ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫ
әл-Фараби атындағы Қазақ ұлттық университетінің

ХАБАРЛАРЫ

ИЗВЕСТИЯ

НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК
РЕСПУБЛИКИ КАЗАХСТАН
Казахский национальный университет
имени аль-Фараби

N E W S

OF THE ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
al-Farabi Kazakh National University

SERIES
PHYSICO-MATHEMATICAL

6 (340)

NOVEMBER – DECEMBER 2021

PUBLISHED SINCE JANUARY 1963

PUBLISHED 6 TIMES A YEAR

ALMATY, NAS RK

NAS RK is pleased to announce that News of NAS RK. Series physico-mathematical journal has been accepted for indexing in the Emerging Sources Citation Index, a new edition of Web of Science. Content in this index is under consideration by Clarivate Analytics to be accepted in the Science Citation Index Expanded, the Social Sciences Citation Index, and the Arts & Humanities Citation Index. The quality and depth of content Web of Science offers to researchers, authors, publishers, and institutions sets it apart from other research databases. The inclusion of News of NAS RK. Series of chemistry and technologies in the Emerging Sources Citation Index demonstrates our dedication to providing the most relevant and influential content of chemical sciences to our community.

Қазақстан Республикасы Ұлттық ғылым академиясы «ҚР ҰҒА Хабарлары. Физикалық-математикалық сериясы» ғылыми журналының Web of Science-тің жаңаланған нұсқасы Emerging Sources Citation Index-те индекстелуге қабылданғанын хабарлайды. Бұл индекстелу барысында Clarivate Analytics компаниясы журналды одан әрі the Science Citation Index Expanded, the Social Sciences Citation Index және the Arts & Humanities Citation Index-ке қабылдау мәселесін қарастыруда. Webof Science зерттеушілер, авторлар, баспашылар мен мекемелерге контент тереңдігі мен сапасын усынады. ҚР ҰҒА Хабарлары. Химия және технология сериясы Emerging Sources Citation Index-ке енуі біздің қоғамдастық үшін ең өзекті және беделді химиялық ғылымдар бойынша контентке адалдығымызды білдіреді.

НАН РК сообщает, что научный журнал «Известия НАН РК. Серия физико-математическая» был принят для индексирования в Emerging Sources Citation Index, обновленной версии Web of Science. Содержание в этом индексировании находится в стадии рассмотрения компанией Clarivate Analytics для дальнейшего принятия журнала в the Science Citation Index Expanded, the Social Sciences Citation Index и the Arts & Humanities Citation Index. Web of Science предлагает качество и глубину контента для исследователей, авторов, издателей и учреждений. Включение Известия НАН РК в Emerging Sources Citation Index демонстрирует нашу приверженность к наиболее актуальному и влиятельному контенту по химическим наукам для нашего сообщества.

«ҚР ҰҒА Хабарлары.
Физика-математикалық сериясы».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Меншіктеуші: «Қазақстан Республикасының Ұлттық ғылым академиясы» РҚБ (Алматы қ.). Қазақстан Республикасының Ақпарат және қоғамдық даму министрлігінің Ақпарат комитетінде 14.02.2018 ж. берілген **No 16906-Ж** мерзімдік басылым тіркеуіне қойылу туралы куәлік.
Тақырыптық бағыты: *математика, информатика, механика, физика, ғарыштық зерттеулер, астрономия, ионосфера.*
Мерзімділігі: жылына 6 рет.
Тиражы: 300 дана.
Редакцияның мекен-жайы: *050010, Алматы қ., Шевченко көш., 28, 219 бөл., тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Типографияның мекен-жайы: «Аруна» ЖК, Алматы қ., Мұратбаев көш., 75.

«Известия НАН РК.
Серия физика-математическая».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Собственник: Республиканское общественное объединение «Национальная академия наук Республики Казахстан» (г. Алматы).
Свидетельство о постановке на учет периодического печатного издания в Комитете информации Министерства информации и общественного развития Республики Казахстан **No 16906-Ж** выданное 14.02.2018 г.
Тематическая направленность: *математика, информатика, механика, физика, космические исследования, астрономия, ионосфера.*
Периодичность: 6 раз в год.
Тираж: 300 экземпляров.
Адрес редакции: *050010, г. Алматы, ул. Шевченко, 28, оф. 219, тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Адрес типографии: ИП «Аруна», г. Алматы, ул. Муратбаева, 75.

News of the National Academy of Sciences of the Republic of Kazakhstan. Physical-mathematical series.
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Owner: RPA «National Academy of Sciences of the Republic of Kazakhstan» (Almaty). The certificate of registration of a periodical printed publication in the Committee of information of the Ministry of Information and Social Development of the Republic of Kazakhstan **No. 16906-Ж,** issued 14.02.2018
Thematic scope: *mathematics, computer science, mechanics, physics, space research, astronomy, ionosphere.*
Periodicity: 6 times a year.
Circulation: 300 copies.
Editorial address: *28, Shevchenko str., of. 219, Almaty, 050010, tel. 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Address of printing house: ST «Aruna», 75, Muratbayev str, Almaty.

NEWS
OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X
Volume 6, Number 340 (2021), 81–91 https://doi.org/10.32014/2021.2518-1726.105

IRSTI 28.23.37
UDC 004.75

Tashenova Zh[1*], Nurlybaeva E[2], Abdugulova Zh[3], Amanzholova Sh[4]

[1,3] L.N. Gumilyov Eurasian National University, Department of Information technology, Nur-Sultan, Kazakhstan;
[2]Kazakh National Academy of Arts named after T. Zhurgenov, Almaty, Kazakhstan;
[4]Kurmangazy Kazakh National Conservatory, Almaty, Kazakhstan.
E-mail: zhuldyz_tm@mail.ru

ASSESSMENT OF THE SECURITY STATUS OF THE COMPANY'S DATA CENTER NETWORK INFRASTRUCTURE

Abstract. The purpose of this article is based on an assessment of the current state of network security in a company's data center. Analysis of the architecture and design principles of the data center network, development of proposals and recommendations for increasing the level of network security of the company's data center without serious loss of performance using both existing network elements and additional security elements. The data center performs the functions of processing, storing and distributing information, as a rule, in the interests of corporate clients - it is focused on solving business problems by providing information services. Attacks on the network infrastructure are also considered; they can be both active and passive (depending on the malware used by the attackers). A thorough assessment of the security of the network infrastructure was carried out, which depends on the complexity of the telecommunication and IT solutions used, security solutions, as well as on the time, resources and raw data available for analysis. An analysis was also carried out based on the output of configuration commands with hidden real IP addresses and passwords, the specification of the active network equipment in use. In the assessment, the main efforts were focused on analyzing the measures taken to effectively protect each individual network layer, analyzing the performance requirements, as well as the monitoring and control systems used. The perimeter of the data center is considered, which the current architecture of building the network perimeter is organized on powerful ASR1001 routers designed for use in large data processing centers and intended for aggregating WAN (Wide Area Network) connections. A number of recommendations for increasing the level of network security are provided.

Key words: network security, data center, network, Cisco, virtual private server, proxy servers.

Introduction. "Data transmission network" is a set of terminal communication devices (terminals) connected by data transmission channels and switching devices (network nodes) that provide messaging between all terminal devices. "Infrastructure" is a complex of interconnected service structures or facilities that make up and provide the basis for the functioning of the system. A "network segment" is a logically or physically separate part of a network.

"Datacenter" is a data processing center that provides a complex of network and computing equipment with a high level of availability. A high level of availability is also provided by uninterruptible power supply systems, climate control, security and other systems. A data center (from the English data center), or a data center (storage and processing center) is a specialized building for hosting server and network equipment and connecting subscribers to Internet channels.

The data center performs the functions of processing, storing and distributing information, as a rule, in the interests of corporate clients — it is focused on solving business problems by providing information services. Consolidation of computing resources and data storage facilities in the data center makes it possible to reduce the total cost of ownership of the IT infrastructure due to the possibility of efficient use of technical means, for example, load redistribution, as well as by reducing administration costs.

Data centers are usually located within or in close proximity to a communications hub or a point of presence of one or more telecom operators. The main criterion for evaluating the quality of any data center is the server availability time (uptime).

A data center or data center (Data Processing Center) is a high-tech room, the space of which is filled with telecommunications equipment and other devices, thanks to which the collection, storage and processing of various information opens up opportunities for users to work on the World Wide Web. A distinctive feature inherent in stable data centers is the reliability of the building, internal layout and modern infrastructure, which best meets the requirements of stable and safe use of the data center by its key customers.

The services of the data center are mainly used by corporate clients to successfully solve business problems, because thanks to the capabilities of the data center, customers really save the company's finances, since there is no need to equip a special room for storing server equipment and hire expensive IT personnel.

Data centers differ primarily in their technical capabilities and the types of services they provide. Corporate data centers that individually serve the interests of a large company share the palm with commercial data centers whose task is to serve organizations and private businesses of various sizes.

Each data center has its own set of infrastructures, the tasks of each of which are strictly individual:

Informational - provides the main functions of the data processing center, from which we will highlight the processing and storage of your data.

Telecommunications - provide reliable communication and data transfer between individual servers and their users.

Engineering infrastructure - guarantees stable and uninterrupted functioning of all systems of the server platform.

Modern data centers scan and are ready to offer their business partners and key customers a wide range of care and support services. Let 's highlight as the main:

Rack rental - allows you to host your own servers, renting an entire rack for them with a profit. This service is suitable for companies whose security policy does not allow placing equipment in a common rack.

Hosting (physical server hosting) provides opportunities to host your own server hardware in dedicated racks in a data center.

Renting servers is an ideal option if your company does not have the personal equipment of the necessary configuration to ensure data stability. The main task in this case is to rent server capacity in the data center for a long time.

VPS (virtual private server) is suitable when there is an objective need to rent a virtual dedicated server for your project.

Virtual hosting is an indispensable service designed for hosting and successful, uninterrupted functioning of the web pages of a modern company.

Network security is a set of requirements and policies that are imposed on the corporate network infrastructure to analyze its operation and prevent attackers from accessing data, changing this data, modifying it, as well as the failure of the network or its individual resources.

Regardless of the scale and type of business, wherever the network infrastructure is used, hardware solutions and software products are needed to ensure network security.

Principles of network security

Among the fundamental principles of corporate network security, the following can be distinguished:

Protection of devices connected to the network. In order to reliably protect devices connected to the network, it is necessary to use modern high-tech solutions. For example, computers that can be attacked by viruses need to be protected with reliable antivirus software and set up automatic updates of their signature databases to minimize the risk of an attack.

Network devices must be resistant to failures and provide for the possibility of rapid recovery. It is important to systematically monitor the infrastructure in order to understand exactly what state a particular device, application, service is in and, if necessary, implement means to protect them.

The network bandwidth must be continuously monitored. If an attack is committed, it always entails considerable costs for restoring the system's operability. Therefore, it is necessary to use means of protection against targeted attacks and methods of preventing intrusions into the infrastructure. This will minimize the risks of success of the attackers, and will also minimize the company's data recovery costs.

The local network of the enterprise should be fault-tolerant and provide for the possibility of rapid recovery if necessary. It will not be possible to protect the network 100% under any circumstances, but it is possible

to provide for a quick transition from one resource to another in case of failure of the first one, which will happen unnoticeably for network users.

Network security tools

Attacks on the network infrastructure can be both active and passive (depending on the malicious software used by the attackers). Therefore, to ensure the security of the network, comprehensive measures are used:

- proxy servers;
- systems for detecting and preventing hacking threats;
- means of protection against targeted attacks;
- firewalls;
- network monitoring systems;
- VPN.

With the help of the tools described above, you can:

- protect corporate infrastructure from hacking;
- ensure a secure connection to the network of external devices;
- monitor and control the operation of the software;
- safely conduct banking transactions, etc.

"Network security" is a set of requirements imposed on the infrastructure of an enterprise's computer network and policies for working in it, which ensure the protection of network resources from unauthorized access.

The purpose of this article is to assess the current state of network security of the company's data center. Also, analysis of the architecture and design principles of the datacenter network, development of proposals and recommendations for improving the level of network security of the company's datacenter without serious performance losses using both existing network elements and additional security elements.

The field of activity of the work is the network infrastructure of the datacenter, which has several levels responsible for connecting to an external network, routing in the core of the network, etc. For effective network protection at each level of the network infrastructure, a multi-level end-to-end modular protection system based on the recommended Cisco SAFE architectures, the deployment of security systems taking into account the platform and the necessary functionality, the use of intelligent network mechanisms to improve control and management is necessary.

The thoroughness of the network infrastructure security assessment depends on the complexity of the telecommunications and IT solutions used, security solutions, as well as time, resources, and source data available for analysis.

The analysis was carried out on the basis of the following initial data

- conclusions of configuration commands with hidden real IP addresses and passwords;
- спецификация specification of the operated active network equipment;

In this assessment, the main efforts were focused on analyzing the measures taken to effectively protect each individual network layer, analyzing performance requirements, as well as the control and management systems used.

Materials and methods. The article provides a general description of the technologies used to protect the datacenter network. The network infrastructure of the datacenter has several levels responsible for connecting to an external network, routing in the core of the network, etc. For effective network protection at each level of the network infrastructure, a multi-level end-to-end modular protection system based on the recommended Cisco SAFE architectures, the deployment of security systems taking into account the platform and the necessary functionality, the use of intelligent network mechanisms to improve control and management is necessary. The network access layer consists of a connection to an Internet provider (network perimeter), and a consolidated LAN (Local Area Network) and SAN (Storage Area Network) connection to a network of servers (internal network). The core layer of the network consists of a virtual switching system - Virtual Switch System (VSS). [1]

The "Level-separated datacenter scheme" is shown in Figure 1.

Fig. 1- Data center diagram divided by levels

Figure 2 also provides an overview of the data center network architectures. [2]

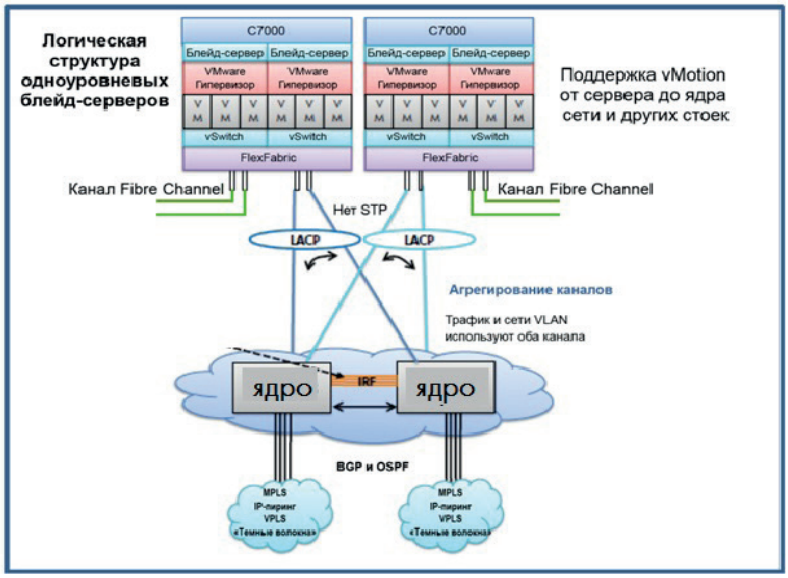

Fig. 2- Overview of the data center network architectures

Perimeter fault tolerance is provided by two ASR1001 series routers and the GLBP (Gateway Load Balancing Protocol) protocol. [3]

The fault tolerance of the network core is provided by two Catalyst 6504E switches combined into a single virtual switching system - VSS and the technology used for uninterrupted switching - NSF/SSO (Nonstop Forwarding with Stateful Switchover). The following security features are configured on the perimeter of the network:

- Protection against fake IP addresses URPF (Unicast Reverse Path Forwarding);
- Access list without session status monitoring on the external interface;
- Encryption and authentication of remote users by IPsec protocol (VPN);

The core of the network is configured with basic network protection in the form of segmentation on VLAN (Virtual Local Area Network).

Results. The composition of the perimeter equipment and the core of the network. The company's network equipment consists of 2 units of routers, 2 units of switches and 2 units of traffic balancer modules installed in the core switch.

Summary configuration data for routers, switches, and load balancer modules are shown in Table 1.

Table 1- Equipment of the perimeter and core of the company's network

Модель	**Operating system**	**Proces-sor**	**Flash**	**RAM**	**Num-ber of line cards (pcs.)**	**Ports quantity /(speed)/type**	**Power supply unit quantity (pcs.)/ power (Вт.)**
Cisco Systems, Inc. ASR1001	asrl001-universalk 9.03.04.02-S.151-3.S2.bin	N/A	7741 Mbytes	4194 Mbytes		12/(1000)/ optical	2/400
Cisco Systems, Inc. ASR1001	asr!001-universalk 9.03.04.02.S.151-3.S2.bin	N/A	7741 Mbytes	4194 Mbytes		12/(1000)/ optical	2/400
Cisco Systems, Inc. WS-C6504-E 4 slot switch	s72033-ipbasek 9-mz.l22-33.SXJ2.bin	600 Mhz			1	49/(10/100/1000)/ copper 2/(1000)/ optical 2/(10000)/ optical	2/2700
Cisco Systems, Inc. WS-C6504-E 4 slot switch	s72033-ipbasek 9-mz.l22-33.SXJ2.bin	600 Mhz			1	49/(10/100/1000)/ copper 2/(1000)/ optical 2/(10000)/ optical	2/2700

The Cisco router of the following model serves as a platform for the organization of the network Perimeter;

- Cisco ASR1001

The network core layer is built on hardware;

− Cisco Cisco Catalyst WS-C6504-E with ACE30-MOD-K9 service modules

Incoming traffic from the Internet is terminated at the IP address of the ACE traffic balancer and sent further to the back-end of the server.

Now let's consider the organization of the physical connection of the network. Each perimeter router with an Internet provider is connected via 3 GigEthernet links combined into a logical Etherchannel.

Perimeter routers are connected to core switches integrated into the VSS virtual switching system also by means of 3 GigEthernet links integrated into the Etherchannel logical channel.

The core switches are combined by one TenGigEthernet link to organize a virtual switching link - VSL (Virtual Switch Link), and the subsequent organization of a virtual switching system - VSS (Virtual Switch System).

Connection to the server farm is organized through interfaces with bandwidth - TenGigEthernet.[4]

The "Physical connection organization scheme" is shown in Figure 3.

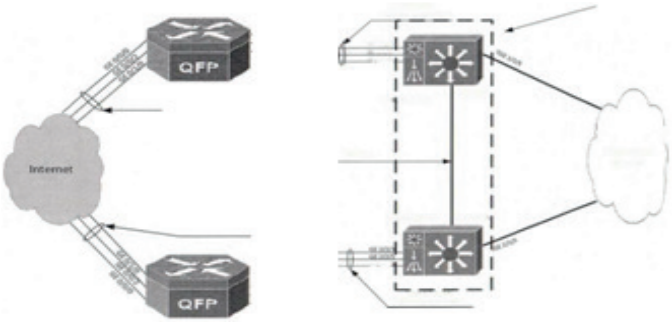

Fig. 3- Diagram of the organization of the physical connection.

Consider the logical infrastructure of the network. The logical infrastructure of the network consists of virtual IP networks for various purposes. Two instances of the dynamic OSPF protocol (Open Shortest Path First) with a virtual switching system and the dynamic routing protocol eBGP (External Border Gateway Protocol) with the provider's equipment for Internet access are running on perimeter routers.

The OSPF protocol, along with IS-IS, belongs to the Link State class of routing protocols. The principles of this class are that in addition to all optimal routes to remote networks, there should be a complete network map in the router's memory, including with active connections between other routers. OSPF was originally created as an open protocol, which made it the most common among routing protocols. Its algorithm makes it quite easy to build a protocol stack for OSPF. Therefore, for specialists related to networks, it is important to understand, at least, the general principles of its work. [5]

The bgp dynamic routing protocol allows you to dynamically monitor the status of the main and backup Internet channels, and also allows you to announce public addresses of your own private autonomous system (AS-65244).

The first instance of the OSPF protocol includes a public network with a virtual IP address of back-end servers, and also generates a default route for the internal network.

The second instance of the OSPF protocol provides connectivity of internal networks with a private pool of a remote access network (VPN). The diagram of the logical network of the company is shown in Figure 4.

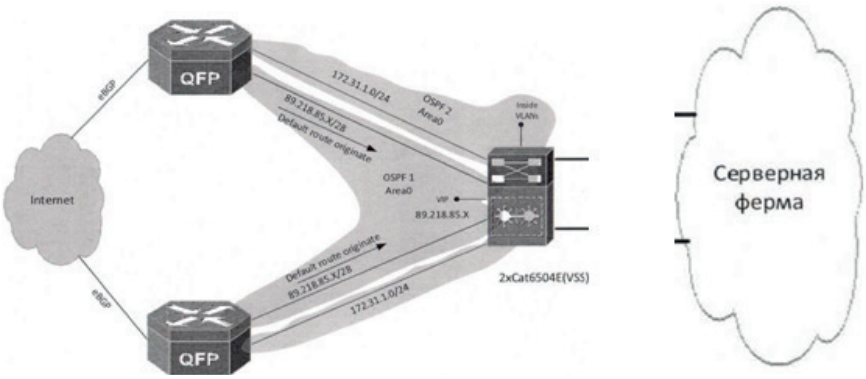

Fig. 4 - The scheme of the logical network of the company.

Discussion. Consider the perimeter of a datacenter, the current architecture of building a network perimeter is organized on powerful ASR1001 routers designed for use in large data processing centers and designed for aggregation of WAN (Wide Area Network) connections.[6]

The ZBF function is activated and configured on perimeter routers with the inspection of the state of transit traffic and traffic from/to routers. However, the interfaces are not set up in the appropriate zones, and accordingly there is no traffic inspection.

The password for the SNMP (Simple Network Management Protocol) community is set by default.

The reason for the last reboot of the ASR1001-01 router is an emergency reboot, with information about the reasons in the crash info file, which is located in flash memory.

The database of accounts for authentication of remote access to the management of network perimeter equipment, and for providing access to the internal network is performed locally on perimeter routers. There is no authorization and accountingthe connection.

Remote control of perimeter equipment is performed both via the secure SSH protocol (Secure Shell Secure) and via the non-secure Telnet protocol. There is no list of restrictions on which IP networks or IP addresses of hosts are allowed to manage the network perimeter equipment.

The core layer of the datacenter- the core of the network is a virtual switching system - VSS.

VSS is implemented on the Catalyst 6504E modular switches.

The core switches, in addition to switching traffic, also routes traffic with the perimeter of the network.

Network segmentation using - VLAN (Virtual Local Area Network) has been implemented on the switches, but there are no access filtering lists between segmented networks.

For fault tolerance of the topology at the L2 level, the RPVSTP (Rapid PerVLAN Spanning Tree Protocol) protocol has been applied, but the STP (Spanning Tree Protocol) Toolkit has not been applied, providing predictable behavior of the Spanning Tree Protocol.

There is no logging (syslog) of events on the network core hardware.

The database of accounts for authentication of the management of the network core equipment is made locally on the switches. There is no authorization and accountingthe connection.

Remote control of the kernel hardware is performed both via the secure SSH protocol (Secure Shell) and via the non-secure Telnet protocol. There is no list of restrictions on which IP networks or IP addresses of hosts are allowed to manage the network core equipment.

The switches do not have protection against unidirectional channels – UDLD (Unidirectional Link Detection).

There are no lists of allowed VLANs on the switch interfaces configured in - trunk mode.

Network management: There are no data center network management tools to protect and optimize the network.

On perimeter routers, network management is performed from a dedicated network, but there are no filtering lists that allow you to restrict access for management.

There is no direct connection to the dedicated management network (OOV-Out-of-Band) on the core switches.

Intrusion prevention system: there are no means of deep traffic inspection on a behavioral and signature basis in the network to prevent intrusion into the network.

Recommendations for improving network security. [7]

1. Around the perimeter of the datacenter. Traffic inspection.

Observation: on perimeter routers, interfaces are not installed in the corresponding zones, and accordingly, there is no packet inspection of traffic between zones.

Impact: the absence of packet inspection with status control does not allow for stricter traffic control on the network perimeter, dynamically monitoring the status of both open and semi-open sessions.

Recommendation: following modern approaches in building protection at the network level when using IOS (Interworking Operation System), it is recommended to use the built-in tools of this operating system. [8]

2. On the protection of SNMP (Simple Network Management Protocol).

The SNMP protocol was developed to test the functioning of network routers and bridges. Subsequently, the scope of the protocol also covered other network devices, such as hubs, gateways, terminal servers, LAN Manager servers, Windows NT machines, etc. In addition, the protocol allows for the possibility of making changes to the functioning of these devices.

Surveillance: On perimeter routers, the password for SNMP community is set by default.

Influence: allows you to read various data from the equipment.

The main interacting persons of the protocol are agents and management systems. If we consider these two concepts in the language of "client-server", then the role of the server is performed by agents, that is, the very devices for which the protocol we are considering was developed. Accordingly, the role of clients is assigned to management systems - network applications necessary to collect information about the functioning of agents. In addition to these two subjects, two more can also be distinguished in the protocol model: the control information and the data exchange protocol itself.

"Why do I need to poll the equipment at all?" - you ask. I will try to shed some light on this issue. Sometimes, during the operation of the network, it becomes necessary to determine certain parameters of a certain device, such as, for example, the size of the MTU, the number of packets received, open ports, the operating system installed on the machine and its version, to find out whether the forwarding option is enabled on the machine, and much more. To implement this, SNMP clients are the best suited.

In addition to the above, the protocol in question has another very important feature, namely the ability to modify data on agents. Of course, it would be stupid to allow modification of absolutely any parameter, but, despite this, the number of those parameters for which a write operation is allowed is simply frightening. At first glance, this completely refutes the entire theory of network security, but if you delve into the question, it becomes clear that not everything is as running as it seems at first glance. "To be afraid of wolves is not to go into the forest." After all, with a little effort by the network administrator, you can reduce the risk of successful completion of the attack to a minimum. [9]

Recommendation: replace the password with a complex one, limit the list of control systems connected to perimeter routers via the SNMP protocol using access lists - ACLs (Access Control List). [10]

3. By the core of the data center network, that is, traffic limitation between network segments.

Observation: on switches, network cores are segmented using - VLANs, but there are no access filter lists between networks.

Impact: various kinds of attacks from internal network segments to neighboring networks. Reduced network performance by parasitic traffic.

Recommendation: configure access filter lists between segmented internal networks.

4. On the stability and security of STP.

STP the operation of the spanning tree protocol is not "flawless", and there are hidden security risks in the operation of STP, so it is necessary to use the STP security mechanism to eliminate these potential risks. In this experiment, three STP security mechanisms will be presented: Bpdu Guard, RootGuard, Loop Guard.

The principle of operation in a switched environment, STP selects root and supports STP operation by sending BPDUs during operation. STP security rules are also implemented through BPDU "monitoring". The security rule for implementing STP is to restrict the connected switching equipment (the switch will send BPDU information when it is connected to the switching environment). Prohibit the switch from accessing the network, only access to the terminal; prohibit the switch from sending information to displace the root role, etc.

Observation: STP Toolkit is not applied on core switches, which provide predictable behavior of Spanning Tree Protocol.

Impact: The lack of the Spanning Tree Toolkit negatively affects the stable and secure operation of STP.

Recommendation: You should make the most of the set of additions to STP from Cisco - Spanning Tree Toolkit, containing the following commands: [11]

- Rootguard
- Loopguard
- UplinkFast
- UDLD
- BPDU Guard
- Root Guard
- PortFast
- Port Security

4. By using the UDLD (Unidirectional Link Detection) protocol.

Unidirectional Channel Detection (UDLD) is a data channel layer protocol from Cisco Systems designed to monitor the physical configuration of cables and detect unidirectional channels. UDLD complements the Spanning Tree Protocol, which is used to eliminate switching loops.

- Unidirectional Link Detection (UDLD) is one of the two main functions (UDLD and loop guard) in Cisco switches to prevent layer 2 loops.

- The Spanning Tree Protocol (STP) resolves redundant physical topology into a tree-like forwarding topology without loops by blocking one or more ports. The advantages of using UDLD on optical channels are obvious. In optical communication lines, light is used for data transmission, when using which there is no need for a closed circuit, as in the case of copper cables (in which each pair of conductors is a closed circuit). In this regard, there is a possibility of failure of only one direction of data transmission on the communication line.

Observation: Unidirectional protection (UDLD) is not applied on switches.

Impact: UDLD helps STP work by preventing switching errors on optical distribution frames.

Recommendation: use UDLD aggressive mode on optical channels for maximum protection against partially failed (unidirectional) connections. [12]

5. By event logging.

Observation: No event logging on core switches.

Impact: lack of log entries about important / critical events on the network.

Recommendations: configure event logging to a remote server - syslog. [13]

6. According to the list of VLANs on trunk ports.

Observation: on the interfaces of the switch configured in trunk mode, there are no lists of allowed VLANs.

Impact: Unwanted traffic on backbones leads to reduced network security and performance.

Recommendation: configure the list of allowed VLANs on trunk ports configured in trunk mode. [14]

7. By intrusion prevention.

Observation: The network does not have deep traffic inspection tools that work on a behavioral and signature basis.

Impact: the risk of various malicious acts being carried out through the data network. Failure of the network, as well as IT systems and servers.

Best practice: Install an intrusion prevention system (IPS) with sufficient performance to monitor network traffic anomalies. It is advisable to install the intrusion prevention system in the IDS (Intrusion Detection System) mode, and analyze the traffic after the balancing system - ACE. This design of the IPS layout will allow you to analyze unencrypted SSL (Secure Socket Layer) traffic. [15]

8. Management and monitoring. Remote connection.

Monitoring: there is a possibility of remote control of the perimeter and network core equipment using an unprotected protocol - Telnet.

Impact: credentials (login / password) are transmitted by the telnet protocol in cleartext. There is a risk of intercepting credentials.

Recommendation: leave the SSHv2 protocol for remote control of equipment. Limit the list of IP addresses from which it is possible to connect to active network equipment using ACLs. [16]

9. By account base

Observation: The management and dial-up credentials database is stored locally in the hardware configuration file.

Impact: risks of compromising credentials, lack of flexible authorization and accounting mechanisms.

Recommendation: to use an external system for Authentication, Authorization and Accounting, operating under the secure protocol TACACS + (Terminal Access Controller Access Control System). TACACS+ (English Terminal Access Controller Access Control System plus) is a session protocol, the result of further improvement of TACACS undertaken by Cisco.

Protocol security (encryption) has been improved, and the separation of authentication, authorization and accounting functions has been introduced, which can now be used separately.

TACACS+ uses the concepts of sessions. Within the framework of TACACS+, it is possible to establish three different types of AAA sessions (English authentication, authorization, accounting). Establishing one type of session generally does not require prior successful establishment of any other. The protocol specification does not require opening an authorization session to open an authentication session first. The TACACS+ server may require authentication, but the protocol itself does not stipulate this. [17]

10. By dedicated management (DED) *

Monitoring: Not all active network equipment is managed from a dedicated network.

Impact: secure connection, management, and monitoring of network equipment, reducing network downtime.

Recommendation: use an alternative secure access through a dedicated management network to connect to network equipment. [18]

11. By monitoring

Best practice: Use solutions to efficiently and centrally deliver all aspects of security policies for firewalls (ZBF), virtual networks (VPNs), intrusion prevention tools (IPS).

Network monitoring and diagnostics tools are needed that provide data about network devices, automate routine network management tasks, collect and provide data on device loading, and provide functions for localizing and diagnosing network problems. Figure 4 “Recommended circuit with additional network components” [19]

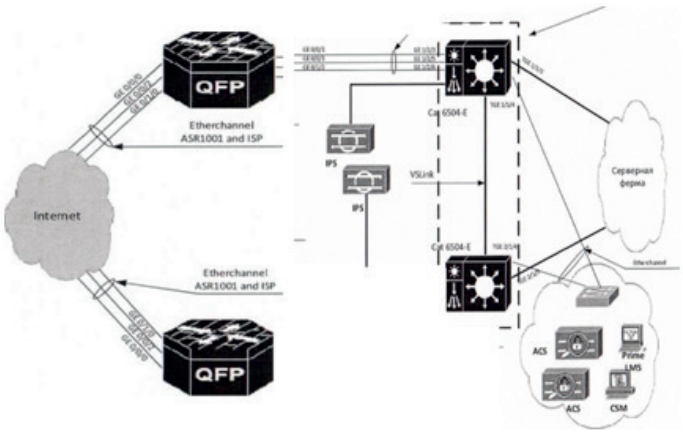

Fig. 4- “Recommended circuit with additional network components”

Conclusion. In conclusion, the security assessment of the network infrastructure of the data center was carried out on the basis of a study of technological materials provided by the company’s specialists. The results of the assessment allow us to make the following statements:

− the infrastructure of the company’s data center is built on a high-performance hardware platform;

− the design of the network is built using technology to ensure high availability of the network;

− the traffic inspection function with monitoring the network session status is available and configured at the network perimeter;

− remote network management has weak protection against various kinds of attacks on the data transmission network;

− There are no “best practices” solutions focused on building secure networks, and some are not used effectively enough.

Each perimeter router with an Internet provider is shown connected via 3 GigEthernet links combined into a logical Etherchannel. Perimeter routers are connected to core switches integrated into the VSS virtual switching system also by means of 3 Gig Ethernet links integrated into the Etherchannel logical channel. The core switches are combined by one Ten Gig Ethernet link to organize a virtual switching link - VSL, and the subsequent organization of a virtual switching system - VSS. Connection to the server farm is organized through interfaces with bandwidth – Ten Gig Ethernet.

It is said about the logical infrastructure of the network, which consists of virtual IP networks for various purposes. Two instances of the dynamic OSPF protocol with a virtual switching system and the eBGP dynamic routing protocol with the provider’s equipment for Internet access are running on perimeter routers. The bgp dynamic routing protocol allows you to dynamically monitor the status of the main and backup Internet channels, and also allows you to announce public addresses of your own private autonomous system (AS-65244). The first instance of the OSPF protocol includes a public network with a virtual IP address of back-end servers, and also generates a default route for the internal network.

The second instance of the OSPF protocol provides connectivity of internal networks with a private pool of a remote access network (VPN).

Based on the above statements, in order to improve the security, reliability, availability of the data center network, to minimize the risks in the operation of the data transmission infrastructure, and also considering that the data transmission network is one of the most important components of the IT infrastructure, it is necessary to follow the recommendations given in the article.

Ташенова Ж.М.[1*], Нурлыбаев Э.Н.[2], Абдугулова Ж.К.[3], Аманжолова Ш.А.[4]

[1,3]Л. Гумилев атындағы Еуразия ұлттық университеті, Нұр-Сұлтан, Қазақстан;
[2] Т.Қ. Жүргенев атындағы Қазақ Ұлттық өнер академиясы, Алматы, Қазақстан;
[4]Құрманғазы атындағы Қазақ ұлттық консерваториясы, Алматы, Қазақстан.
E-mail: zhuldyz_tm@mail.ru

ДЕРЕКТЕР ОРТАЛЫҒЫНЫҢ ЖЕЛІЛІК ИНФРАҚҰРЫЛЫМЫНЫҢ ҚАУІПСІЗДІК ЖАҒДАЙЫН БАҒАЛАУ

Аннотация. Бұл мақаланың мақсаты компанияның деректер орталығындағы желі қауіпсіздігінің ағымдағы жағдайын бағалауға негізделген. Дата-орталық желісінің архитектурасы мен дизайн принциптерін талдау, қолданыстағы желі элементтерін де, қосымша қауіпсіздік элементтерін де пайдалана отырып, өнімділікті жоғалтпай компанияның деректер орталығының желілік қауіпсіздік деңгейін арттыру бойынша ұсыныстар мен ұсынымдарды әзірлеу. Дата-орталық ақпаратты өңдеу, сақтау және тарату функцияларын, әдетте, корпоративтік клиенттердің мүдделері үшін орындайды – ақпараттық қызмет көрсету арқылы бизнес мәселелерін шешуге бағытталған. Желілік инфрақұрылымға шабуылдар да қарастырылады, олар белсенді және пассивті болуы мүмкін (шабуылдаушылар пайдаланатын зиянды бағдарламаға байланысты). Желілік инфрақұрылымның қауіпсіздігіне мұқият бағалау жүргізілді, ол қолданылатын телекоммуникациялық және АТ шешімдерінің күрделілігіне, қауіпсіздік шешімдеріне, сондай-ақ талдау үшін қол жетімді уақытқа, ресурстарға және бастапқы деректерге байланысты. Сондай-ақ жасырын нақты IP мекенжайлары мен құпия сөздері бар конфигурация командаларының шығуы, қолданыстағы желілік жабдықтың спецификациясы негізінде талдау жүргізілді. Бағалауда негізгі күш әрбір жеке желі деңгейін тиімді қорғау бойынша қабылданған шараларды талдауға, өнімділік талаптарын талдауға, сондай-ақ пайдаланылатын мониторинг және бақылау жүйелеріне бағытталды. Желінің периметрін құрудың ағымдағы архитектурасы ірі деректерді өңдеу орталықтарында пайдалануға арналған және WAN (Wide Area Network) қосылымдарын біріктіруге арналған қуатты ASR1001 маршрутизаторларында ұйымдастырылған деректер орталығының периметрі қарастырылады. Желінің қауіпсіздік деңгейін арттыру бойынша бірқатар ұсыныстар берілген.

Түйінді сөздер: желілік қауіпсіздік, деректер орталығы, желі, Cisco, виртуалды жеке сервер, прокси-серверлер.

Ташенова Ж.М.[1*], Нурлыбаев Э.Н.[2], Абдугулова Ж.К.[3], Аманжолова Ш.А.[4]

[1,3]Евразийский национальный университет имени Л.Н. Гумилева, Нур-Султан, Казахстан;
[2]Казахская национальная академия искусств имени Т.К. Жургенова, Алматы, Казахстан;
[4]Казахская национальная консерватория имени Курмангазы, Алматы,
Казахстан.
E-mail: zhuldyz_tm@mail.ru

ОЦЕНКА СОСТОЯНИЯ БЕЗОПАСНОСТИ СЕТЕВОЙ ИНФРАСТРУКТУРЫ ДАТА-ЦЕНТРА

Аннотация. Цель данной статьи основана на оценке текущего состояния сетевой безопасности дата-центра компании. Анализ архитектуры и принципов проектирования сети ЦОД, разработка предложений и рекомендаций по повышению уровня сетевой безопасности ЦОД компании без серьезных потерь производительности с использованием как существующих сетевых элементов, так и дополнительных элементов безопасности. Дата-центр выполняет функции обработки, хранения и распространения информации, как правило, в интересах корпоративных клиентов - он ориентирован на решение бизнес-задач путем оказания информационных услуг. Также рассматриваются атаки на сетевую инфраструктуру, они могут быть как активными, так и пассивными (в зависимости от используемого злоумышленниками вредоносного ПО). Проводилась тщательная оценка безопасности сетевой инфраструктуры, которая зависит от сложности используемых телекоммуникационных и ИТ-решений, решений безопасности, а также от времени, ресурсов и исходных данных, доступных для анализа. Также проводились анализ на основе вывода команд конфигурации со скрытыми реальными IP-адресами и паролями, спецификация эксплуатируемого активного сетевого оборудования. В оценке

основные усилия были сосредоточены на анализе мер, принятых для эффективной защиты каждого отдельного сетевого уровня, анализе требований к производительности, а также используемых систем контроля и управления. Рассмотрены периметр дата-центра, текущая архитектура построения периметра сети которой организована на мощных маршрутизаторах ASR1001, рассчитанных на использование в крупных вычислительных центрах обработки данных и предназначенных для агрегации WAN (Wide Area Network) соединений. Приведены ряд рекомендации по повышению уровня безопасности сети.

Ключевые слова: сетевая безопасность, дата-центр, сеть, Cisco, виртуальный частный сервер, прокси-серверы.

Information about the authors:

Tashenova Zhuldyz – PhD, L. N. Gumilyov Eurasian National University, Department of Information technology, Nur-Sultan, Kazakhstan. E-mail: zhuldyz_tm@mail.ru , ORCID: 0000-0003-3051-1605;

Nurlybaeva Elmira – PhD, Kazakh National Academy of Arts named after T. Zhurgenov, Almaty, Kazakhstan. E-mail: nuremuk@mail.ru, ORCID: 0000-0002-0479-7542;

Abdugulova Zhanat – PhD, L. N. Gumilyov Eurasian National University, Department of Information technology, Nur-Sultan, Kazakhstan. E-mail: janat_6767@mail.ru, ORCID: 0000-0001-7462-4623;

Amanzholova Sh. – assoc.professor, Kurmangazy Kazakh National Conservatory, Almaty, Kazakhstan. E-mail: schirin75@ mail.ru, ORCID: 0000-0002-6674-2766.

REFRENCES

[1] Foundation Learning Guide: Designing Cisco Network Service Architectures (ARCH), Cisco Press Third Edition.

[2] Securing Networks with Cisco Routers and Switches, Volume 1 Version 3.0.

[3]Cisco SAFE Reference Guide, *http: //www.cisco.eom/c/en/us/td/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg/chap4.html.*

[4]Internet Edge Solution Overview, *http: //www.cisco.eom/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/Internet_Edge/*InterEdgeOver.html#wp7206.

[5] Zapechnikov S.V. Information security of open systems. In 2 volumes. Vol. 1 - Threats, vulnerabilities, attacks and approaches to protection / S.V. Zapechnikov, N.G. Miloslavskaya. - M.: GLT, 2017.-- 536 p.

[6] Zapechnikov S.V. Information security of open systems. In 2 volumes. V.2 - Protection means in networks / S.V. Zapechnikov, N.G. Miloslavskaya, A.I. Tolstoy, D.V. Ushakov. - M.: GLT, 2018 .-- 558 p.

[7] Tashenova Z., Nurlybaeva E., Tulegulov A., Abdugulova Z. Sql-attack research and protection/ Journal of Theoretical and Applied Information Technologythis link is disabled, 2021, 99(19), 4536–4545 p.

[8] Malyuk A.A. Information security: conceptual and methodological foundations of information security / A.A. Malyuk. - M .: GLT, 2016 .-- 280 p.

[9] Partyka T.L. Information security: Textbook / T.L. Partyka, I.I. Popov. - M.: Forum, 2016.- 432 p.

[10] Petrov S.V. Information security: Textbook / S.V. Petrov, I.P. Slinkova, V.V. Gafner. – M.: ARTA, 2016.- 296 p.

[11] Semenenko V.A. Information security: Textbook / V.A. Semenenko. - M.: MGIU, 2017 -- 277 p.

[12] Chipiga A.F. Information security of automated systems / A.F. Chipiga. - M.: Helios ARV, 2017.-- 336 p.

[13] Babash A.V. Cryptographic methods of information protection: Academic pos.: Vol. 1 / A.V. Babash-2izd. -ITS RIOR, SIC INFRA-M, 2016-413s (/ A.V. Babash. - Moscow: Mir, 2016.-- 597 p.

[14] Baranova E.K. Information security and protection. Textbook / E.K. Baranova, A.V. Babash. - M.: RIOR, Infra-M, 2016.-- 324 p.

[15] Borisov M.A. Fundamentals of organizational and legal protection of information / M.A. Borisov O.A. Romanov. - M.: Lenand, 2014.-- 248 p.

[16] Borisov M. A. Fundamentals of software and hardware information security / M.A. Borisov, I.V. Zavodtsev, I.V. Chizhov. – M.: Librokom, 2013.-- 376 p.

[17] Varlataya S.K. Cryptographic methods and means of ensuring information security. Study guide / S.K. Varlataya, M.V. Shakhanov. - M.: Prospect, 2015.-- 152 p.

[18] Vasilenko O. N. Number-theoretic algorithms in cryptography / O.N. Vasilenko. – M.: Moscow Center for Continuous Mathematical Education (MCNME), 2006. - 856 p.

[19] Emelyanova N.Z. Information protection in a personal computer / N.Z. Emelyanova, T.L. Partyka I.I. Popov. - M.: Forum, 2009.- 368 p.

МАХМҰНЫ

ФИЗИКА

ИНФОРМАТИКА

МАТЕМАТИКА

СОДЕРЖАНИЕ

ФИЗИКА

ИНФОРМАТИКА

МАТЕМАТИКА

CONTENTS

PHYSICS

COMPUTER SCIENCE

MATHEMATICS

Publication Ethics and Publication Malpracticein
the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethicalguidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any otherlanguage, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайтах:

www:nauka-nanrk.kz

http://physics-mathematics.kz/index.php/en/archive

ISSN2518-1726 (Online),
ISSN 1991-346X (Print)

Редакторы: *М.С. Ахметова, А. Ботанқызы, Д.С. Аленов, Р.Ж. Мрзабаева*
Верстка на компьютере *Г.Д.Жадыранова*

Подписано в печать 10.12.2021.
Формат 60x881/8. Бумага офсетная. Печать –ризограф.
9,5 п.л. Тираж 300. Заказ 6.

Национальная академия наук РК
050010, Алматы, ул. Шевченко, 28, т. 272-13-19