KAPITEL 6 / *CHAPTER 6* [6]
OPTIMIZATION OF NETWORK INFRASTRUCTURE TO ENSURES RESILIENCE, SECURITY AND SCALABILITY

DOI: 10.30890/2709-2313.2025-40-02-017

6.1. Determination of key parameters and criteria of network infrastructure: essence, state, problems and theoretical basis

6.1.1. Justification of the role and importance of network infrastructure.

Network infrastructure is the backbone of today's digital world, enabling connectivity between computers, servers, cloud services, and Internet of Things (IoT) devices. Think of it as a network of roads that data travels on: if the roads are wide, safe, and free of congestion, everything works quickly and reliably. If there are holes, obstacles or accidents, everything stops. In the context of the topic "Optimizing Network Infrastructure for Fault Tolerance, Security, and Scalability", we will look at what network infrastructure is, why it is important, what its current state is, what problems exist, and how to investigate them. Everything is explained as easily as possible so that even people without technical training can understand the essence.

Network infrastructure is a collection of hardware (routers, switches, servers), software (protocols, management systems), and communication channels (fiber, Wi-Fi, 5G) that allow data to be transferred between devices. It's like a circulatory system that delivers information where it's needed.

Without a network, companies cannot work. For example, online stores, banks, or streaming platforms (like Netflix) depend on fast and reliable data transfers. If the network "crashes", customers go to competitors, and the business loses money.

Networks provide video calls, social networks, access to news. During the pandemic, Zoom and Microsoft Teams became "saviors" for work and study, but without a powerful network, they would not have coped.

---

[6]***Authors:*** *Antonenko Artem Vasylovych, Golubenko Oleksandr Ivanovych, Tverdokhlib Arsenii Oleksandrovich, Balvak Andrii Anatolijovych, Buriak Myroslav Serhiiovych, Vostrikov Sergii Oleksandrovych, Yurii Mishkur Valentynovych, Ziniar Denys Arkadiiovych, Dziysiak Vladyslav Hennadiiovych*
Number of characters: *48917*
Author's sheets: *1,22*

New technologies like IoT (smart homes, sensors), autonomous cars, or telemedicine require networks that can handle huge amounts of data without delay.

The network is a gateway for hackers. If it is not secured, attackers can steal data, stop services, or even threaten national security. Fault tolerance – the network must work even if something breaks. Security – protection against hackers, viruses and data leaks. Scalability is the ability to "grow" when new users or services are added. Performance – speed and low latency for comfortable work.

Network infrastructure is the foundation of the digital economy. Without it, there will be no online banking, no smart cities, or even the opportunity to watch the series in the evening. Network optimization makes it reliable, secure, and future-ready.

6.1.2. Determination of the current state of network infrastructure

Modern networks are complex systems that are constantly evolving. Here's what their fortune looks like in 2025. 5G mobile networks give speeds of up to 10 Gbps and allow you to connect millions of devices like IoT sensors. Cloud platforms: Companies like AWS or Azure allow you to quickly add servers or storage, making networks flexible. SDN (Software-Defined Networks): Network management has become centralized, like in the control room, which simplifies setup and response to failures. Artificial intelligence optimizes data routes and detects cyberattacks in real time.

According to Cisco (2023), global internet traffic is growing by 25% every year due to streaming, IoT, and cloud services. By 2025, 30 billion connected IoT devices are predicted, from smart refrigerators to medical sensors. The pandemic has shown that networks have to support millions of video calls at the same time.

Cyberattacks are becoming more sophisticated. For example, DDoS attacks (network congestion) increased by 40% in 2024 (Fortinet report). Data breaches cost companies an average of $4 million per incident (IBM, 2023). Old networks (for example, with outdated routers) cannot cope with the new requirements. High modernization costs: Switching to 5G or SDN requires significant investments. Shortage of specialists – according to Gartner (2024), 60% of companies are experiencing a shortage of network engineers.

Today's networks are powerful, but they face enormous challenges: more data, more devices, more threats. For everything to work, you need to constantly optimize the infrastructure using new technologies.

Optimizing any system begins with a deep understanding of its current state. In the context of network infrastructure, this means not just a list of hardware, but a comprehensive analysis of its functionality, performance, security, and scalability. Determining the state of the art is the foundation for identifying bottlenecks, potential risks, and opportunities for improvement, which is critical to ensuring fault tolerance, security, and future scalability.

The first and most important step is to take a complete inventory of all the components of the network.

Hardware – Routers, switches (all levels), firewalls, Wi-Fi access points, servers (physical and virtual), storage systems (SAN/NAS), uninterruptible power supplies (UPS), network printers, and any other devices connected to the network. For each device, the model, serial number, firmware/operating system version, and physical location must be recorded.

Software – operating systems on servers and workstations, network services (DNS, DHCP, Active Directory/LDAP), virtualization platforms, database management systems, application software. It is important to note the versions and availability of installed updates/patches.

Logical infrastructure – definition of all VLANs, subnets, IP addressing settings, routing tables, routing protocols (OSPF, BGP, EIGRP), NAT settings.

Based on the collected data, it is necessary to create an up-to-date network topology that reflects both physical and logical connections. These can be diagrams showing device connections, data flows, security zones (DMZ, internal networks), and the location of key services.

Evaluating network performance is key to understanding its ability to handle current and future workloads.

Bandwidth – measurement of actual bandwidth on key areas of the network (Internet connection, trunk channels, connections between segments, access to

servers). It is important to compare it with the maximum available throughput of equipment.

Latency is the detection of data transfer delays between different network nodes, which is especially important for latency-sensitive applications (VoIP, video conferencing, interactive systems).

Packet Loss – monitoring the percentage of lost packets, which may indicate overload, equipment malfunctions, or poor quality of communication channels.

Central processing unit (CPU) and memory (RAM) usage – monitoring resource usage on network devices (routers, switches, firewalls). High load may indicate insufficient power or incorrect configuration.

Traffic monitoring – using NetFlow/sFlow tools to analyze traffic types, identify bandwidth "consumers" and identify anomalies.

These indicators should be collected over a long period (days, weeks) to detect peak loads and seasonal fluctuations.

Analyzing the current security state of network infrastructure is critical to identify vulnerabilities and weaknesses.

Analysis of firewall settings – checking filtering rules, the presence of unnecessary or conflicting rules, and the correctness of NAT and VPN settings.

Verification of Intrusion Detection/Prevention Systems (IDS/IPS) – relevance of signatures, correctness of settings, effectiveness of threat response.

Analysis of access control policies – verification of authentication, authorization, and accounting (AAA) settings for users and devices. Observance of the principle of least privilege.

Patch and update status assessment – checking all devices and systems for the latest security updates and patches.

Vulnerability scanning – conducting automated network scans for known vulnerabilities in software and hardware.

Log analysis and event audit – checking the presence of a centralized log collection (SIEM system), the correctness of their configuration and the regularity of analysis for suspicious activity.

Penetration Testing – optionally, conducting a controlled attack on your own network to identify real vulnerabilities that can be exploited by attackers.

The fault tolerance of the network ensures its continuous operation even in the event of a failure of individual components.

Redundancy check – determination of the availability of redundant communication channels, redundant devices (routers, switches, firewalls), cluster configurations.

Uninterruptible Power Supply (UPS) Analysis – Verify the availability, power, and performance of a UPS for critical equipment.

Disaster Recovery Plan – availability and relevance of recovery plans, data backup procedures and testing.

Service availability monitoring – checking the availability of key network services and applications, determining Single Point of Failure.

The quality of the cable infrastructure is an assessment of the condition of the physical cable system, which is the foundation of the network.

Scalability determines the ability of a network to grow and adapt to new needs. Assessment of current IP address usage and availability of free address space for future expansion. Determine the maximum number of ports, supported speeds, and performance of existing hardware. The ability of the current infrastructure to support new technologies such as Wi-Fi 6/7, 5G, IoT devices, cloud services, SDN/NFV. Assessment of the complexity of making changes to the network configuration, the availability of automation tools.

Equally important is the analysis of the quality of current documentation and internal policies. Does the existing documentation (diagrams, configurations, instructions) correspond to the real state of the network? Having well-defined security policies, understanding and compliance with staff. Availability and adherence to procedures for regular maintenance, updates, and monitoring of the network.

An integrated approach to determining the current state of network infrastructure allows you to get a complete picture of its strengths and weaknesses. This information is the basis for developing sound optimization recommendations that will ensure that

it improves its fault tolerance, security, and scalability in the long term.

6.1.3. Study of problems and the level of theoretical basis of the state of network infrastructure

Single Points of Failure (SPOF): If one router or cable breaks, the entire network can stop. For example, a Google Cloud data center outage in 2019 left millions of users without access to services. Older systems can take minutes or hours to "come to life" after a failure. Hackers use phishing, ransomware, or DDoS to shut down networks. The attack on the Colonial Pipeline in 2021 showed how weak defenses can stop critical infrastructure. Employees by negligence or maliciously can cause data breaches. Older routers can't handle peak loads. Adding new servers or channels can take weeks and be expensive. Even 100ms latency can ruin a video call or online game. Without proper traffic management, the network "freezes" during peak hours.

Research on network infrastructures is based on the works of leading scientists. Tanenbaum and Wetteroll (Computer Networks, 2021) describe fault tolerance architectures like router redundancy and HSRP/VRRP protocols. Столлінгс (Cryptography and Network Security, 2022) детально аналізує шифрування (TLS, VPN) і модель Zero Trust для безпеки.

Kouros and Ross (Computer Networking, 2021) investigate scaling via SD-WAN and NFV. Zhang (2023) shows how AI can predict attacks and optimize traffic. The problem is that theory often lags behind practice. For example, while SDN and AI are well described in the literature, their implementation in real-world networks faces technical and financial barriers. In addition, there is a lack of universal models that would combine fault tolerance, safety and scale. Understanding the problems and theoretical background helps to find network weaknesses and develop solutions. Without this, we will simply "patch holes" and not build reliable infrastructure.

6.1.4. Collection and analysis of necessary empirical and statistical information

To optimize your network, you need to collect real-world data about how it works (empirical data) and statistics (such as the frequency of failures or attacks). Tools like

Nagios or Zabbix are used to keep an eye on traffic, delays, crashes. For example, you can measure how long it takes to recover from a router failure. They conduct simulations of attacks (for example, DDoS) or equipment shutdowns to check how the network responds. Experts talk about real problems, for example, the complexity of SDN setup or lack of resources.

Analyze how often hardware failures or software errors occur. For example, an IDC report (2023) shows that 30% of network failures are due to hardware issues. They collect statistics on the types of attacks (DDoS, phishing) and their impact. A report by Fortinet (2024) states that 60% of companies experience at least one attack per year. Measure bandwidth (how much data is transferred per second) and latency. For example, networks with 5G have latencies of up to 1ms, while 4G has latencies of up to 20ms. They analyze how much it costs to implement SDN, cloud, or AI. According to Gartner (2024), the transition to cloud platforms pays off in 2-3 years. Compare the performance of networks with different technologies (for example, SDN vs. traditional). For example, the rise of IoT devices increases the need for edge computing. Use AI to predict future problems, such as network congestion during major events.

Netflix collects traffic data to understand when users watch videos, such as in the evenings or during premieres. They use AWS Auto Scaling to add servers during peak hours and AI to predict load. This allows you to process 200 million simultaneous connections without delay. Without data, we work "blindly". Empirical and statistical information shows where the network is weak, which technologies work and which do not. This is the basis for smart decisions: whether it is worth buying a new router or whether it is better to switch to the cloud.

Network infrastructure is the heart of the digital world, but it can get sick due to failures, attacks, or congestion. The role and significance show why networks are the foundation of business and society. The current state of affairs helps to understand where we are now and where we are headed. Problems and theory point out weaknesses and provide a scientific basis for solving them. Data is an "X-ray" that shows what needs to be treated. Understanding these aspects allows you to create networks that not

only work, but are also ready for the challenges of the future — from smart cities to global corporations.

6.2. Designing a network infrastructure model

6.2.1. Study of the topology of network infrastructure. Integration of cloud solutions for scaling and redundancy

A topology is a diagram that shows how devices in a network (computers, routers, servers) are connected to each other. It's like a city map: it determines which roads lead to the houses and how quickly you can get from point A to point B. The right topology makes the network fast, reliable and easy to manage. Types of topologies:

1. Star. All devices are connected to the central switch, like spokes to a wheel. Simple and popular in offices, but if the center "falls", everything stops.

2. Tree. Several "stars" are united in a hierarchy. Suitable for large companies because it allows you to add new devices.

3. Grid. All devices are connected to each other like in a spider's web. Very reliable (if one way breaks, there are others), but expensive. It is used in data centers.

4. Ring. The devices are connected in a circle. Cheap, but if one device fails, the entire ring can stop.

For a small office, the "star" topology is suitable - simple and inexpensive. A global company with offices in different countries requires a "grid" or "tree" to ensure speed and reliability. If the network is to support IoT (such as smart sensors), a hybrid topology is needed that combines a "tree" and a "mesh" to scale. Programs like Cisco Packet Tracer or SolarWinds help you draw a map of the network and test how it will work. Traffic analysis shows where there may be "traffic jams" (congestion).

Netflix uses a "grid" topology in data centers so that data (video) reaches users through the fastest path, even if one server fails.

The correct topology is the foundation of the network. It determines how quickly the data "arrives", how easy it is to add new devices, and what happens if something breaks. Without a good topology, the network will be slow, vulnerable, and difficult to

manage.

Cloud platforms like Amazon Web Services (AWS) or Microsoft Azure are like renting servers, storage, and network resources in a huge "virtual warehouse." They allow the network to grow (scale) and have a backup plan (redundancy) in case of failures. Clouds allow you to add resources quickly. For example, if your site is visited by millions of people during a sale, AWS Auto Scaling automatically launches additional servers. Global data centers (in Europe, Asia, USA) provide quick access for users around the world. Clouds use Disaster Recovery (DR) — plans in case of major failures. For example, if a data center in the United States fails, the data is automatically transferred to the center in Europe. Data backups are stored in the cloud to restore work in minutes.

A combination of on-premises servers (in your office) and cloud resources. For example, Microsoft Azure Hybrid allows you to keep critical data "at home" but scale through the cloud.

Technologies for integration:

1. SD-WAN optimizes communication between offices and the cloud by choosing the fastest channels.

2. APIs allow on-premises systems to "talk" to cloud platforms.

Netflix uses AWS to scale: When a new season of a series is released, AWS adds servers to handle millions of viewers. If one data center fails, cloud redundancy redirects traffic, and users don't notice problems.

Cloud solutions make the network flexible and reliable. They allow you to save on equipment, quickly respond to traffic growth and be prepared for accidents. It's like having a spare engine for a ship that will turn on if the main one breaks down.

6.2.2. Configuring security mechanisms in the network infrastructure

Ensuring the security of network infrastructure is a critical aspect for its fault tolerance and scalability. Unauthorized access, data breaches, malware, and cyberattacks can paralyze the functioning of the network, leading to significant financial and reputational losses. Effective configuration of security mechanisms

requires an integrated approach, including the implementation of organizational, software and hardware protection tools.

Network segmentation is a fundamental step in improving its security. Dividing a large, flat network into smaller, isolated segments (VLANs, subnets) limits the spread of attacks and malware. This allows the principle of least privilege to be implemented, limiting the access of users and systems to only those resources that they absolutely need.

VLAN (Virtual Local Area Network): Using a VLAN allows you to logically divide a network into separate broadcast domains, even if the devices are physically connected to the same switch. This is effective for isolating different departments, types of traffic (e.g., voice, video, data), or devices (servers, workstations, IoT devices).

Subnets and Routing: Proper design of subnets and configuration of routing between them allows you to control the flow of traffic and enforce security rules at the boundaries of each segment.

For mission-critical applications or sensitive data, it is recommended to use micro-segmentation that isolates even individual virtual machines or containers, allowing for highly granular security policies. This is achieved through software-defined networking (SDN) and virtualized security measures.

Firewalls (MEs) are the primary means of filtering network traffic. They analyze data packets and, according to given rules, allow or block their passage. Modern MEs are divided into several categories:

Stateful Firewalls – These MEs monitor the status of connections, which allows them to make decisions about traffic throughput not only based on addresses and ports, but also taking into account the context of the session.

Next-Generation Firewalls NGFW integrate advanced security features such as Deep Packet Analysis (DPI), Intrusion Prevention Systems (IPS), Antivirus Scanning, Application Control, and URL Filtering. This allows them to detect and block more complex threats at the application layer.

Web Application Firewalls WAFs are specifically designed to protect web

applications from attacks such as SQL injection, XSS (Cross-Site Scripting), CSRF (Cross-Site Request Forgery), and other threats that target web applications.

Intrusion detection systems (IDS) and intrusion prevention systems (IPS) are vital components for monitoring and actively protecting the network from malicious activity.

IDS (Intrusion Detection System) passively analyzes network traffic or system logs for suspicious activity using signature analysis (comparison with known attack patterns) and/or anomaly analysis (detection of deviations from normal behavior). When a threat is detected, IDS generates an alert.

IPS (Intrusion Prevention System), unlike IDS, actively blocks malicious traffic in real time, preventing attacks from penetrating the network. IPSs are often integrated into NGFW or operate as separate network devices.

AAA (Authentication, Authorization, and Accounting) systems play a key role in controlling access to network resources and monitoring user actions.

Authentication – The process of verifying the identity of a user or device (e.g., using username and password, digital certificates, biometrics).

Authorization – determining the access rights of an authenticated user to certain resources or performing certain operations.

Accounting is the maintenance of detailed logs of user actions, which allows you to track who, what, when and how long did it on the network. This is critical for auditing, incident investigation, and regulatory compliance. The use of protocols such as RADIUS or TACACS+, combined with centralized directories (e.g., Active Directory, LDAP), provides efficient access control. A VPN provides secure remote access to the corporate network and protection of data transmitted over unsecured networks such as the Internet.

Site-to-Site VPN creates an encrypted tunnel between two or more networks (for example, between a head office and a branch office). Remote Access VPN allows individual users to securely connect to the corporate network from anywhere. IPsec (Internet Protocol Security) is a set of protocols for ensuring the security of IP communications by authenticating and encrypting each IP packet. SSL/TLS VPN uses

SSL/TLS protocols to create a secure tunnel, often used for remote access through a web browser. SIEM (Security Information and Event Management) systems aggregate, normalize, correlate and analyze security events from various sources in the network (network devices, servers, applications, security systems). This allows:

Centralized monitoring – gathering all logs and events in one place.

Detection of complex attacks that may not be visible to individual defenses.

Incident response is all about providing tools to quickly investigate and respond to identified threats.

Regulatory Compliance – Assistance in complying with regulatory requirements for journaling and auditing.

Encryption is the cornerstone of data privacy and integrity. It must be applied at different levels of network infrastructure.

Data at Rest – protection of data stored on servers, databases and other media (for example, full disk encryption).

Data in transit is the protection of data during its transmission over the network using protocols such as HTTPS, SSH, SFTP, IPsec, TLS.

Key Management – This strong cryptographic key management is critical for encryption efficiency.

Network Access Control (NAC) allows you to control the devices that connect to the network, ensuring that only authorized and security-compliant devices can access.

Device identification: Determination of device type, operating system, patch status, and antivirus software.

Enforcing policies that require devices to meet certain security requirements before granting access. Automatically isolate or move non-compliant devices to the quarantine zone until issues are fixed.

The network is like a house: if the door is not closed, burglars (hackers) can steal or break everything. Cyberattacks like DDoS or phishing are becoming more frequent, and without protection, the network can stop and data can fall into the hands of attackers.

Modern firewalls like Palo Alto Networks (NGFW) act as guards: they check all

the data in and out. They not only block dangerous IP addresses, but also analyze behavior to stop attacks like DDoS.

TLS (Transport Layer Security) protects data in transit, such as when you enter a password on a site. It's like sending a letter in a safe.

VPN (Virtual Private Network) creates a secure "tunnel" for remote workers to prevent their data from being intercepted.

The Zero Trust model is a "never trust, always verify" rule. Each device or user must verify their identity (for example, through a password or two-factor authentication), even if they are inside the network. This protects against insider threats like stolen employee passwords.

Intrusion Detection Systems (IDS/IPS) monitors suspicious activity like a surveillance camera, while IPS blocks attacks like a security guard. For example, if someone tries to hack a server, IPS will stop it in seconds.

Artificial intelligence analyzes traffic and finds anomalies, such as an unusually large amount of data. The Darktrace system can detect 95% of attacks at an early stage.

In 2021, hackers attacked Colonial Pipeline using a stolen password. If the company had used Zero Trust and NGFW, the attack would have been stopped because suspicious access would have been blocked immediately.

Security is the shield of the network. Without it, hackers can stop business, steal data, or cause damage. Setting up security mechanisms makes the network a fortress that is difficult to penetrate.

6.2.3. Optimization for fault tolerance of network infrastructure

Fault tolerance is the ability of a network to work even if something breaks, such as a router, cable, or server. It's like a plane with two engines: if one fails, the second allows you to fly.

Install spare routers and servers. For example, in active/active mode, all devices work simultaneously, distributing the load, which provides 99.99% availability (Tanenbaum, 2021).

The HSRP and VRRP redundancy protocols create a "virtual router" that switches

to a spare device in 1–2 seconds if the primary one breaks.

RSTP (Rapid Spanning Tree Protocol): Prevents loops in the network and quickly opens backup paths if the primary connection is lost.

Software-defined networks (SDNs) act as a central "brain" that redirects traffic in milliseconds if one path fails. For example, an OpenDaylight controller can do this in 50 ms.

Cloud platforms like AWS store data in multiple data centers. If one center stops, the other takes over the work in minutes.

Systems like Nagios monitor the network 24/7 and report problems. AI can automatically reconfigure the network to avoid outages.

In 2019, Google Cloud crashed due to a hardware failure that stopped services for 4 hours. If SDN and cloud redundancy were used, downtime would be reduced to 30 minutes.

Fault tolerance is network insurance. It ensures that business does not stop and users do not lose access to services. This is critical for banks, hospitals, or streaming platforms.

Designing a network infrastructure model is like creating the perfect city for data. Each element must work together:

1. Topology defines how data moves to avoid "traffic jams".
2. Cloud solutions allow the network to grow and have a backup plan.
3. Security protects against hackers like locks on a door.
4. Fault tolerance ensures that the network does not stop even if something breaks.

These principles are already being applied by giant companies like Netflix or AT&T to ensure a smooth experience for millions of users. Understanding them allows you to create networks that not only work, but are also ready for the challenges of the future — from smart cities to global businesses.

6.3. Practical implementation and monitoring of network infrastructure

6.3.1. Configuring the Test Environment

A test environment is like a sandbox where we build and test the network before launching it in the real world. This allows you to find problems without the risk of stopping the real network. Imagine that you are testing a new car on a track rather than on a busy track.

Selection of equipment and programs:

1. Hardware - routers (for example, Cisco), switches, servers. Virtual machines can be used to save money.

2. Emulator software like GNS3 or Cisco Packet Tracer allows you to create a virtual network on your computer.

3. AWS or Azure cloud platforms for testing cloud solutions.

Topology design. Choose a network diagram, for example, a "star" topology (all devices are connected to one switch) for a small office or a "mesh" (many connections between devices) for a data center. We add redundant routers and servers for fault tolerance.

Setting up basic functions:

1. We set IP addresses for devices so that they can "talk".

2. We set up protocols like HSRP or VRRP that switch traffic to a spare device if the main one breaks down.

3. We connect test computers or IoT devices to simulate real users.

Test scenarios:

1. We simulate traffic growth (for example, thousands of requests, as during streaming).

2. Turn off the router to check if the network switches to backup.

3. We simulate an attack to see how the defense reacts.

A company that launches an online store creates a test network in GNS3. They check whether the network can withstand 10,000 concurrent buyers and whether it switches to a backup server in 2 seconds in case of a failure.

A test environment is a safe way to "play around" with the network, find bugs, and make sure everything will work in real conditions. Without this, we risk launching a network that will "freeze" on the first day.

6.3.2. Implementation of protective systems

A network without protection is like a house without locks: hackers can steal data, stop services, or cause damage. Protective systems are "security" that stops intruders and ensures security. We install a modern firewall like Palo Alto Networks (NGFW), which checks all traffic and blocks suspicious requests. For example, it can stop a DDoS attack when hackers overload the network. We set up rules to allow only the necessary traffic (for example, for a website) and block everything else. We use TLS to protect data transmitted over the network (for example, passwords on the site). We set up a VPN so that remote workers securely connect to the network as if they were in the office.

The Zero Trust model. All devices and users must verify their identity (for example, through a password and code from the phone), even if they are online. This protects against stolen passwords. We restrict access, for example, the accountant sees only financial data, and not the entire server. We use intrusion detection systems (IDS/IPS). We install IDS (Intrusion Detection System), which monitors suspicious activity like a surveillance camera. IPS (Intrusion Prevention System) automatically blocks attacks, like a security guard stopping a burglar.

We use systems like Darktrace that analyze traffic and find anomalies (for example, an unusually large amount of data). AI can stop an attack before it even causes damage. The bank establishes NGFW and Zero Trust to protect customer data. When a hacker tries to penetrate through a stolen password, the system blocks access because it has not passed two-factor authentication. Protective systems are the shield of the network. They stop hackers, protect data, and allow businesses to operate without fear of attacks. Without them, the network is an easy target.

Effective implementation of security systems is a key step in building a fault-tolerant, secure, and scalable network infrastructure. This process goes beyond simply

installing software or hardware, requiring a systematic approach, careful planning, and constant adaptation to the changing cyber threat landscape.

Before starting the implementation of any protective systems, it is necessary to conduct a comprehensive risk assessment. Identify all critical data, systems, and network components. Analysis of potential cyber threats that may affect identified assets (e.g., DDoS attacks, malware, phishing, insider threats). Identifying weaknesses in existing infrastructure that can be exploited by attackers. Assessment of the potential consequences of the implementation of threats (financial losses, reputational losses, business continuity violations).

Based on this assessment, a cybersecurity strategy is developed that identifies priorities, goals, and a roadmap for the implementation of defensive systems. It is important to consider compliance with industry standards and regulatory requirements (e.g. GDPR, ISO 27001).

Once the strategy is defined, a detailed security architecture is developed. This includes:

- Selection of specific security systems (firewalls, IPS/IDS, SIEM, NAC, etc.) and their manufacturers, based on needs, budget and existing infrastructure.

- Determination of the optimal placement of security systems in the network (for example, peripheral firewalls, internal segmentation MEs, host-based agents).

- Creation of demilitarized zones (DMZ) for public services, isolation of critical network segments.

- Planning the interaction between different defense systems to ensure centralized management, monitoring and correlation of events. For example, the integration of firewalls with SIEM systems for automatic collection and analysis of logs.

- Ensuring high availability and fault tolerance of the protective systems themselves (redundancy, clustering, load balancing).

Launch of pilot projects to test new systems in a controlled environment before full-scale deployment. Customization of each protection system in accordance with the developed security policies. This includes:

- Establishment of strict rules for allowing/prohibiting traffic, the principle of

"banning everything that is not allowed".

- Loading of up-to-date signatures, optimization of rules to reduce the number of false positives.

- Define access rules for different types of devices and users.

- Setting up log sources, correlation rules, and alert mechanisms.

- Implementation of the principles of least privilege, multi-factor authentication (MFA), regular password changes.

- Thorough documentation of all implementation stages, configuration files, network diagrams, and security policies.

Once implemented, rigorous testing is critical to verify the effectiveness and correctness of the settings.

Functional testing: Checking the correct operation of each protective system in accordance with its purpose. Simulate real attacks to identify vulnerabilities and check the resilience of defense systems. This can be done by internal teams or by engaging third-party specialists. Automated network scanning for known vulnerabilities. Audit of compliance of real settings with developed security policies. The test results are used to adjust and optimize the settings of the protective systems.

The implementation of protective systems is not a one-time action, but a continuous process. Active monitoring of event logs and alerts from all security systems using a SIEM system. Development and implementation of a security incident response plan that includes procedures for detection, analysis, localization, remediation, and recovery. Ensuring timely updates of software, firmware, signature databases and rules for all security systems. Conducting regular trainings for IT staff and all users on the basics of cyber hygiene and security policies. Continuous evaluation of the effectiveness of defense systems, analysis of new threats and vulnerabilities, as well as adaptation and optimization of existing protection mechanisms to maintain a high level of security of the network infrastructure.

6.3.3. Installation of data collection tools and tests to verify performance and fault tolerance

Data collection and testing tools are like diagnostic equipment in a hospital. They show how the network works, whether it is fast enough, whether it can withstand failures. Without this, we will not know where the problems are and whether the network is ready for real operation. Nagios or Zabbix monitor the network 24/7, measuring speed, latency, resource usage. For example, they show if the router is overloaded. Wireshark analyzes traffic to see what data is being transmitted and if there are any suspicious requests. CloudWatch (AWS) monitors cloud servers, showing how they handle the load.

We conduct performance tests. Speed test – we use iPerf to measure bandwidth (how much data the network transmits per second). For example, a network with 5G should give up to 10 Gbps. Latency test – check how long it takes for the data to "arrive". For video calls, the latency must be less than 100ms. Load testing – simulate a peak load (for example, 10,000 users at the same time) to see if the network can withstand it.

We conduct fault tolerance tests. Turn off the router or server to check if the network switches to a backup device. For example, HSRP should do this in 1 to 2 seconds. We simulate a cable break or a failure in the data center to check the cloud redundancy.

We automate tests. We use scripts (for example, in Python) to automatically run tests every day. This saves time and allows you to quickly find problems.

Zoom is testing the network by simulating 1 million simultaneous calls. They use Zabbix to monitor latency and iPerf to test speed. If the router fails, SDN redirects traffic in 50ms and calls are not interrupted. Tools and tests are the "X-ray" of the network. They show you if it's fast enough, if it can withstand crashes, and help you prepare for real-world conditions like peak traffic or an attack.

6.3.4. Analysis of logs and performance indicators of the prototype for detection weaknesses

Logs are a "diary" of the network, where everything that happens is recorded: which devices are working, where there were failures, who tried to attack. Analyzing logs and metrics is like reading this blog to find where the network is weak and fix it.

Firewalls, routers, and servers record logs of who connected, what errors there were, how much traffic passed. Tools like Splunk or ELK Stack collect all logs in one place for easy analysis.

We analyze the performance indicators – check whether the speed and latency meet the requirements. For example, if the latency exceeds 100 ms, video calls can "slow down". Fault tolerance – we look at how long it takes to recover from a failure. If more than 2 seconds, protocols like HSRP need to be reconfigured. Security – we look for traces of attacks, for example, many requests from one IP address (DDoS is possible).

We identify weaknesses. Congestion – If one router handles 90% of the traffic, it can "freeze". You need to add another one or optimize traffic via SDN. Slow recovery – If the network recovers within 10 seconds of a failure, it's a good idea to replace STP with a faster RSTP. Weak security – if logs show failed login attempts, two-factor authentication or stronger passwords may be required.

We automate the analysis. AI systems like Darktrace analyze logs in real time and warn of problems. For example, they can find an anomaly, as an unusual amount of data, in seconds.

The online store analyzes logs after a test for 10,000 users. They see that one server is overloaded, and it takes 5 seconds to recover from a failure. The store adds another server via AWS and configures RSTP, reducing the recovery time to 1 second. Log analysis is a way to "talk" to the network and find out what is bothering it. Without it, we won't know why something isn't working and we won't be able to fix weaknesses.

Practical implementation and monitoring is like building and caring for a house. Each step makes the network better:

1. The test environment allows you to find errors without risk.

2. Defense systems stop hackers and protect data.

3. Test tools show whether the network is fast and reliable.

4. Log analysis helps to find and fix weaknesses.

These actions are already being used by companies like Zoom or Netflix to keep their services running smoothly for millions of users. Understanding these steps allows you to create a network that not only works, but is also ready for any calls, from peak traffic to cyberattacks.

6.4. Summarizing the results and developing practical recommendations

6.4.1. Analysis of the results of the study and assessment of the level of safety

Analyzing the results is like looking at a "photo album" after testing the network. We look at what worked and what didn't, and evaluate how secure the network is from hackers. This helps to understand whether we have achieved the goal (reliability, security, scale) and where there are weaknesses.

Check if the network is fast. For example, if the bandwidth reaches 10 Gbps and the latency is less than 100 ms, it's good for video calls or streaming. If the tests show "freezing" at 10,000 users, you need to add servers or optimize traffic through Quality of Service (QoS). Let's see how the network reacts to failures. For example, if disconnecting the router stops the network for 5 seconds, it is bad. Protocols like HSRP or RSTP should reduce the time to 1-2 seconds. We check cloud redundancy: if one data center fails, does the network switch to another in minutes. We analyze logs (records of network operation) for attacks. For example, if a firewall (NGFW) stopped 95% of test DDoS attacks, this is a good result. We check the Zero Trust model to see if each user verifies their identity. If someone has bypassed the protection, two-factor authentication is required. We evaluate encryption (TLS, VPN), whether data is protected from interception. If the goal was 99.99% availability and we only achieved 99%, reservations need to be improved. If the network can withstand only 50% of attacks, it is worth adding AI systems like Darktrace to detect anomalies.

The online store tested the network and found that latencies reach 200 ms at peak

load, and the firewall missed 10% of test attacks. They added QoS to reduce latencies to 80ms and set IPS to block all attacks.

The analysis shows whether the network meets the requirements of the business or users. Without it, we won't know what needs to be fixed and risk a network that "crashes" or becomes a target for hackers.

6.4.2. Checking scalability and determining the most effective solutions

Scalability is the ability of a network to "grow" when new users, devices, or services are added. Imagine that your small shop has become a supermarket, or there is enough space for new customers. The scalability test shows whether the network is ready for such growth.

We conduct scaling testing:

1. We simulate traffic growth, for example, from 1,000 to 10,000 users (whether the network can withstand it).

2. We add virtual IoT devices, for example, 1,000 sensors (whether the speed is maintained).

3. We check cloud platforms like AWS Auto Scaling (whether servers are added automatically when loaded).

We assess the following technologies:

1. SD-WAN: Optimizes wide area networks by distributing traffic between links. If SD-WAN reduces costs by 40% (according to Cisco), this is an effective solution.

2. NFV (virtualization): Replaces physical devices with applications, which saves 30% on scaling (Kouros, 2021).

3. 5G: Provides speeds of up to 10 Gbps for IoT and mobile networks. If the tests show latencies of less than 1ms, 5G is a good choice.

4. Edge Computing: Processes data closer to users, reducing latencies to 10ms.

We determine the best solutions:

1. If the network is for small businesses, cloud platforms (AWS) and SD-WAN are the simplest and most economical.

2. For data centers, NFV and SDN provide flexibility and rapid scaling.

3. For IoT (smart cities), 5G and edge computing are the most efficient due to low latency.

Netflix tested the zoom by simulating 200 million concurrent viewers. AWS Auto Scaling added servers in seconds, and SD-WAN streamlined video delivery, allowing the network to withstand the load without lag. Scalability checks ensure that the network doesn't "suffocate" from growing traffic or new devices. Choosing effective solutions saves time and money, making the network future-ready.

6.4.4. Formation of practical recommendations for network infrastructure optimization

Practical recommendations are like instructions on how to make the network better: what to add, what to change, how to avoid problems. These are tips that can be applied right away to keep your network fast, secure, and flexible.

Recommendations for fault tolerance:

1. Use backup routers in active/active mode for 99.99% availability.

2. Configure HSRP/VRRP protocols to switch in 1-2 seconds and RSTP to quickly restore communication.

3. Apply cloud redundancy (AWS, Azure) to recover minutes after failures.

Safety recommendations:

1. Install next-generation firewalls (NGFWs) like Palo Alto Networks to stop 95% of attacks.

2. Enable Zero Trust: Each user must verify their identity through two-factor authentication.

3. Use TLS 1.3 for encryption and AI systems (Darktrace) for anomaly detection.

Recommendations for scalability:

1. Use AWS Auto Scaling to automatically add resources at peak load.

2. Use SD-WAN for WAN to reduce costs by 40%.

3. Implement 5G and edge computing for IoT so that latencies do not exceed 10ms.

Performance recommendations:

1. Set up QoS to prioritize critical traffic (such as video calls), reducing latency by 25%.

2. Use caching via CDN (like Cloudflare) to download content quickly.

1. Apply AI to optimize routes, increasing throughput by 15%.

General tips:

1. Constantly monitor the network with tools like Zabbix or Nagios to detect problems in real time.

2. Run regular tests (load, crash, attack) to check network readiness.

3. Train staff to avoid setup errors that can stop the network.

The bank applied the recommendations: installed NGFW and Zero Trust for security, used AWS for scaling, and configured HSRP for fault tolerance. The result is 99.99% availability, 98% attack protection, and the ability to process 50,000 transactions simultaneously. Recommendations are a "recipe" for the perfect network. They help businesses save money, avoid disruptions, and be ready for growth without wasting time fixing mistakes.

Summarizing the results and recommendations is like the final stage in building a network:

1. Analyzing the results shows what is working and what needs to be improved.

2. Scalability testing ensures that the network is ready for growth.

3. The recommendations provide a clear plan of action for businesses and engineers.

4. Publications spread knowledge, making the world of networking a better place.

These steps have already helped companies like Netflix or AT&T build networks that can withstand millions of users and protect against attacks. Understanding this process allows us to build infrastructure that not only works today, but is also ready for tomorrow's challenges — from smart cities to global businesses.