JOURNAL OF SCIENTIFIC PERSPECTIVES
E-ISSN: 2587-3008
October 2018, Vol:2, Issue: 4
http://ratingacademy.com.tr/journals/index.php/jsp/

CYBERSECURITY IMPLEMENTATION ASPECTS AT SHIPPING 4.0 AND INDUSTRY 4.0 CONCEPTS REALIZATION

Assoc. Prof. Dr. Vladlen SHAPO

National University "Odessa Maritime Academy", Ukraine,
E-mail: vladlen.shapo@gmail.com

ARTICLE INFO

Article History:
Received: *3 October 2018*
Accepted: *28 October 2018*

Keywords*: Industry 4.0, IoT, IIoT, Shipping 4.0, cybersecurity, firewall, Unmanned Cargo Ship Development Alliance, Distributed Intelligent Vessel Components software, Advanced Autonomous Waterborne Applications Initiative, Maritime Autonomous Surface Ships*

DOI:
10.26900/jsp.2018445371

ABSTRACT

Last few years took place true jump in approaches to developing, control and exploitation of different complex technical systems. In industry, transport, energetic and so on data exchange technologies, based on Industry 4.0, IoT, IIoT, Shipping 4.0, etc. concepts are implementing very actively. In maritime branch information technologies became inextricably linked to the classical approaches and allow to perform intelligent remote control and create fully unmanned objects and complex technical systems. So, some companies have founded Unmanned Cargo Ship Development Alliance; newly developed Distributed Intelligent Vessel Components software, which provides new protocol for devices connecting and data transferring; recently created Advanced Autonomous Waterborne Applications Initiative autonomous ship research project and Maritime Autonomous Surface Ships direction.

It's possible to highlight following ship automation levels.

1. *Ship can be controlled remotely.*
2. *Ship may work in unmanned mode partly or periodically.*
3. *Ship may perform self-driving with operator help, if necessary.*
4. *Additionally to the level 3, self-driving possible without operator's intrusion.*
5. *Fully unmanned ship with the same functionality and possibilities as classic ship.*

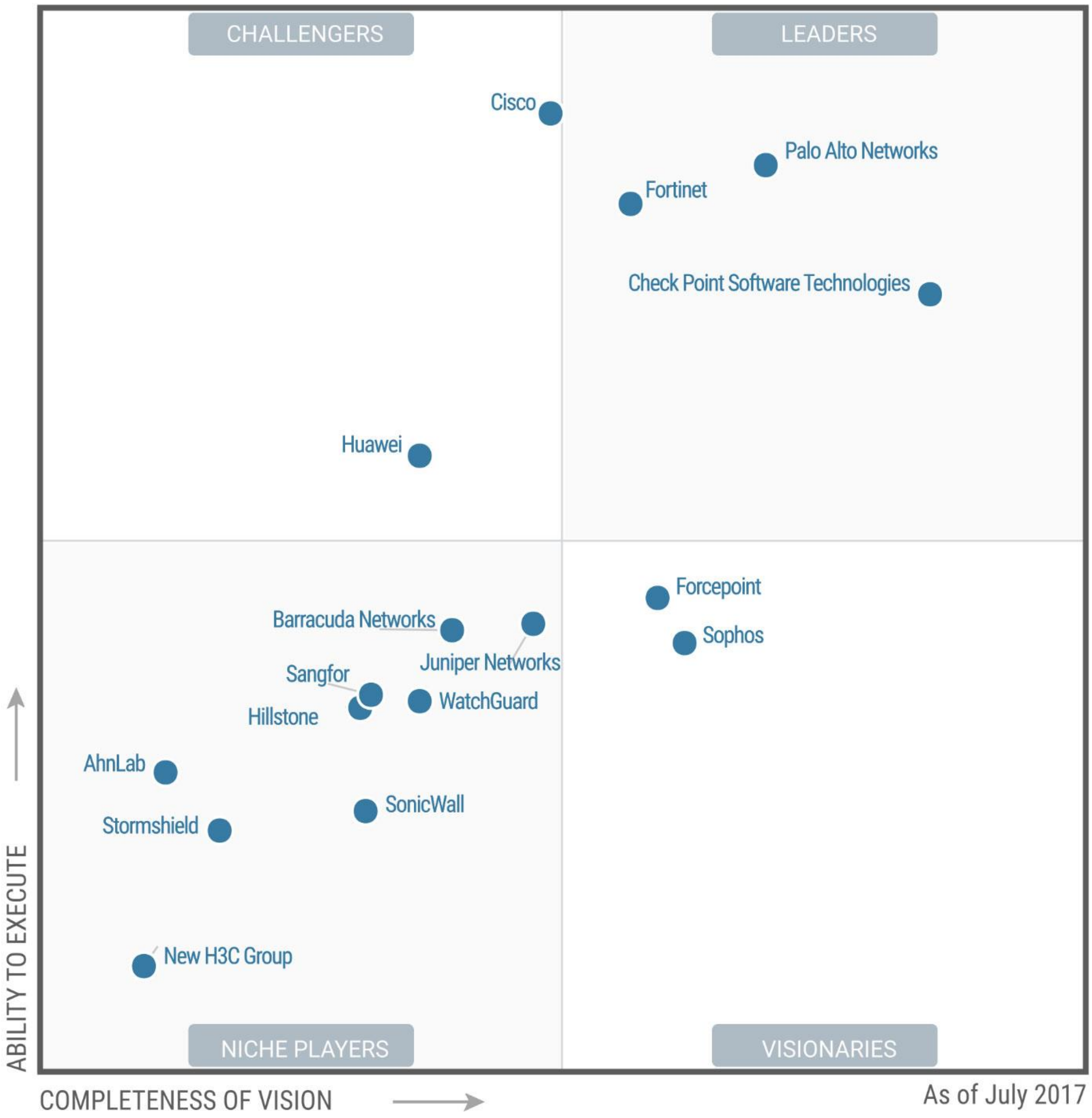
But complexity and vulnerability for external intrusion of such ships is also growing enormously. So, in 2017 and 2018 years at least two large shipping companies were attacked by hackers and had to stop significant part of business activity and lost huge amounts. That's why the task of cybersecurity providing, including highly productive firewalls implementing, is very actual.

Ways of modern concepts and technologies implementing in maritime branch are briefly analyzed. Possible levels of ships' autonomy and automation with most modern technical decisions are shown. Existing problems and vulnerabilities of highly automated ships are described. Approach on vulnerabilities influence minimizing with firewalls using is proposed.

1. INTRODUCTION

Last 10-15 years it's become absolutely clear that software and hardware cybersecurity systems are very significant for of any information system operability assurance. Modern equipment in any branch of industry, transport, etc. became much more automated, complex and expensive, supporting of business processes become much more intelligent, software become much more complex and sophisticated, data flows in corporative networks (inside separate networks and between territorially distributed subdivisions in different cities, countries and even continents) and industrial networks become enormous and still growing. Idle time of equipment, facility, information system, etc. leads to huge financial losses and these values are growing as well. For example, idle time at waterside (arrival and departure), constitute 38 per cent of the total port stay for a container ship, which cost billions of USD per year to the shipping lines [1]. So the best situation is when any complex equipment will be fully loaded 24 hours per day. Different kinds of cyberattacks or malicious software intrusion may be a reason of such problems, and implementation of firewalls for defence of information systems may significantly reduce these risks. For instance, ransomware attacks on Maersk's operations in June 2017 took nearly a month to recover and approximate losses were about USD 250 Millions [2]. In 2018 hackers attacked successfully Maersk again [3], and also were successfully attacked Cosco [4], ports of San Diego [5] and Barcelona [6, 7]. Thus different approaches on cybersecurity providing are highly necessary, and one of these approaches is different types of firewalls application.

Figure 1. Magic Quadrant for Small/medium Business and Enterprise Network Firewalls



Firewall (FW) have to control access between trusted and untrusted (internal/external) networks using beforehand created rules. FW may be a hardware (physical device, installed between the external and internal networks; more expensive but much more productive), software (protects a single computer; will not analyzed below) that is used to prevent unauthorized program or users from untrusted network from accessing a private network or a single computer. All data from external network have to pass through the FW, which analyzes them for specified beforehand security criteria. FW is necessary to protect network in general, its separate resources from users or devices which have no corresponding rights and from malicious users and accidents that originate outside of our network.

At shaping FWs application services strategy it's necessary to understand deeply the application architectures of company. Mostly application services are network and security services (often referred to as Open System Interconnection (OSI) model levels 4–7 services or application delivery services), and also availability, performance, security, and identity and access management. Typical application services include north-south and east-west load balancing, web application firewalls, DDoS prevention/protection, application analytics/monitoring, SSL instantiation and termination.

FW can stop hackers from computer accessing; protect personal information; block “pop up” ads, invalid packets and cookies; determine which programs can access the internet. Personal FW can't prevent e-mail viruses. FW requires periodic updates to the rule sets and the software itself. In June/July 2017 have been appeared next reports (Magic Quadrants) of Gartner (Fig. 1).

Gartner is global research and advisory company providing insights, advice, tools for leaders in IT, Finance, Marketing, Sales, etc. These reports are dedicated to Unified Threat Management (UTM) – for Small and Medium-sized Business (SMB) Multifunction Firewalls and for Enterprise Network Firewalls. Most famous developers on this market are following companies: F5 Networks, Riverbed, Cisco, Fortinet, Huawei, Palo Alto Networks, Check Point Software Technologies, Sophos, Forcepoint, Barracuda Networks, Juniper Networks, SonicWall, Hillstone Networks, WatchGuard, Sangfor, AhnLab, Stormshield, H3C, Rohde & Schwarz cyber security, Untangle, Alien Vault, Algosec, etc. [8, 9]. These companies permanently develop new software, hardware and combined solutions. Main problem for end customer is to choose specific solution satisfying on performance/expenses ratio, also taking into consideration some additional characteristics like number of monitored ports (typical values are 4, 5, 7, 8), expansion slots (typical values are 1, 2), maximum number of protected nodes (typical values are 200, 450, 500, 1000, 5000), maximum throughput (typical values are 50 Mbps, 100 Mbps, 200 Mbps, 500 Mbps, 1Gbps), internal storage subsystem (typical values are 64, 180, 240 GBytes). So it's necessary to formalize procedure of firewall characteristics analyzing, calculating and choosing.

2. MAIN TEXT

The FW is very important component for modern network security. Main types of FWs are stateless and stateful FWs, transparent FWs, FWs at various levels of the network reference architectures, FWs with deep packet inspection (DPI), FWs with intrusion detection features. In addition, FWs are necessary to restrict communication to the desired patterns and communication relationships at other parts of the network. But FWs can also enlarge transmission latency and reduce network throughput, the use of a dedicated FW is not always possible. In such cases, professional network switches can also use less powerful stateless filtering rules. These rules are usually not referred to as FW rules, but to access control lists (ACL). ACLs are suited for situations when rapid filtering must take place within a network. Thus it's necessary to make optimal choice.

1. Packet filter FWs analyze each packet, entering or leaving the network, and accept or reject it, using beforehand defined rules. Packet filtering is quite effective and transparent to users, but it's difficult to configure, and it's vulnerable to IP-addresses spoofing.

2. In application gateway FWs remote host or network communicates only with proxy server, which is responsible for hiding the details of the internal network. Users work with TCP/IP applications. This is very effective but can be reason of performance decreasing.

3. Circuit level gateway works at the session layer of the OSI model. It's standalone system or a specialized application. It does not permit an end to end TCP connection and creates two TCP connections. A typical use of the circuit level gateway is a situation, when network administrator trusts the internal users. FW can be configured to support application level or proxy service on incoming connections and circuit level functions for out coming connections.

4. Stateless FWs. Communications between devices may have some states. Communication is usually initiated in 1st phase, data exchange is performed in 2nd phase, the connection is ended in 3rd phase. Stateless FWs can't react to the state of a connection nor differentiate between the various phases. Thus, it can only be determined that individual devices or applications may communicate with one another. But it can't be determined whether the participants conduct the communication according to the normal procedure. So, the FW cannot recognize or prevent any attacks resulting from anomalous protocol behaviour. Especially vulnerable devices with minimal self defence are put at risk by denial of service (DoS) attack, by which device communication interface is specially flooded and overloaded with forged or mistaken communication requests.

5. Stateful FWs. In contrast to stateless, stateful FWs can monitor the communication process of the participants and thus use the behaviour of the partners during essential communications operations, such as the initiation or termination of the connection, as the foundation for the packet filtering. Thus, attacks which attempt to communicate over connections already made can be recognized and prevented. Equally, attacks which use a known faulty connection in order to load and overload a system can be prevented. These FWs have high level of defence, may work at all 7 levels of OSI model, transparent for applications, have quite good performance and scalability. In the same time cost is also quite high. DPI FWs is subtype of stateful FWs. Stateful FW typically examines the packets in the network as deep as the header at the beginning of the packet, because it contains the information used by FW for communication state determining and monitoring. DPI also allows examination beyond the communication header all the way to the packet payload. Thus highly specialized attacks, hidden deep in the communication flow, can be discovered. DPI FWs are often implemented as additional components of a stateful packet inspection FW only for certain protocols and application purposes. DPI FW offers a high level of security, but it demands a great amount of FW computing power. It also requires a sophisticated configuration interface in order to command the complexity of it. As the result DPI FWs are applied only at certain points in the network. At that location they create a significantly stronger communications security.

6. Packet filter, screening filter. This type has following positive sides: low cost, transparency for application, high performance. But possibilities of analysis are

restricted (up to 4th OSI model level), level of defence is low and may be easily bypassed; settings FW and monitoring parameters are complex.

7. Proxy (application layer gateway). This type has following positive sides: high level of defence, working at all 7 levels of OSI model, possibilities of web filtering, e-mail checking. Negative sides: number of supported protocols is restricted, absence of transparency (it's necessary to specify at client computers proxy server address); duplicating of connections number; low performance; high requirements to proxy server productivity, bad scalability.

Additionally, to traffic filtering FWs may include content filtering, static or dynamic network addresses translation (NAT), virtual private networks (VPN) organization (site to site, point to point, point to site), intrusion detection systems (IDS), Demilitarized Zone (DMZ) organization. For traffic defense may be applied following protocols: IPSec (IP Security), Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), Open VPN, etc., which use algorithms DES (56 bit key encryption) Data Encryption Standard, Triple Data Encryption Algorithm 3DES TDES Triple (168 bits key encryption), Advanced Encryption Standard AES (128/192/256 bits key encryption). AES is newest and realized by Intel company in Core i7 processors. For execution of most of these functions high processing power is necessary. That's why it's reasonable to prefer special hardware FW solutions or in some cases application of separate stand alone computers with high productive central processors.

It's possible to highlight following criteria of FW choosing.

1. Functionality and supported functions in three main subsets: firewall/intrusion prevention system (IPS) / VPN gateway, secure Web gateway security (URL filtering, Web antivirus) and messaging security (anti-spam, mail antivirus) and also NAT, VPN, base routing system, WAN-technologies supporting, etc.

2. Number and types of necessary interfaces (DMZ, modem pools, etc.).

3. Possibilities of integration with existing equipment and software, communications between wireless and wired networks, possibilities of FW integration directly to the wireless access point.

4. Total cost of ownership (price, expenses for additional training of network administrator and his salary, technical support, licenses, expenses for two typical FW management tasks [10, 11]: the integration of a new FW in an existing network and the management of multiple FWs with network management tools) [Ismail, 12, Mohan, 13].

5. Presence of actual in close future functions: Firewall as a Service, working with private and public clouds, close integration with IaaS platforms (Amazon Web Services, Google Cloud, Microsoft Azure), Cloud Access Security Brokers (CASB) using, outgoing Transport Layer Security (TLS) inspection, Multi tiered DMZs, solutions for SaaS security, growing sophistication and more close integration of Security Information and Event Management (SIEM) systems.

Installation of new FW in existing network is pretty complex task. If FW is configured liberally, the network traffic will pass without problems, but FW will not be significant obstacle for hacker. If FW is configured too restrictively, it blocks hacker's activity, but also slows down network traffic. It's important to configure the FW to permit the desired communication and to prevent the undesirable traffic in the same time. Without a complete view of all communication relationships, the integration of a FW in an existing network is far from easy. High end FW may work in analysis mode when it analyzes the relationships between devices in a network during a freely specified learning stage. The FW records all data exchanges between network devices without any restrictions. As a result an administrator can detect desired or undesired communication relationships quickly and easily and create a custom configuration of the FW partly or fully automatically. It saves time and enables a functional and secure configuration without time losses and failures.

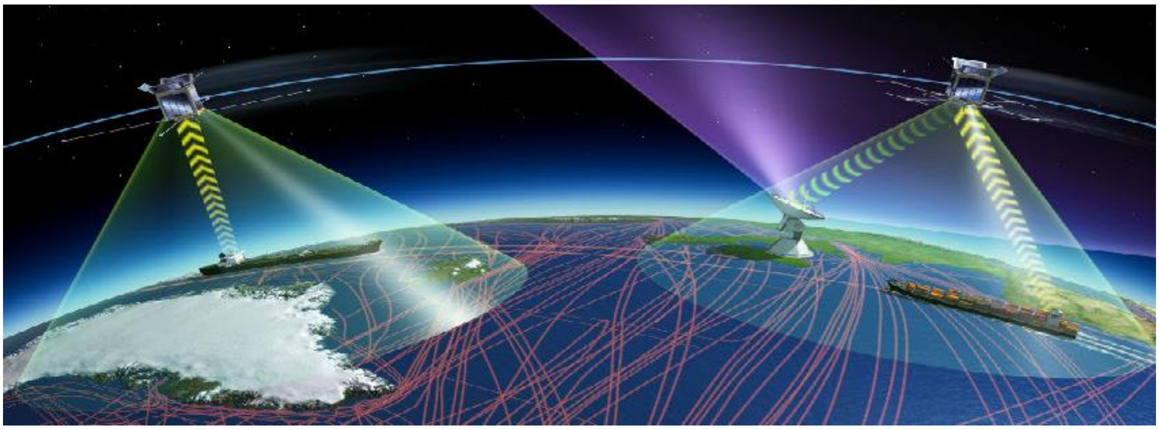
The use of multi level FW application model is very important aspect of the defence in depth. If an attacker has overcome an initial obstacle, additional FWs with more sophisticated rules can prevent further penetration. The use of multiple FWs requires additional management and configuration of these devices. Without a powerful software management tool this task is very time-consuming and may be additional reason for faults and errors. That's why it's very important that the FWs can be managed and monitored centrally by software network management tools. This approach will allow to implement standard configurations quickly on newly installed FWs, as well as making changes to the configuration. If all FWs must be configured individually, a lot of parameters must be manually entered on each FW. With software network management tool this task may be simultaneously, quickly and reliably performed for all FWs at once.

In maritime branch it's necessary to use satellite technologies to provide data exchange between the ship and land office. FW must be installed between ship's network and external network in general and Internet particularly. Most popular satellite technologies in maritime branch are Inmarsat and in last decade also VSAT.

Inmarsat provides Mobile Packet Data Service (MPDS), Integrated Service Digital Network (ISDN), Public Switched Telephone Network (PSTN) and low cost voice telephony. Real-time telemetry, Supervisory Control and Data Acquisition (SCADA) and messaging applications may be provided as well. Also 64 kbps ISDN connectivity, enabling high-speed data transfer and high quality voice, fax and video, a 3.1 kHz audio channel for the connection of analogue devices as well as low cost "Inmarsat mini M" voice telephony and fax and 128 kbps ISDN service are available.

Fig. 2 presents typical scheme of satellites application for data exchange between ship and land office.

Figure 2. Scheme of satellites application for data exchange between a ship and land office

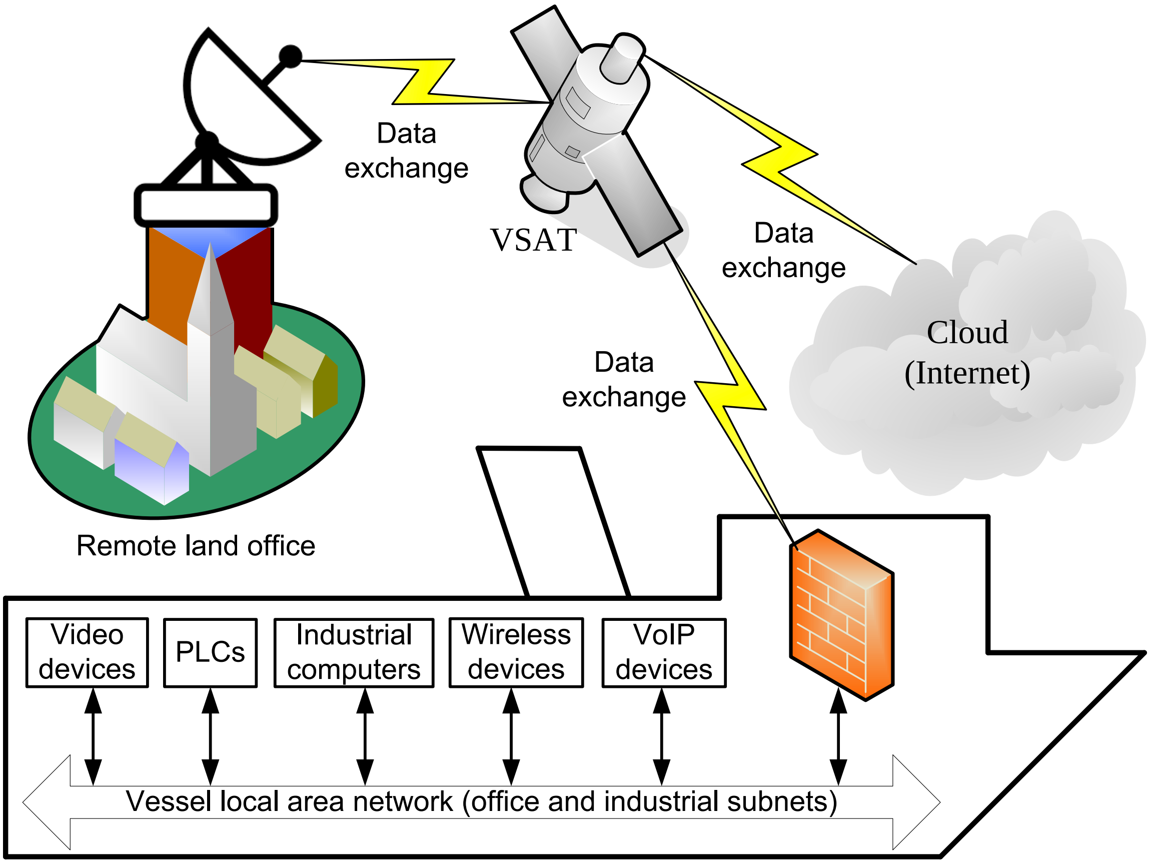


Much more modern VSAT based technologies provide multiple service options starting at 32 kbps, broadband, two-way SCADA data exchange through IP or serial interface for entire ship network. VSAT products family offers new embedded technologies including acceleration, built-in accelerated VPN, advanced QoS, high inbound bit rates, advanced encryption, improved access scheme and modulations resulting in maximum bandwidth efficiency and performance from satellite network.

Maritime operators realize VSAT possibilities by proposing higher throughput services. As a result installed number of equipment is actively growing. VSAT data rates in some segments increased from 10 Mbps in 2007 to 100 Mbps in 2013, largely driven by streaming video and bandwidth-intensive business applications. [Comsys 14]. On some ships a multi-band and multi-orbit VSAT service also provided. It worked with Intelsat, SES and Telesat satellite operators for the satellite coverage and delivers super-fast broadband service, peaked at 3.1 Gbps [15].

Fig. 3 presents scheme of data exchange between land office network (Internet) and computerized subsystems on board a ship (office and industrial networks) with satellites using.

Figure 3. Scheme of satellites application for data exchange between computerized subsystems on board a ship and land office with satellites using



In complex distributed structures (separate local area networks (LAN) in remote subdivisions or big complex campus network), among others in maritime branch, it makes sense installing of several FWs (Fig. 4) for each subdivision or workgroup as defence facility from internal attacks. Centralized FW is based on a perimeter defence model assuming attacks from outside a network. But this model fails if an attack comes from inside the network (users can connect to an internal network using wireless access, VPN tunnels, etc.). Traditional FWs typically can’t effectively deal with such attacks, but a distributed FW adds one more defence layer. Also growing of internet access speeds and appearance of new complex protocols, that FWs must analyze, causes that stand alone FW may become congestion point. Distributed FWs help solve this problem by using processing power in different network points. A distributed FW is security software application, which protects the entire network and must be installed additionally to traditional FWs. Distributed FWs have following standard set of capabilities.

1. Centralized management and reporting: configuration with "push out" security policies.
2. Fine-Grained Access Control: standard FWs cannot readily accommodate without greatly increasing their complexity and processing requirements.
3. All FWs have the ability to set security policies to allow or deny access, depending on determined criteria. Distributed FWs usually also have features that guarantee the integrity of the policy during transfer.
4. Distributed FWs typically support “pull” and “push” distribution methods: pinging the central management server to check whether it’s in working conditions, then requesting its policies, and the last step is ensuring that the hosts always have updated policies at all times.

Fig. 4 presents hardware or distributed FW multiplicity application with data flows specification.

Figure 4. Multiple (distributed) firewalls implementation in complex distributed structure with variety of LANs

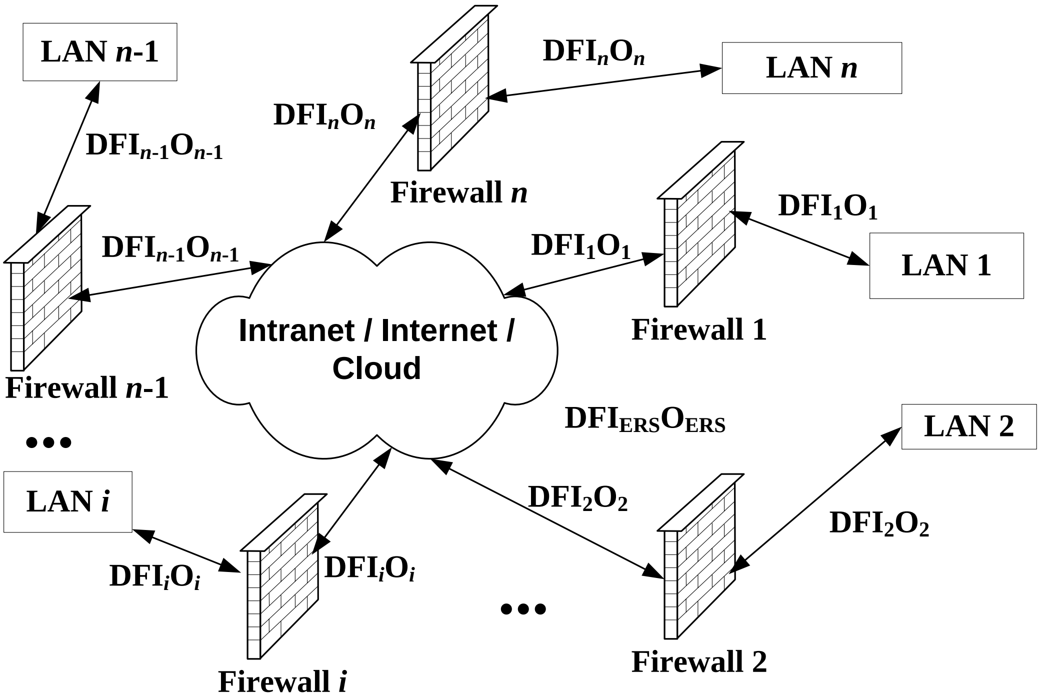


Fig. 4 contains following abbreviations: DFI – Data Flow Input, DFO – Data Flow Output.

Traditional physical and virtual FWs have started to hinder assurances of modular protection in modern network environments. Distributed FWs can work as additional fix for some new problems that arise when dealing with the challenges of maintaining a secure network in a business environment. Distributed FWs allow to maintain internal and external security with the theoretically limitless expansion properties.

Let (C_{mp}, C_{es}, C_{pn}, C_{tp}, C_{ss}) is vector of FW characteristics (any model; any manufacturer): C_{mp} is number of monitored ports, C_{es} is number of expansion slots, C_{pn} is maximum number of protected nodes, C_{tp} is maximum throughput (Gbit/s), C_{ss} is internal storage subsystem (GBytes). Then (C_{mpi}, C_{esi}, C_{pni}, C_{tpi}, C_{ssi}) is vector of FW characteristics for one of model (number i) of any manufacturer (quantity z of models in device line has to be defined by manufacturer). Then ($C_{mpi\mathrm{l}}$, $C_{esi\mathrm{l}}$, $C_{pni\mathrm{l}}$, $C_{tpi\mathrm{l}}$, $C_{ssi\mathrm{l}}$) is vector of FW characteristics for one of model (number *i*) of manufacturer number l (quantity *z* of models in device line has to be defined by manufacturer).

Let (P_{1k}, P_{2k}, …, P_{nk}, …, $P_{(z-1)k}$, P_{zk}) is vector of FW prices (manufacturer *k*, number of devices *z*). In the case when price factor is dominant and expenses for FW purchase are restricted, it's possible to choose some different models (more than 1) from device lines of different manufacturers (fig. 5). In this case will suppose that FW models of any manufacturer sorted by descending (model with the best characteristics will be placed on the top of device line, having number 1, but the price in this case will be maximum). Unfortunately, this particular approach, when expenses are restricted, is dominant in most cases. Very often it leads to wrong decision taking, discrepancy between FW characteristics and needs of concrete task at information system defense, and necessity of additional expenses, time wasting and specialists retraining.

In the general case volume of transferring data V_f and minimal demanded data transfer channel bandwidth B_f in network segment or Internet at ship information system cooperative exploitation are accordingly

$$V_{inpf} = \sum_{k=1}^{n} V_{\mathrm{inp}k} \quad \mathbf{(1)}$$

$$B_{inpf} = \sum_{k=1}^{n} B_{inpk} \quad \mathbf{(2)}$$

$$V_{outf} = \sum_{k=1}^{n} V_{outk} \quad \mathbf{(3)}$$

$$B_{outf} = \sum_{k=1}^{n} B_{outk} \quad \mathbf{(4)}$$

where V_{inpk} – volume of data, transferring to ship network (information system) from *i*-number local or remote user; B_{inpk} – data transfer network bandwidth, demanded for data transferring from *i*-number user; V_{outk} – volume of data, transferring to ship network (information system) from *i*-number local or remote user; B_{outk} – data transfer network bandwidth, demanded for data transferring from *i*-number user.

From the technical point of view V_{inpk} is data volume, generated by control commands, and B_{inpk} is bandwidth, necessary for control commands transferring. V_{outk} and B_{outk}, generated by digital devices in ship network (information system), but it's necessary to take into account possible outgoing malicious traffic presence and detection of possible problems with FW settings.

Figure 5. Choosing of firewall characteristics
(price is point of departure, characteristics are in second order)

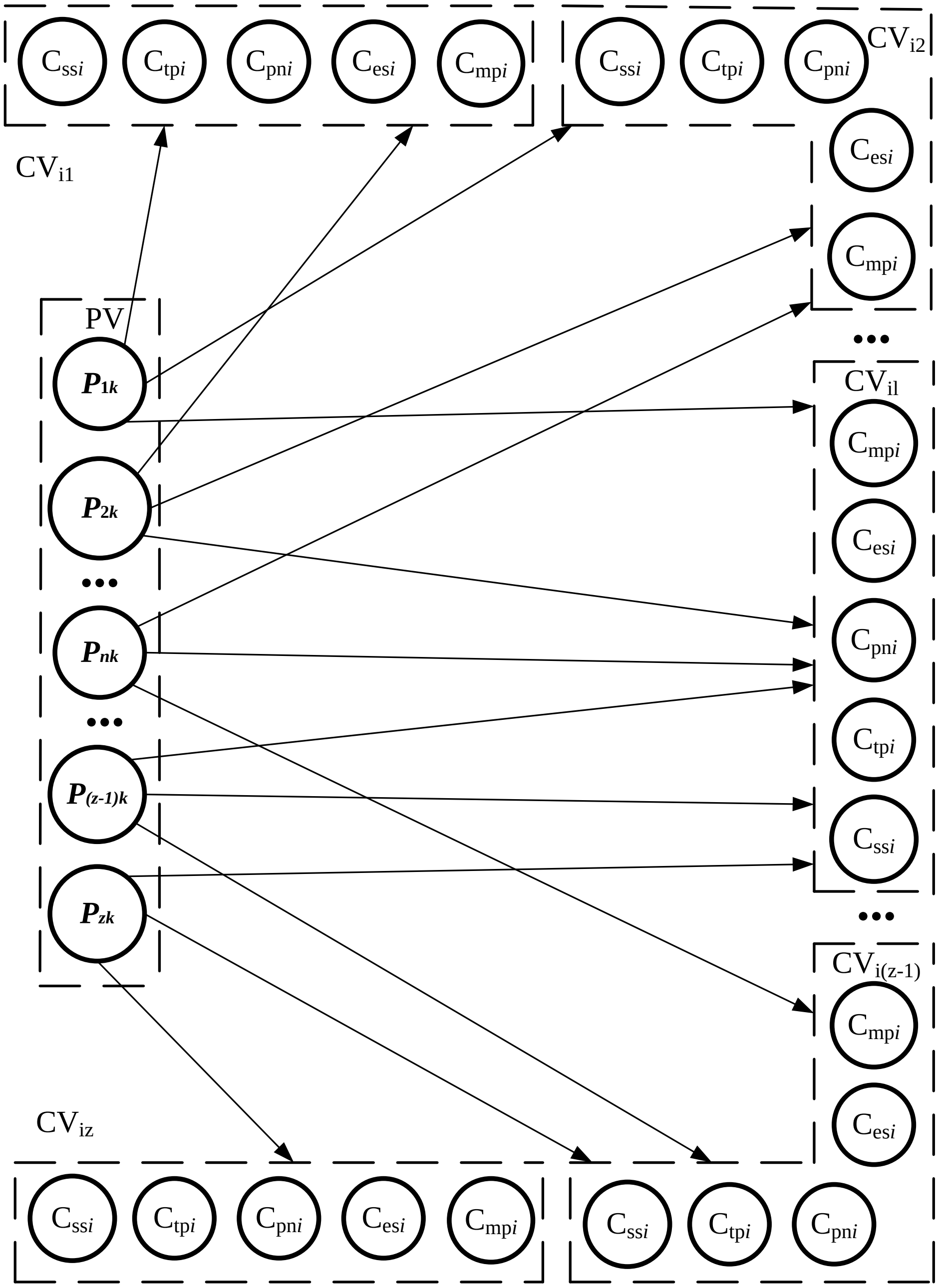


Fig. 5 contains following abbreviations: PV – Price Vector, CV – Characteristics Vector.

Situation is possible, when some same type devices transfer identical data volumes to local or cloud control computational system and create identical network segment or channel loading. In this case volume of transferring data V_f and minimal demanding network segment or Internet channel bandwidth B_f it's possible to count using following formulas:

$$V_f = \sum_{i=1}^{n} k_i V_i \qquad (5)$$

$$B_f = \sum_{i=1}^{n} k_i B_i \qquad (6)$$

where k_i – number of same type devices of i-type, which generate identical volume of data, transferring to local or cloud control computational system, creating similar network loading.

Let in the network structure there are m local digital devices, which transfer data to central control computational system (cloud). In this case volume of data V_{fc}, transferring to central control computational system and minimal demanding bandwidth B_{fc} of corresponding network segment or Internet channel are accordingly

$$V_{fc} = \sum_{k=1}^{m} V_{fk} \tag{7}$$

$$B_{fc} = \sum_{k=1}^{m} B_{fk} \tag{8}$$

where V_{fk} – volume of data, transferring to cloud central control computational system from local digital device number k;

B_{fk} – network bandwidth, demanding for data transfer from digital device number k.

Formulas (1) - (8) allow to calculate volumes of transferring data and necessary bandwidth between ship network and land office and to facilitate choosing of network equipment, firewall and model of cloud services taking into account performance, data transfer rate and cost aspects.

Implementation of one or more local data processing device in ship network (information system) to reduce expenses for cloud system model choosing taking into consideration following parameters: necessary processor(s) productivity, random access memory volume, data store volume and productivity and to minimize expenses for Internet channel rent. Local control computational system may be used if some users use the same network (cloud) service but simultaneously work in the same local network.

Possible also opposite situation, when it's necessary to choose concrete characteristics of FW and concrete manufacturer because of presence of already installed hardware, software, network equipment, compatibility problems, recommendations of equipment manufacturers, prepaid support service and so on.

3. CONCLUSION

Firewall role as a necessary central element in maritime branch cybersecurity providing is shown. Model on optimal firewalls characteristics choosing with taking into consideration price/productivity ratio is proposed. Mathematical expressions which allow to calculate volumes of transferring data and necessary bandwidth are proposed.

REFERENCES

[1] Identification and measurement if idle times port visit of container ships through an explorative and simulation study: the case of Algeciras's terminal. 29.09.2018. <https://www.researchgate.net/publication/320345921_IDENTIFICATION_AND_MEASUREMENT_OF_IDLE_TIMES_PORT_VISIT_OF_CONTAINER_SHIPS_THROUGH_AN_EXPLORATIVE_AND_SIMULATION_STUDY_THE_CASE_OF_ALGECIRAS_S_TERMINAL>

[2] Maersk IT systems, websites hit in global cyber-attack. 29.09.2018. http://www.seatrade-maritime.com/news/europe/26227.html?highlight=Im1hZXJzayBjeWJlciI=

[3] Maersk hit another cyber attack. 29.09.2018. <https://splash247.com/maersk-hit-another-cyber-attack/>

[4] Cosco's US operations hit by cyber attack. 29.09.2018. <http://www.seatrade-maritime.com/news/americas/cosco-says-cyberattack-only-affected-us-operations.html<

[5] Port of San Diego hit by cyber attack. 29.09.2018. <https://splash247.com/port-of-san-diego-hit-by-cyber-attack/>

[6] Port of Barcelona Suffers Cyberattack. 29.09.2108. <https://www.bleepingcomputer.com/news/security/port-of-barcelona-suffers-cyberattack/>

[7] Ports on alert as cyber attacks proliferate. 29.09.2018. https://splash247.com/ports-on-alert-as-cyber-attacks-proliferate/

[8] Unbiased reviews from the tech community. 27.07.2018 <www.itcentralstation.com/landing/report-firewalls>

[9] Unbiased reviews from the tech community. 27.07.2018 <www.itcentralstation.com/categories/security-information-and-event-management-siem>

[10] Centralized Firewall Configuration and Update Management. 30.07.2018 <www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/panorama-overview/centralized-firewall-configuration-and-update-management>

[11] Firewall management. 2.08.2018. <https://www.algosec.com/firewall-management/>

[12] Nick Ismail, Going global: 3 key strategies for managing international firewalls. 30.07.2018 <www.information-age.com/going-global-three-key-strategies-managing-international-firewalls-123462232/>

[13] Vinod Mohan, Best Practices for Effective Firewall Management. 4.08.2018. <http://cdn.swcdn.net/creative/v9.3/pdf/Whitepapers/Best_Practices_for_Effective_Firewall_Management.pdf>

[14] The Coming Wave of Maritime VSAT Growth. 28.09.2018. <https://www.satellitetoday.com//long-form-stories/maritime-vsat/>

[15] Martyn Wingrove. HTS and hybrid networks enhance maritime connectivity. <http://www.marinemec.com/news/view,hts-and-hybrid-networks-enhance-maritime-connectivity_54296.htm>