Apply Network Segmentation to a Traditional Data Center

Summary

Industry

Financial Services

Use Case

Apply network segmentation for effective protection of mission-critical applications and data in a traditional data center.

Business Benefits

Support the capital investment and lifespan of the traditional data center infrastructure while inherently protecting sensitive data (e.g., intellectual property, regulated data [PII and PCI]).

Operational Benefits

Continue to run legacy applications in the data center with an added degree of data security; minimize business disruption during the implementation of network segmentation; maintain consistent security and management across legacy computing and network perimeter environments.

Security Benefits

Reduce the ability of attackers to move freely across data center resources; reduce the risk of unauthorized insider access based on user visibility and privilege levels; minimize risk of data exfiltration from the traditional data center.

Business Problem

Despite the cloud computing trend, many financial institutions (FIs) still have significant capital investments in traditional IT infrastructure components in their data centers. These facilities typically contain essentially flat, open networks, as network segmentation for cybersecurity was not a consideration when these were built years ago. However, malicious actors continue to find success in such open environments, where much of the lucrative data and systems are readily accessible after compromising a device elsewhere in the network. Several years ago, a series of attacks on SWIFT member institutions brought this into sharp focus. In 2020, many FIs suffered ransomware attacks that stemmed from phishing or some other initial infection. Once inside the victims' networks, the malicious actors moved laterally in search of suitable targets to be encrypted for ransom or exposed to the public to cause reputational damage.

A move to public or private cloud computing offers an opportunity to include network segmentation or a complete Zero Trust philosophy in inaugural designs. However, not all business applications are virtualization- or cloud-friendly. Certain legacy and mainframe applications may be unsuitable for migration to the cloud, and these will continue to run in private data centers with traditional architectures. Moreover, capital investments already made in classic data center networks would not be discarded on a whim, instead typically serving out their life expectancy and depreciation accordingly. Consequently, this legacy infrastructure, its indigenous legacy applications, and their associated data also need the protection afforded by network segmentation for that duration. However, as these environments are home to mission-critical resources, they cannot tolerate business disruptions even during such a transition.

Business Drivers

To maximize return on investment in traditional data center infrastructure while ensuring the full protection of business-sensitive data, such as intellectual property, regulated data (e.g., personally identifiable information [PII] and payment card industry [PCI] data), and other non-public information, FIs need segmentation of the data center network. In years past, the design philosophy of a hardened, protected perimeter and a secure, trusted interior was sufficient. Today's landscape, with more sophisticated adversaries, multiple attack vectors, and insider threats, warrants the compartmentalization of the internal network to limit exposure of sensitive data and resources as well as minimize financial and reputational damage in the event of a data breach or ransomware attack. Proper segmentation of the internal network can also reduce the scope of PCI audits by demonstrating clear separation of cardholder data environments from the rest of the IT infrastructure. Over the past few years, new consumer privacy regulations (e.g., GDPR, CCPA) have further raised the stakes for all enterprises to properly protect customer information.

Traditional Approach

Networking and security teams have historically relied on protections at the network perimeter to secure the entire enterprise. The internal network was deemed trusted and secure. While everything outside was considered "dirty," everything on the internal network was considered "clean," and application traffic would flow unrestricted. Consequently, there was no reason to deploy segmentation gateways internally for security purposes. Back then, applications were simpler and typically had single functions. Today, applications are multifaceted and handle several functions, such as messaging, file sharing, and screen sharing. Over time, malicious actors have become experts at finding ways to break into enterprise networks. This has made the open internal network a cybersecurity liability.

From purely a network perspective, separating the data center from end user environments is a reasonably simple approach. However, introducing network segmentation to an existing data center network is not to be taken lightly. Inserting any new device into live traffic flows always carries some risk of business disruption. For mission-critical and/or mainframe applications in a traditional data center, this is a daunting proposition despite the anticipated benefits of network segmentation. The use of traditional firewalls for this purpose further exacerbates the risk, as they cannot distinguish between multiple applications that use the same port numbers.

Palo Alto Networks Approach

An alternative model for information security, Zero Trust is intended to remedy the deficiencies of perimeter-centric strategies and the legacy devices and technologies used to implement them. This is accomplished by promoting "never trust, always verify" as its guiding principle. With Zero Trust, there is no default trust for any entity—including users, devices, applications, and packets—regardless of what it is or where it resides on the corporate network. In addition, it becomes mandatory to verify that authorized entities are always doing only what they're allowed to do.

In terms of moving toward a Zero Trust model, it is not necessary to wait for the next comprehensive overhaul of the organization's entire network and security infrastructure. A Zero Trust architecture is conducive to progressive implementation. To that end, segmenting the traditional data center from the various end user environments can be viewed as a step toward Zero Trust. The use of Palo Alto Networks Next-Generation Firewall (NGFW) as a segmentation gateway leverages its inherent networking capabilities for seamless deployment into an existing environment and allows for controlled introduction of security controls over traffic traversing the data center. The concept of Zero Trust extends the practice of network segmentation to granting access based on specific applications, allowing user access based on credentials, and controlling the content that can be sent across each segmentation point. Visibility into applications, users, and content allows you to confirm the identity of your data center applications and block unexpected or rogue users or applications from accessing the data center resources.

Network segmentation can be applied at numerous points in a network, but for the remainder of this paper, we will focus on the architectural considerations for, and highlight a customer deployment of, data center network segmentation to separate traditional computing resources from end user environments.

Architectural Vision

To segment traditional data center infrastructure from the branch and campus networks where end users reside, a high availability pair of NGFWs would serve to control all ingress and egress traffic. These appliances would be incorporated into the network architecture at the point where the traditional data center resources are aggregated, and they have visibility into all data flowing to and from legacy data center applications and services. This vantage point allows the NGFWs to function as the segmentation gateway for the traditional data center.

To minimize any potential disruptions to the environment, the security appliance is not deployed inline with the existing network devices, as shown in figure 2. Placed alongside the Layer 2 aggregation point, the NGFW can inspect and control inbound and outbound traffic without the need for physical recabling, changes to IP addresses of the original devices (servers), or the addition of new switches. Use of the VLAN tag rewriting capability of Palo Alto Networks NGFWs allows it to be logically in the flow of traffic, acting as both a Layer 2 bridge and an enforcement point. The advantages of this approach are that existing physical connections are

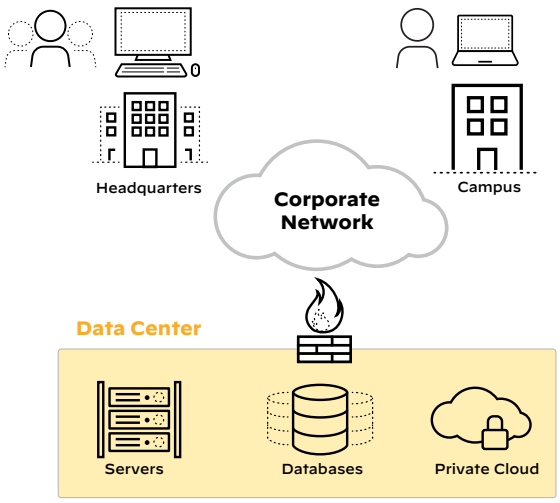

Figure 1: Network segmentation of data center from end user environments

untouched and desired traffic flows can be placed under firewall control one device at a time, if desired. This granularity allows for a controlled migration of traffic through the firewall, which is critical for the phased introduction of network segmentation to a live, traditional data center.

Actual Financial Services Customer Deployment

In this real-world example, one of the world's largest financial institutions has a traditional three-tier data center network design for a portion of its environment. The organization was not yet ready to rearchitect its entire data center, adopt an overall leaf-spine design, or migrate entirely to a private cloud model. Like many of its peers, this financial institution had an open internal network. This left its traditional data center network exposed to undesirable internal traffic, which the organization viewed as a significant security gap. Although there was no specific regulatory requirement for network segmentation, the institution saw the inherent value of this best practice and committed to the concept to get ahead of the game.

Ultimately, the institution chose Palo Alto Networks NGFWs to segment its traditional data center network from its end user population. This project was undertaken to improve the security of the IT environment by installing a mechanism to control end user access to critical data center resources as well as between those sensitive resources. Success was defined as the isolation of targeted applications and systems from one another, and from the internal network, while providing the connectivity required for business functions. As this effort was carried out against running environments, minimal changes to the existing data center architecture and IP address space were critical requirements to minimize risk. In short, the firewall deployment could not be inline, no server IP addresses could be changed, and traffic from specific servers had to be steered through the firewalls in a tightly controlled, phased migration.

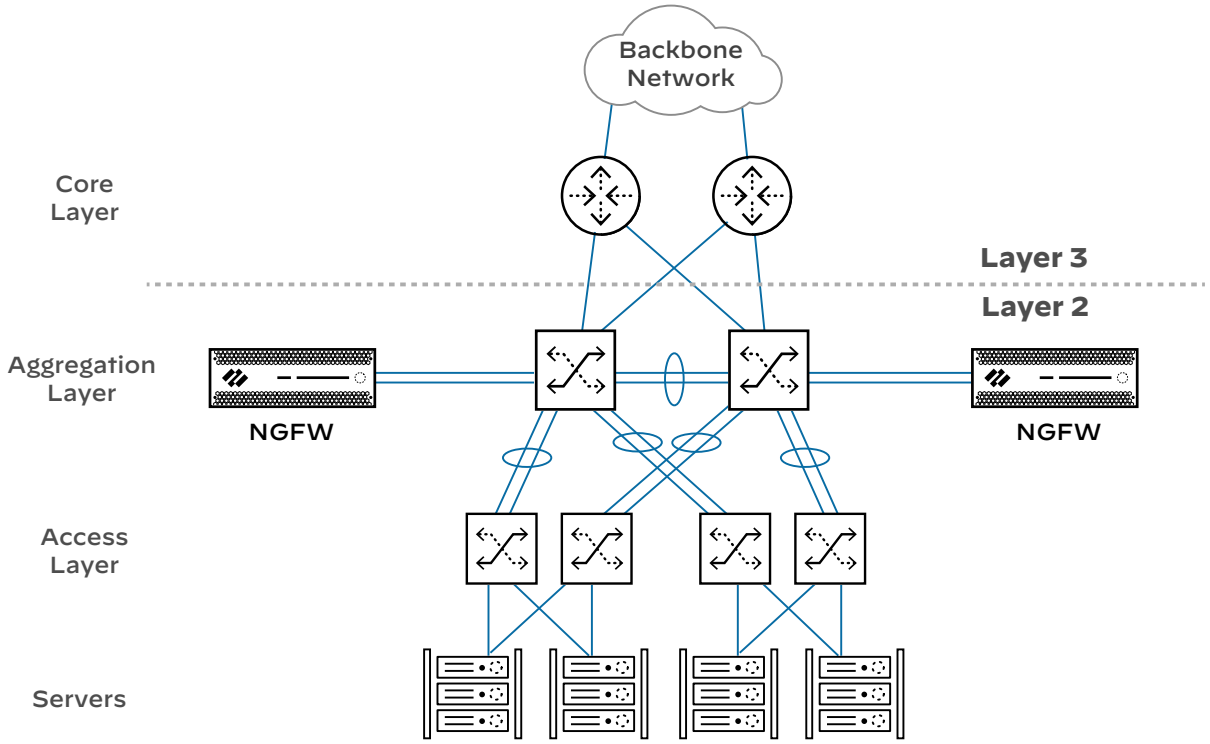

Figure 2: Transparent firewalls in a classic three-tier data center network design

A Layer 2 "firewall on a stick" design enabled the financial institution to control traffic flowing through the NGFWs by manipulating the VLAN assignment of the servers. As servers were moved to a new set of VLANs (one per application), traffic would be safely enabled by passing through the NGFWs. This allowed for precise, controlled migration of traffic to the firewalls for a phased implementation of network segmentation on the live data center.

Implementation Overview

Products Deployed

- NGFWs (PA-7000 Series) with the Threat Prevention security service
- Panorama™ network security management

How Customer Implemented Network Segmentation (High Level)

- Installed redundant Palo Alto Networks NGFW appliances at the data center aggregation layer, in a Layer 2, out-of-band configuration, to minimize physical disruptions to the live production environment.
- Secured north-south traffic to selected critical applications and systems in the classic three-tier data center architecture. The set of applications to be protected was defined by the institution's Risk and Audit organization.
- Secured east-west traffic within the traditional data center network using the same set of firewalls.
- Implemented firewall security policies based on application awareness through App-ID™ technology for granular control over traffic flows.
- Centrally managed all next-generation firewall instances with Panorama for consistent security policies across the entire three-tier data center network estate.

How Customer's Network Segmentation Works (High Level)

As selected traffic enters or leaves the traditional data center network, it passes through the out-of-band firewalls at the aggregation layer by virtue of VLAN tag rewriting. Traffic is then subjected to granular control policies based on App-ID and Content-ID™ technologies. NGFWs with application-based rules offer more specific and precise control over traffic than port/protocol-based firewalls can provide. Traffic is also inspected for known threats through the Threat Prevention security service, which includes intrusion prevention services.

To place traffic under the control of the NGFWs, servers are selectively reassigned to new (protected) VLANs. This is done to logically bundle servers belonging to a particular application into a common VLAN and steer that traffic through the firewalls. No server IP addresses need to be changed, which reduces risk to the production environment (see figure 3). This allows for a tightly controlled migration of traffic to the firewall—even as granular as one server at a time. Due to concerns over business disruptions, the customer ruled out a mass migration cutover for network segmentation. This level of control for a phased migration was a key requirement.

Within the traditional data center environment, traffic to/from servers on any of the protected VLANs would also flow through the firewalls. This facilitated safe enablement of server-to-server (east-west) traffic within the three-tier data center network.

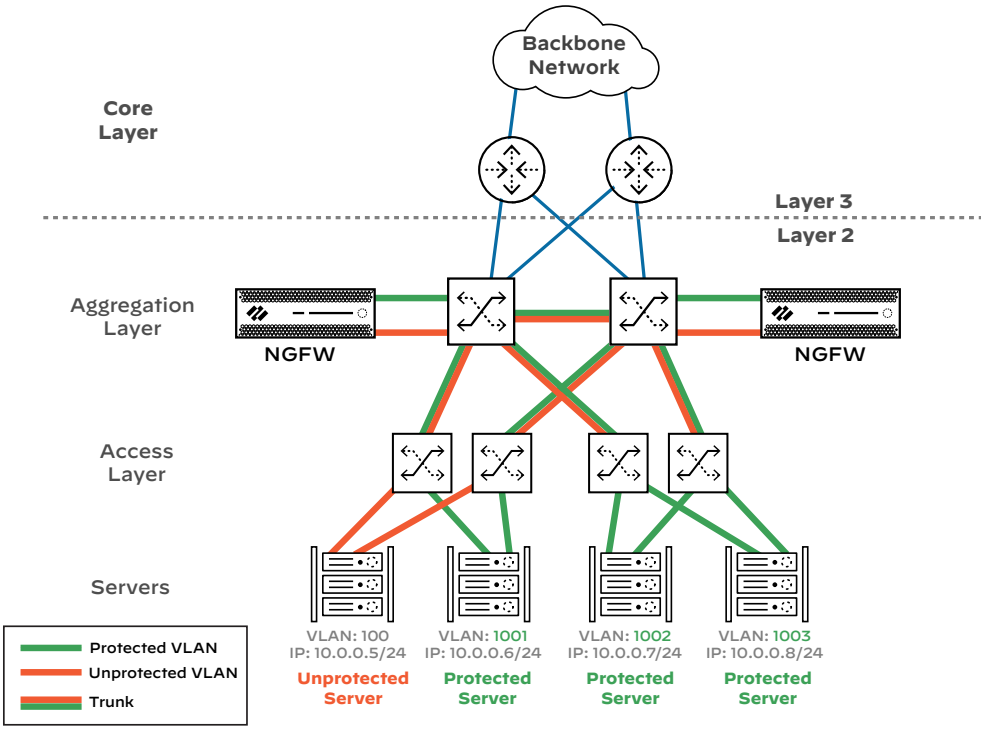

Figure 3: Unprotected and protected VLANs on one subnet

Benefits of Using Palo Alto Networks for Network Segmentation in the Traditional Data Center

Business Benefits

- Support the capital investments already made in the legacy data center while inherently protecting sensitive data, such as IP, regulated data, and other critical data, in these environments.

Operational Benefits

- Continue to run legacy applications in the traditional data center for the lifespan of that infrastructure, but with an added degree of data security.
- Minimize potential for business disruption during the implementation of data center network segmentation. Targeted traffic can be placed under NGFW control by modifying the VLAN associated with the server or group of servers. No physical recabling of the servers or access layer switches is required. Server IP addresses are untouched as well.
- Maintain consistent security and management across both traditional data center and network perimeter environments. Use of Palo Alto Networks NGFW appliances in both locations, along with Panorama, allows for a common management tool and consistency of security policies through the data center and network edge.
- Reduce time and resources required for PCI compliance audits, as the scope is minimized through effective network segmentation. Cardholder data is held in a separate environment (e.g., VLAN) protected by the NGFWs from the rest of the network.

Security Benefits

- Reduce the ability of an attacker to roam freely into and throughout the traditional data center.
- Minimize exposure by compartmentalizing systems and data belonging to specific applications and/or business units.
- Limit unauthorized lateral movement into and across the data center.
- Prevent exfiltration of data from the data center.
- Use better security controls—based on App-ID, User-ID™, and Content-ID technology—than firewall rules based on ports, protocols, and IP addresses can provide.
- Prevent previously seen and brand-new malware on the data center network.
- Reduce the risk of unauthorized insider access to data center resources.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com