologies successfully, the following steps would be in order in a phased approach: (1) start pilot programs with OpenDaylight SD-WAN and Zero Trust in less business-critical parts of the network. (2) invest in IT teams' training on how to manage new technologies efficiently; (3) ensure clear communication and user engagement to reduce resistance to new access controls and security measures and lastly (4) work with the OpenDaylight Project community and service providers for seamless integration and compatibility.

In the long run, the benefits of SD-WAN and Zero Trust, including enhanced security, greater flexibility, optimized performance and future growth, outweigh the challenges of implementation, especially as digital transformation accelerates across industries.

VII. References

Casey, J. (2021, December 7). Understanding the capabilities of SD WAN. Netify. https://www.netify.com/learning/what-are-the-capabilities-of-sd-wan/

Cisco. (n.d.). *Limitations and restrictions: Cisco Catalyst 9500 Series switches, software release 17.9*. Retrieved November 26, 2024, from https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-9/release_notes/ol-17-9-9500/limitations_and_restrictions.html

Cloudflare. (2018). *What is BGP? | BGP routing explained*. Cloudflare.com. https://www.cloudflare.com/en-ca/learning/security/glossary/what-is-bgp/

Gerend, J. (2021, July 29). *Border Gateway Protocol (BGP)*. Learn.microsoft.com. https://learn.microsoft.com/en-us/windows-server/remote/remote-access/bgp/border-gateway-protocol-bgp

Jahan, R. (2024). *SDN Interconnection (SDNi) in OpenDaylight: Implementation and use cases* [PowerPoint slides]. Tata Consultancy Services. https://events.static.linuxfound.org/sites/events/files/slides/ODL-SDNi_0.pdf

Kumar, R., & Rodrigues, J. J. P. C. (2023). Spine-leaf architectures for data centers. *Journal of Network and Computer Applications*, 221, 103491.

Medeiros, B., Antonio, M., Melo, C., Antonio, M., & Raffael, D. (2015, May 18). Applying Software-defined Networks to Cloud Computing. https://www.researchgate.net/publication/283275261_Applying_Software-defined_Networks_to_Cloud_Computing/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6Il9kaXJlY3QiLCJwYWdlIjoiX2RpcmVjdCJ9fQ

Mijumbi, R., et al. (2022). The role of OpenDaylight in network programmability. *IEEE Communications Surveys & Tutorials*, 24(1), 3-25.

Microsoft. (2024, September 19.). *Identity management best practices in Azure*. Microsoft. Retrieved November 26, 2024, from https://learn.microsoft.com/en-us/azure/security/fundamentals/identity-management-best-practices

Microsoft Azure. (n.d.). Data residency in Azure. Microsoft. Retrieved November 24, 2024, from https://azure.microsoft.com/en-us/explore/global-infrastructure/data-residency

NetworkLessons.com. (n.d.). Introduction to SDN & OpenDaylight. Retrieved November 26, 2024, from

https://networklessons.com/cisco/ccna-routing-switching-icnd2-200-105/introduction-to-sdn-opendaylight

OpenDaylight: Open source SDN platform (n.d.). OpenDaylight. Retrieved November 22, 2024, from https://www.opendaylight.org/

Oswalt, T. (2014, September 11). *SDN protocols part 4: OpFlex and declarative networking*. Oswalt.dev. https://oswalt.dev/2014/09/sdn-protocols-part-4-opflex-and-declarative-networking/

Palo Alto Networks. (n.d.). *What is a site-to-site VPN?* Palo Alto Networks. Retrieved November 26, 2024, from https://www.paloaltonetworks.ca/cyberpedia/what-is-a-site-to-site-vpn

Pioth, J. (2023, January 30). How SD-WAN Failover Helps Keep Your Network Up. Coeosolutions.com. https://www.coeosolutions.com/news/sd-wan-network-up

SDxCentral. (n.d.). *OpenDaylight Project: Definition and overview*. Retrieved November 26, 2024, from https://www.sdxcentral.com/cloud/open-source/definitions/opendaylight-project/

Server Simply. (2024, May 6). *Understanding spine-leaf architecture: Revolutionizing data center networks*. Retrieved from https://www.serversimply.com/blog/what-is-spine-leaf-architecture

Singh, J. (2021). Deployment of SDN controller and configuring Cisco devices using NETCONF (Capstone Project, Master of Science in Internetworking, University of Alberta). https://era.library.ualberta.ca/items/e8ef05e9-9cf9-4fa5-ab0e-716d9a82f73c/view/fcc8d752-2610-49eb-a0bd-4049f78038da/Deployment%20of%20SDN%20Controller%20and%20configuring%20Cisco%20devices%20using%20NETCONF.pdf

User guide: Time series data repository (TSDR).(n.d.). OpenDaylight. Retrieved November 22, 2024, from https://docs.opendaylight.org/projects/tsdr/en/latest/user-guide.html