DLINE JOURNALS

Journal of Information Security Research

Print ISSN: 0976-4143
Online ISSN: 0976-4151

JISR 2024; 15 (3)
https://doi.org/10.6025/jisr/2024/15/3/89-102

Effectiveness of Application Software in the Simulation Boundary for Critical Data Protection

Liliia P. Galata, Bogdan Y. Korniyenko, Alexander K. Yudin
National Aviation University
Kiev, Ukraine
galataliliya@gmail.com, bogdanko@i.ua, yak333@ukr.net

Received: 23 February 2024
Revised: 3 June 2024
Accepted: 11 June 2024
Copyright: with Author(s)

ABSTRACT

This work develops and implements a simulation boundary designed to safeguard essential data assets using the application software GNS3. At the core of computer network security lies the Cisco ASA 5520 firewall, which segments the organization's network into a demilitarized zone, encompassing an internal and external network. Within this demilitarized zone, web and FTP servers are set up. A network scan was conducted with the Zenmap utility to evaluate the effectiveness of the simulation boundary for critical data protection. Additionally, a stress test of the network was carried out using the hping3 utility. The measures taken to counter these simulated attacks were identified and documented.

Keywords: Simulation Polygon, Critical Information Resources, Security, Threats, Computer Network

1. Introduction

The main problem that needs to be solved while constructing a cybersecurity polygon which consists of real hardware is the high price of components for building a secure network. Sometimes, even if the company has all necessary equipment, it will be used in its own network and will not be provided for testing, network interconnection, and so on. For small companies, building of network for training purposes, for testing various network equipment, flexible configuration or testing various security policies are almost impossible, because it requires a lot of costs [1-4].

Therefore, it was decided to build a secure computer network based on a special emulator platform, which allows you to virtualize various network equipment and create a real virtual network on their base. So, as a platform for building a secure network, you need to use a full-fledged emulator that allows you to run a complete model of the network device and run the original software. The emulator runs the real Cisco IOS operation system, so it allows to run full-featured network device, whether it's a router or a switch, or a firewall. It means that, this network equipment will have all the features that are available on real equipment. There is also the possibility of launching a multivendor heterogeneous network, which allows you to use not only Cisco network devices, but also Juniper, Microtik, Check Point. Also, in order to build a fully secured virtual computer network, it is necessary to have the ability to add workstations and servers to the network [5].

2. Emulator Platforms

To build a secure virtual network, you can now use one of two most suitable platforms: UNetLab (Unified Networking Lab, UNL) or GNS3 (Graphical Network Simulator-3). Firstly, both emulators are completely free, unlike the same VIRL or Boson NetSim, and secondly, have a similar functionality with certain features. The main disadvantage of such emulators is the impossibility of using them in the topology of wireless network devices, so you can`t build and test wireless networks.

GNS3 (Graphical Network Simulator). GNS3 is a graphical network emulator that allows you to simulate a virtual network of network equipment from more than 20 different companies on a local computer, connect a virtual network to the real one, add a computer to the network, support other software for network packets analyzing, for example Wireshark. It also supports the SolarWinds Response Time Viewer utility, which accepts traffic logs and analyzes the network callback time and data volumes. Depending on the hardware platform for GNS3, it is possible to build complex projects consisting of Cisco, Cisco ASA, Juniper routers, and servers with network operation systems. For ease of testing, it supports virtualization software, which allows you to add a virtual machine to the network and make appropriate network tests, including VMware and VirtualBox. GNS3 is a graphics shell for Dynamips, it also has full support for QEMU and Cisco IOU, with all advantages and disadvantages of each technology [6-9].

Dynamips works on most Linux systems, Mac OS X and Windows, that allows the emulation of the routers’s hardware part by downloading and interacting with real Cisco IOS images. The main purpose is to test and experiment with different versions of Cisco IOS, checking the configuration before using it on real hardware, and to use as a training laboratory.

Main benefits of Dynamips:

- A real IOS image is used for work, not partial emulation of some of its capabilities.

- Ability to work in hypervisor mode, for load balancing between multiple computers.

- Capture traffic on interfaces using the PCAP library (for example, using Wireshark).

- Connect the emulated network equipment to a real network.

Main drawbacks are:

- High system requirements, as a real IOS image is downloaded into memory.

- Impossibility to emulate Catalyst switches and some router models due to the large number of ASICs in them. QEMU - free open source software for emulating various platforms hardware. UNetLab as GNS3 uses QEMU to emulate ASA, ASAv, IPS firewalls, and L2-switches, that are not emulated by Dynamips. The advantage of using QEMU in UNetLab is no RAM limitations and the number of connections for QEMU, compared to GNS3, which has a 2 GB RAM limit and 16 connections for various emulated devices.

Cisco IOU (Cisco IOS for UNIX) - Cisco emulator for internal use. It installs over UNIX, may work under Linux (IOS on Linux). The emulator has complete support for L3, L2 devices, with low CPU resources requirements (RAM is required a lot). There are no restrictions on the boards and interfaces. In the settings, you simply specify how much and what you need. It supports both GNS3 and UNetLab.

Emulator UNetLab (Unified Networking Lab, UNL). UNenLab (Networking Lab Unified, UNL) is a multivendor and multi-user environment for creating and modeling various laboratories that allows you to simulate a virtual network with routers, switches, security devices and connect them to a real network, connect a virtual machine with any operation system or real computer. It allows you to use both Cisco images (Dynamips emulator) and Juniper or QEMU components. In addition, since UNetLab 0.9.54 release, it contains a multi-user functionality. By using the same virtual machine, each authorized user can create their stands independently of each other, and collaborate with a common stand that shares several users at one time. In this case, users have the opportunity to launch a common stand independently of each other.

Main features: boards and interfaces. In the settings, you simply specify how much and what you need. It supports both GNS3 and UNetLab.

Emulator UNetLab (Unified Networking Lab, UNL). UNenLab (Networking Lab Unified, UNL) is a multivendor and multi-user environment for creating and modeling various laboratories that allows you to simulate a

- It is a completely free product.

- It has web interface. So, there is no need to install a custom user client.

- Allows you to simulate virtual networks with switches, routers, security devices, and more. Capabilities are limited only by resources of the computer or the server.

- Almost full support for L2 level switches.

- Can be installed on both physical server and virtual machines VMware Player, VMware Workstation, VMware ESXi with Vsphere vClient, etc.

- The multi-user functionality allows UNetLab to be used as a network laboratory in educational institutions without any restrictions.

Built-in characteristics of platform functionality for emulation of computer networks. Today, there are three Cisco VIRL, GNS3 and UNetLab emulators, which can be used for building and quality testing a secure computer network. The comparison of the disadvantages and advantages of each of them is given in Table 1. The main disadvantage of these emulators are the impossibility of emulating wireless network devices, as a result, the impossibility of including them in the network topology, which greatly reduces the functionality of the cybersecurity polygon.

Characteristics	Cisco VIRL	GNS3	UNetLab
Serial Interfaces support	-	+	+
Advanced Cisco Network Equipment support	+	+	+
Other vendors support	-	+	+
Out-of-Band management	+	-	+
Multiuser platform	+	-	+
Easy to deploy	+	+	-
Network connections limitations	-	+	+
User support	+	+	-
Price	-	+	+
Emulation of wireless network devices	-	-	-

Table 1. Comparative characteristics of the emulator's functionality

Cisco ASA Firewall Configuration. Cisco ASA is a hardware firewall with stateful session's inspection. ASA is able to work in two modes: routed (router mode, by default) and transparent (transparent firewall when ASA works as a filtration bridge) [10].

In routed mode, each ASA interface configures the IP address, mask, security level, interface name, and also the interface must be forced to "up", because by default all interfaces are in the "disabled by administrator" mode.

The security level parameter is a number from 0 to 100, which allows you to compare 2 interfaces and determine which of them are more "secure". The parameter is used qualitatively, not quantitatively, that is important only "more or less." By default, the traffic that goes "outside", from the interface with a high level of security to the interface with a lower level of security, is skipped, the session is remembered and back passes only the answers to these sessions. Traffic going "inside" by default is forbidden.

So, firewall occurs between the logical vlan interfaces. As a rule, the level of security of interfaces is selected for the maximum match to the logical topology of the network. The topology represents a security zone and the rules of interaction between them. A classical model has various interfaces with different levels of security. There are no prohibitions about the same level of security for different interfaces, but by default exchange of traffic between such interfaces is forbidden. The "name of the interface" parameter (nameif) allows you to use in the settings not the physical name of the interface, this name can be chosen to mean its purpose (inside, outside, dmz, partner).

Between interfaces with the same level of security there is no firewall, but only routing. Therefore, this approach applies to interfaces that relate to the same logical security zone.

As any router (ASA also uses a routing table for package transfer), the configured interfaces automatically fall into the routing table with the tag "attached" (connected), for only «up» interfaces. Package routing between these networks is automatic.

The networks that for ASA not known should be described additionally. It is necessary to specify the interface for "next-hop", because ASA does not make such search (as opposed to the usual cisco router).

The routing table only gets one route to the destination network, as opposed to classical routers, where up to 16 parallel paths can be used. The default route is specified by hand additionally. If the ASA does not have a record in the routing table about destination network for some package, it will discard the package.

ASA, like most cisco devices, provides several ways to remote control. The telnet is easiest and no most dangerous way. More secure command line access is provided by the SSH protocol. However, when you use SSH, you should specify which hosts you can use to manage, and you must also specify the RSA keys that are required to encrypt user data.

Cisco Routers Configuration. First of all, the physical connection should be configured and the parameters of the interfaces should be set up. This phase includes the configuration of the physical interfaces - port speed, duplex, flow control, EtherChannel creation, 802.1Q sub-interfaces for using VLANs in the network.

Then you should configure the router's IP-address, the local and global interfaces.

The next step is to configure routing functions:

- Routing settings, including static and dynamic routing;

- Setting of automation issuing for DHCP addresses, including creation dynamic pools, static bindings;

- NAT Address Conversion Settings - dynamic and static rules for port wrap;

- Secure access configuration, including a access list of physical interfaces and a list for virtual ports;

- users, authorization, privileged mode;

- setting up access control list (ACL);

Access Control List (ACL) is a consistent list of permission or prohibition rules that apply to higher-level addresses or protocols. ACLs allow you to effectively monitor incoming and outgoing network traffic. ACLs can also be configured for all network routing protocols.

ACL is an array of IOS commands that defines, if router sends package or resets them, based on the information in the package header. ACLs do such tasks of limit network traffic to improve network performance.

Access control lists provide the basic security level of access to the network. ACLs can open access to a part of the network of one node and close it to other nodes.

ACLs filter traffic based on the type of traffic.

Access control lists sort nodes to determine if network services access is required. Using ACLs, you can allow or deny access to certain types of files, such as FTP or HTTP.

4. Testing software

Hping3. Hping3 is a free package generator and analyzer for TCP/IP protocol. Hping is one of the mandatory tools for auditing security and testing of firewalls and networks. Like most tools used in computer security, hping3 is useful for security experts, and is used to:

- Traceroute/ping/probe hosts;

- test firewall rules;

- testing of IDS (intrusion detection systems);

- Network research;

- Stress tests of the network;

- study TCP/IP (Hping was used in AFAIK network courses);

- writing real programs related to TCP/IP testing and security;

- automate tests for traffic filtering;

- create a working model of exploits;

- Network and security intelligence studies when emulating the complex TCP/IP behavior;

Zenmap. Zenmap is the official GUI for Nmap Security Scanner. Zenmap is an open source utility for network research and security testing. It was designed to quickly scan large networks, although it works well for single purposes.

Zenmap uses IP-packages in its original ways to determine which hosts are available on the network, which services (program name and version) they offer, which operation systems (and OS versions) they use, which types of package filters/ firewalls are used and other features. Zenmap is commonly used for security testing, but many network and system administrators find it useful for common tasks such as network structure control, service scheduling management, and host/service time tracking.

Nmap Output is a list of scanned targets with additional information for each one. The main information is the "important ports table". This table contains the port number, protocol, service name, and state. The state may be "open", "filter", "close", or "unfilter". "Open" state means that the application on the target machine is ready for connection/ accepting of package to this port. "Filter" state means that the firewall or some network filter in the network blocks the port, and Nmap can`t say if the port open or closed. "Close" ports are not associated with any application, so they can be opened at any time.

Wireshark. Wireshark is a network traffic analyzer. Its task is to intercept network traffic and detail display it. Wireshark can intercept the traffic of various network devices, displaying its name (including wireless devices). Supporting of any device depends on many factors, such as the operation system, and has many protocol decoders (TELNET, FTP, POP, RLOGIN, ICQ, SMB, MySQL, HTTP, NNTP, X11, NAPSTER, IRC, RIP, BGP, SOCKS5, IMAP4, VNC, LDAP, NFS, SNMP, MSN, YMSG and others). Wireshark allows you to save and open previously saved network traffic. System administrators use it to solve network problems, developers' use it to debug network applications, and ordinary users use it to study the network protocols.

5. Practical implementation of the cyber security polygon on the GNS3 applicable software For the construction of a cybersecurity polygon based on the GNS3 applicable software, a distributed simplified network topology for small enterprises has been selected. This network topology uses one Cisco ASA 5520 firewall, which divides the company's network into a demilitarized zone, an internal and an external network. The zonal model is fairly flexible, interfaces are assigned to zones, and the checking policy is assigned to the traffic that is transmitted between zones. The network topology built with GNS3 is shown on Figure 1.

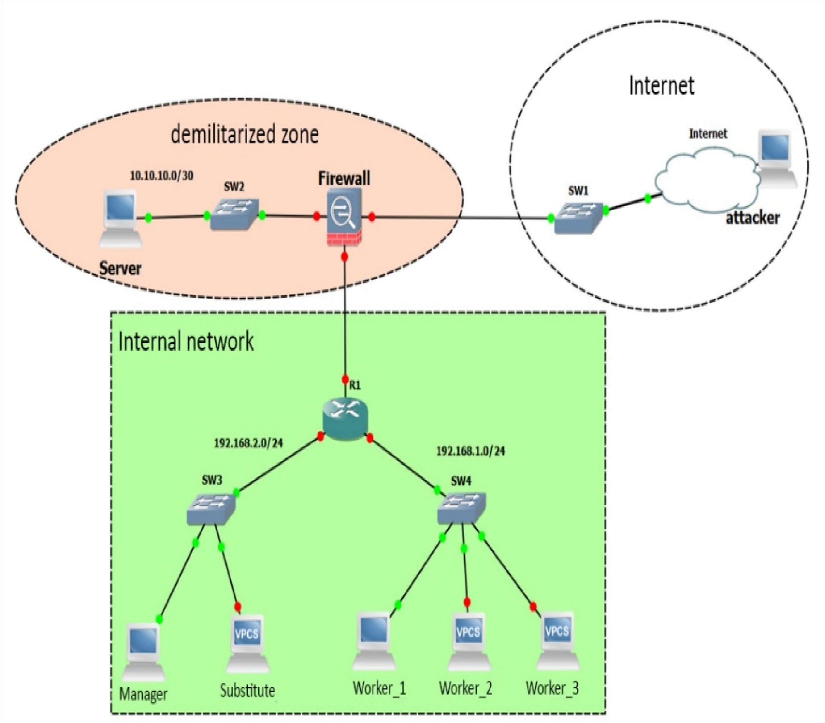
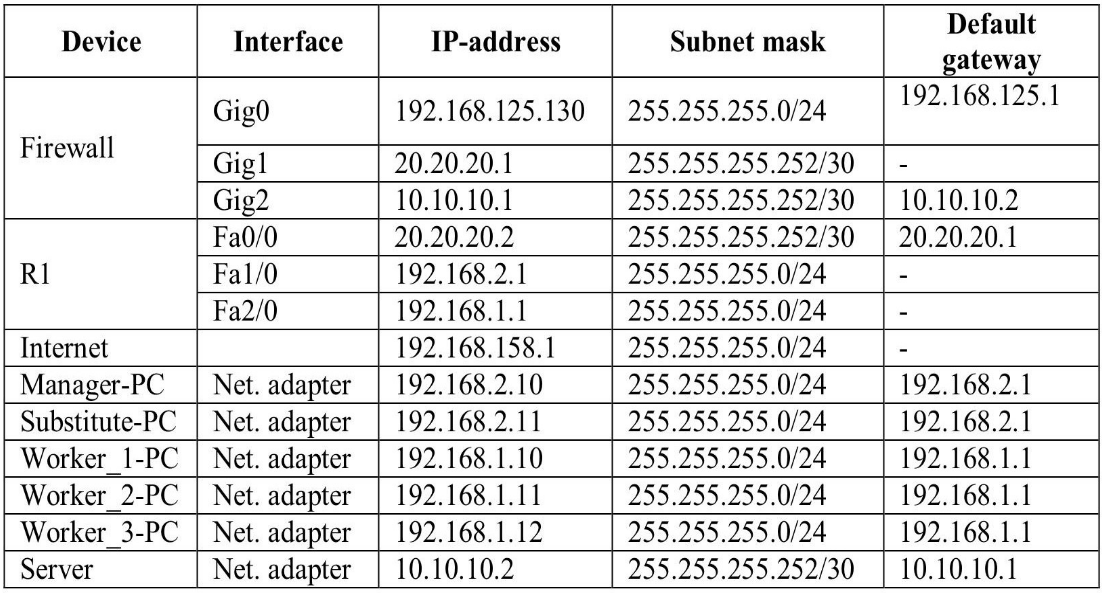


Figure 1. Network topology in GNS3

The virtual network routing table is shown below in Table2. Our topology of the network is divided on the subnet, all network devices have their interfaces for connecting with IP address, subnet mask and default gateway.



Device	Interface	IP-address	Subnet mask	Default gateway
Firewall	Gig0	192.168.125.130	255.255.255.0/24	192.168.125.1
	Gig1	20.20.20.1	255.255.255.252/30	-
	Gig2	10.10.10.1	255.255.255.252/30	10.10.10.2
R1	Fa0/0	20.20.20.2	255.255.255.252/30	20.20.20.1
	Fa1/0	192.168.2.1	255.255.255.0/24	-
	Fa2/0	192.168.1.1	255.255.255.0/24	-
Internet		192.168.158.1	255.255.255.0/24	-
Manager-PC	Net. adapter	192.168.2.10	255.255.255.0/24	192.168.2.1
Substitute-PC	Net. adapter	192.168.2.11	255.255.255.0/24	192.168.2.1
Worker_1-PC	Net. adapter	192.168.1.10	255.255.255.0/24	192.168.1.1
Worker_2-PC	Net. adapter	192.168.1.11	255.255.255.0/24	192.168.1.1
Worker_3-PC	Net. adapter	192.168.1.12	255.255.255.0/24	192.168.1.1
Server	Net. adapter	10.10.10.2	255.255.255.252/30	10.10.10.1

Table 2. Virtual network routing table

Description of network devices. In this topology, for the construction of a cyber security polygon, the following network devices are used: the Cisco ASA 5520 firewall (hostname: Firewall), the Cisco 3745 router (hostname: R1), network switches (SW1, SW2, SW3, SW4). The loopback interface (Internet) is used to access to the Internet. Also there are two virtual machines with the operation system Windows XP SP3 (Manager PC, Worker_1-PC) to simulate real computers in the network. Virtual PC Simulator (VPCS) is used to simulate other PCs in the network (Worker_2-PC, Worker_3-PC and Substitute-PC). VPCS uses insignificant PC resources. VCPS creates virtual interfaces for its work and uses only 2 UDP ports - one for transmitting information, another for reading. VCPS has quite limited functionality, but it can save PC resources.

Description of network topology and network device tasks. The managers' network and workers network is located on the firewall interface Gig1. The router R1 routes traffic between them. Cisco ASA configures NAT to prevent and limit external requests to internal hosts. Firewall is configured to connect to the ASDM via HTTPS, for more management and monitoring. Access to Cisco ASDM is done directly through a Web browser from any Javabased network computer, thus allow security administrators quickly and securely to access Cisco ASA security devices and have a similar functionality as the console connection. For safe remote connection to the R1 router, it is configured with SSH version 2, and all other non-SSH connections are forbidden. In the demilitarized zone there is a server that acts as a Web server and an FTP server. The web server is accessible for Managers and Workers, and from the Internet. Users have access to the Internet only through the 80th port and FTP. Other ports are closed. From the Internet the access is open only to the Web site and only to the 80th port.

Cisco ASA 5520 specifications. The Cisco ASA 5500 is the latest multifunction device that uses the most advanced information security technologies, by combining proven products from Cisco: firewall, network intrusion prevention, network anti-virus and VPN services. The Cisco ASA 5520 can enhance the security of applications by blocking network worms, by using AIP SSM - a high-performance intrusion prevention system, by using CSC SSM - a full-featured anti-malware service.

The Cisco ASA 5520 has the following specifications:

- Bandwidth: 225 Mbps

- Simultaneous VPN session: 750

- Simultaneous SSL VPN Scripts: 750

- Interfaces: Four 10/100/1000 Ethernet ports, control port, two USB ports Cisco 3745 specifications. The Cisco 3745, is a high-performance router with modular architecture, allows you to implement integrated data, voice, and fax transmissions over TCP/IP networks. It has the following technical characteristics:

- Bins for network modules: 4 pcs.

- Bins for WAN Interface Cards (WIC): 3 pcs.

- Embedded Local Area Network (LAN) ports: 2 10/100 Ethernet ports

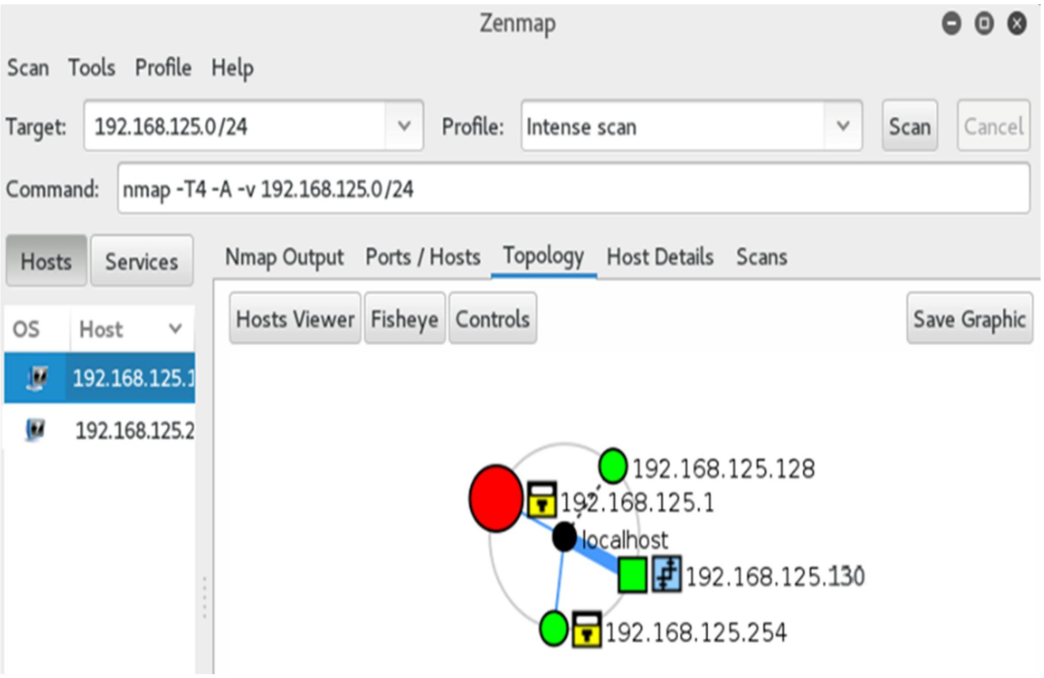
- It is possible to use a backup power supply

- Performance - 225.000 packs/second.

Possible modules for Cisco 3700 series routers: LAN modules, WANs, combined network modules, voice and service modules.

6. Network scan and testing

The Zenmap program is the official GUI (Graphical user interface) for Nmap Security Scanner, network exploration utility and port scanner. Ranges of IP-addresses are selected for save time of scanning process. We was got the information about the network from global network, as a result of the NAT setting, only the configured Cisco ASA interface is displayed, as shown in Figure 2.



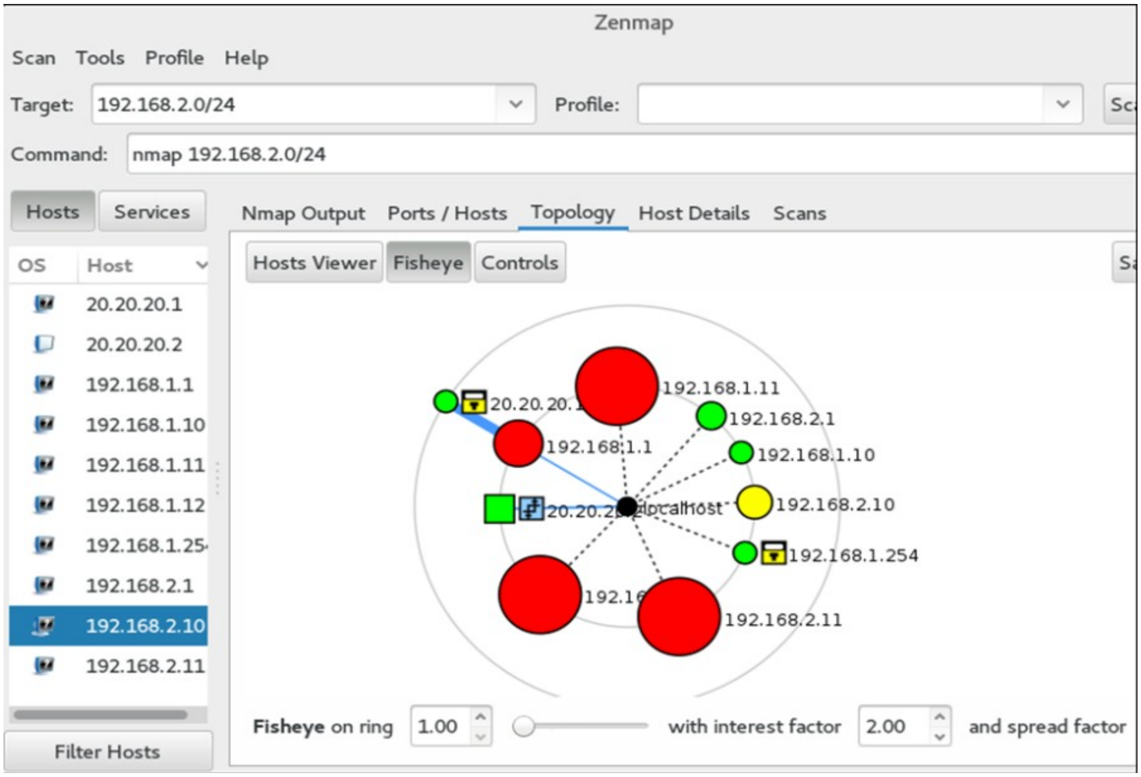
Target: 192.168.125.0/24

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.125.0/24

Figure 2. Local network scan from the external network

If an attacker has access to the network from within, then he will be able to scan the topology of the network and find possible vulnerabilities. The utility allows you to determine which hosts are available in the network (scanned network topology is shown in Figure 3), the version of the operation system, running services, the names of running applications and ports number and ports state, for example, if you do not disable the standard connection to the router through Telnet protocol, then Zenmap will detect it, the result is shown in Figure 4.

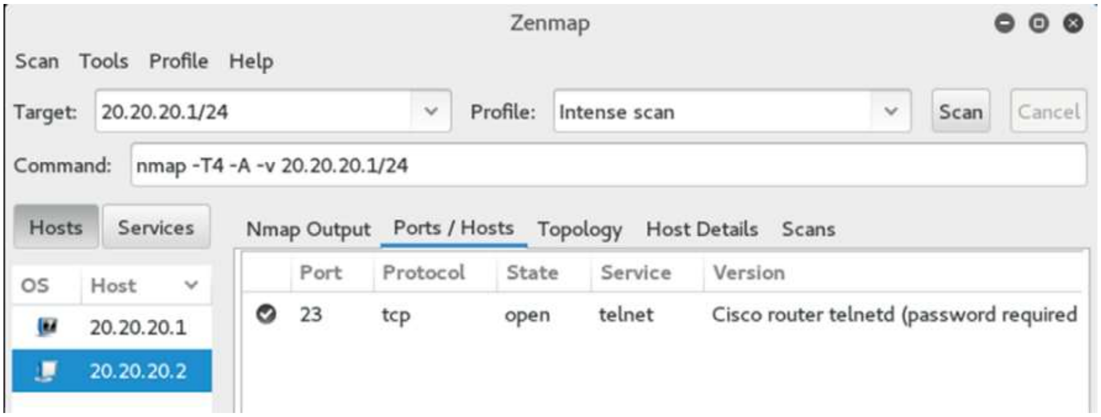


Target: 192.168.2.0/24
Profile:
Command: nmap 192.168.2.0/24

OS	Host
	20.20.20.1
	20.20.20.2
	192.168.1.1
	192.168.1.10
	192.168.1.11
	192.168.1.12
	192.168.1.25
	192.168.2.1
	192.168.2.10
	192.168.2.11

Fisheye on ring 1.00 with interest factor 2.00 and spread factor

Figure 3. Local network scan from the inside



Target: 20.20.20.1/24
Profile: Intense scan
Command: nmap -T4 -A -v 20.20.20.1/24

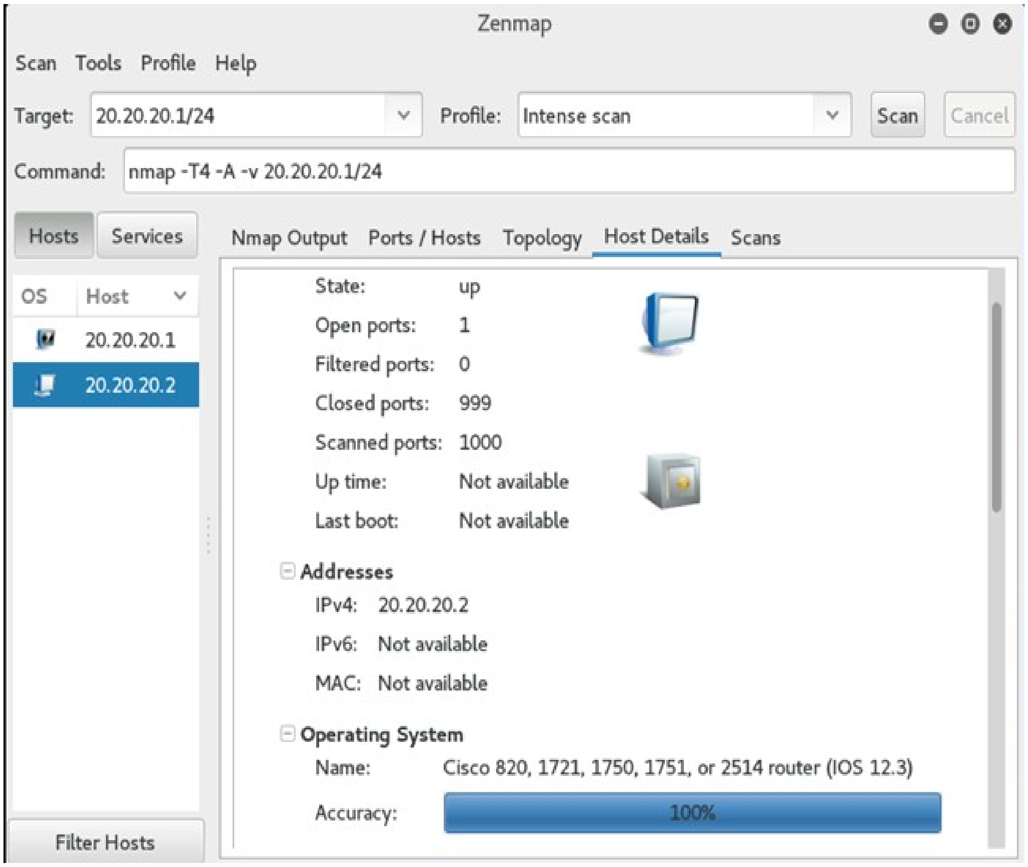
OS	Host
	20.20.20.1
	20.20.20.2

	Port	Protocol	State	Service	Version
✓	23	tcp	open	telnet	Cisco router telnetd (password required

Figure 4. Scan of Cisco 3745 Router with enabled Telnet

In general, after a detailed scan of the network device, we will have the next result: the Cisco 3745 utility with enabled Telnet, the operation system, open port, network address, as shown in Figure 5.

In general, after a detailed scan of the network device, we will have the next result: the Cisco 3745 utility with enabled Telnet, the operation system, open port, network address, as shown in Figure 5.



Target: 20.20.20.1/24
Profile: Intense scan
Command: nmap -T4 -A -v 20.20.20.1/24

20.20.20.1
20.20.20.2

State: up
Open ports: 1
Filtered ports: 0
Closed ports: 999
Scanned ports: 1000
Up time: Not available
Last boot: Not available

Addresses
IPv4: 20.20.20.2
IPv6: Not available
MAC: Not available

Operating System
Name: Cisco 820, 1721, 1750, 1751, or 2514 router (IOS 12.3)
Accuracy: 100%

Figure 5. Zenmap detailed information about scanned host

Cisco ASA has a scanning protection function, so if the messages contain the same source address, this message may be about gathering basic information or about trying to scan ports. Such IP package is rejected by the ACL, as shown in Figure 6.

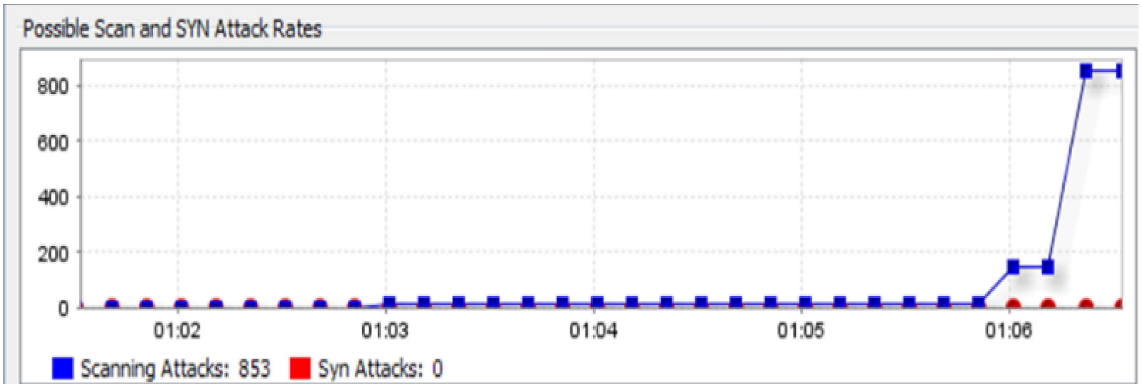


Figure 6. Cisco ASA rejected package statistics

Network Stress-Test. In computer terminology, denial-of-service attack (DoS) or distributed denial-of-service attack (DDoS) is an attempt to make the machine's resources inaccessible to users. However goals of the DoS can be different, its main purpose is to suspend the services of the Internet-connected host for some period of time.

One of the common methods of attack is the saturation of the target machine with external connection requests, so it can not respond to legitimate traffic or corresponds so slowly that it is seams unavailable.

Syn-Flood Attack is an attack where an initiator puts a fake Source IP-address in the SYN package or ignores replies from the server - Syn + Ack. When you open thousands of such half-hearted sessions, the resources of the server are consumed, server is forced to memorize the parameters of such session and as a result may refuse.

For DoS attack, we have used the Hping3 tool (Kali Linux tool), by using the random IP address for DoS source. This program has no graphical interface. The following commands are selected for the Syn-Flood Attack, it is shown in Fig. 7:

- hping3 - the name of the application.

- c 10000 - the number of packages to send.

- d 120 - the size of each package that will be sent to the target machine.

- S - send only SYN packets.

- w 64 - the size of the TCP window.

- p 80 - destination port, you can use any port.

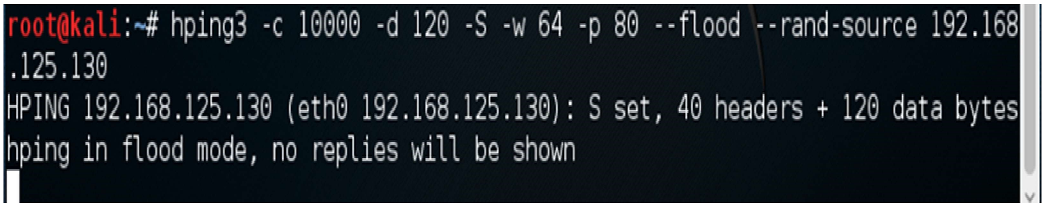
- flood - send package as fast as possible without taking care of displaying incoming package (Syn-Flood Attack).

- rand-source - use of random source IP addresses. You can also use -a or -spoof to hide hostname

- 192.168.125.130 - IP address of the target machine. You can also use the site's address.

Cisco ASA automatically transmits packages that arrives on the server by port 80, and in case of Dos attack the server is under additional load, which means a denial of access to ordinary users.

We have pinged the network without loading and the network under load. We have also used the Wireshark program to analyze Ethernet network packages or other networks (sniffer). We can analyze a DoS attack by using the Wireshark. After filtering traffic between an at tacker and Cisco ASA by ICMP criterion, it can be seen that due to a DoS attack, the Cisco ASA becomes under the load, so processing requests queues are created and responses come with a certain delay or response absolutely absent, as shown in Figure 8.

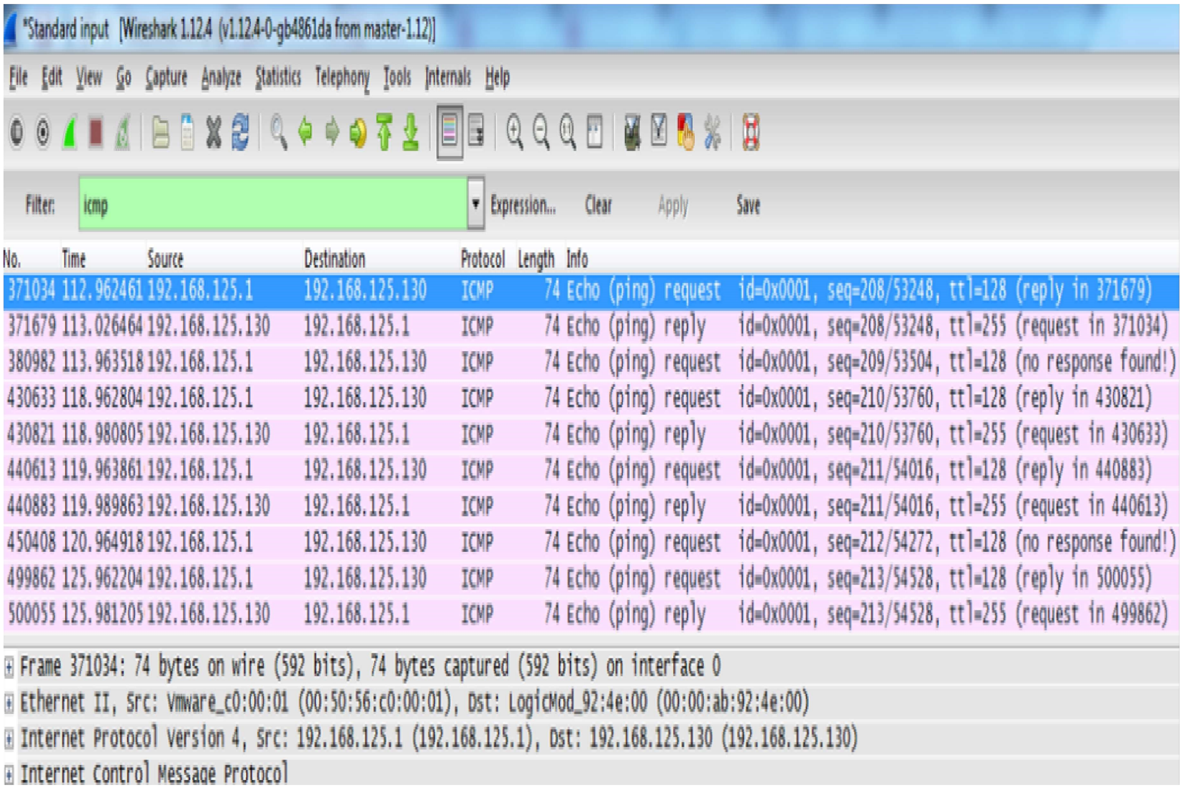


```
root@kali:~# hping3 -c 10000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168
.125.130
HPING 192.168.125.130 (eth0 192.168.125.130): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

Figure 7. DoS attack with Hping3

To solve this problem, ASA uses TCP SYN Cookies: ASA protects the server and does not broadcast all connections to it. Instead of remembering all these half-sessions, the ASA responds to each of them, but the actual connection to the server only occurs after receiving Ack's 3rd response. Embryonic-conn-max 5 means that the maximum resolution is up to 5 half-connections. You need to set the following settings:

```
access-list outside_mpc line 1 extended access tcp for any object dmz-server real

class-map no-syn-flood-class

match access-list outside_mpc

policy-map NO-SYN-FLOOD

class no-syn-flood-class

set connection conn-max 0 embryonic-conn-max 5 per-client-max 0 per-clientembryonic-conn-max 0
random-sequence-number enable

service-policy NO-SYN-FLOOD interface outside
```


*Standard input [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression...
Clear
Apply
Save

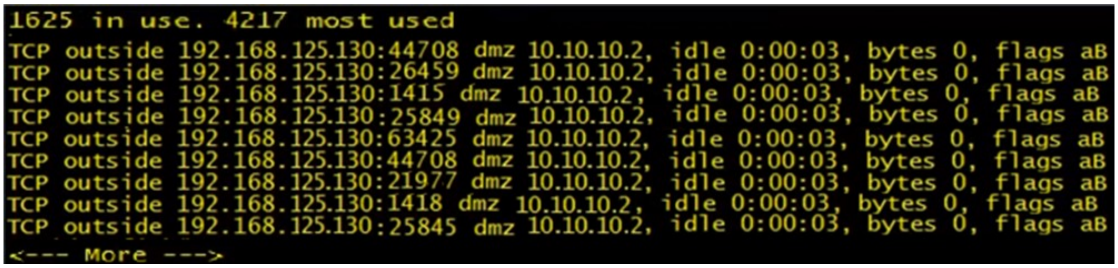
Filter: icmp

```
No.    Time       Source          Destination     Protocol Length Info
371034 112.962461 192.168.125.1   192.168.125.130 ICMP     74 Echo (ping) request  id=0x0001, seq=208/53248, ttl=128 (reply in 371679)
371679 113.026464 192.168.125.130 192.168.125.1   ICMP     74 Echo (ping) reply    id=0x0001, seq=208/53248, ttl=255 (request in 371034)
380982 113.963518 192.168.125.1   192.168.125.130 ICMP     74 Echo (ping) request  id=0x0001, seq=209/53504, ttl=128 (no response found!)
430633 118.962804 192.168.125.1   192.168.125.130 ICMP     74 Echo (ping) request  id=0x0001, seq=210/53760, ttl=128 (reply in 430821)
430821 118.980805 192.168.125.130 192.168.125.1   ICMP     74 Echo (ping) reply    id=0x0001, seq=210/53760, ttl=255 (request in 430633)
440613 119.963861 192.168.125.1   192.168.125.130 ICMP     74 Echo (ping) request  id=0x0001, seq=211/54016, ttl=128 (reply in 440883)
440883 119.989863 192.168.125.130 192.168.125.1   ICMP     74 Echo (ping) reply    id=0x0001, seq=211/54016, ttl=255 (request in 440613)
450408 120.964918 192.168.125.1   192.168.125.130 ICMP     74 Echo (ping) request  id=0x0001, seq=212/54272, ttl=128 (no response found!)
499862 125.962204 192.168.125.1   192.168.125.130 ICMP     74 Echo (ping) request  id=0x0001, seq=213/54528, ttl=128 (reply in 500055)
500055 125.981205 192.168.125.130 192.168.125.1   ICMP     74 Echo (ping) reply    id=0x0001, seq=213/54528, ttl=255 (request in 499862)

⊞ Frame 371034: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
⊞ Ethernet II, Src: Vmware_c0:00:01 (00:50:56:c0:00:01), Dst: LogicMod_92:4e:00 (00:00:ab:92:4e:00)
⊞ Internet Protocol Version 4, Src: 192.168.125.1 (192.168.125.1), Dst: 192.168.125.130 (192.168.125.130)
⊞ Internet Control Message Protocol
```

Figure 8. Filtered ICMP traffic during a DoS attack

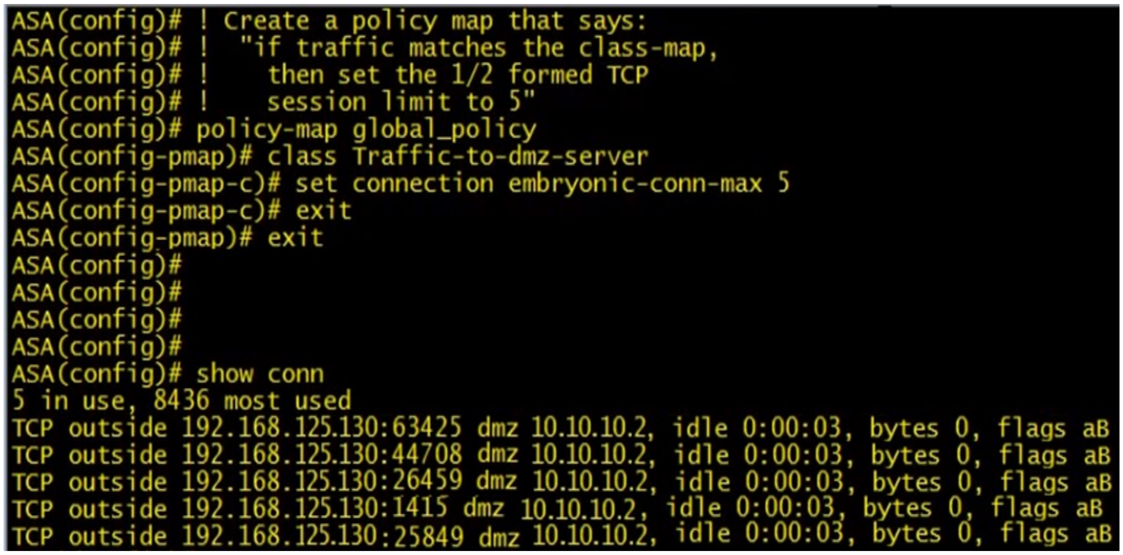
Without additional settings for Syn-Flood attack, we have 1625 active connections to the server, so as a result we have a denial of service, as shown in Figure 9.

With such protection settings, the ASA will create a separate queue for half-sessions, it will not be able to affect the server, and as a result we get only 5 half-connections, as shown in Fig. 10. It indicates the protection efficiency from shown attack type with the correct setting of the firewall.



```
1625 in use. 4217 most used
TCP outside 192.168.125.130:44708 dmz 10.10.10.2, idle 0:00:03, bytes 0, flags aB
TCP outside 192.168.125.130:26459 dmz 10.10.10.2, idle 0:00:03, bytes 0, flags aB
TCP outside 192.168.125.130:1415 dmz 10.10.10.2, idle 0:00:03, bytes 0, flags aB
TCP outside 192.168.125.130:25849 dmz 10.10.10.2, idle 0:00:03, bytes 0, flags aB
TCP outside 192.168.125.130:63425 dmz 10.10.10.2, idle 0:00:03, bytes 0, flags aB
TCP outside 192.168.125.130:44708 dmz 10.10.10.2, idle 0:00:03, bytes 0, flags aB
TCP outside 192.168.125.130:21977 dmz 10.10.10.2, idle 0:00:03, bytes 0, flags aB
TCP outside 192.168.125.130:1418 dmz 10.10.10.2, idle 0:00:03, bytes 0, flags aB
TCP outside 192.168.125.130:25845 dmz 10.10.10.2, idle 0:00:03, bytes 0, flags aB
<--- More --->
```

Figure 9. SYN-flood attack active sessions without protection settings



```
ASA(config)# ! Create a policy map that says:
ASA(config)# !  "if traffic matches the class-map,
ASA(config)# !    then set the 1/2 formed TCP
ASA(config)# !    session limit to 5"
ASA(config)# policy-map global_policy
ASA(config-pmap)# class Traffic-to-dmz-server
ASA(config-pmap-c)# set connection embryonic-conn-max 5
ASA(config-pmap-c)# exit
ASA(config-pmap)# exit
ASA(config)#
ASA(config)#
ASA(config)#
ASA(config)#
ASA(config)# show conn
5 in use, 8436 most used
TCP outside 192.168.125.130:63425 dmz 10.10.10.2, idle 0:00:03, bytes 0, flags aB
TCP outside 192.168.125.130:44708 dmz 10.10.10.2, idle 0:00:03, bytes 0, flags aB
TCP outside 192.168.125.130:26459 dmz 10.10.10.2, idle 0:00:03, bytes 0, flags aB
TCP outside 192.168.125.130:1415 dmz 10.10.10.2, idle 0:00:03, bytes 0, flags aB
TCP outside 192.168.125.130:25849 dmz 10.10.10.2, idle 0:00:03, bytes 0, flags aB
```

Figure 10. SYN-flood attacks active sessions with protection settings

7. Conclusions

The ways of constructing a virtual cybersecurity polygon on different platforms have been described, and received conclusions for each of the emulators based on the advantages and disadvantages each of them. The topology of the cybersecurity polygon have been developed and implemented on the basis of the GNS3 application software. The topology of a computer network consists of a Cisco ASA 5520 firewall that divides the company's network into a demilitarized zone, an internal and an external network. The router Cisco 3745 has been configured routing traffic between Workers and Management networks and remote connection through secure protocol SSH version 2. In a demilitarized zone, a Web server have been configured to access both from the external network (Cisco ASA automatically transmits packages to the server by 80 port) and from the internal network. Also the FTP server is been configured for only internal network access. Cisco ASA has configured static NAT, for Internet access to the local server, and for external forbidden access to the internal network and also has the Cisco ASDM graphical interface. The network settings have been corrected.

The cybersecurity polygon have been tested by network scanning and network devices ports scanning with

Zenmap utility. As a result of the ASA and NAT settings, the external scanning gave only information about IP address of the ASA interface, and the internal scanning presented all information about an internal network including an internal Cisco ASA interface.

The Hping3 utility has been used for a network stress-test. The Syn-Flood Attack has been implemented and shown counteraction ways to this attack.

References

[1] Korniyenko, B. (2012). Model of open systems interconnection terms of information security. *Science Intensive Technology, (15)*, 83–89. https://doi.org/10.18372/2310-5461.15.5120

[2] Korniyenko, B., Yudin, O., Novizki, E. (2013). Open systems interconnection model investigation from the viewpoint of information security. *The Advanced Science Journal, (8)*, 53–56.

[3] Korniyenko, B., Yudin, O. (2013). Implementation of information security in a model of open systems interconnection. In *Abstracts of the VI International Scientific Conference "Computer Systems and Network Technologies" (CSNT-2013)* (p. 73).

[4] Korniyenko, B. (2016). *Information security and computer network technologies: Monograph*. Saarbrucken, Germany: LAMBERT Academic Publishing.

[5] Korniyenko, B., Galata, L., Kozuberda, O. (2016). Modeling of security and risk assessment in information and communication systems. *Sciences of Europe, 2*(2), 61–63.

[6] Korniyenko, B. (2016). The classification of information technologies and control systems. *International Scientific Journal, (2)*, 78–81.

[7] Korniyenko, B., Yudin, O., Galata, L. (2016). Risk estimation of information systems. *Wschodnioeuropejskie Czasopismo Naukowe, (5)*, 35–40.

[8] Korniyenko, B., Galata, L., Udowenko, B. (2016). Simulation of information security of computer networks. In *Intellectual Decision-Making Systems and Computing Intelligence Problems (ISDMCI'2016): Collection of Scientific Papers of the International Scientific Conference* (pp. 77–79). Kherson, Ukraine.

[9] Korniyenko, B. (2017). *Cyber security: Operating systems and protocols*. Saarbrucken, Germany: LAMBERT Academic Publishing.

[10] Korniyenko, B., Galata, L. (2017). Design and research of a mathematical model for an information security system in a computer network. *Science Intensive Technology, (34)*, 114–118.