Bulletin of Electrical Engineering and Informatics
ISSN: 2302-9285
Vol. 5, No. 3, September 2016, pp. 366~372, DOI: 10.11591/eei.v5i3.615

Security Technology by using Firewall for Smart Grid

Ayla Hasanalizadeh-Khosroshahi*[1], Hossein Shahinzadeh[2]
[1-]Young Researchers and Elite Club, Tabriz Branch, Islamic Azad University, Tabriz, Iran
[2-]Department of Electrical Engineering, Amirkabir University of Technology (Tehran Polytechnic), Tehran, Iran
*Corresponding author, e-mail: ayla.hasanalizadeh@gmail.com

Abstract

Due to the increasing development of computer systems and information networks, power grids should change extensively too. Nowadays, substantial movement has begun to implement the Smart Grid industry around the world. Since with the creation of smart electricity grids, it is possible to access the internal network from the external spaces, it is also necessary to protect information and data against unauthorized access. Therefore, a firewall should be used for information security. The firewall based on existing security regulations, decides which data is incoming to the network or going out of the network. Considering the discussions of passive defense topics at the national level and also the high importance of information security in Smart Grids, in this paper, in addition to examining the Firewalls, its advantages and disadvantages are also stated. Although the firewall has a major role in establishing security, and its installation and appropriate configuration can only be one of the primary activities in this field, we should also take advantage of other security mechanisms to enhance the security of the Smart Grid.

Keywords: *Smart Grid; Firewall; Information Security; Data Packets*

1. Introduction

Nowadays, an extensive movement has begun to implement the Smart Grid industry, whereby old networks are being replaced by Smart Grids around the world and modernization of the current electrical grid is of main concern with many electricity companies in the world. Smart Grids, based on the use of effective communication technologies between smart components, have an important role in operational efficiency, cost savings, and reliability improvement, since the intelligence of smart grid is built based on information exchange across the power grid [1-6].

Certainly, achieving the goals of these networks without proper communication infrastructures is not possible. As stated in [7] a smarter grid equipped with intelligent devices cannot survive if the communication infrastructure is insecure and vulnerable. In general, communication and information exchange systems used in the Smart Grids should have characteristics such as: reliability, high longevity, low maintenance, high compatibility between different manufacturers' products using standard protocols, low prices, low installation costs, low power consumption, and for sure high information security [8-9]. Connection to telecommunications and computer networks, whether through a local network or via a phone line, allows external users to access the internal network. For this reason, information and data protection against any unauthorized access is required. Generally a computer network is exposed to four types of attacks: interruption, eavesdropping, data manipulation and adding information [10-11]. Very similar to these, security issues for Smart Grids are classified into four categories: jamming, eavesdropping by nodes outside the network, eavesdropping by malicious nodes inside the network and launching security attacks by nodes in the network [2].

Information security of computer networks against these attacks is an undeniable necessity in Smart Grids. Today, discussing the issue of information security is felt to be more essential than ever, because both human and non-human factors have a defined position in the engineering of information security [12-14].

A firewall is one of the indispensable elements of the system's engineering for information security and using it has become an inevitable necessity for information security in the Smart Grid. Firewalls are located in different places of the connection in order to secure and manage incoming and outgoing traffic. The system administrator sets the rules of the firewall according to desired security level. Firewalls, depending on their types, provide possible ways

Received November 27, 2015; Revised July 2, 2016; Accepted July 15, 2016

for traffic management based on indicators such as: traffic type, sender addresses and ports, receiver addresses and ports, conditions and connection state, etc...

Generally, safety and security of the information in a Smart Grid can be achieved in two ways:

- Using a firewall for supervising information and accesses.
- Data encryption, so that even if someone gets the data, they cannot use and take benefit of their contents.

But as it was stated in [15], the lack of a standardized encryption scheme between system components opens the door to integrity concerns and insider threats. In this paper, structure of firewalls and their advantages and disadvantages are discussed.

2. Firewall

A firewall is a system which is located between the users of a local network and external networks. In addition to access control, firewall monitors the arrival and departure of information at all levels. In fact, firewall is a hard dam that is placed between a number of valuable assets from one side and a communications series on the other side. It should be noted that a firewall is not used to isolate the different network in an organization or different groups in an organization. The information is not secure in organizations and agencies whose information is accessible to all individuals in their internal network. Practically, the Firewall traps information packets inside and outside networks, analyzes them, and then lets them enter or exit, or just takes them out of the way. Firewalls are a subsystem of computer software and hardware that prevent entering or exiting malicious data. These firewalls are the parts that decide which data enters the network or exits within the network, based on security policy. Also, firewalls may have some security commands that change the content of packets with a specific procedure before sending them [16-17].

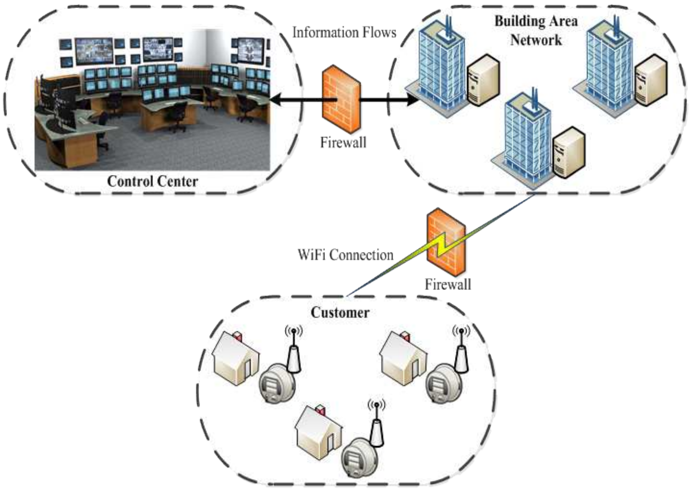

Figure 1. Network model for Smart Grid

Basically, networks based on the modes of security and security level can be divided logically into three categories: 1- Public Networks, 2- Semi-Private networks, 3- Private networks [18]. By this categorizing, the public network is the external network of an organization or a company, internet is an obvious example for this type of networks. In such a network, practical security is minimal and security mechanisms are carried out based on external systems (for example, the service provider's systems). A semi-private network is the part of the network that needs to access the network of the organization from outside (the public network side). For example, the web server of the organization in which the organization portal is placed. This part of the network is also called “Demilitarized Zone (DMZ)” (on firewall ports usually indicated with this name). This part of organizations has a medium security level. Maximum level of security is in Private networks, which includes an internal network that is accessible only from inside the organization [19-20].

3. Efficient Factors in Selecting a Strong Firewall

Important attributes of a strong firewall for a secure network are:

3.1. Registration and Notification Capabilities

Event registration is one of the important features of a firewall and it allows Smart Grid administrators to control the hacker attacks. Also, the network manager can handle traffic generated by authorized users with the help of the recorded information. In a proper way of record, Smart Grid administrators can easily access the critical data. In addition to data recording, a good firewall should be able to inform the Smart Grid manager of critical situations by sending him a warning [21-22].

3.2. Visiting High Volume of Data Packets

One of the capabilities of the firewall is the ability of viewing a high volume of packets without dramatically reducing the efficiency of the Smart Grid. The volume of data that a firewall can handle differs for different networks, but a firewall, certainly, should not become a bottleneck in its protected network. Several factors are involved in the speed of information processing by the firewall. Most restrictions on the effectiveness of firewall are imposed by processor speed and optimization of software code. Interface cards which are installed in the firewall could be another source of restrictions. The firewall which shares some of its tasks, such as warnings, URL based access control and log revision, with other software has enhanced speed and efficiency [22].

3.3. Configuration Ease

Generally, configuration ease includes abilities like firewall quick setup and quick error and diagnostic view. Indeed, many of the security problems which occur in Smart Grids are due to the incorrect configuration of the firewall. Fast and simple configuration of a firewall reduces errors. For example, the graphical representation ability of the network architecture or a tool that can indicate security policies in the configuration, is very important for a firewall [23].

3.4. Selecting the Installation Location of Firewalls

Like selecting the appropriate type of firewall and its full configuration, selecting the appropriate installation location is also particularly important. Some tips that should be considered for finding a suitable location to install a firewall include:

3.4.1. Installation Location from Topological Point of View

It usually seems fine to install firewall in the Input/ Output port of a private network. This contributes to creating the best security cover for private network with the help of firewall from one side and isolation of the private network from the public network on the other side [24].

3.4.2. Accessibility and Security Areas

If there are servers which should be accessible to the public network, it would be better to put them after the firewall and in the DMZ area. Placing these servers in the private network and setting the firewall to allow external users to access these servers is equal to hacking the internal network because you yourself have opened the way for hackers in the firewall. On the other hand, by using the DMZ area, accessible servers for the public network are physically isolated from the private network; thus if hackers would be somehow able to penetrate to these servers, the firewall is still ahead [25].

3.5. Asymmetrical Routing

Most of the modern firewalls try to save information about the different connections through which the internal network has been connected to the public network. This information contributes to the entrance only of the allowed information packets to the private network. As a result, it is very important for the input and output gate for all of the information to/from a private network pass through a firewall [22].

3.6. Layered Firewalls

In networks with a high degree of security, it is better to use two or more firewalls along the way. If the first firewall faces a problem, the second firewall continues the work. It is usually more beneficial if we use two or more firewalls from different companies. In this way, if there is some software bug or a security hole in one of them, others would be able to provide the network security. Figure 2 shows an example of firewall configuration and architecture in the Smart Grid [24].

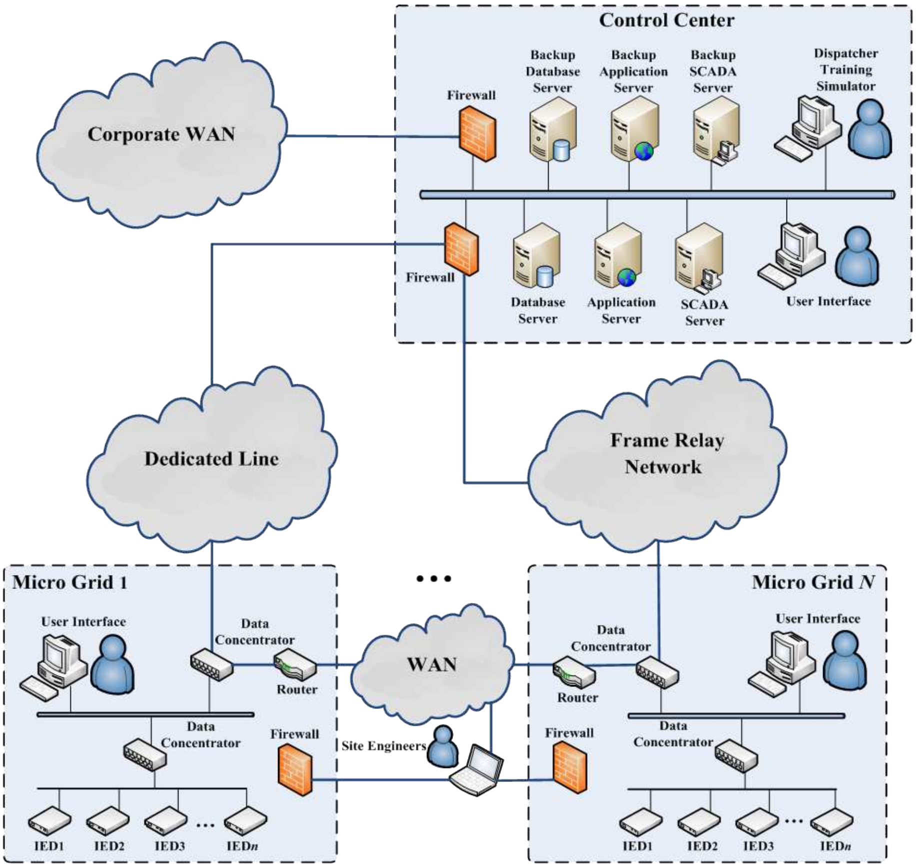

Figure 2. An example of firewall architectures in Smart Grid

4. Firewall Security Policies

A firewall protects the network against undesired traffic and other persons penetrating the computers. The primary functions of a firewall is letting “good traffic” to pass and blocking “bad traffic”. A set of firewall rules is also known as security policy. The security policy of a network is a finite set of security rules that is defined in one of the firewall layers due to their nature:

- The rules determining blocked packages (black package) in the first layer of firewall
- The rules closing some ports belonging to services such Telnet or FTP in the second layer
- The rules analyzing header of an email or web page in the third layer

4.1. The First Layer of Firewall

The first firewall layer works based on the analysis of the IP packet and its header fields. In the IP packet, the following fields are available for monitoring and evaluation [26]:

1- Source address: Some machines inside or outside the network with a specific IP address cannot send packets and their packets are removed upon entering the firewall.

2- Destination address: Some machines inside or outside the network with a specific IP address cannot receive packets and their packets are removed upon entering the firewall. (Unauthorized IP addresses are defined by the firewall manager).
3- Fragmented datagram ID (Identifier&Fragment Offset): packets that have been fragmented or belong to a particular datagram should be removed.
4- Protocol number: packets which belong to a particular higher protocol layer should be removed. I.e. checking which protocol the packet is belonged to and whether it is legal to deliver packet to this protocol or not.
5- Packet lifetime: The packets which have passed more than a certain number of routers are suspicious and they should be removed.
6- Other fields could be reviewed based on security rules of firewall manager.

The main feature of the first firewall layer is that, in this layer, packets are examined separately and independently and there is no need to keep previous or future packets. For this reason, the simplest and fastest decision-making is done at this layer. Nowadays, some routers are released with the first firewall layer, which means besides routing, they act as the first firewall layer and are called “Packet Filtering Routers”. So, prior to routing, the router filters IP packets based on a table. Setting this table is done according to the network manager and some security rules.

Due to the high speed of this layer, since the percentage of security rules in this layer is more precise and more stringent, processing volume at higher layers is lower and the penetration possibility is lower too. But, in practice, for a billion diverse IP addresses, it would be possible to penetrate through this layer with spoofed addresses and this weakness should be compensated in the higher layers.

Using the techniques of this layer, the eavesdropping in Smart Grid wireless communications could be totally blocked [27].

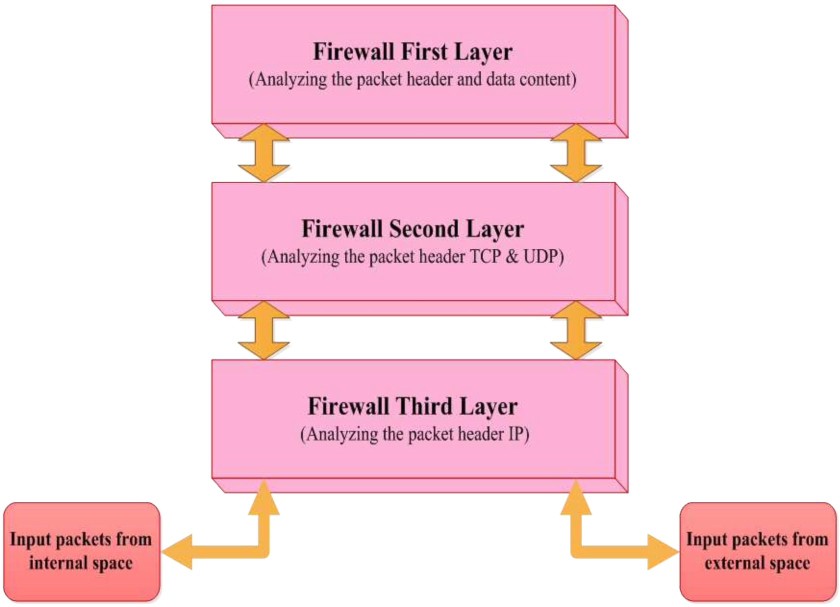
Firewall First Layer
(Analyzing the packet header and data content)
Firewall Second Layer
(Analyzing the packet header TCP & UDP)
Firewall Third Layer
(Analyzing the packet header IP)
Input packets from internal space
Input packets from external space

Figure 3. The structure of firewall layers

4.2. The Second Layer of Firewall

In this layer, header fields of the transport layer are used to analyze the packet. The most popular fields of transport layer packets to be inspected in the firewall are:
1- Port number of origin and destination process: Since the standard ports are known, the firewall manager may want the FTP service to be accessible only in the LAN environment and external machines would not have such accessibility. Thus, the firewall can remove FTP-related TCP packets that want to enter/exit to/from the network.

2- Number field and acknowledgment field: These two fields also could be used based on the rules defined by the Smart Grid manager.

3- Control codes (TCP code Bits): By checking these codes, Firewall perceives the nature of the packet and applies necessary policies for it. The one of the most important features of this layer is that all TCP connection requests must pass through this layer and since, in the TCP connection, data transfer is not possible until the completion of its three steps, the firewall can prevent any unauthorized connection prior to any data exchange. In other words, the firewall can check TCP connection requests before submission to the destination machine and block communication if it is not reliable. The firewall of this layer needs a table of unauthorized port numbers.

4.3. The Third Layer of Firewall

In this layer, protection is done based on the type of service and application. In other words, it analyzes the data considering the protocol in the fourth layer. The numbers of headers in this layer are very diverse depending on the type of service. So, in the third firewall layer, a series of unique processing and security rules should be defined for each service (such as Web, email, etc.) and this cause increase size and complexity of process in the third layer. In order to decrease the burden of the third layer, it is strongly advised to block all unnecessary services and unused port numbers in the second layer.

For example, suppose a financial institution sets up its email service, but there are concerns about the disclosure of confidential information. In this case, the third firewall layer can contribute by blocking certain email addresses, and also can search for some sensitive keywords in text of unencrypted letters, and can eliminate encrypted texts if it is not able to decrypt them [28].

5. Key Points of Firewall Security in Smart Grids

Firewall security is one of the dominant points in a secure network. A firewall that cannot provide its own security definitely will let hackers and attackers enter other parts of the network. Two-part firewall security provides a secure firewall and network:

5.1. Firewall's Operating System Security

In the security of the Smart Grid, a key issue that must be addressed is the balance between the benefits of enhanced communications in the smart grid and the privacy of homeowners [7].

If the firewall software is working on a separate operating system, security weak points of the operating system can be considered as firewall weak points as well. Therefore, the security and stability of the operating system and updating it, is one of the important points in firewall security.

5.2. Firewall's Secure Access for Network Administrators

In a firewall, specific security mechanisms should be considered for access of network administrators. These methods can use encryption with appropriate methods to identify the user, in order to properly face hackers.

6. Conclusions

Smart Grids without a firewall, are vulnerable against a wide set of malicious programs. Therefore, if the precautions and necessary protections have not been done in the Smart Grid, subversion or misuse of the information network would be likely to occur. By using Firewalls, we can create an appropriate security level to mitigate threats. But, all of the Smart Grid's security should not be limited to firewalls and other facilities or specific security policies should be used as well. So, it is concluded that firewalls are only one of the primary steps in Smart Grid's security. Using cryptographic algorithms, updating system antivirus and updating system software, such as operating systems, browsers, etc. are some of the necessary steps in creating cyber-security in the Smart Grids.

References

[1] Wang W, Xu Y, Khanna M. A survey on the communication architectures in smart grid. *Computer Networks*. 2011; 55(15): 3604–3629.

[2] Wang X, Yi P. Security framework for wireless communications in smart distribution grid. *IEEE Transactions on Smart Grid*. 2011; 2(4): 809–818.

[3] El-hawary ME. The Smart Grid—State-of-the-art and Future Trends. *Electric Power Components and Systems*. 2014; 42(3-4): 239–250. Available at: http://www.tandfonline.com/doi/abs/10.1080/15325008.2013.868558 [Accessed March 19, 2014].

[4] Hasanalizadeh-Khosroshahi A. Sensor Networks in Demand Side of Smart Grid. In *8th International Conference on Technical and Physical Problems of Power Engineering*. Norway, Fredrikstad, Ostfold University College. 2012: 5–7.

[5] Memari A et.al. Performance Assessment in a Production-Distribution Network Using Simulation. *Caspian Journal of Applied Sciences Research*. 2013; 2(5): 48–56.

[6] Din NM et.al. Early Warning System for Transmission Tower Landslide Hazard Monitoring in Malaysia. *Caspian Journal of Applied Sciences Research*, 2(AICCE'12 & GIZ' 12). 2013: 119–123.

[7] Naruchitparames J, Gunes MH, Evrenosoglu CY. Secure communications in the smart grid. In *2011 IEEE Consumer Communications and Networking Conference (CCNC)*, IEEE. 2011: 1171–1175.

[8] Gellings CW. *The smart grid: enabling energy efficiency and demand response*. The Fairmont Press, Inc. 2009.

[9] Ghorbani J et.al. Investigation of communication media requirements for self healing power distribution systems. In *Energytech, 2013 IEEE*. IEEE. 2013: 1–7.

[10] Li F, Luo B, Liu P. Secure information aggregation for smart grids using homomorphic encryption. In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*. IEEE. 2010: 327–332.

[11] Baghar-Nasrabadi S, Shahinzadeh H. Evaluation of Existing Protocols to Improve Information Exchange Security in the Smart Grid. *Journal of Basic and Applied Scientific Research (JBASR)*. 2013; 3(1): 558–563.

[12] Shahinzadeh H, Hasanalizadeh-Khosroshahi A. "Implementation of Smart Metering Systems: Challenges and Solutions". *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2014; 12(7).

[13] Wang W, Lu Z. Cyber security in the Smart Grid: Survey and challenges. *Computer Networks*. 2013: 57.

[14] Shahinzadeh H et.al. Evaluation of SCADA Security in smart grids. *3rd International Conference on Computer Technology and Development (ICCTD 2011)*. 2011.

[15] Lee A, Brewer T. Smart grid cyber security strategy and requirements. *Draft Interagency Report NISTIR*. 2009: 7628.

[16] Al-Shaer ES, Hamed HH. Firewall policy advisor for anomaly discovery and rule editing. In *Integrated Network Management, 2003. IFIP/IEEE Eighth International Symposium on*. IEEE. 2003: 17–30.

[17] Ericsson GN. Cyber security and power system communication—essential parts of a smart grid infrastructure. *IEEE Transactions on Power Delivery*. 2010; 25(3): 1501–1507.

[18] Valenzano A, Durante L, Cheminod M. Review of security issues in industrial networks. *IEEE Transactions on Industrial Informatics*. 2013; 9(1): 277–293.

[19] Eppstein D, Muthukrishnan S. Internet packet filter management and rectangle geometry. In *Proceedings of the twelfth annual ACM-SIAM symposium on Discrete algorithms*. Society for Industrial and Applied Mathematics. 2001: 827–835.

[20] Jadhav SS, Jadhav SM, Agrawal RR. Fast and Scalable Method to Resolve Anomalies in Firewall Policies. *International Journal of Advanced and Innovative Research (IJAIR)*. 2013; 2(3): 753–756.

[21] Chapman DB, Zwicky ED, Russell D. *Building internet firewalls*, O'Reilly & Associates, Inc. 1995.

[22] Mayer A, Wool A, Ziskind E. Fang: A firewall analysis engine. In *Proceedings. 2000 IEEE Symposium on Security and Privacy, 2000. S&P 2000.* IEEE, 2000: 177–187.

[23] Cheswick WR, Bellovin SM, Rubin AD. *Firewalls and Internet security: repelling the wily hacker*, Addison-Wesley Longman Publishing Co., Inc. 2003.

[24] Gouda MG, Liu XY. Firewall design: Consistency, completeness, and compactness. In *Proceedings. 24th International Conference on Distributed Computing Systems, 2004*. IEEE. 2004: 320–327.

[25] Shahinzadeh G, Shahinzadeh H, Paknejad A. Infrastructure Evaluation for using Smart Metering System (AMI & AMR) in Power Distribution Networks. *International Journal of Computing and Digital Systems (IJCDS)*. 2013; 2(3): 181–186.

[26] Al-Shaer E, Hamed H. Design and implementation of firewall policy advisor tools. *DePaul University, CTI, Tech. Rep*. 2002.

[27] Goel S, Negi R. Guaranteeing secrecy using artificial noise. *IEEE Transactions on Wireless Communications*. 2008; 7(6): 2180–2189.

[28] Julkunen H, Chow CE. Enhance network security with dynamic packet filter. In *Proceedings. 7th International Conference on Computer Communications and Networks, 1998*. IEEE. 1998: 268–275.