IJDI-ERET

INTERNATIONAL JOURNAL OF DARSHAN INSTITUTE ON ENGINEERING RESEARCH AND EMERGING TECHNOLOGIES
Vol. 10, No. 1, 2021
www.ijdieret.in

(Review Article)

Protecting Networks from Modern Threats with Next-Generation Firewalls

Rutvik Patel[1*]

[1*]*Institute of computer science and technology (Ganpat University) Ahmedabad, Gujarat, INDIA*

Abstract

Traditional firewalls have long been incapable of dealing with the new threats that everyday Internet users face. The next-generation firewalls are the subject of this article. The paper's first section discusses current threats and assaults. We went through the attacks in great detail since they are among the most common and can harm the device. Then we went over the theoretical foundations of firewalls and the features of next-generation firewalls. We conducted various tests of next-generation firewalls in the following section, reviewing and reporting. The paper aimed to see whether next-generation firewalls are suitable to replace traditional firewalls and thus lead to adequate Internet user security.

Keywords: Next-generation firewall, security, DoS attack, APT attack.

1. Introduction

The use of the Internet is increasing daily, and so is the number of users. The global network has become an indispensable tool, both in performance work commitments and leisure, and has practically changed the way we live our lives. However, when using the Internet, users and organizations in which users operate are vigilant of many threats. Attackers try to use malicious software to prevent the use of the Internet, destroy or illegally obtain critical information, intellectual property, etc., to obtain a financial advantage or a competitive advantage. Therefore, organizations need to provide adequate protection against these attacks.

.

The situation has changed drastically in the last few years. Due to globalization, much more accessible the possibilities of connectivity, mobility, virtualization, and the emergence of cloud computing have entirely changed the realities of networking. The rapid evolution of the Internet and applications has brought a completely different way of communicating users to the Internet. Of course, they did in parallel; they also spread and developed threats that threaten users, and standard one's firewalls are no longer up to par, and there is a need for more advanced system protection [1].

Experts in network security have developed the *"Next Generation Firewall,"* based on an innovative approach to network traffic analysis; and ensuring safety. Because next-generation firewalls are a relatively new product on the market, there are no standards yet that they must meet. Also, the price of such firewalls is higher compared to traditional ones.

Because traditional firewalls are no longer enough to ensure an organization's security, we are decided to perform a firewall performance, and performance analysis of the following generation and help organizations determine whether such a firewall is the right choice to improve their network security.

In the following, we will overview modern network threats and attacks and list some information on network threats, network technology itself, network security, and firewalls.
We also performed a practical test on the cisco firewall of the next generation with purpose: -

- analyze the capabilities of firewalls and thus check whether they meet today's requirements for high-speed internet connection,
- analyze the effectiveness of next-generation firewalls in protecting the network from the most common modern threats, such as DoS attacks and APT attacks,
- assess whether the next-generation firewalls are adequate and sufficient protection for modern networks of organizations.

In the concluding part, we examined the test results, commented on them, and assessed whether the next-generation firewall helps improve information security.

[*]*Corresponding Author: e-mail: rutvikonline@gmail.com,*
ISSN 2320-7590

2. Modern Network Threats and Attacks

As the number of users connected to the World Wide Web increases, so does the number of threats that prey on an individual user or organization. IT experts note that most cyber threats pass into the organization's network from the Internet.

Years ago, the biggest threats to Internet users were the following [2]:

- viruses and worms,
- Trojan horses,
- SPAM oz. unsolicited email,
- phishing oz. fishing,
- packet Sniffing oz. sniffing,
- websites with malicious code,
- password attacks

With the advancement of information technology and the rapid increase in the number of devices and Internet-connected users, threats have also evolved and changed. Cybernetic crime has become a means of obtaining a financial gain, and a natural system has been developed for support for cybercriminals. Anyone can quickly come up with different tools today for creating threats and attacks - buy them on the black market. Specialization and easy accessibility to such tools has led to an incredible increase in threats and cybercrime.

Thus, today we can trace the following internet threats:

- DoS (Denial of Service) attacks oz. denial of service attacks,
- APT (Advanced Persistent Threat) oz. advanced persistent threats,
- Zero-day attacks,
- Ransomware oz. extortion viruses,
- Watering Hole attacks,
- identity theft,
- attacks on mobile devices,
- Phishing attacks and attacks with social engineering

3. Firewall

A firewall acts as a barrier between a trusted network and other networks such as the Internet. The firewall controls access to resources within the network with a positive control model. This means that only well-defined network traffic is allowed, and all other traffic is rejected. The term firewall is borrowed from extinguishing and preventing fires where a firewall is located used as a barrier to prevent the spread of fire.

Before the advent of firewalls, in the late 1980s, there was the only proper form of networking ACLs (Access Control List). ACL lists will determine which IP addresses are granted network access and which are not. The rapid spread of the Internet and, consequently, more excellent connectivity between networks has led to this the type of traffic filtering was no longer enough to successfully protect the system, as they are in the header package only basic information. Digital Equipment Corp launched the first commercial firewall, DAC SEAL, in 1992. Since that day, firewall technology has constantly been evolving develops to be able to withstand the rapid rise of sophisticated cyber-attacks.

3.1 Principles of firewall operation

3.1.1 TCP / IP reference model: TCP / IP stands for Transmission Control Protocol and Internet Protocol. This is a model that is used in the current architecture of the Internet. Protocols are a set of rules that govern the whole network communication. These protocols describe the movement of data between source and destination and all communication on the Internet.

The United States Department of Defence developed TCP / IP as part of a project to exploring network connections to connect remote devices. The principles they followed that led to the TCP / IP model are:

- support for a flexible architecture
- adding new devices to the network was easy,
- the network was robust and fault
- tolerant.

Connections are made as long as the devices are not interrupted.

The basic idea in the development was to enable applications on a single computer to communicate (sending packets) to another application running on another computer.

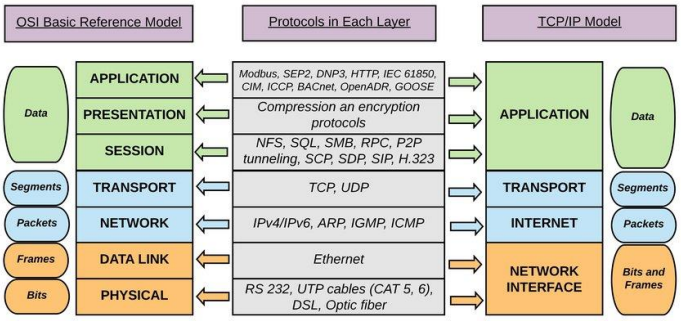

Figure 1. TCP/IP Reference Model

The TCP/IP model consists of four layers [3]:

I. **The connection layer indicates** how data is physically transmitted over the network, including how devices are directly connected to the network medium (coaxial cable, copper cable, optical cable) signal bits. The protocols

used in this layer are: *Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS- 232, v.35.*

II. **Internet layer** - defines the details of grouping packets into IP frames that contain source and destination IP address information. This information is then used for transmission frames over the network. It also performs IP frame routing. The protocols used in this layer are *IP, ICMP, ARP, RARP.*

III. **Transport layer** - allows you to manage a communication session between computers. Specifies the level of service and connection status used for data transmission. The protocols used in this layer are *TCP, UDP, RTP.*

IV. **Application layer** - defines the protocols of TCP / IP applications and defines how programs communicate with a transport layer for network use.

The protocols used in this layer are *HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP, X Windows*, other user protocols.

3.1.2 NAT - network address translation: NAT (Network Address Translation) is a mapping method from one IP address to another by changing the IP address information in the IP frame header while crossing a traffic routing device. The lack of public or IP addresses suitable for routing on the Internet is crucial today. It enables communication to all computers from a specific local area network to the Internet via a single IP address. So makes a significant contribution to maintaining the global address space [4].

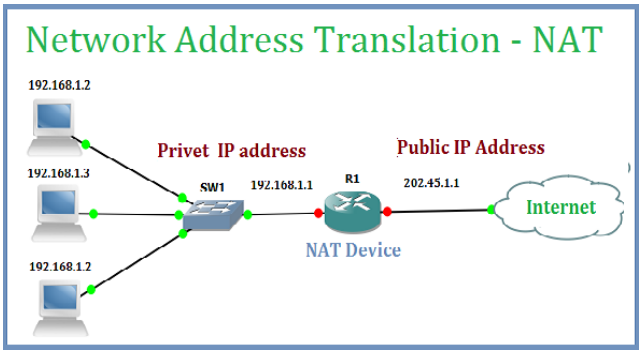

Figure 2. NAT

NAT is implemented by a device placed on the edge between the local network and the Internet. Because v most of today's networks this firewall, this is the basic functionality of all firewalls.

3.1.3 Batch filtering: The original firewalls operated using packet filtering. Batch filters work with insight into the "packets" that are transmitted between computers on the Internet. If the package does not match packet filter rules, the filter will discard it. Conversely, if the package matches one or more programmed filters, the firewall drops it into the network. This type of filtering doesn't matter if it is a packet part of an existing traffic stream - it does not store any connection status information.

Packet filtering is based only on the information contained in the package itself (most often it is a combination of the source and destination IP address, protocol, TCP or UDP traffic, and number neck). It works on the network layer.

3.1.4 Stateful inspection or condition control: Stateful inspection, also known as dynamic packet filtering. It's firewall technology, which monitors the status of active connections as they traverse the firewall and uses this information for determining which network packets to drop through the firewall. Stateful inspection has largely replaced the older static packet technology filtering.

In static packet filtering, the firewall only scanned the IP packet header. The firewall uses this scanning mode to monitor currently active connections. Stateful inspection records information about the source and destination IP address, port, applications, and other connection information [5].

For example, if there is a rule on the firewall that allows the computer to connect to the web server, the firewall records the connection information. When the server responds, the firewall detects that a response is expected from the webserver to the computer. Drop the answer through the firewall without a reviewed database of security rules. The security rule must allow for initial outgoing traffic, and then the firewall writes the link in the connection table.

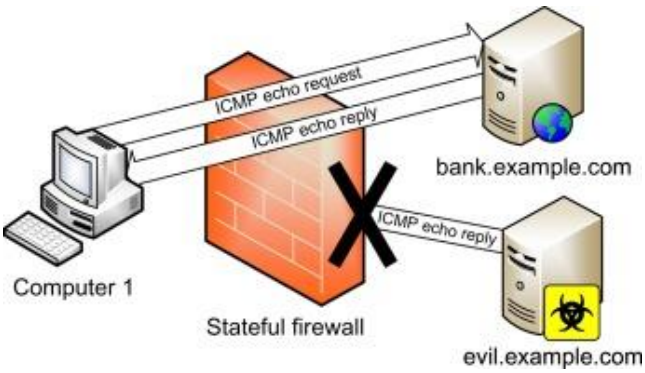

Figure 3. Stateful inspection

3.2Next-generation firewalls

The Next Generation Firewall (NGFW) is a firewall that can detect and block advanced attacks, using application-level security policies and at the gateway level and protocols. Next-generation firewalls combine three key aspects: high performance, a system for intrusion prevention (IPS), and application control. Much like the introduction of "stateful inspection" in the first generation of firewalls, the firewalls also bring the next generation an additional dimension in the

firewall decision-making process. With the ability to detail analysis and understanding of traffic, can take adequate measures to block traffic and prevent the exploitation of vulnerabilities [6].

Next-generation firewalls combine the capabilities of traditional firewalls - including packet filtering, network address translation (NAT), URL blocking pages, with functionalities and features not found in traditional firewalls. These include the Intrusion Prevention System (IPS), SSL protocol review and decryption, deep packet analysis, malware detection, and application recognition.
This technology has been developed to prevent an increasing number of threats and attacks on the TCP / IP reference model.

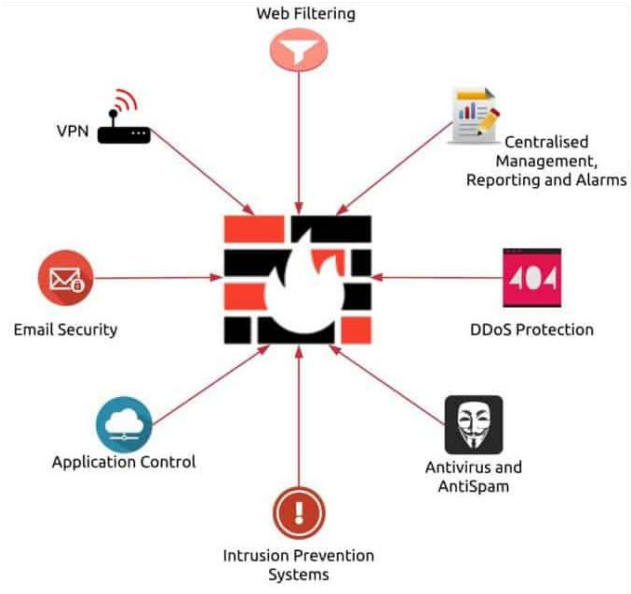

Figure 4. Next-Generation Firewall

3.2.1 Application recognition: The biggest difference between traditional firewalls and NGFW is the fact that the latter aware of applications. Traditional firewalls rely only on the standard doors they are supposed to apply and decide whether to allow traffic. NGFW, not v, further assumes that a particular application uses only specific ports. He can monitor traffic on all layers and determine what type of traffic is being sent and received. The most common example is the current use of HTTP port 80. Traditionally, this port is used only for HTTP traffic, but this is no longer the case; many different applications still use this port for communication and data transmission between the end-user and the server.

One port can be used for different types of traffic between the most common of which is the so-closed "tunneling" of application. The traffic at the source is hidden in HTTP packet data fields and then unwrapped to the destination through the tunnels. From the point of view of a traditional firewall looks like a simple HTTP web traffic packet, but NGFW detects its true purpose and blocks it before it reaches its goal.

3.2.2 User identification: Another big difference between traditional firewalls and NGFW is that the latter can determine the identity of the source of network traffic - user or device. That means the firewall connects IP addresses with users for more accessible and more efficient execution control of permitted traffic. The firewall connects to existing ones for identity information organization authentication systems (active directory, LDAP). This way, network administrators control who can use specific applications, not just which traffic is allowed or not.

3.2.3 Antivirus and malware protection: Next-generation firewalls can detect viruses and malware in traffic destined for the network. In this way, they can block such traffic on their early transmission and reduce the risk of computer infections in the system. Most firewalls of the next generation use a database of virus definitions of well-known antivirus manufacturers programs, and some companies maintain their base.

3.2.4 Advanced IPS system: The IPS (Intrusion Prevention System) or intrusion prevention system is responsible for attack detection. Attack detection is based on several different techniques, including threat signatures, definitions of known exploitation attacks, detection of unusual network activity, and behavioral analysis of traffic.

A system where a traditional firewall is installed is often next to the firewall an intrusion detection system (IDS) or IPS is also installed. Usually, this appears as a stand-alone device or a separate logical unit within a single device. In firewalls the following generation, the IPS system is fully integrated. IPS functionality as such has not changed compared to a stand-alone system. However, because in this case, it is related to other advanced functionalities and thus has more information about the traffic itself, it is much more effective compared to a stand-alone system.

3.2.5 SSL decryption: More and more network traffic between clients and servers takes place over the Secure Socket (SSL) Layer standard, also called a layer of safe sockets. Next-generation firewalls can decipher such traffic and thus check for the possible presence of traffic threats that they do so that they act as an intermediate link (Man in the middle) in the communication between servers and clients. In this way, they can provide additional protection against pests applications and activities that some try to hide by using encryption. Without that option, firewalls would not be able to detect threats in running traffic as they would not detail analyze packages.

3.2.6 "Sandbox" - security analysis of files in the cloud or sandbox: Today's attackers have learned how to bypass various antivirus and intrusion protection based on definitions

and signatures databases. They can quickly change their usual malware and create so-called "Zero-day" threats. A new system was needed to detect threats that allow files that the firewall has not encountered so far; we analyze in a safe environment and determine if they want to harm us. Such a system we call sandbox.

There are two types of unknown threats:

- Threats based on known vulnerabilities and changing very quickly, in seconds or minutes. Signature-based control cannot follow such changes;
- threats based on unknown or *zero-day* vulnerabilities. Even with such threats, it has no signature-based system, no detection, and elimination options.

The best way to detect these unknown threats is to have files that contain such threats run in a secure and virtual environment. In such an environment, the file is run under control, and so her malicious behavior can be detected. When the system detects a threat, it examines it and creates a detailed description of it, or "signature." With the help of these signatures, this guy will attack can also detect and block the traditional intrusion prevention system.

Not all sandboxes are equally effective at detecting malicious code. Also, attackers are familiar with sandbox solutions and can develop such malicious software that can detect that it is located in the sandbox and is not running.

4. Perform firewall testing

With testing, we want to determine if next-generation firewalls are powerful enough to manage to meet today's needs for high-speed Internet connections and at the same time provide effective protection of the organization's network against modern threats.

We will describe and graphically present our test environment and the necessary settings equipment itself. Then we will explain the firewall with there exceptional advanced features to enhance the network's security.

4.1 Cisco ASA 5510 by cisco:

Figure 5. Cisco ASA 5510

Cisco Adaptive Security Device Manager (ASDM) is a graphical management manager ASA firewalls

The **Home** tab provides an overview of basic information about equipment, i.e., used hardware, processor load, status, and a load of individual interfaces; at the very bottom is a listing of the device's Syslog. The **Configuration** tab is used for settings individual firewall functions; this tab is then further divided into sub-tabs Device Setup, Firewall, Remote Access VPN, Site-to-Site VPN, Device Management, IPS.
After clicking on the given sub-tab, a list will appear above them in the left margin Settings. For some settings, an additional column may appear in the right margin. The last **Monitoring** tab contains detailed information, statistics, and graphs device. Again, it is divided into sub-tabs Interfaces, VPN, Botnet Traffic Filter, Routing, Properties, logging.

4.2 Firewall Functions

*4.2.1 Creating Network Objects and ACLs:*When creating ACLs, IP addresses and port numbers are generally not used, but for larger ones, Clarity creates objects and groups of objects that give given IP addresses and protocols represent.

I. Go to Configuration > Firewall > Objects > Network Objects / Groups. Here you create objects named ASA_Inside, ASA_DMZ, ChP_Inside and ChP_DMZ and assign them IP addresses and masks according to the topology

II. Go to Configuration > Firewall > Access Rules. Here you see three interfaces, which you configured at the beginning of the task and one called global, if you assign ACLs to the global interface, that ACL is applied to all active interfaces.

III. Press add, and a window for creating ALC rules will open. You specify here which interface the ACL will apply to, whether the ACL will allow traffic or discard, source and the target object, protocol, and logging level. To the source fields, destination, user, and service, you can add multiple objects separately from each other comma, in which case when evaluating the rule applies between objects in the given field logical function OR. Leave the Enable Logging field checked, default value means that messages related to a given ACL will be generated in the Syslog with level 6.

When you click *more options,* you can specify in which direction the rule will be applied, you can also set the source protocol and port. The last is the possibility of defining the time period in which the rule will be active.

Create a rule on the *inside* interface that allows all traffic to everyone in your *Inside zone* to your *DMZ zone*, further allow communication from your *Inside zone* to *DMZ of the CheckPoint Network zone*, finally enable communication on the *outside* interface from *the Checkpoint Network Inside*

zone to your *DMZ zone,* but only for protocols FTP and ICMP. Block all other communication.

IV. If your neighbor has also performed a basic ACL configuration, verify functionality by sending a ping, connecting to FTP and HTTP server on both computers in the *DMZ zones.*

If your network is not working, try resolving the issue by exploring the Syslog on your firewall or SmartView Tracker on your neighbor's firewall. Open Syslog on the *Monitoring > Logging > Real-Time Log Viewer* set the viewing level to *debugging*; after opening the window, you can pause the report at the top of the window by clicking the *Pause* button

4.2.2 Web Authentication: This type of authentication prompts you to enter credentials through a web browser when accessing defined network services, and it is a very commonly used type of authentication in many companies. Its significant advantage is that you do not have to install any applications on your computer.

I. Go to *Configuration > Firewall > AAA Rules,* click *add here authentication rule.* Users will authenticate using a local database stored on the firewall, so leave the *AAA Server Group* entry on *LOCAL*, action will be *Authenticate*, the source will be *any*, and the destination is the IP address of the firewall interface leading to your *inside* zone, i.e., *GigabitEthernet 1*, enter HTTP as the service. Finally, in the command terminal, enter the command **aaa authentication listener HTTP inside port www redirect**.

The steps you have now taken will give you access to the web authentication portal.

II. Now, create a second rule where your *Inside Zone* network and destination will be the source neighbor *DMZ zone,* services will be HTTP and ICMP, leave *user*-item empty.

III. Wait for the neighbor to complete his part of the configuration. On the *PC_3_Client* The computer opens a command prompt and pings the *PC_2_Server continuously* located in the neighbor's *DMZ zone*.

IV. Open a browser and enter the IP address of the *PC_2_Server* computer. *The* browser would take you to prompt for credentials if the firewall access portal does not access it by entering **http://10.200.10.1/netaccess/connstatus.html**.

Enter your username and password, i.e., *admin,* and you should see "Welcome to CheckPoint network web server PC_2".

V. Create another user with the username *user* and the password *user* (so you can execute either via the command console with the same command you used at the beginning when creating the *admin* user or you can do it via ASDM in *Configuration > Firewall > Objects > Local Users*). Create the appropriate objects, ACLs, and AAA rules that allow everyone in your *Inside Zone to* access the web to the Internet only if you log in as user *admin*, no one must not have access to the page "csfd. cz". Don't forget to enable DNS protocol.

4.2.3 Static and dynamic NAT: Use NAT on the firewall instead of the router has significant advantages, for example, if a router is connected to the network, which performs NAT and which the firewall does not know about, it can evaluate its behavior as IP spoofing and therefore, it is good to apply NAT directly on the firewall and configure it together with appropriate rules so that it does not block the traffic. The downside is that NAT extensively uses the processor, so since the firewall has yet to perform the inspection operation, it is advisable to implement NAT only on firewalls that are sufficient efficiently.

I. Go to *Configuration > Firewall > Objects > Network Objects / Groups,* click the *ASA_Inside* object, click NAT, check *Add* **A***utomatic Address Translation Rules,* set the type to *Dynamic (PAT)* and the field *Translated Addr*. insert the interface *outside* and confirm the configuration with the *Apply button*.

Go to *Configuration > Firewall > NAT Rules*, here; you can see that you automatically created a rule that translates the source address of everyone on the network *ASA_Inside* to the IP address *outside* the firewall interface.

Enable the ICMP protocol towards the Internet and run an uninterrupted ping on Google's DNS server at IP address 8.8.8.8, on the computer where you are running virtual machines, run the Wireshark program, activate traffic logging on your physical interface.

II. Your neighbor also had the task of configuring NAT in his *Inside Zone the* same the way you do now that you know that a neighbor's firewall also translates addresses in your own *Inside the zone* on its external interface, so set your firewall to receive traffic from the *Inside zone* in the *Checkpoint Network* to your *DMZ zone*.

Your neighbor's job is to do the same when he completes the configuration. Give it a try communication between your *Inside zone* and the neighboring *DMZ zone*.

III. Create a static NAT with your web server located at *PC_4_Server* will listen on the public IP address 10.1.0.25 on TCP port 8080 and create appropriate objects representing this IP address port.

NAT-compiled traffic must also comply with the ACL policy. After completing the configuration, ask your neighbor if he can get out of his *Inside zone* to connect to your web server via the address http://10.1.0.25:8080

4.2.4 Site-to-Site VPN configuration: This type of VPN is commonly used to connect branches to the company's headquarters via the Internet. The main advantage is that the communication is entirely transparent for clients, and no additional configuration or installation is required on client computers. In other software, a VPN tunnel is formed only between border firewalls. The downside is that on each side of the Tunnel, a network device supports SSL / TLS or IPsec protocol, and for larger networks also dynamic routing protocols.

In this part of the task, you will connect your *DMZ zone* to *the* neighbor's *DMZ zone* using IPsec Site-to-Site VPN

I. On the PC_3_Client computer, launch Cisco ASDM-IDM Launcher and log in to the firewall IP address of the interface to which *PC_3_Client is* connected. Use username and password **admin**.

II. In the top pane, click *Wizards > VPN Wizards > Site-to-Site VPN Wizard,* click *next.*

III. On the *Peer device Identification page,* type the IP address in the *Peer IP Address* field external interface with Checkpoint firewall. The VPN Access Interface field must be the interface that connects your firewall to the Checkpoint firewall. Click *next*.

IV. On the *IKE Version page,* check only the *IKEv1* protocol. *C*lick *next*.

V. On the *Traffic to protect page*, enter your *DMZ zone* in the *Local Network* field and the *Remote Network* field, enter *the* neighbor's *DMZ zone,* click *next*.

VI. On the *Authentication Methods page,* in the *pre-shared key field,* enter at least 8 local passwords, which can be agreed with the neighbor. This password in Firewalls will authenticate with each other if each of you enters a different password Authentication will fail, and the VPN tunnel will not be established. In the *Device Certificate* item leave *none,* click *next.*

VII. On the *Encryption Algorithms page,* under *IKE Policy,* click manage a delete all predefined items. Create a new one with parameters:

Priority: *10*
Authentication: *Pre-share*
Encryption: *aes-256*
Diffie-Hellman Group: *2*
Hash: *sha*
Lifetime: *2 hours (7200 seconds)*
Mode: *Tunnel*
ESP Encryption: *AES-256*
ESP Authentication: *SHA*

IX. On the *Miscellaneous* page, leave *Enable inbound IPsec sessions to* checked *bypass interface access lists,* this will ensure that we do not have to create ACLs for this VPN session. Complete the wizard with the button *finish.*

X. Go to *Configuration > Site-to-Site VPN > Connection Profiles,* here you will create a profile named *10.1.0.10,* edit it and in the item *Advanced > Crypto M*ap *Entry,* set *Security Association Lifetime* to 1 hour, confirm the setting, click *Apply*

XI. Wait for your neighbor to complete his or her part of the configuration. On the computer where you run virtual machines, start the Wireshark program, activate traffic logging on your physical interface. Try ICMP, HTTP, and FTP transfer between *PC_2_Server* and *PC_4_Server*.

4.2.5 Remote Access SSL VPN: This VPN is mainly used to connect employees who work from home or travel to a corporate network. The advantage is that it works via TCP port 443, as well as HTTPS, so it doesn't have as much trouble passing through NAT as in IPsec. Also, communication is less likely to be blocked external firewall. The disadvantage is that you must have a client installed on your computer software

I. In the top pane, click *Wizards > VPN Wizards > AnyConnect VPN Wizard,* click *next.*

II. On the *Connection Profile Identification page*, name the profile *Remote_VPN*. The *VPN Access Interface* field is the external interface of your firewall. Click *next.*

III. On the *VPN Protocols page,* leave only the SSL protocol checked in the *Device* field. Leave the *certificate none,* click *next.*

IV. On the *Client Images page,* do not change anything and click *next.*

V. On the *Authentication Methods page,* leave *AAA Server group LOCAL,* v database you already have pre-created user accounts *admin* and *user,* click *next*.

VI. On the *Client Address Assignment page*, create a new *IPv4 Address Pool,* named *VPN_Pool*, and assign it the range 10.10.10.1 - 10.10.10.10 and the mask / 24.

VII. Do not change anything on the following pages. Complete the wizard with the *finish* button.

VIII. When clients connect to the cisco firewall via VPN, it is by default, all its communication is routed to the Tunnel. This is not usually desirable because the client often wants to have access to resources on its network Therefore, we need to configure it to be routed to the tunnel-only defined type of communication. This is called *split tunneling.* On the *Configuration* tab > *Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles*, edit the *Remote_VPN* profile just created.

On the *Basic* tab next to *Group Policy*, press *Manage*, and edit *GroupPolicy_Remote_VPN*. Go to *Advanced > Split Tunneling*. For items *Policy* and *Network List*, uncheck the *Inherit* box and select *Tunnel* in the *Policy* field *Network List Below*. This means that only the specified networks will be tunneled using the ACL in *Network List. P*ress *Manage* for this entry and create *an* ACL *standard* named *Tunneled_Networks* and select your *Inside and DMZ zone*
Next, on the *General* tab, click the *More Options* item next to the IPv4 filter item create an *extended* ACL that will specify that if your neighbor over The VPN logs in as the *admin* user so it will have access to both your *Inside and DMZ zones* and if he logs in as a *user*, he will only have access to your *DMZ zone*.

IX. Wait for your neighbor to complete his part of the configuration, then ask him to connect to your firewall from PC_1_Client using *Cisco AnyConnect*, which is located on the desktop of his virtual PC. Test if a neighbor has access to the entire *ASA Network* when he logs in as *admin* (password: *admin*) and if as a *user* (password: *user*), then he should only have access to your *DMZ zone*

In Wireshark, on your host computer, you should observe the communication encrypted with TLSv1.

X. Your neighbor also has the task of setting up SSL and IPsec Remote Access VPN. Until you will ask for testing, there is a *Check* shortcut on your PC_3_Client desktop *Point Mobile*, launch it, and the icon should appear in the notification area, click on it and connect to the Checkpoint firewall via its external IP address if you log in as *admin* (password: *admin*), you should have access to *Inside* and *DMZ zone* on the *Checkpoint Network*, and if you log on as a user (password: *user*), so you should only have access to the *DMZ zone* in the *Checkpoint* network *Network*.

Use a web browser to connect to an SSL VPN (don't forget to disconnect from IPsec VPN *Checkpoint Mobile Client*), enter the address **https://10.1.0.10/sslvpn/Login/Login** and confirm the exception for the certificate. Again log in with the above-mentioned login details, and on the *Native Application page*, press *Connect*. The browser will show you about five prompts from the Java application. All agree with them. You should have access to the *Inside* and *DMZ zone* on the *Checkpoint Network* if you log on as a user *admin* and if you log in as a *user*, then you should only have access to the *DMZ zone* on the *Checkpoint Network*.

4.2.6 Web URL Filtering: Web address filtering based on IP addresses is inefficient, IP addresses of web address servers change frequently, so it is better to filter URLs directly. But that requires a firewall, which can analyze the application layer of packets, application analysis layer is also computationally intensive. In this part of the task, you will try filtering web addresses based on search keywords in the HTTP packet.

I. Go to *Configuration > Firewall > Service Policy Rules*, click *add* a create a new *Service policy* on the *inside* interface, and leave it named *Inside – policy,* click next.

II. Now, let's create a new *Traffic class and* name it *Block_HTTP*. *F*or the *Traffic match criteria*, check the *source and destination IP address (uses ACL),* click *next.*

III. You will filter traffic from your *inside zone* to the Internet, so give as a source *ASA_inside* , and the target will be *any*, the protocol is *HTTP*, click *next.*

IV. On the *Protocol inspection* tab, check *HTTP* and click *configure*.

V. Click *Select an HTTP to inspect the map for fine control over the inspection* and click and *add.*

VI. Name the new map *HTTP_Inspect and* click *Details*, uncheck *Check for protocol violations*, click the *Inspections* tab and click *add.*

VII. The item *Criterion* is set to *Request Header Field* for entry *Field*, type *the predefined*, and value will be *guest.* In the *Value field*, enter *Regular Expression Class* and click on Manage.

VIII. In the *Manage Regular Expression Class Maps* window, click *Add*, new map name it *Blocked_HTTP_Sites* and create two new *Regular Expressions* and name them *csfd. cz* and *idnes.cz*, enter the pages you will be in the *value* window block, ie *csfd.cz* and *idnes.cz.* Then assign the created expressions to the *Configured Match Conditions* window.

IX. the *value* window block, ie *csfd.cz* and *idnes.cz.* Then assign the created expressions to the *Configured Match Conditions* window

X. Confirm everything and open a web browser and enter in the address bar csfd.cz and idnes.cz. Pages should not load now.

XI. The facebook.com website uses the HTTPS protocol. Unfortunately, the ASA 5520 cannot filter the HTTPS protocol because it is encrypted by the TLS protocol. However, it is possible to work around this. We will block DNS requests, the DNS protocol does not use any encryption, and since today's Internet is so dependent on it by stopping, we achieve the desired result.

4.2.7 Remote management using Telnet and SSH: Telnet and SSH protocols have been designed for remote device management. The SSH protocol was intended to replace the outdated Telnet, which does not encrypt communications and is quickly eavesdropped on. However, Telnet can still be used on secure networks.

I. Go to *Configuration > Device Management > Management Access > ASDM / HTTPS / Telnet / SSH*, set here so that anyone can access the device from the outside via SSH and via Telnet.

II. As a messenger, you must set up users accessing via SSH or Telnets were authenticated through a local database stored on the firewall. The setting is in *Configuration > Device Management > Users / AAA > AAA Access*.

III. Wait for your neighbor to complete his / her part of the configuration. On *PC_3_Client* open a command prompt and connect to the Checkpoint firewall via SSH and link to via Telnet

5. Conclusion

Firewalls are one of the critical elements in maintaining security. They are placed in the "first battle line" as they separate secure networks from unsecured ones. Traditional firewalls already have not undergone a radical change for some time and cannot keep up with technical progress. Therefore, the arrival of more advanced and "smarter" devices was necessary.

In the paper, we wanted to investigate whether the next-generation firewalls are capable meet today's needs for high connection speeds and whether they contribute to adequate protection of increasingly compromised modern networks.

Next-generation firewalls, in our opinion, are not only a suitable but a necessary tool in modern information security. They offer innovative insights into network traffic and much more advanced functionalities, without which security will no longer be possible in the future. Of course, a firewall alone is not enough to protect and must be meaningfully included in a comprehensive security system of organizations.

Managers, administrators, and employees need to be aware importance of safety and good practices and to be well educated. No system is completely protected before intrusions. An attacker, with the right combination of knowledge, patience, motivation, and resources, will sooner or later hack into any system adjacent to the external network. In the modern reality of information security, the organization must decide which information is most important to it and accept additional measures to protect them in the event of an intrusion into the system.

References

1. Janet Abbate from Virginia Tech University, Virginia, USA “The Internet: Global Evolution and challenges “2009.
2. Kaspersky, (2015). Retrieved from https://www.kaspersky.com/resource-center/threats/web
3. Studytonight, “The TCP/IP Reference Model”. Retrieved from https://www.studytonight.com/computer-networks/tcp-ip-reference-mod
4. Ido Dubrawsky, “Network Address Translation” from Embedded Software (Second Edition), 2012
5. Derrick Rountree, “Stateful Inspection” in Security for Microsoft Windows System Administrators, 2011
6. Cisco, “What is a Next-Generation Firewall” 2021 Retrieved from https://www.cisco.com/c/en_in/products/security/firewalls/what-is-a-next-generation-firewall.html

Biographical notes

Rutvik Patel is Perceiving his Btech from Ganpat University in Computer Science and Engineering. His research interest includes cyber security and network security.