Abstract

The chapter introduces firewalls and their design as the first line of defense mechanism. This chapter goal is twofold:

(1) to cover major aspects of the firewall design and operation for security professional education:

-provides the firewall definition, discusses the functions, possible architectures and operational models concentrating on presentation of their advantages and drawbacks.

-includes the step-by-step guide to firewall design and implementation process ranging from planning to deployment and maintenance

(2) to explain how artificial intelligence and machine learning techniques and technologies are employed for enhancing firewalls and the security they provide.

-moves the reader from basic rules design to sophisticated AI and ML employment algorithms that improve it.

-the emphasis is placed on using rules to set up, configure and modify the firewall's policy.

- both generic and specific rules are discussed as well as their formulation and editing with firewall tools. Substantial rules design principles and conflict avoidance and resolution are presented.

- the modern AI based developments are presented at the end.

Learning Outcomes

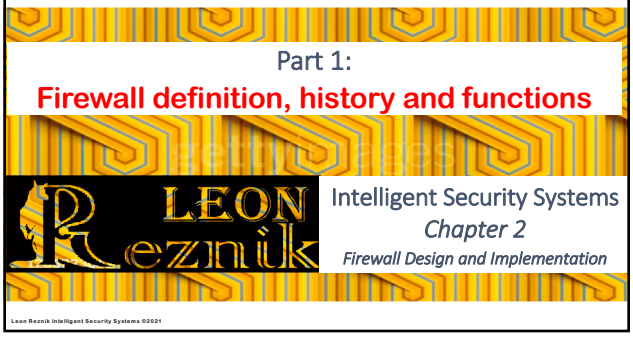
Upon completion of this lesson, students will be able to:

- to understand firewall functions, to classify them into various groups and to use a professional terminology in the field
- to understand and apply the main firewall design principles
- to analyze the firewall performance

Contents

Required and Recommended Reading

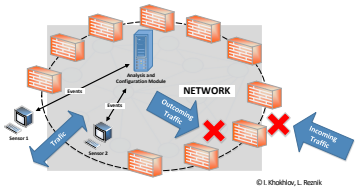
- *Required*:
- L.Reznik **Intelligent Security Systems:** How artificial intelligence, machine learning, and data science work for and against computer security. IEEE-Wiley, 2022, **Chapter 2**
- K. Scarfone, P. Hoffman. NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy, Sep. 2009 available at : *http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf* (accessed March 30, 2018)
- *Recommended:* Firewall section of any textbook on computer security



Contents

What is a firewall?

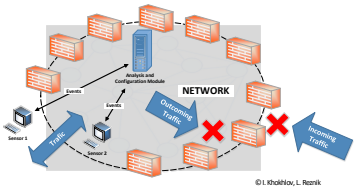
Firewall is a *device* or *program* that controls the flow of network traffic between networks or hosts that employ differing security postures (NIST Guide)



Source: K. Scarfone, P. Hoffman. NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy, Sep. 2009 available at : http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf

What is a firewall's main function?

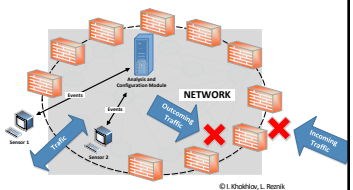
Firewall isolates organization's internal net from larger Internet, allowing some traffic to pass, blocking others.



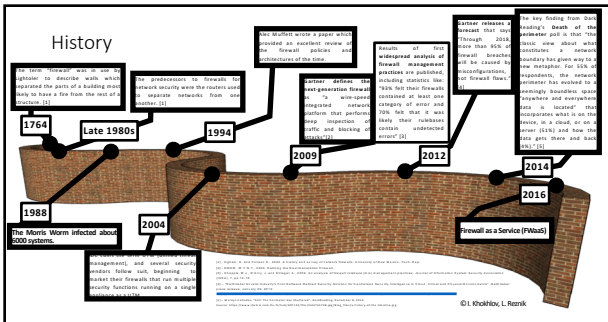
Source: K. Scarfone, P. Hoffman. NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy, Sep. 2009 available at : http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf

What else does a firewall do?

- Junction point between two networks. A private and a public network – support privacy protection
- Sets a border line for a network administration responsibility.



History



Firewall generations and types

Firewall generation	Year developed	Type	Operational level in network OSI model	Typical implementation	Functionality
1st	1980s	Packet filters	Network/ transport	Hardware or software	Filters packets based on source and destination addresses, ports and protocols
2nd	1990s	Stateful inspection	Network/ transport	Software	Filters packets based on traffic state, which it keeps on track and context of packets with
3rd	2000s	Application proxy	Application	Software	Separates services with a special proxy designated for each and redirecting traffic correspondingly
Next	2010s	Next generation	Application	Software	Performs a deeper analysis of the packet's both header and payload data if possible. Merges firewalls and intrusion detection functionality.

New requirements: Novel protection and intrusion detection for new living environment

Robots, drones, self-driving cars and other digital systems require novel protection and malware detection
Images taken at CES 2018 @ I.Khokhlov and L.Reznik

watch video

- What is a Firewall and How Does it Work?
  https://www.youtube.com/watch?v=5geL5yHpa2Q
  Time: 2:21
  What is a Firewall?
  https://youtu.be/x1YLj06c3hM
  Time: 1:53

Answer the questions:

What is the difference between the firewall definitions given in these videos?

PAUSE

Exercise

Find out and analyze various definitions of a firewall

Answer the questions:

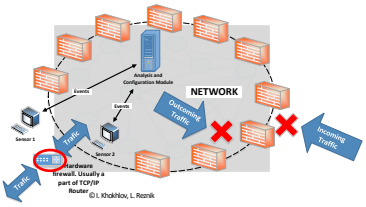
What is their common part?

What are variations?

What is your favorite? Why?

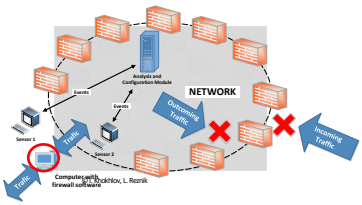
Hardware Firewalls

- High speed
- Hard to upgrade
- More expensive
- Many routers have basic ones embedded



Software Firewalls

- More flexible
- Easy to upgrade
- Cheaper
- Many OS have them embedded



Firewall functions

- **Block** bad traffic
- **Allow** only approved traffic to pass in and out
- **Make fast** decisions
- **Log** information
- **Direct** traffic

What is the major role of a firewall?

The major firewall function is NOT in completely eradicating potential attacks as this would be impossible to accomplish, but reducing a protected system's and network's vulnerability.

The more layers and the higher complexity a firewall has, the more refined an attack needs to get to slip through a firewall.

Despite being the first line of defense, a firewall cannot replace all other security tools and mechanisms but should work along with them.

Other security systems, like an intrusion detection, may check and analyze traffic too. What is the difference between them?

Unlike an intrusion detection system that can *only* analyze the traffic and signal the detection of certain traffic, a firewall is able to take an action and actually block the specified traffic.

Other possible firewall features

- Network address translation (NAT):

replaces an internal source IP address with its own address plus port number

- Virtual private network (VPN)
- Dynamic filters
- Policy
- Demilitarized zone (DMZ)

includes two firewalls around the protection area

- What is a Firewall?

https://youtu.be/kDEX1HXybrU

Time: 6:25

What is a Firewall?

Answer the questions:

What are major firewall types and functions

Part 2:

Firewall operational models

LEON Reznik

Intelligent Security Systems

Chapter 2

Firewall Design and Implementation

Firewall operational models

Packet filters

help in allowing or denying access for traffic packets to a network by looking at the packet content, for example, source and destination addresses, and ports. The headers of every packet are checked against the predefined ruleset, and as a result the allow/deny decision is made.

- Stateful inspection

firewalls keep track of the active/inactive status of every packet flowing through the network, whether incoming or outgoing. The firewall not only checks the headers of the packets but performs a more complicated analysis before making a decision to allow or deny, by taking into consideration the session and history information.

- Application-proxy gateways

used when we want to hide the internal network IP addresses from the unknown networks of the outside world. In this way, your network becomes invisible to hackers, thus preventing them from attacks that may cause harm to a protected network or system.

- Circuit level gateway

close to application proxy mode

TCP/IP Layers

Application Layer. This layer sends and receives data for particular applications, such as Domain Name System (DNS), Hypertext Transfer Protocol (HTTP), and Simple Mail Transfer Protocol (SMTP). The application layer itself has layers of protocols within it. For example, SMTP encapsulates the Request for Comments (RFC) 2822 message syntax, which encapsulates Multipurpose Internet Mail Extensions (MIME), which can encapsulate other formats such as Hypertext Markup Language (HTML).
Transport Layer. This layer provides connection-oriented or connectionless services for transporting application layer services between networks, and can optionally ensure communications reliability. Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are commonly used transport layer protocols.
IP Layer (also known as the Network Layer). This layer routes packets across networks. Internet Protocol version 4 (IPv4) is the fundamental network layer protocol for TCP/IP. Other commonly used protocols at the network layer are Internet Protocol version 6 (IPv6), ICMP, and Internet Group Management Protocol (IGMP).
Hardware Layer (also known as the Data Link Layer). This layer handles communications on the physical network components. The best known data link layer protocol is Ethernet.

Source: K. Scarfone, P. Hoffman. NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy, Sep. 2009 available at: http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf

Packet Filtering Firewall

Application Layer
Transport Layer
IP Layer
Hardware Layer

Traffic if filtered based on specified rules, including source and destination IP address, protocol type, port number etc.

- The most basic feature of a firewall
- Known as *stateless inspection firewalls*
- The most common example of a pure packet filtering device is a network router that employs access control lists
- Filtering **inbound traffic** is known as ***ingress filtering***
- **Outgoing traffic** can also be filtered, a process referred to as ***egress filtering***

Source: K. Scarfone, P. Hoffman. NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy, Sep. 2009 available at : http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf

Packet Filtering Example

- **Example 1**: **IF** *IP protocol field* = 17 **AND** (*source port* = 23 **OR** *destination port* = 23) **THEN** block incoming **AND** outgoing datagrams
  - All incoming and outgoing UDP flows and telnet connections are blocked.
- **Example 2**: **IF** *ACK field* = 1 **THEN** Block inbound TCP segments.
  - Prevents external clients from making TCP connections with internal clients, but allows internal clients to connect to outside.

Packet filtering firewall problems

- Stateless packet filters are generally vulnerable to attacks and exploits that take advantage of problems within the TCP/IP specification and protocol stack.
- Packet filters are unable to detect when a packet's network layer addressing information has been spoofed or otherwise altered
- Fragmented packets being blocked by firewalls is a common cause of VPN interoperability issues. Some firewalls can reassemble fragments before passing them to the inside network

Source: K. Scarfone, P. Hoffman. NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy, Sep. 2009 available at : http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf

Stateful Inspection

Stateful inspection improves on the functions of packet filters by tracking the state of connections and blocking packets that deviate from the expected state.

Stateful inspection in a firewall examines certain values in the TCP headers to monitor the state of each connection. Each new packet is compared by the firewall to the firewall's **state table** to determine if the packet's state contradicts its expected state.

Stateful inspection monitors a sequence of packets.

State Table Example

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	192.0.2.71	80	Initiated
192.168.1.102	1031	10.12.18.74	80	Established
192.168.1.101	1033	10.66.32.122	25	Established
192.168.1.106	1035	10.231.32.12	79	Established

Data Source: K. Scarfone, P. Hoffman. NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy, Sep. 2009 available at : http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf

watch video

5 Types of Firewalls
https://youtu.be/uGaERP4Npys
Time: 2:18
Firewall Stateful versus Stateless
https://youtu.be/gMvXruavqDI
Time: 5:28
Stateful Inspection and Packet Filtering
https://youtu.be/9wRgvyLZOKc
Time: 2:41

Answer the questions:

1. What are the major differences between stateless and stateful firewalls?
2. Offer your ideas how to further advance the stateful inspection concept in firewall design

Application Firewalls

Application Layer
Transport Layer
IP Layer
Hardware Layer

Traffic if filtered based on specified application rules, such as specified application (e.g. a browser) or a protocol

- **Application Firewalls** improve upon standard stateful inspection by adding data analytics ability - an inspection engine that analyzes protocols at the application layer
- Application firewall can allow or deny access based on how an application is running over the network
- Application firewalls can enable the identification of unexpected sequences of commands

Source: K. Scarfone, P. Hoffman. NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy, Sep. 2009 available at : http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf

Application-Proxy Gateways

An **application-proxy gateway** is a feature of advanced firewalls that combines lower-layer access control with upper-layer functionality.

- Contains a proxy agent that acts as an intermediary between two hosts that wish to communicate with each other, and never allows a direct connection between them
- The proxy is meant to be transparent to the two hosts
- The proxy agent interfaces directly with the firewall ruleset to determine whether a given instance of network traffic should be allowed to transit the firewall
- An application-proxy gateway offers a higher level of security than application firewalls

Source: K. Scarfone, P. Hoffman. NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy, Sep. 2009

Host-Based Firewalls and Personal Firewalls

- Provide an additional layer of security against network-based attacks
- Monitor and control the incoming and outgoing network traffic for a single host
- Host-based firewalls are available as part of server operating systems such as Linux, Windows, Solaris, BSD, and Mac OS, and they can also be installed as third-party add-ons
- Many host-based firewalls can also advance to intrusion prevention systems (IPS)
- A personal firewall is software that runs on a desktop or laptop PC with a user-focused operating system such as Microsoft Windows Vista or Mac OS

Source: K. Scarfone, P. Hoffman. NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy, Sep. 2009

Limitations of Firewall Inspection

- IP spoofing: router cannot know if data "really" comes from the claimed source
- Firewalls commonly pass UDP traffic through without inspection in order to preserve the maximum bandwidth
- Firewalls can only work effectively on traffic that they can inspect
- Firewalls cannot read application data that is encrypted
- An organization should have policies about how to handle traffic in cases, such as either permitting or blocking encrypted traffic that is not authorized to be encrypted

Source: K. Scarfone, P. Hoffman. NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy, Sep. 2009

Summary of Recommendations

- Organizations should only permit outbound traffic with the source IP addresses in use by the organization.
- Compliance checking is only useful in a firewall when it can block communication that can be harmful to protected systems.
- When choosing the type of firewall to deploy, it is important to decide whether the firewall needs to act as an application proxy.
- Management of personal firewalls should be centralized to help efficiently create, distribute, and enforce policies for all users and groups.

Source: K. Scarfone, P. Hoffman. NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy, Sep. 2009

Part 3:

Basic firewall architectures

Intelligent Security Systems

Chapter 2

Firewall Design and Implementation

Firewalls and Network Architectures

- Network Layouts with Firewalls
- Firewalls Acting as Network Address Translators
- Architecture with Multiple Layers of Firewalls
- See K. Scarfone, P. Hoffman, 2008. Guidelines on firewalls and firewall policy. *NIST Recommendations SP 800-41* for more info

Source: K. Scarfone, P. Hoffman. NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy, Sep. 2009

watch video

Firewall Architectures
https://youtu.be/xRs4VS-SKLo
Time: 6:43

Answer the questions:

1. Why do we need different firewall architectures?
2. What is the major deployment domain for each of them?

Basic Firewall Architectures

- Screening Router
- Dual Homed gateway
- Screened Host Gateway
- Screened Subnet Network Layouts with Firewalls

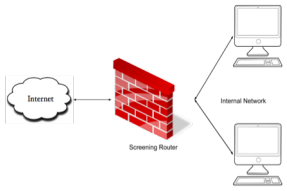
Source: K. Scarfone, P. Hoffman. NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy, Sep. 2009

Screening Router

The most basic and simplest firewall architecture.

Router itself acts as a firewall.

The external network packets are screened at the router making it a point of connection between internal network resources to all other network resources.



Advantages

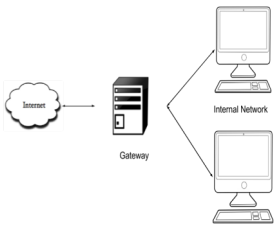
- 1. This architecture is visible to both internal and external networks.
- 2. It is easy to implement and a cheaper solution to security when compared to other architectures.

Disadvantages

- 1. There is a necessity of complex filtering rules on the router. Hence, the configuration process is not easy.
- 2. This architecture lacks the capability of logging thereby making it impossible to check whether or not the router is under attack
- 3. There is only one check point which means that failure at one point of the system will bring the whole system down.
- 4. The internal structure of the network cannot stay hidden and also there's no way of checking user authentication on the router.

Dual Homed Gateway

The hosting device, called the Bastion host is placed between two network interfaces – one internal and another external.
These internal and external networks can communicate with the dual home gateway but not with each other, so the network structure remains hidden.
The feature of packet forwarding is commonly disabled, so the packets cannot be transferred unless the host machine is configured accordingly.
Dual homed gateways are recommended when the amount of data flowing through the network is small and it does not contain any security critical information.



Advantages

- 1. The structure of the internal network remains hidden to the external networks.
- 2. Like screening routers, it is another cheap solution for network security.

Disadvantages

- 1. As the feature of packet forwarding does not exist, proxies are required for providing services but their availability cannot be guaranteed as they are not always available which makes this architecture less flexible.
- 2. The overall performance of the firewall depends solely on the performance of the host machine that serves as the dual homed gateway.
- 3. Dual homed gateways consist of a single point of failure that can bring down the entire system.
- 4. This architecture shows some usability and feasibility issues which makes it not simple to use.

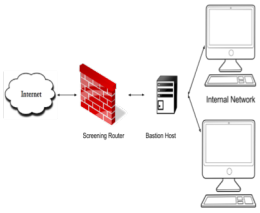
Screened Host Gateway

Routers are used in combination along with the hosts to work together as a firewall.

As opposed to a dual homed gateway, the Bastion host is only connected to the safeguarded side of the gateway which is the internal network with the help of a screened router.

At the router, packet filtering is performed.

This architecture permits the flow of certain trusted network packets from the external network to the internal network. If any packet of the external origin wants to have access to internal network or resources, it first has to establish connection with the Bastion host. The further communication is decided by the Bastion host depending on the level of security that is set within it. The packets can flow from the internal networks to the outside only if their origin is the application gateway



Advantages

- 1. As compared to a dual homed gateway, a screened host gateway is more flexible since it allows some of the trusted services from the traffic to flow from the external to internal network direction.
- 2. The main components required for this architecture are a router and one host machine that makes it relatively easy to implement another not expensive security mechanism.

Disadvantages

- 1. This architecture, like the dual homed gateway provides a single point of failure.
- 2. Although it is more flexible, it might prove to be less secure in some cases as it allows packets to flow from the external to the internal networks.
- 3. If an intruder is successful in attacking Bastion host somehow, there is no way of saving the internal hosts from being compromised.

Screened Subnet

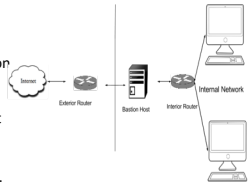
An extension of the Screened Host Gateway with a similar architecture.

Consists of a router at the entry point that is responsible for managing the traffic flow between the host and external networks by packet filtering based on certain predefined rules.

Unlike the Screened Host Gateways, there is another router that monitors the traffic flow between the host and internal networks.

In order to successfully intrude the network via this architecture, the attacker has to face two checkpoints. This solves the problem of the single point of failure.

Multiple number of Bastion hosts and its application gateways can be used in this architecture by replication of the single Bastion host and its application gateways.



Advantages

- 1. Since there are two routers used, the problem of a single point of failure is solved. Even if the attacker bypasses the Bastion host, it will have to go through another security check at the second internal router.
- 2. Use of multiple hosts allows to use different configurations of servers for different machines.
- 3. Internal network structure remains hidden from the external network.

Disadvantages

- 1. Due the presence of two critical security checkpoints- the router and the host, additional complex rules and configurations have to be applied.
- 2. In few cases, some of the services which are untrusted are allowed to bypass through the router if there are loopholes in the rules.

Firewalls Acting as Network Address Translators (NAT)

- Most firewalls can perform NAT, which is sometimes called port address translation (PAT) or network address and port translation (NAPT)
- Prevents a host outside the firewall from initiating contact with a host behind NAT
- A NAT acts as a router that has a network with private addresses on the inside and a single public address on the outside

Source: K. Scarfone, P. Hoffman. NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy, Sep. 2009

Architecture with Multiple Layers of Firewalls

- The goal of multiple layers of firewalls is to provide defense-in-depth
- Can help to solve issues with presence of internal users with varying levels of trust
- A firewall between the access points and the rest of the internal network can prevent visitors from accessing the local network with the same privileges as an employee
- Placing a firewall within a network that already has one at the edge requires good planning and policy coordination to prevent inadvertent security lapses
- Increases difficulty in detecting firewall problems

Source: K. Scarfone, P. Hoffman. NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy, Sep. 2009

Part 4: Process of firewall design, implementation, and maintenance

Intelligent Security Systems

Chapter 2

Firewall Design and Implementation

Firewall Design and Implementation

1. **Plan**. Identify all requirements that an organization should consider
2. **Configure**. includes installing hardware and software as well as setting up rules.
3. **Test.** Testing a prototype of the designed solution in a lab or test environment. The goal is to evaluate the functionality, performance, scalability, and security of the solution, and to identify any issues.
4. **Deploy**. The deployment of the firewall into the enterprise environment.
5. **Manage**. The firewall is managed throughout its lifecycle to include component maintenance and support for operational issues.

Source: K. Scarfone, P. Hoffman. NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy, Sep. 2009

Planning phase

- **Current and Future Needs**. Will the firewall meet the future needs of the organization
- **Use devices as they were intended to be used.** Firewalls should not be constructed of equipment not meant for firewall use.
- **Create defense-in-depth.** Defense-in-depth involves creating multiple layers of security.
- **Pay attention to internal threats.** Focusing attention solely on external threats leaves the network wide open to attacks from within.
- **Document the firewall's capabilities.** Each model of firewall has different capabilities and limitations.
- **Security Capabilities**. Which areas of the organization need to be protected?
- **Management**. Which protocols does the firewall support for remote management?
- **Performance**. What amount of throughput, maximum simultaneous connections, connections per second etc.?
- **Integration**. Will the firewall require specific hardware to properly integrate within the organization's network infrastructure?
- **Personnel**. Who will be responsible for managing the firewall?
- ?

Source: K. Scarfone, P. Hoffman. NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy, Sep. 2009

Configuration phase

- **Hardware and Software Installation**. During the installation and configuration, only the administrator doing that work should be able to manage the firewall
- **Policy Configuration**. The end result is a set of rules called a *ruleset* that describes how the firewall acts.
- **Logging and Alerts Configuration**. Logging is a critical step in preventing and recovering from failures as well as ensuring that proper security configurations are set on the firewall.

Source: K. Scarfone, P. Hoffman. NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy, Sep. 2009

Firewall Policy: NIST Recommendations

- Firewalls should block all inbound and outbound traffic that has not been expressly permitted by the firewall policy
- Traffic with invalid source or destination addresses should always be blocked
- Traffic with an invalid source address for incoming traffic or destination address for outgoing traffic (an invalid "external" address) should be blocked at the network perimeter
- Traffic from outside the network containing broadcast addresses that is directed to inside the network should be blocked

Source: K. Scarfone, P. Hoffman. NIST, SP.800-41 , Revision 1, Guidelines on Firewalls and Firewall Policy, Sep. 2009

Firewall Policy: NIST Recommendations, part 2

- An organization's firewall policy should be based on a comprehensive risk analysis
- Firewall policies should be based on blocking all inbound and outbound traffic, with exceptions made for desired traffic
- Policies should take into account the source and destination of the traffic in addition to the content
- Many types of IPv4 traffic, such as that with invalid or private addresses, should be blocked by default
- Organizations should have policies for handling incoming and outgoing IPv6 traffic
- An organization should determine which applications may send traffic into or out of its network and make firewall policies to block traffic for other applications

Source: K. Scarfone, P. Hoffman. NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy, Sep. 2009

IPv6

- The firewall should be able to use IPv6 addresses in all filtering rules that use IPv4 addresses
- The administrative interface should allow administrators to clone IPv4 rules to IPv6 addresses to make administration easier
- The firewall needs to be able to filter ICMPv6, as specified in RFC 4890, Recommendations for Filtering ICMPv6 Messages in Firewalls
- The firewall should be able to block IPv6-related protocols such as 6-to-4 and 4-to-6 tunneling, Teredo, and Intra-site Automatic Tunnel Addressing Protocol (ISATAP) if they are not required

Source: K. Scarfone, P. Hoffman. NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy, Sep. 2009

Testing phase

Should be tested:

- **Connectivity.** Users can establish and maintain connections through the firewall.
- **Ruleset**. Traffic that is specifically allowed by the security policy is permitted. All traffic that is not allowed by the security policy is blocked.
- **Application Compatibility**. Host-based or personal firewall solutions do not break or interfere with the use of existing software applications.
- **Management**. Administrators can configure and manage the solution effectively and securely.
- **Logging**. Logging and data management function in accordance with the organization's policies and strategies.
- **Performance**. Solutions provide adequate performance during normal and peak usage.
- **Security of the Implementation**. Test implementation for possible vulnerabilities exploitation.
- **Component Interoperability**. Components of the firewall solution must function together properly.

Source: K. Scarfone, P. Hoffman. NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy, Sep. 2009

Common Reasons for Firewall Failures

- Insider's attacks
- Installation errors
- Insufficient architecture
- Policy too permissive
- Users circumvent
- Users relax other security
- Attract attacks (less common)

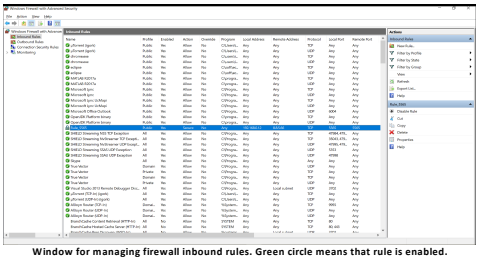
Part 5:
Firewall policy formalization with rules

Intelligent Security Systems

Chapter 2

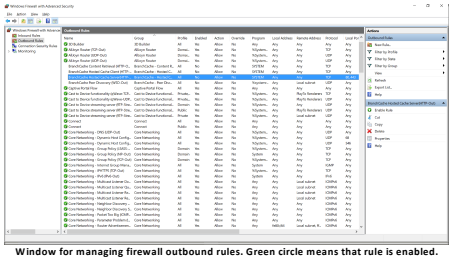
Firewall Design and Implementation

Windows Firewall (inbound rules)



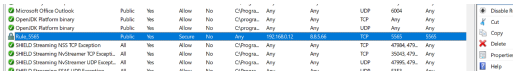
Window for managing firewall inbound rules. Green circle means that rule is enabled.

Windows Firewall (outbound rules)



Window for managing firewall outbound rules. Green circle means that rule is enabled.

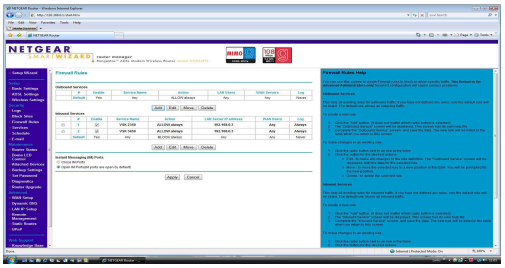
Firewall Rules Samples (Windows Firewall)



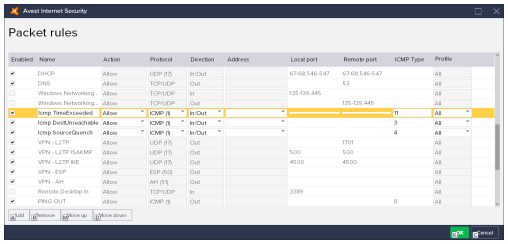
IF *device connected* to a public network **AND** communication channel is not secured **THEN** *block traffic from internal address 192.168.0.12, port 5565, to external address 8.8.5.56, port 5565.*

ELSE, *this rule has to be ignored*.

Netgear Router Firewall policy rules



Avast – Rule management



Managing firewall rules. Rules can be modified in the same window (using dropdown lists and edit boxes)

Rule samples

Purpose: to block any access to the firewall router
The firewall device should never be allowed to get accessed directly from a public network. This is a very obvious rule as allowing outsiders to directly access firewall can lead to dangerous consequences if they have bad intentions.

Source Address	Source Port	Destination Address	Destination Port	Action
Any	Any	10.20.30.1	Any	Deny
Any	Any	10.20.30.2	Any	Deny
10.20.30.1	Any	Any	Any	Deny
10.20.30.2	Any	Any	Any	Deny

Rule samples

Purpose: Prevent external users from utilizing Telnet traffic
Protected systems should not be allowed telnet access from public networks. Although this protocol is not used much in Windows systems, it is still employed by system admins on Unix or Linux systems. Typically, the request for telnet service from the external network can indicate an attack. To allow telnet services for internal network, the Allow rule should be added first.

Source Address	Source Port	Destination Address	Destination Port	Action
10.20.30.0	Any	10.20.30.0	23	Allow
Any	Any	10.20.30.0	23	Deny

Rule samples

Purpose: to prevent reconnaissance attacks by pinging.
The simplest typical form of reconnaissance attacks is sending to the protected system a ping request to gather information, first of all, which ports are open. Ping employs the Internet Control Message Protocol (ICMP). All inbound ICMP data should be denied with all inbound traffic to port #7 denied.

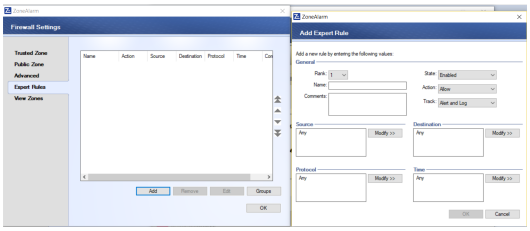
Source Address	Source Port	Destination Address	Destination Port	Action
10.20.30.0	Any	Any	7	Allow
Any	Any	10.20.30.0	7	Deny

Rule samples

Purpose: to improve security by adding Deny All rule.
This rule is also known as clean-up rule. Generally, while constructing rule set for firewalls, it is a good practice to have this rule. The rule states that if any packet is not explicitly allowed in a network then the packet has to be blocked.

Source Address	Source Port	Destination Address	Destination Port	Action
Any	Any	Any	Any	Deny

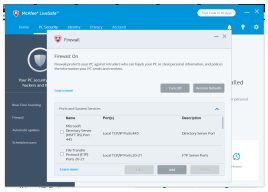
ZoneAlarm - Rule creation



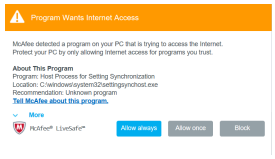
Window for managing and creating custom rules

Creating new rule

McAfee - Rule creation

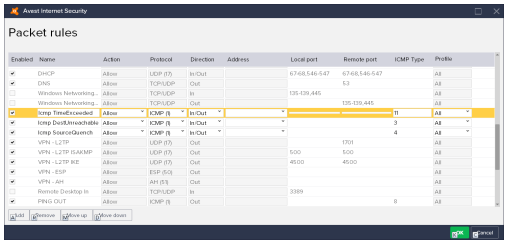


Window for managing and creating rules



Automatic rule creation. Application tries to access network for the first time. McAfee firewall suggests to create rule for this application

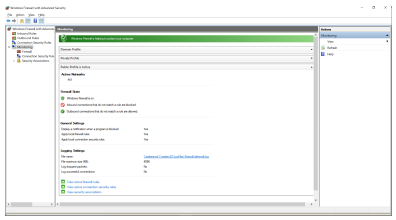
Avast – Rule management



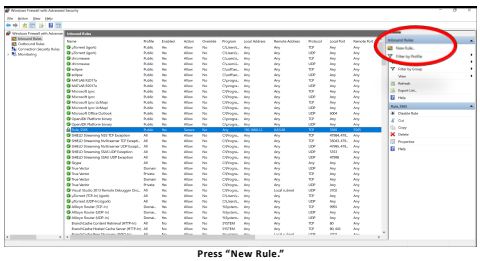
Managing firewall rules. Rules can be modified in the same window (using dropdown lists and edit boxes)

Windows Firewall (monitoring)

- **Monitoring** shows short statistics about firewall.
- **Firewall** submenu allows to manage **all** rules (inbound and outbound) in one place.
- **Connection Security Rules** allows to manage rules that can be applied only to secured traffic.
- **Security association** is the information about secure channel between to computers.

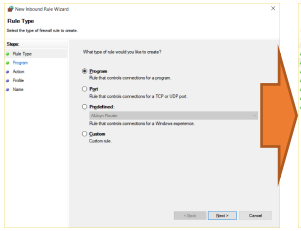


Windows Firewall – Rule creation

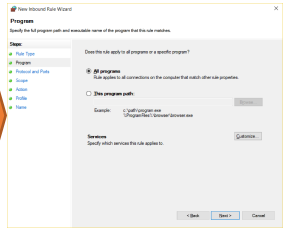


Press "New Rule."

Windows Firewall – Rule creation

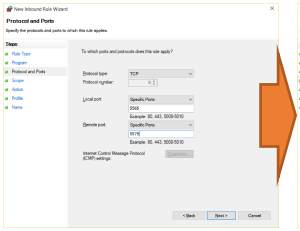


1. Type of rule.

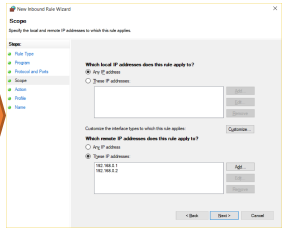


2. Name of application or process to which the rule has to be applied.

Windows Firewall – Rule creation

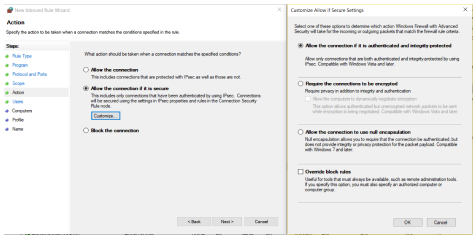


3. Type of protocol and port to which the rule has to be applied.



4. Here the source and destination IP addresses should be specified.

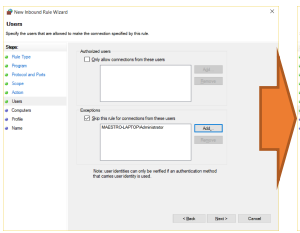
Windows Firewall – Rule creation



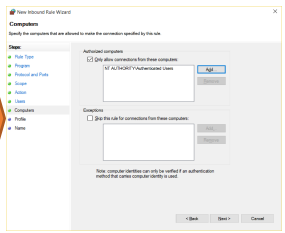
5. What action should be performed: block or allow

6. What type of connection should be affected

Windows Firewall – Rule creation

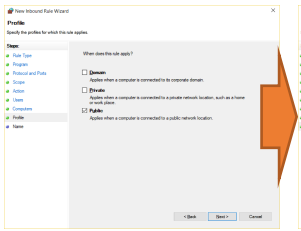


7. What users should be affected

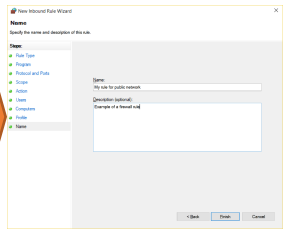


8. What computers should be affected

Windows Firewall – Rule creation



9. Specify to which network profile the rule should be applied



10. Final step. Rule name and description.

watch video

How to Create Firewall Rules in the Windows Firewall
https://youtu.be/hqnEyGmMDcQ
Time: 3:11
Best Practices for Firewall Rules
https://youtu.be/r5yiJYpNPJc
Time: 5:01

Answer the questions:
Is it easy to mange firewall rules?

Rules composition

- Consistency
- Completeness
- Compactness

- **Conflicts:**

Rules:

- **Allow** all traffic from 10.10.10.10
- **Block** all traffic from 10.10.10.10

What rule will be applied?

Rules:

- Allow incoming traffic from 10.10.10.10
- Block incoming traffic from 10.10.10.10 and port 5050
- What rule will be applied?

Rule conflicts

Rules:

- **Allow** all traffic from 10.10.10.10
- **Block** all traffic from 10.10.10.10

What rule will be applied?

Rules:

- Allow incoming traffic from 10.10.10.10
- Block incoming traffic from 10.10.10.10 and port 5050
- What rule will be applied?

Among similar rules that rule which has higher order or more specific than others is applied.

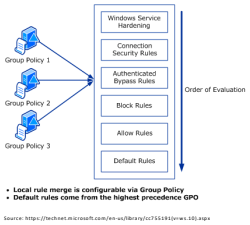
Indication of rule conflicts in firewall support

Outbound Firewall Rules (Drag and drop rows to change rule order)

Rule	Protocol	Source IP Port	Destination IP Port	Policy	
Rule 1	Any	Any	219.104.175.0/24	Deny	✕
Rule 2	Any	Any	219.104.175.222	Allow	✕
Default	Any	Any	Any	Allow	

Add Rule

Rules Order (Windows Firewall)



- **Local rule merge is configurable via Group Policy**
- **Default rules come from the highest precedence GPO**

Source: https://technet.microsoft.com/en-us/library/cc755191(v=ws.10).aspx

- **Windows Service Hardening**. This type of built-in rule restricts services from establishing connections in ways other than they were designed.
- **Connection security rules**. This type of rule defines how and when computers authenticate using IPsec.
- **Authenticated bypass rules**. This type of rule allows the connection of specified computers or users even when inbound firewall rules would block the traffic.
- **Block rules**. This type of rule explicitly blocks a particular type of incoming or outgoing traffic. Network traffic that matches both an active block and an active allow rule is blocked.
- **Allow rules**. This type of rule explicitly allows a particular type of incoming or outgoing traffic.
- **Default rules**. These rules define the action that takes place when a connection does not match any other rule. The inbound default is to block connections and the outbound default is to allow connections.

Rules composition

- Consistency
- Completeness
- Compactness

- **Completeness**

There is no rule matching a packet
What to do?
Add default rule at the end

Compactness

- Determines firewall efficiency

What to do?
Order: start with more generic rules

Part 6:

Firewall's evaluation and current development

Intelligent Security Systems

Chapter 2

Firewall Design and Implementation

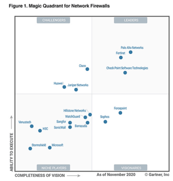
Firewall evaluation

Typically includes:

- **Firewall Verification**: a test to verify that the built firewall is able to drop or accept the given packets.
- **Firewall Implication**: a test that evaluates the firewall effectiveness by comparing its performance on the given set of packets against other firewalls
- **Firewall Equivalence**: a test of similarity between two firewalls to check, whether the firewall under consideration accepts and drops the same packets as the known firewall does.
- **Firewall Adequacy**: a test of functionality, whether the firewall drops or accepts at least one packet.
- **Firewall Redundancy**: a test that checks if modifying or dropping a given rule changes the firewall output
- **Firewall Completeness**: a test to confirm that the firewall makes a binary decision (block or accept) on each and every packet and no packet is left undecided.

Magic Quadrant for Network and Web Application Firewalls - @Gartner 2019-20

Figure 1. Magic Quadrant for Network Firewalls



Source: Gartner (November 2020)

Figure 1. Magic Quadrant for Web Application Firewalls

Source: Gartner (September 2019)

Comparing firewall solutions guidelines

Capability to look for	Description	Questions to ask your vendor
Application Visibility and Control	When you have visibility into the applications being used, you're able to make educated decisions about what to allow, what to prioritize, and what to block, so your bandwidth is used to best effect and you don't waste time blocking applications that aren't a problem. If you look into the reports from most firewalls, the majority of network traffic will show as 'unclassified' or 'general internet,' as there are many apps which are custom, obscure, evasive, or simply using generic HTTP or HTTPS and therefore, remain unidentified.	• Does your firewall integrate with the hosts on the network to identify all evasive and unknown applications generating encrypted or HTTP type traffic? • Can you provide a sample firewall report showing what traffic is actually identified? • Does your app control provide per-user and group-level visibility and policy enforcement? • Does it provide application control by category, risk level, technology, or characteristics (such as misuse, low productivity)?
Web and App Traffic Shaping	Enhanced traffic shaping (QoS) options by web category or application to limit or guarantee upload/ download or total traffic priority and bitrate individually or shared.	• Does your solution enable traffic shaping or QoS based on app, category, user, group, or rule?
URL Filtering	Controls web usage to prevent non-compliant surfing and keep inappropriate content and malware off the network.	• Does your firewall contain an inheritance-based web gateway policy engine? For example, if you need to do something just a little different for a user, do you need to create a whole new web policy, or can you define just what you want to do differently, and let it inherit the rest? Are there pre-configured policies for workplaces, CIPA compliance, etc.? • Beyond blocking, can it also warn about potentially inappropriate websites allowing the user to proceed? • Does your firewall include web keyword monitoring and can I upload my own lists, as relevant to my sector or region?
Web Compliance Features	Ensures compliance and identifies risky behavior when browsing, searching or using Google Apps.	• Can your web control solution enforce our Google Apps domain? • Does it enforce SafeSearch and YouTube restrictions on a user or group policy basis? • Can it enforce additional image filtering such as only those with a Creative Commons license? • Can it identify potentially problematic behavior related to bullying, self-harm, or radicalization based on dynamic content filtering and keyword monitoring? • Does it allow staff members such as teachers to set up temporary policy exceptions for users or groups?
User Risk Assessment	Provides an overview of riskiest users based on their network activity and recent history.	• Does your firewall provide insights into high-risk users based on their recent network behavior and activity? • Is there a widget on the dashboard for easy access to information? • Is there a full, detailed report?
Application Risk Assessment	Provides an overall risk metric for your organization's network.	• Does your firewall provide an overall application risk assessment? • Is there detailed historical reporting on application usage?
HTTPS Scanning	Provides visibility into encrypted web traffic to ensure compliance and identify hidden threats.	• Does your firewall offer HTTPS man-in-the-middle decryption? • Does it offer exceptions handling options? • Does it block unrecognized SSL/TLS protocols and invalid certs? • Does it support scanning of traffic that is encrypted using the the latest encryption protocols?

Source: Next-Gen Firewall Buyers guide, Sophos, 2020

Firewalls: to the future
Strategic Planning Assumptions

- By 2020, stand-alone web application firewall (WAF) hardware appliances will represent fewer than 20% of new WAF deployments, which is a decrease from today's 35%.
- By 2023, more than 30% of public-facing web applications will be protected by cloud web application and API protection (WAAP) services that combine distributed denial of service (DDoS) protection, bot mitigation, API protection and WAFs. This is an increase from fewer than 10% today.
- Source: Gartner report By Jeremy D'Hoinne, Adam Hils, Ayal Tirosh, Claudio Neiva

accessed on 09/26/18 at https://www.gartner.com/doc/reprints?id=1-5CQY77N&ct=180814&st=sb&mkt_tok=eyJpIjoiWkRSbU16RTFNVEF4TlRReiIsInQiOiJHVjlcL1B6cngxRnJmS25XWmhtb2p1RXh0cElUMnJrTGFxVUFIMFVKMkJ2TXFUSFJXdDJLS2g5bGJOQW1CdjZHZmNWUVlpYjdwK2NseitxK0RDN1VXZTBFaThkdTVQbVJuQ0FDeWszRGU4VGZoNDBXb2F3c3RlTXZmdndmNTVcLzh1In0%253D

Suggested directions for improvement with AI

- Improving the rules set composition by eliminating inconsistences in the set
- Finding inconsistences in the organization policies and investigating if the firewalls of different parts in the same network are following similar policies or not, especially in industrial networks.
- Generating rules directly based on the descriptive semantics derived from policies.
- Modifying and generalizing rules by their reformulation as fuzzy rules with the membership functions assigned to describe various packet data
- Optimizing the rules set composition and ordering

Making firewalls robust with fuzzy logic

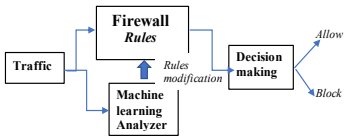
- Replace rules:

IF source address XXX AND destination address YYY THEN ALLOW

with

- Rule 1: IF TRUST in source address XXX is HIGH AND TRUST in destination address YYY is HIGH ALLOW with HIGH confidence
- Rule 2: IF TRUST in source address XXX is LOW AND TRUST in destination address YYY is LOW ALLOW with LOW confidence.
- Rule 3: IF TRUST in source address XXX is HIGH AND TRUST in destination address YYY is LOW ALLOW with MEDIUM confidence.
- Rule 4: IF TRUST in source address XXX is LOW AND TRUST in destination address YYY is HIGH ALLOW with LOW confidence.

Suggested directions for improvement



Dynamic firewall modification with a machine learning based analyzer

Conventional vs. Next Generation firewalls

Goals	Conventional (Gens 1-3) FW	Next Generation FW
Advanced intelligent attack prevention and integration with other tools	Targets only some part of network/system security in its implementation, e.g. with URL filtering, gateway, antimalware products Typically manages security tools separately	Includes all features of conventional firewall Integrated package is easy to install, configure, deploy and manage as a unit which reduces administrative cost Enables management automation as a separate until Includes integrated security technologies in one Package A NGFW is an all-in-one solution. The best offerings come complete with anti-virus, spam filtering and deep packet inspection, among others IT staff can manage one device, rather than needing to keep racking up, bolting on and updating new devices. Sandbox integration
Traffic inspection	Cannot inspect encrypted packets Attacker might be able to build tunnels to exchange command and control message	Employs Deep Packet inspection technology to inspect traffic in both inbound and outbound direction Capable to decrypt a payload Able to detect and block botnet command and control message

Source: K. Neupane, R. Haddad and L. Chen, "Next Generation Firewall for Network Security: A Survey," SoutheastCon 2018, St. Petersburg, FL, 2018, pp. 1-6, doi: 10.1109/SECON.2018.8478973

Conventional vs. Next Generation firewalls

Goals	Conventional (Gens 1-3) FW	Next Generation FW
Web applications control	No application recognition or control	Includes application intelligence and control facilities Capable to recognize a specific application Has tools to visualize and control traffic by application
User management	Does not separate or identify traffic by users	Allows to introduce an application control at an individual user or group level Allows to identify traffic by an individual user or group who pose security threats or involuntarily affect productivity through traffic visualization
Tradeoff control between security and performance	Traditional firewalls can degrade the speed performance of a network. As protection services are added on, the throughput of the firewall tends to plummet. Administrator is capable to turn off monitor on specific ports, disable firewall rule and limit packet inspection to boost performance	The throughput on a NGFW doesn't change regardless of how much protection is enabled. A NGFW should deliver visibility and control including content scanning, which is computationally intensive in high-throughput networks with little tolerance for latency. Enables parallel processing hardware architecture Includes efficient techniques

Source: K. Neupane, R. Haddad and L. Chen, "Next Generation Firewall for Network Security: A Survey," SoutheastCon 2018, St. Petersburg, FL, 2018, pp. 1-6, doi: 10.1109/SECON.2018.8478973

Firewall as a Service (FWaaS)

- Firewall as a Service (FWaaS) is a new and revolutionary way of delivering firewall and other network security capabilities as a cloud service.
- **FULL VISIBILITY**. With all WAN and Internet traffic going through the security company cloud there are no blind spots and no need to deploy multiple appliances.
- **SCALABILITY**. Security company can inspect any traffic mix (encrypted and unencrypted) and ensures capacity is available to provide the service the customer subscribed to.
- **UNIFIED SECURITY POLICY**. Security company enforces one granular policy and rule base that can extend from one user to the entire business.
- **SIMPLE LIFE CYCLE MANAGEMENT**. Without the need to size, upgrade, patch or refresh firewalls, customers are relieved of the on going grunt work of keeping their network security up to date against emerging threats and evolving business needs.

Source: http://www.catonetworks.com/solutions/firewall-as-a-service-fwaas/ accessed on 06-29-2021