DEVELOPMENT OF RECOMMENDATIONS ON IMPROVEMENT OF CISCO NETWORK SECURITY SYSTEM BASED ON SDN TECHNOLOGY

Norkuvvat Chunaev

Tashkent University of Information Technologies

named after Muhammad Al-Xorazmiy,

Khakimbekov Doniyorbek

Tashkent University of Information Technologies

named after Muhammad Al-Xorazmiy,

Annotation: *This master's dissertation is dedicated to the topic "Development of recommendations for improving the security system of Cisco networks based on SDN technology," which substantiates the necessity of modern solutions to address security challenges in Cisco networks. The dissertation comprehensively analyzes the structure of traditional Cisco networks, the threats directed at them, existing protection tools, and the capabilities of Software Defined Networking (SDN) technology. Within the framework of the study, SDN-based security measures were developed in the Cisco Packet Tracer environment, achieving a 98% reduction in disruptive attacks (e.g., DoS attacks) by limiting ICMP traffic to 9.5 packets per second. Additionally, a mechanism for applying SDN solutions to identify and mitigate high-priority risks in network security is proposed.*

Key words*: DoS and DDoS attacks, SDN technology, traditional networking, SDN based solutions, methodology of risk.*

Introduction

Cisco networks, as infrastructural backbone underpinning organizational operations globally, in great measure define the performance and reliability of digital communication networks, offering distributed robust connectivity and data processing. The subject dissertation, "Development of recommendations for improving the security system of Cisco networks based on SDN technology", seeks to enhance their security through Software Defined Networking (SDN), adhering to the growing demand for secure, scalable network architecture. We rely heavily on Cisco networks today for business applications, remote access, and critical services, yet their traditional architectures are strained to meet today's cybersecurity demands, saving time and resources only if they are securely protected.

The truth, however, is that traditional Cisco networks are increasingly vulnerable to sophisticated cyber threats, such as Denial of Service (DoS) and intrusion, which exploit weaknesses like slow response times, lack of centralized visibility, and poor scalability. Such susceptibilities can significantly lead to service downtime, loss of data, and revenue loss, posing serious security threats. The global rise of DDoS attacks in 2023 by 61% against financial institutions and the growing compliance cost (e.g., DORA in Europe). The purpose of the study is to enhance the security and resilience of Cisco networks by developing recommendations based on Software Defined Networking (SDN) technology to address modern cybersecurity threats.

Main part

Traditional Cisco networks face significant limitations: slow response to threats due to manual configuration of Access Control Lists (ACLs), lack of centralized visibility requiring device-by-device monitoring, and poor scalability as network size increases. These issues, rooted in distributed control, hinder rapid adaptation to modern threats like DoS attacks. Whenever it comes to networks, new trends keep on adding up and thus it becomes essential to know about the dissimilarities that SDN Networks and Traditional Networks possess. Given the ever-increasing need for the expansion, fault tolerance, and resource optimization of the networks that connect today's business environments, organizations, and IT practitioners are generally in a dilemma over the type of network architectures to adopt. This article will try to solve this confusion by explaining and comparing the major differences between SDN and Traditional Networks to decide which one suits you. SDN stands for Software Defined Network which is a networking architecture approach. It enables the control and management of the network using software applications. Through Software Defined Network (SDN) networking behavior of the entire network and its devices are programmed in a centrally controlled manner through software applications using open APIs. Software Defined Network improves performance through network virtualization. In SDN software controlled applications or APIs work as the basis of complete network management that may be directing traffic on the network or communicating with underlying hardware infrastructure. So in simple, we can say SDN can create a virtual network or it can control a traditional network with the help of software.

SDN is comprised of three key components: the data plane, the control plane, and the application layer. The data plane is responsible for forwarding network traffic, while the control plane manages network infrastructure and makes decisions about how network traffic should be handled. The application layer consists of software applications that run on top of the SDN infrastructure.

Benefits of SDN. SDN offers several key benefits over traditional networking approaches. For example, SDN allows for more efficient network management, as network administrators can automate many tasks that would otherwise be done manually. SDN also allows for more flexible and customizable network configurations, as network infrastructure can be reconfigured on the fly.

SDN has a wide range of applications, from data center networking to wide area networks (WANs) and even the Internet of Things (IoT). SDN is particularly useful in situations where network infrastructure needs to be highly flexible and scalable.

Advantages of SDN:

– centralized Control: It eases the management of the network for it presents a single interface for the management of the network;

– scalability: It is flexible for operation in network with many users as well as in a network where users are limited and keep on changing the location of their seats;

– automation: Automates many networks management decisions via programmable network requirements which decrease the amount of times that a human has to step in and make a decision;

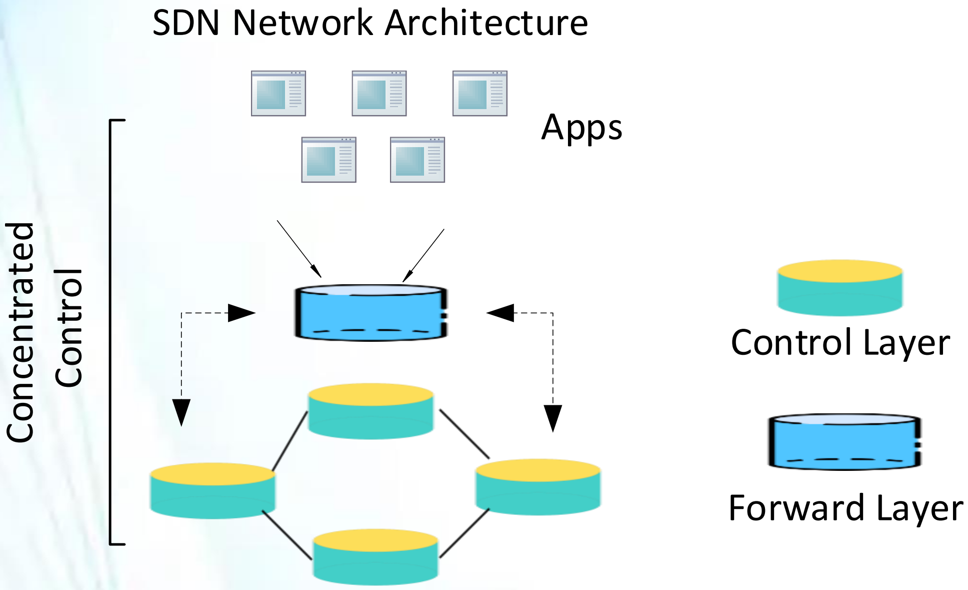
– cost-efficiency: Increases access and decreases circumstance when specialized hardware and software are required in other kinds of architectures.

– Disadvantages of SDN;

– security Risks: Centralized control is particularly disadvantageous as it becomes a weak link if protection and security is not well implemented;

– complexity: It comes with the need to have prior knowledge on network programming and may at times be a bit complex for the users;

– initial costs: While overall costs are lower the initial costs as well as the conversion costs might be high.



Pic. 1.3. Architecture of software defined network

Traditional network refers to the old conventional way of networking which uses fixed and dedicated hardware devices such as to control network traffic. Inability to scale and network security and Performance are the major concern now a days in the current growing business situation so that SDN is taking control to traditional network. Traditional network is static and based on hardware network appliances. Traditional network architecture was used by many companies till recent years but now a days due to its drawbacks Software Defined Network has been developed and in coming years it will be used more.

Components of Traditional Network

– Network devices: Traditional networks use physical network devices, such as routers, switches, and firewalls, to manage and direct network traffic.

– Cabling: Traditional networks use physical cabling to connect network devices to each other.

– Protocols: Traditional networks rely on standard networking protocols, such as TCP/IP and Ethernet, for communication between network devices.

– Advantages of Traditional Network

– Well-established: Traditional networks are well-established and widely used in various organizations.

– Predictable performance: Traditional networks offer predictable performance as network devices are configured based on specific requirements

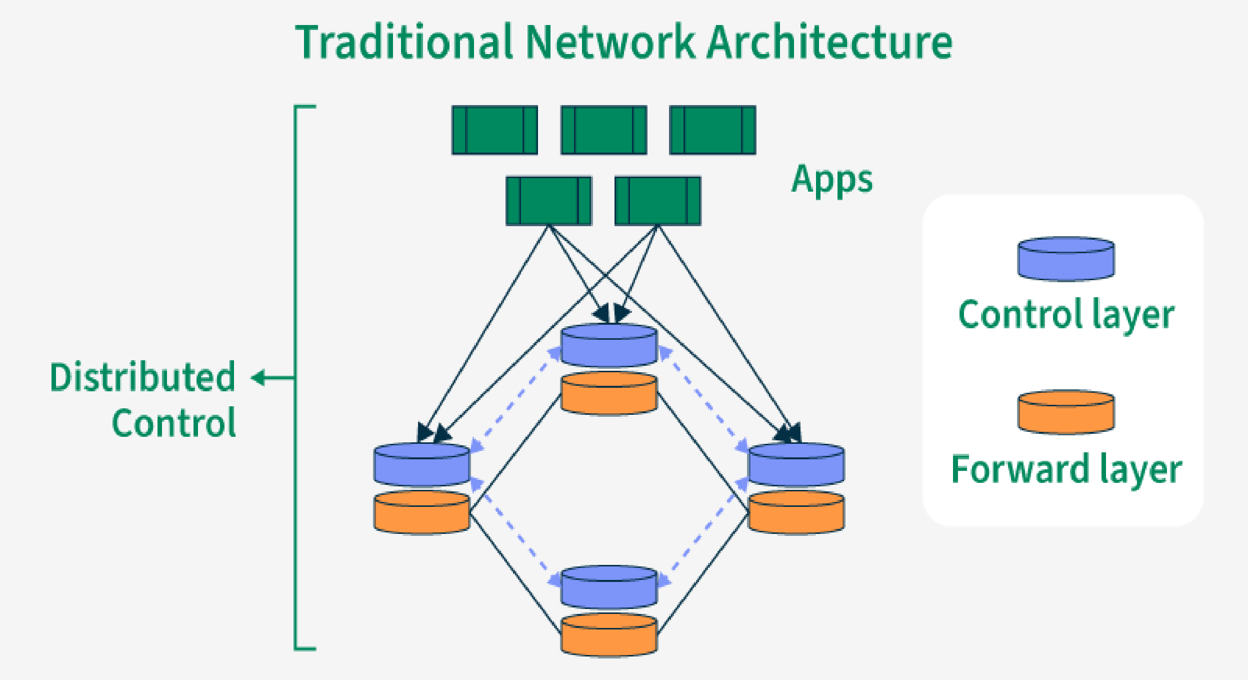
– Familiarity: Traditional networks are familiar to network administrators and require minimal training.

– Disadvantages of Traditional Network

– Limited scalability: Traditional networks have limited scalability due to the dependence on physical hardware devices.

– Limited automation: Traditional networks have limited automation capabilities and require significant manual intervention.

– Rigid architecture: Traditional networks have a rigid, hierarchical architecture that is difficult to modify or adapt to changing business needs.



Pic. 1.4. Architecture of traditional network

Here are some similarities between Software Defined Network (SDN) and traditional network. In the table 1 indicated differences of SDN with traditional network, observed some fields.

Table 1. Comparison SDN with traditional network.

SDN	**TRADITIONAL NETWORK**
Software Defined Network is virtual networking approach.	Traditional network is the old conventional networking approach.
Software Defined Network is centralized control.	Traditional Network is distributed control.
This network is programmable.	This network is non programmable.
Software Defined Network is open interface.	Traditional network is closed interface.
In Software Defined Network data plane and control plane are decoupled by software.	In traditional network data plane and control plane are mounted on same plane.

It supports automatic configuration so it takes less time.	It supports static/manual configuration so it takes more time.
It can prioritize and block specific network packets.	It leads all packets in the same way no prioritization support.
It is easy to program as per need.	It is difficult to program again and to replace existing program as per use.
Cost of Software Defined Network is low.	Cost of Traditional Network is high.
Structural complexity is low in Software Defined Network.	Structural complexity is high in Traditional Network.

The study of Software Defined Networking (SDN) differs from other forms of Networking in that it brings to light the many issues embedded within traditional networks, while at the same time highlighting how SDN has the capacity to solve those issues. Traditional networks face an array of challenges, including: a slow response to network security threats due to labor-intensive ACL management. The fact that Visibility is not centralized –therefore, monitoring has to be done on a per-device basis, along with poor scalability as the size of the network increases further add to the issues of manual control configuration and distributed control sub networks. These shortcomings prevent them from being able to effectively respond to modern and evolving threats such as DoS attacks, or even meeting the flexible demands posed by modern business environments. Conversely, SDN has been able to solve these problems using centralization, SCADA, and automation. By separating the control from the data plane, and the planar decoupling control, SDN enables rapid configuration, greater scalability, efficiency resource optimization, congested performance in numerous applications like data centers, WANs, and IoT.

With less manual interaction required, SDN’s software-driven approach directly reduces maintenance costs while providing the flexibility to control and shift focus regarding the importance of handled traffic, in addition to dynamically shifting focus based on need shifts. On the flip side, having centralized control also poses some level of risk in terms of security, in addition to initial costs steep setup expenses and complexity, presenting challenges. The familiarity and simplicity within traditional networks has a catch, which is the unshakable rigid arc along the radius.

Conclusion

This thesis has established a comprehensive foundation for understanding the complexities of network security within widely utilized network infrastructures, underscoring the indispensable need for effective protection mechanisms to safeguard operational continuity. It has explored the fundamental elements that constitute a secure network environment, emphasizing their pivotal role in ensuring reliable communication and data integrity. Alongside this, the chapter has illuminated significant challenges inherent in existing systems, including sluggish response times that hinder timely threat mitigation, a lack of comprehensive visibility into network operations, and persistent scalability issues that complicate the expansion of security measures. These shortcomings expose networks to a variety of vulnerabilities that undermine their resilience against external and internal pressures. The analysis has further uncovered a diverse array of threats that pose substantial risks, ranging from overwhelming attacks that disrupt service availability to unauthorized intrusions that jeopardize sensitive information, highlighting the dynamic and escalating nature of cyber dangers. Collectively, these findings reveal the inadequacy of conventional approaches, which struggle to adapt to the rapidly evolving threat landscape, thereby necessitating a reevaluation of current practices. The insights derived from this exploration provide a compelling case for the adoption of innovative solutions that can address these critical limitations and effectively neutralize the identified risks. By establishing a clear understanding of the current security landscape and its deficiencies, this chapter sets a solid groundwork for subsequent investigations into advanced technologies and practical strategies. These efforts aim to enhance network resilience, offering a pathway to fortify defenses and ensure sustained operational integrity in the face of ongoing and future challenges. This foundation encourages a forward-looking approach, paving the way for the development of robust, adaptable solutions to secure network environments.

LITERATURE

1. Nyale, Duncan & Karume, Simon. (2023). Examining the Synergies and Differences Between Enterprise Architecture Frameworks: A Comparative Review. International Journal of Computer Applications Technology and Research. International Journal of Computer Applications Technology and Research. 1-13. 10.7753/IJCATR1210.1001.

2. Blessing, Moses & Olusegun, John. (2024). The Impact of Software-Defined Networking (SDN) on Traditional Network Architectures: Opportunities and Challenges.

3. Danish, Muhammad & Shahid, Shaheryar & Ghafar, Abdul & Hamid, Khalid & Ali, Noman & Ghani, Amarah & Ibrar, Muhammad & Mandan, Sikandar. (2025). Security of Next-Generation Networks: A Hybrid Approach Using ML-Algorithm and Game Theory with SDWSN. 3. 18-36. 10.63075/wdpwrr31.

4. Cavusoglu, Huseyin & Raghunathan, Srinivasan & Cavusoglu, Hasan. (2009). Configuration of and Interaction Between Information Security Technologies: The Case of Firewalls and Intrusion Detection Systems. Information Systems Research. 20. 198-217. 10.1287/isre.1080.0180.

5. D, Ashok Kumar & Venugopalan S R, Dr. (2023). INTRUSION DETECTION SYSTEMS: A REVIEW. International Journal of Advanced Research in Computer Science. 8. 10.26483/ijarcs.v8i8.4703.