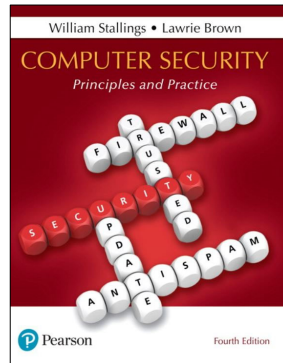




Computer Security: Principles and Practice



• Chapter 9

Firewalls and Intrusion Prevention Systems



2 Dr. Valerio Formicola

Copyright © 2018, 2015, 2012 Pearson Education, Inc. All Rights Reserved

If this PowerPoint presentation contains mathematical equations, you may need to check that your computer has the following installed:

- 1) MathType Plugin
- 2) Math Player (free versions available)
- 3) NVDA Reader (free versions available)

Firewalls can be an effective means of protecting a local system or network of systems from network-based security threats while at the same time affording access to the outside world via wide area networks and the Internet.

Information systems in corporations, government agencies, and other organizations have undergone a steady evolution. The following are notable developments:

- Centralized data processing system, with a central mainframe supporting a number of directly connected terminals

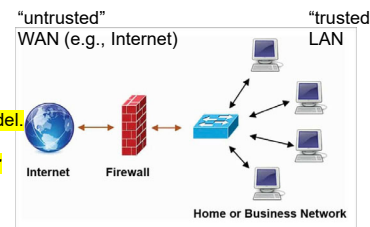
- Local area networks (LANs) interconnecting PCs and terminals to each other and the mainframe
- Premises network, consisting of a number of LANs, interconnecting PCs, servers, and perhaps a mainframe or two
- Enterprise-wide network, consisting of multiple, geographically distributed premises networks interconnected by a private wide area network (WAN)
- Internet connectivity, in which the various premises networks all hook into the Internet and may or may not also be connected by a private WAN
- Enterprise cloud computing, which we will describe further in Chapter 13, with virtualized servers located in one or more data centers that can provide both internal organizational and external Internet accessible services.

The Need For Firewalls

- Firewalls are a category of systems that protect computers from attacks that come from the network
- They are extremely critical if computers are connected to the Internet since machines are reachable from anywhere
- The initial model of a firewall was a device able to protect a LAN
- Inserted between the premises network and the Internet to establish a controlled link
 - Can be a single computer system or a set of two or more systems working together
- Used as a perimeter defense
 - Single choke point to impose security and auditing
 - Insulates the internal systems from external networks

OBSERVATION: The initial model of dividing the world in external is untrusted Vs. internal is trusted, is no longer a reliable assumption.

Shadow IT, Insiders and BYOD are examples that threaten the model. Firewalls are still an important solution, but not enough anymore, since the **attack surface is not physically delimited by the border of a LAN.**



3 Dr. Valerio Formicola

Internet connectivity is no longer optional for organizations. The information and services available are essential to the organization. Moreover, individual users within the organization want and need Internet access, and if this is not provided via their LAN, they could use a wireless broadband capability from their PC to an Internet service provider (ISP). However, while Internet access provides benefits to the organization, it enables the outside world to reach and interact with local network assets. This creates a threat to the organization. While it is possible to equip each workstation and server on the premises network with strong security features, such as intrusion protection, this may not be sufficient and in some cases is not cost effective. Consider a network with hundreds or even thousands of systems, running various operating systems, such as different versions of Windows, MacOS, and Linux. When a security flaw is discovered, each potentially affected system must be upgraded to fix that flaw. This requires scalable configuration management and aggressive patching to function effectively. While difficult, this is possible and is necessary if only host-based security is used. A widely accepted alternative or at least complement to host-based security services is the firewall. The firewall is inserted between the premises network and the Internet to establish a controlled link and to erect an outer security wall or perimeter. The aim of this perimeter is to protect the premises network from Internet-based attacks and to provide a single choke point where security and

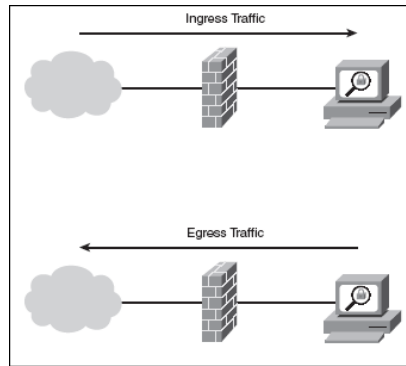
auditing can be imposed. The firewall may be a single computer system or a set of two or more systems that cooperate to perform the firewall function.

The firewall, then, provides an additional layer of defense, insulating the internal systems from external networks. This follows the classic military doctrine of “defense in depth,” which is just as applicable to IT security.

Firewall Characteristics

- **Design goals**

- All traffic from inside to outside (egress traffic), and vice versa (ingress traffic), must pass through the firewall
- Only authorized traffic as defined by the local security policy will be allowed to pass
- The firewall itself is immune to penetration



4 Dr. Valerio Formicola

[BELL94] lists the following design goals for a firewall:

1. All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall. Various configurations are possible, as explained later in this chapter.
2. Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various types of firewalls are used, which implement various types of security policies, as explained later in this chapter.
3. The firewall itself is immune to penetration. This implies the use of a hardened system with a secured operating system, as we will describe in Chapter 12.

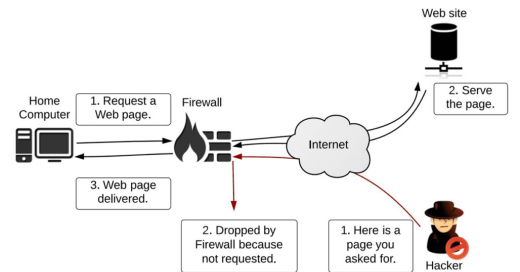
Why do we need a firewall?

- Ingress filtering – controlling traffic into a network
 - Can help to prevent some attacks:
 - DDoS traffic from spoofed IPs
 - Some weird combinations of packet fields
 - Direct access to services from outside
- Egress filtering – controlling of traffic leaving from a network
 - Can help to prevent some attacks, for example:
 - Spoofing from inside the network
 - Some exfiltration attacks
- Note: firewalls are a small but important tool to orchestrate defense from attacks.
In general, more techniques have to be combined to stop some of these attacks




Firewall Access Policy/List (ACL)

- Security admins need to establish the access policy for ingress/egress traffic
 - This lists the types of traffic authorized to pass through the firewall
 - Includes address ranges, protocols, applications and content types



A critical component in the planning and implementation of a firewall is specifying a suitable access policy. This lists the types of traffic authorized to pass through the firewall, including address ranges, protocols, applications and content types. This policy should be developed from the organization's information security risk assessment and policy, that we discuss in Chapters 14 and 15. This policy should be developed from a broad specification of which traffic types the organization needs to support. It is then refined to detail the filter elements we discuss next, which can then be implemented within an appropriate firewall topology.

General mechanisms to define access policies of traffic in a firewall

- **Network/Transmission-level filtering:** IP address and protocol values
 - This type of filtering is used by packet filter and stateful inspection firewalls
 - Typically used to limit access to specific services
 - **Application-level filtering: Application protocol**
 - This type of filtering is used by an application-level gateway that relays and monitors the exchange of information for specific application protocols
 - **User identity**
 - Typically for inside users who identify themselves using some form of secure authentication technology
 - Example, IPSec, a protocol which allows authentication of IP packets and it's used to create VPNs
- ESP is the header in IPSec protocol
- 
- The diagram illustrates the structure of an IPSec packet. It consists of an IP HDR (blue box), followed by an ESP HDR (blue box), then a Data field (light blue box). The Data field is divided into two sections: 'Encrypted' (indicated by a double-headed arrow) and 'Authenticated' (indicated by a double-headed arrow). The packet ends with an ESP Trailer (blue box) and an ESP Auth (blue box).
- **Network activity**
 - Controls access based on considerations such as the time or request, rate of requests, or other activity patterns



7 Dr. Valerio Formicola

NIST SP 800-41 (*Guidelines on Firewalls and Firewall Policy*, September 2009) lists a range of characteristics that a firewall access policy could use to filter traffic, including:

- **IP Address and Protocol Values:** Controls access based on the source or destination addresses and port numbers, direction of flow being inbound or outbound, and other network and transport layer characteristics. This type of filtering is used by packet filter and stateful inspection firewalls. It is typically used to limit access to specific services.
- **Application Protocol:** Controls access on the basis of authorized application protocol data. This type of filtering is used by an application-level gateway that relays and monitors the exchange of information for specific application protocols, for example, checking Simple Mail Transfer Protocol (SMTP) e-mail for spam, or HTTP Web requests to authorized sites only.
- **User Identity:** Controls access based on the users identity, typically for inside users who identify themselves using some form of secure authentication technology, such as IPSec (Chapter 22).

- **Network Activity:** Controls access based on considerations such as the time or request, for example, only in business hours; rate of requests, for example, to detect scanning attempts; or other activity patterns.

Firewall Capabilities and Limits

- **Capabilities:**
 - Defines a single choke point
 - Provides a location for monitoring security events (however, only events in the firewall location)
 - Convenient platform for several Internet functions that are not security related (NAT: network address translation or PAT: port address translation)
 - Can serve as the platform for IPSec (network layer VPN)
- **Limitations:**
 - Cannot protect against attacks bypassing firewall with physical signal sent out from a different path
 - May not protect fully against internal threats
 - Improperly secured wireless LAN can be accessed from outside the organization
 - Laptop, PDA, or portable storage device may be infected outside the corporate network then used internally
 - Cannot protect from attacks that are not visible in communications, e.g., against vulnerabilities in software

Wifi traffic or unsecured wifi can bypass the firewall

Internal traffic (i.e., generated and received within the network) is not protected by the firewall

8 Dr. Valerio Formicola

Before proceeding to the details of firewall types and configurations, it is best to summarize what one can expect from a firewall. The following capabilities are within the scope of a firewall:

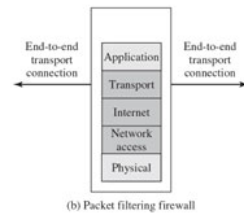
1. A firewall defines a single choke point that attempts to keep unauthorized users out of the protected network, prohibit potentially vulnerable services from entering or leaving the network, and provide protection from various kinds of IP spoofing and routing attacks. The use of a single choke point simplifies security management because security capabilities are consolidated on a single system or set of systems.
2. A firewall provides a location for monitoring security-related events. Audits and alarms can be implemented on the firewall system.
3. A firewall is a convenient platform for several Internet functions that are not security related. These include a network address translator, which maps local addresses to Internet addresses, and a network management function that audits or logs Internet usage.

4. A firewall can serve as the platform for IPSec. Using the tunnel mode capability described in Chapter 22 , the firewall can be used to implement virtual private networks.

Firewalls have their limitations, including the following:

1. The firewall cannot protect against attacks that bypass the firewall. Internal systems may have dial-out or mobile broadband capability to connect to an ISP. An internal LAN may support a modem pool that provides dial-in capability for traveling employees and telecommuters.
2. The firewall may not protect fully against internal threats, such as a disgruntled employee or an employee who unwittingly cooperates with an external attacker.
3. An improperly secured wireless LAN may be accessed from outside the organization. An internal firewall that separates portions of an enterprise network cannot guard against wireless communications between local systems on different sides of the internal firewall.
4. A laptop, PDA, or portable storage device may be used and infected outside the corporate network and then attached and used internally.

Packet filter firewall



- Applies rules to each incoming and outgoing IP packet
 - Typically, a list of rules based on matches in the IP or TCP header
 - Forwards or discards the packet based on rules match
- Filtering rules are based on information contained in a network packet
 - **Source IP address:** e.g., specific 10.1.0.122, or network 10.1.0.0/24
 - **Destination IP address:** e.g., specific 10.1.0.122, or network 10.1.0.0/24
 - **Source and destination transport-level port:** e.g., port 25, 53
 - **Transport protocol field:** e.g., TCP, UDP, ARP, ICMP
 - **Interface:** e.g., eth0, eth2, whatever is used in the firewall
- Two default policies:
 - **Discard - prohibit unless expressly permitted**
 - More conservative, controlled, visible to users
 - **Forward - permit unless expressly prohibited**
 - Easier to manage and use but less secure



9 Dr. Valerio Formicola

A **packet filtering firewall** applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet (Figure 9.1b). The firewall is typically configured to filter packets going in both directions (from and to the internal network). Filtering rules are based on information contained in a network packet:

- **Source IP address:** The IP address of the system that originated the IP packet (e.g., 192.178.1.1)
- **Destination IP address:** The IP address of the system the IP packet is trying to reach (e.g., 192.168.1.2)
- **Source and destination transport-level address:** The transport-level (e.g., TCP or UDP) port number, which defines applications such as SNMP or HTTP.
- **IP protocol field:** Defines the transport protocol
- **Interface:** For a firewall with three or more ports, which interface of the firewall the packet came from or for which interface of the firewall the packet is destined.

The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header. If there is a match to one of the rules, that rule is invoked to determine whether to forward or discard the packet. If there is no match to any rule, then a default action is taken. Two default policies are possible:

- **Default = discard:** That which is not expressly permitted is prohibited.
- **Default = forward:** That which is not expressly prohibited is permitted.

The default discard policy is more conservative. Initially, everything is blocked, and services must be added on a case-by-case basis. This policy is more visible to users, who are more likely to see the firewall as a hindrance. However, this is the policy likely to be preferred by businesses and government organizations. Further, visibility to users diminishes as rules are created. The default forward policy increases ease of use for end users but provides reduced security; the security administrator must, in essence, react to each new security threat as it becomes known. This policy may be used by generally more open organizations, such as universities.

Packet-Filtering: Example rules

Rule	Direction	Src address	Dest address	Protocol	Dest port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

Access to the internal email server from out (SMTP port 25)

Reply to the request from out

Access to the external email server from in (SMTP port 25)

Reply to the request from in

Deny anything else

Problem 1: Rule 4, what if the attacker sends a TCP message to an open port in the internal network (E.g., 8080, a web server for internal use)?

There is no way to stop it from going in.

Fix 1 (not great though): rather than just saying >1023, you can specify source ports in the rule, hence limiting which ports are used.

Problem 2: Rule 3 and 4 consider that the external server SMTP is listening on port 25. What if that port is used for malicious purposes in an external machine? E.g., the malicious host might declare to use source port 25, hence waiting for the replies on that port.

Rule	Direction	Src address	Src port	Dest address	Protocol	Dest port	Flag	Action
4	In	External	25	Internal	TCP	>1023	ACK	Permit



Cal Poly Pomona

10 Dr. Valerio Formicola

Table 9.1 is a simplified example of a rule set for SMTP traffic. The goal is to allow inbound and outbound email traffic but to block all other traffic. The rules are applied top to bottom to each packet. The intent of each rule is:

1. Inbound mail from an external source is allowed (port 25 is for SMTP incoming).
2. This rule is intended to allow a response to an inbound SMTP connection.
3. Outbound mail to an external source is allowed.
4. This rule is intended to allow a response to an inbound SMTP connection.
5. This is an explicit statement of the default policy. All rule sets include this rule implicitly as the last rule.

There are several problems with this rule set. Rule 4 allows external traffic to any destination port above 1023.

As an example of an exploit of this rule, an external attacker can open a connection from the attacker's port 5150 to an internal Web proxy server on port 8080. This is supposed to be forbidden and could allow an attack on the server. To counter this attack, the firewall rule set can be configured with a source port field for each row. For rules 2 and 4, the source port is set to 25; for rules 1 and 3, the source port is set to >1023.

But a vulnerability remains. Rules 3 and 4 are intended to specify that any inside host can send mail to the outside. A TCP packet with a destination port of 25 is routed to the SMTP server on the destination machine. The problem with this rule is that the use of port 25 for SMTP receipt is only a default; an outside machine could be configured to have some other application linked to port 25. As the revised rule 4 is written, an attacker could gain access to internal machines by sending packets with a TCP source port number of 25. To counter this threat, we can add an ACK flag field to each row. For rule 4, the field would indicate that the ACK flag must be set on the incoming packet. Rule 4 would now look like this:

Rule 4

Direction In

Src address External

Src port 25

Dest address Internal

Protocol TCP

Dest port >1023

Flag ACK

Action. Permit

The rule takes advantage of a feature of TCP connections. Once a connection is set up, the ACK flag of a TCP segment is set to acknowledge segments sent from the other side. Thus, this rule allows incoming packets with a source port number of 25 that include the ACK flag in the TCP segment.

Packet Filter Advantages And Weaknesses

- **Advantages**
 - **Simplicity:** simple mechanisms
 - Typically, transparent to users and are very fast
- **Weaknesses**
 - Cannot prevent attacks that employ application specific vulnerabilities or functions: the payload at application level might target a vulnerability in an internal server, but will never be caught by the firewall
 - Limited logging functionality: only information available is related to the rules matched by a packet
 - Do not support advanced user authentication: if a packet passes the filter, there is no way to check where it comes from
 - Vulnerable to attacks on TCP/IP protocol bugs: if the attack is not targeting an anomaly in the protocol, rather in the implementation (e.g., IP spoofing with external spoofed address), no way to catch it.
 - Improper configuration can lead to breaches: easily can lead to error during the configuration



One advantage of a packet filtering firewall is its simplicity. Also, packet filters typically are transparent to users and are very fast. NIST SP 800-41 lists the following weaknesses of packet filter firewalls:

- Because packet filter firewalls do not examine upper-layer data, they cannot prevent attacks that employ application-specific vulnerabilities or functions. For example, a packet filter firewall cannot block specific application commands; if a packet filter firewall allows a given application, all functions available within that application will be permitted.
- Because of the limited information available to the firewall, the logging functionality present in packet filter firewalls is limited. Packet filter logs normally contain the same information used to make access control decisions (source address, destination address, and traffic type).
- Most packet filter firewalls do not support advanced user authentication schemes. Once again, this limitation is mostly due to the lack of upper-layer functionality by the firewall.
- Packet filter firewalls are generally vulnerable to attacks and exploits that take advantage of problems within the TCP/IP

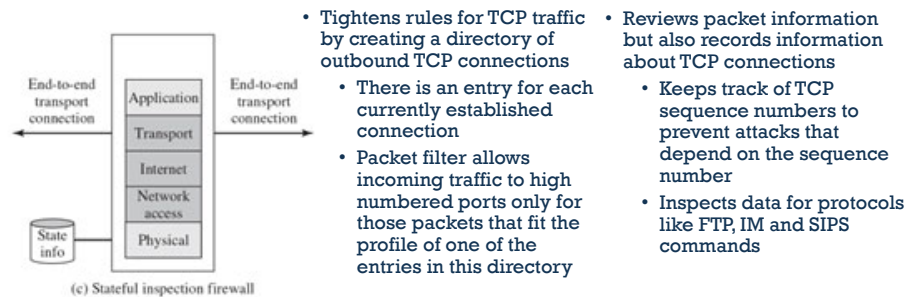
specification and protocol stack, such as *network layer address spoofing* . Many packet filter firewalls cannot detect a network packet in which the OSI Layer 3 addressing information has been altered. Spoofing attacks are generally employed by intruders to bypass the security controls implemented in a firewall platform.

- Finally, due to the small number of variables used in access control decisions, packet filter firewalls are susceptible to security breaches caused by improper configurations. In other words, it is easy to accidentally configure a packet filter firewall to allow traffic types, sources, and destinations that should be denied based on an organization's information security policy.

Some of the attacks that can be made on packet filtering firewalls and the appropriate countermeasures are the following:

- **IP address spoofing** : The intruder transmits packets from the outside with a source IP address field containing an address of an internal host. The attacker hopes that the use of a spoofed address will allow penetration of systems that employ simple source address security, in which packets from specific trusted internal hosts are accepted. The countermeasure is to discard packets with an inside source address if the packet arrives on an external interface. In fact, this countermeasure is often implemented at the router external to the firewall.
- **Source routing attacks**: The source station specifies the route that a packet should take as it crosses the Internet, in the hopes that this will bypass security measures that do not analyze the source routing information. A countermeasure is to discard all packets that use this option.
- **Tiny fragment attacks**: The intruder uses the IP fragmentation option to create extremely small fragments and force the TCP header information into a separate packet fragment. This attack is designed to circumvent filtering rules that depend on TCP header information. Typically, a packet filter will make a filtering decision on the first fragment of a packet. All subsequent fragments of that packet are filtered out solely on the basis that they are part of the packet whose first fragment was rejected. The attacker hopes that the filtering firewall examines only the first fragment and that the remaining fragments are passed through. A tiny fragment attack can be defeated by enforcing a rule that the first fragment of a packet must contain a predefined minimum amount of the transport header. If the first fragment is rejected, the filter can remember the packet and discard all subsequent fragments.

Stateful packet firewall



12 Dr. Valerio Formicola

A traditional packet filter makes filtering decisions on an individual packet basis and does not take into consideration any higher-layer context. To understand what is meant by *context* and why a traditional packet filter is limited with regard to context, a little background is needed. Most standardized applications that run on top of TCP follow a client/server model. For example, for the Simple Mail Transfer

Protocol (SMTP), e-mail is transmitted from a client system to a server system. The client system generates new e-mail messages, typically from user input. The server system accepts incoming e-mail messages and places them in the appropriate user mailboxes. SMTP operates by setting up a TCP connection between client and server, in which the TCP server port number, which identifies the SMTP server application, is 25. The TCP port number for the SMTP client is a number between 1024 and 65535 that is generated by the SMTP client.

In general, when an application that uses TCP creates a session with a remote host, it creates a TCP connection in which the TCP port number for the remote (server) application is a number less than 1024 and the TCP port number for the local (client) application is a number between 1024 and 65535. The numbers less than 1024 are the “well-known” port numbers and are assigned permanently to particular applications (e.g., 25 for server SMTP). The numbers between 1024

and 65535 are generated dynamically and have temporary significance only for the lifetime of a TCP connection.

A simple packet filtering firewall must permit inbound network traffic on all these high-numbered ports for TCP-based traffic to occur. This creates a vulnerability that can be exploited by unauthorized users.

Example Stateful Firewall Connection State Table

Records IP addresses and status of connection to allow packets to pass.
Any packets in the step can bypass the network

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established



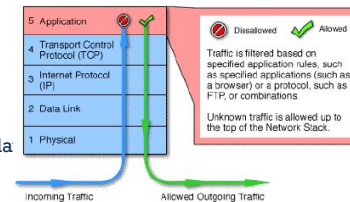
13 Dr. Valerio Formicola

A **stateful inspection packet firewall** tightens up the rules for TCP traffic by creating a directory of outbound TCP connections, as shown in Table 9.2 . There is an entry for each currently established connection. The packet filter will now allow incoming traffic to high-numbered ports only for those packets that fit the profile of one of the entries in this directory.

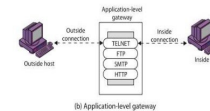
A stateful packet inspection firewall reviews the same packet information as a packet filtering firewall, but also records information about TCP connections (Figure 9.1c). Some stateful firewalls also keep track of TCP sequence numbers to prevent attacks that depend on the sequence number, such as session hijacking. Some even inspect limited amounts of application data for some well-known protocols like FTP, IM, and SIPs commands, in order to identify and track related connections.

Application-Level Gateway

- Also called an **application proxy**
- Acts as a relay of application-level traffic
 - User contacts gateway using a TCP/IP application
 - User is authenticated
 - Gateway contacts application on remote host and relays TCP segments between server and user
- Advantages:
 - Filter application specific commands, e.g., http post/get with specific parameters etc.
 - Inspect the entire packet
 - Tend to be more secure than packet filters
- Disadvantages:
 - additional processing overhead on each connection
 - Vendors must update for new protocols and updates of protocols



Application level gateway



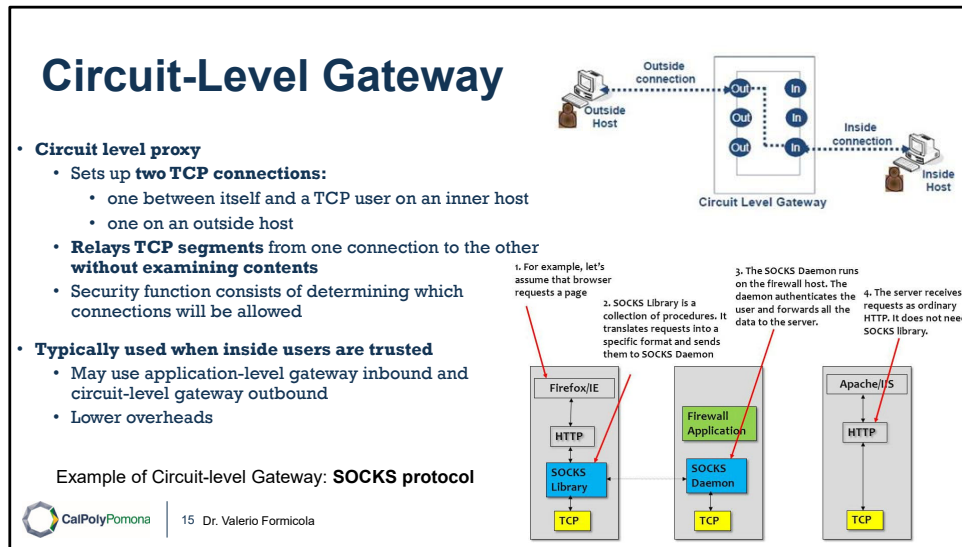
14 Dr. Valerio Formicola

An **application-level gateway**, also called an application proxy, acts as a relay of application-level traffic (Figure 9.1d). The user contacts the gateway using a TCP/ IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed. When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints. If the gateway does not implement the proxy code for a specific application, the service is not supported and cannot be forwarded across the firewall. Further, the gateway can be configured to support only specific features of an application that the network administrator considers acceptable while denying all other features.

Application-level gateways tend to be more secure than packet filters. Rather than trying to deal with the numerous possible combinations that are to be allowed and forbidden at the TCP and IP level, the application-level gateway need only scrutinize a few allowable applications. In addition, it is easy to log and audit all incoming traffic at the application level.

A prime disadvantage of this type of gateway is the additional processing overhead on each connection. In effect, there

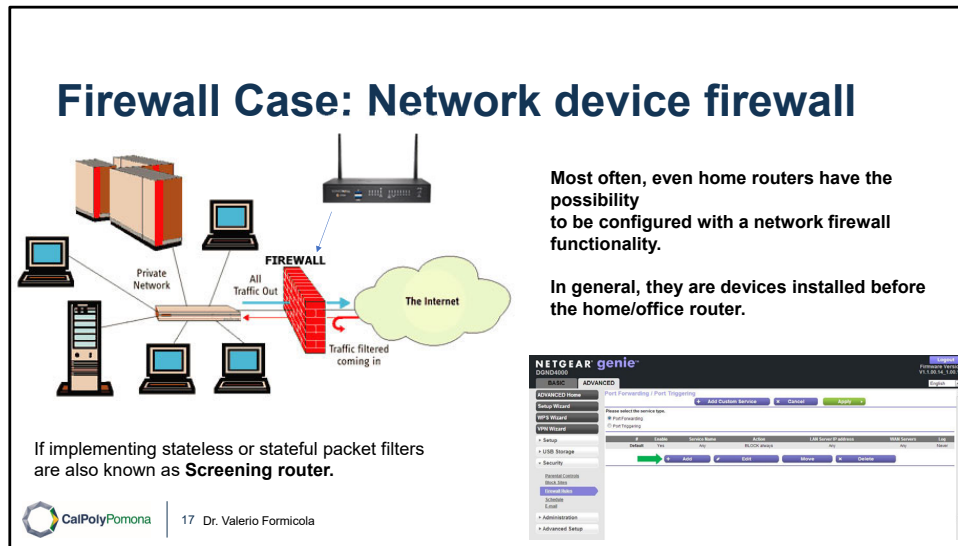
are two spliced connections between the end users, with the gateway at the splice point, and the gateway must examine and forward all traffic in both directions.



A fourth type of firewall is the **circuit-level gateway** or circuit-level proxy (Figure 9.1e). This can be a stand-alone system or it can be a specialized function performed by an application-level gateway for certain applications. As with an application gateway, a circuit-level gateway does not permit an end-to-end TCP connection; rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host. Once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents. The security function consists of determining which connections will be allowed.

A typical use of circuit-level gateways is a situation in which the system administrator trusts the internal users. The gateway can be configured to support application-level or proxy service on inbound connections and circuit-level functions for outbound connections. In this configuration, the gateway can incur the processing overhead of examining incoming application data for forbidden functions but does not incur that overhead on outgoing data.





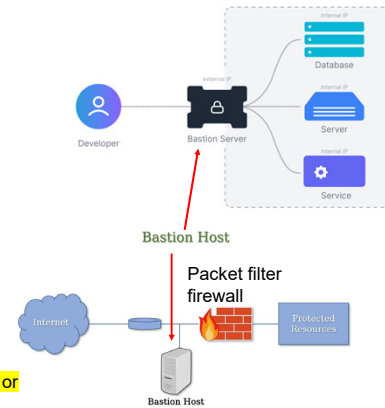
A firewall can monitor network traffic at a number of levels, from low-level network packets, either individually or as part of a flow, to all traffic within a transport connection, up to inspecting details of application protocols. The choice of which level is appropriate is determined by the desired firewall access policy. It can operate as a positive filter, allowing to pass only packets that meet specific criteria, or as a negative filter, rejecting any packet that meets certain criteria. The criteria implement the access policy for the firewall that we discussed in the previous section. Depending on the type of firewall, it may examine one or more protocol headers in each packet, the payload of each packet, or the pattern generated by a sequence of packets. In this section, we look at the principal types of firewalls. The illustrations are as follows. Illustration a labeled, general model, depicts a firewall which is placed between Internal, protected, network, example enterprise network and external, untrusted, network, example internet. Illustration b labeled, packet filtering firewall depicts a firewall with five layers from bottom to top as follows. Physical, Network access, internet, transport, application. The firewall has end to end transport connection on both sides. Illustration c labeled, stateful inspection firewall depicts a firewall with five layers from bottom to top as follows. Physical, Network access, internet, transport, application. A state info is connected to the firewall. The firewall has end to end transport connection on both sides. Illustration d labeled, application proxy firewall depicts a firewall with two sets of five layers. The layers from bottom to top are as follows. Physical, Network access, internet, transport, application. The two application layers are connected to

the each other, and the connection is labeled, application proxy. The transport layer in the first set is connected to the internal transport connection, while the transport layer in the second set is connected to the external transport connection. Illustration e labeled, circuit level proxy firewall depicts a firewall with two sets of five layers. The layers from bottom to top are as follows. Physical, Network access, internet, transport, application. The two transport layers are connected to the each other, and the connection is labeled, circuit level proxy. The transport layer in the first set is connected to the internal transport connection, while the transport layer in the second set is connected to the external transport connection.

Firewall case: Bastion Host + Packet filter

- System identified as a critical strong point in the network's security:
It is the most exposed host to the Internet, hence most attacked
- Serves as a platform for an **application-level or circuit-level gateway**:
 - Usually only a very limited set of applications are protected by the Bastion host
- Common characteristics:
 - Runs secure O/S, only essential services
 - May require user authentication to access proxy or host
 - Each proxy can restrict features, hosts accessed
 - Each proxy is small, simple, checked for security
 - Each proxy is independent, non-privileged
 - Limited disk use, hence read-only code

Usually, the bastion host is located in between two firewalls or outside the internal firewall



18 Dr. Valerio Formicola



A bastion host is a system identified by the firewall administrator as a critical strong point in the network's security. Typically, the bastion host serves as a platform for an application-level or circuit-level gateway. Common characteristics of a bastion host are as follows:

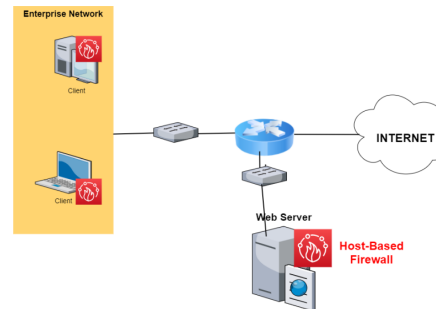
- The bastion host hardware platform executes a secure version of its operating system, making it a hardened system.
- Only the services that the network administrator considers essential are installed on the bastion host. These could include proxy applications for DNS, FTP, HTTP, and SMTP.
- The bastion host may require additional authentication before a user is allowed access to the proxy services. In addition, each proxy service may require its own authentication before granting user access.
- Each proxy is configured to support only a subset of the standard application's command set.
- Each proxy is configured to allow access only to specific host systems. This means that the limited command/feature

set may be applied only to a subset of systems on the protected network.

- Each proxy maintains detailed audit information by logging all traffic, each connection, and the duration of each connection. The audit log is an essential tool for discovering and terminating intruder attacks.
- Each proxy module is a very small software package specifically designed for network security. Because of its relative simplicity, it is easier to check such modules for security flaws. For example, a typical UNIX mail application may contain over 20,000 lines of code, while a mail proxy may contain fewer than 1000.
- Each proxy is independent of other proxies on the bastion host. If there is a problem with the operation of any proxy, or if a future vulnerability is discovered, it can be uninstalled without affecting the operation of the other proxy applications. Also, if the user population requires support for a new service, the network administrator can easily install the required proxy on the bastion host.
- A proxy generally performs no disk access other than to read its initial configuration file. Hence, the portions of the file system containing executable code can be made read only. This makes it difficult for an intruder to install Trojan horse sniffers or other dangerous files on the bastion host.
- Each proxy runs as a non-privileged user in a private and secured directory on the bastion host.

Firewall case: Host-Based Firewalls

- Used to secure an individual host
- Available in operating systems or can be provided as an add-on package
- Filter and restrict packet flows
- **Common location is a server**
- Advantages:
 - Filtering rules can be tailored to the host environment
 - Protection is provided independent of topology
 - Provides an additional layer of protection



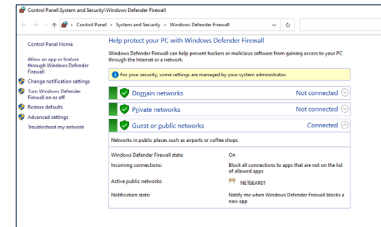
19 Dr. Valerio Formicola

A host-based firewall is a software module used to secure an individual host. Such modules are available in many operating systems or can be provided as an add-on package. Like conventional stand-alone firewalls, host-resident firewalls filter and restrict the flow of packets. A common location for such firewalls is a server. There are several advantages to the use of a server-based or workstation-based firewall:

- Filtering rules can be tailored to the host environment. Specific corporate security policies for servers can be implemented, with different filters for servers used for different application.
- Protection is provided independent of topology. Thus, both internal and external attacks must pass through the firewall.
- Used in conjunction with stand-alone firewalls, the host-based firewall provides an additional layer of protection. A new type of server can be added to the network, with its own firewall, without the necessity of altering the network firewall configuration.

Firewall case: Personal Firewall

- **Similar to Host-based firewall, but related to each Personal computers, not servers**
 - E.g., your MacOS, Windows laptop or smartphone might have one installed.
- Controls traffic between a personal computer or workstation and the Internet or enterprise network
- Can be housed in a router that connects all of the home computers to a DSL, cable modem, or other Internet interface
- Typically, much less complex than server-based or stand-alone firewalls
- Primary role is to deny unauthorized remote access
- May also monitor outgoing traffic to detect and block worms and malware activity



e.g., Windows Firewall



20 Dr. Valerio Formicola

A personal firewall controls the traffic between a personal computer or workstation on one side and the Internet or enterprise network on the other side. Personal firewall functionality can be used in the home environment and on corporate intranets. Typically, the personal firewall is a software module on the personal computer. In a home environment with multiple computers connected to the Internet, firewall functionality can also be housed in a router that connects all of the home computers to a DSL, cable modem, or other Internet interface.

Personal firewalls are typically much less complex than either server-based firewalls or stand-alone firewalls. The primary role of the personal firewall is to deny unauthorized remote access to the computer. The firewall can also monitor outgoing activity in an attempt to detect and block worms and other malware.

Personal firewall capabilities are provided by the *netfilter* package on Linux systems, or the *pf* package on BSD and Mac OS systems, or by the Windows Firewall. These packages may be configured on the command-line, or with a GUI front-end. When such a personal firewall is enabled, all inbound connections are usually denied except for those the user explicitly permits. Outbound connections are usually allowed. The list of

inbound services that can be selectively re-enabled, with their port numbers, may include the following common services:

- Personal file sharing (548, 427)
- Windows sharing (139)
- Personal Web sharing (80, 427)
- Remote login—SSH (22)
- FTP access (20-21, 1024-65535 from 20-21)
- Printer sharing (631, 515)
- IChat Rendezvous (5297, 5298)
- iTunes Music Sharing (3869)

CVS (2401)

- Gnutella/Limewire (6346)
- ICQ (4000)
- IRC (194)
- MSN Messenger (6891-6900)
- Network Time (123)
- Retrospect (497)

- SMB (without netbios–445)
- VNC (5900-5902)
- WebSTAR Admin (1080, 1443)

When FTP access is enabled, ports 20 and 21 on the local machine are opened for FTP; if others connect to this computer from ports 20 or 21, the ports 1024 through 65535 are open.

For increased protection, advanced firewall features may be configured. For example, stealth mode hides the system on the Internet by dropping unsolicited communication packets, making it appear as though the system is not present. UDP packets can be blocked, restricting network traffic to TCP packets only for open ports. The firewall also supports logging, an important tool for checking on unwanted activity. Other types of personal firewall allow the user to specify that only selected applications, or applications signed by a valid certificate authority, may provide services accessed from the network.



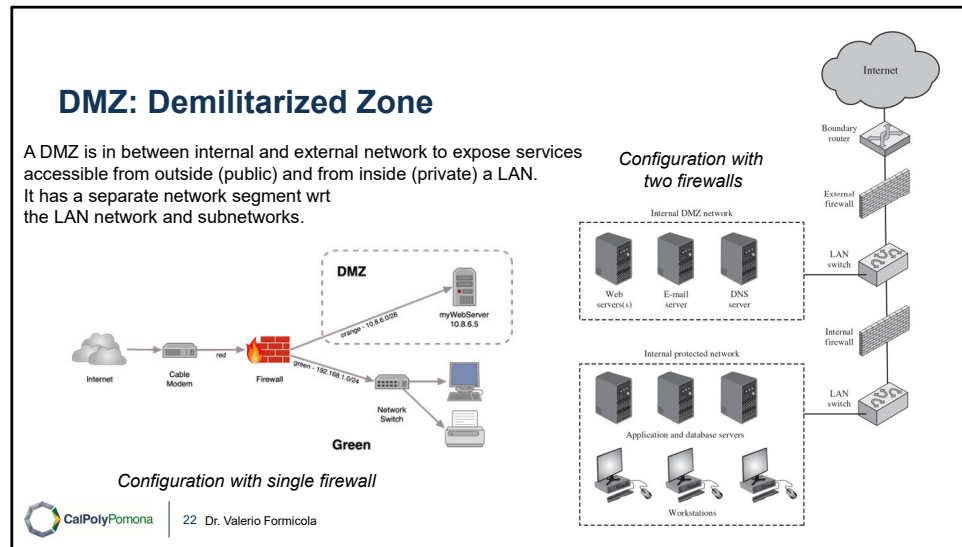


Figure 9.2 illustrates a common firewall configuration that includes an additional network segment between an internal and an external firewall (see also Figure 8.5). An external firewall is placed at the edge of a local or enterprise network, just inside the boundary router that connects to the Internet or some wide area network (WAN). One or more internal firewalls protect the bulk of the enterprise network. Between these two types of firewalls are one or more networked devices in a region referred to as a DMZ (demilitarized zone) network. Systems that are externally accessible but need some protections are usually located on DMZ networks. Typically, the systems in the DMZ require or foster external connectivity, such as a corporate Web site, an e-mail server, or a DNS (domain name system) server.

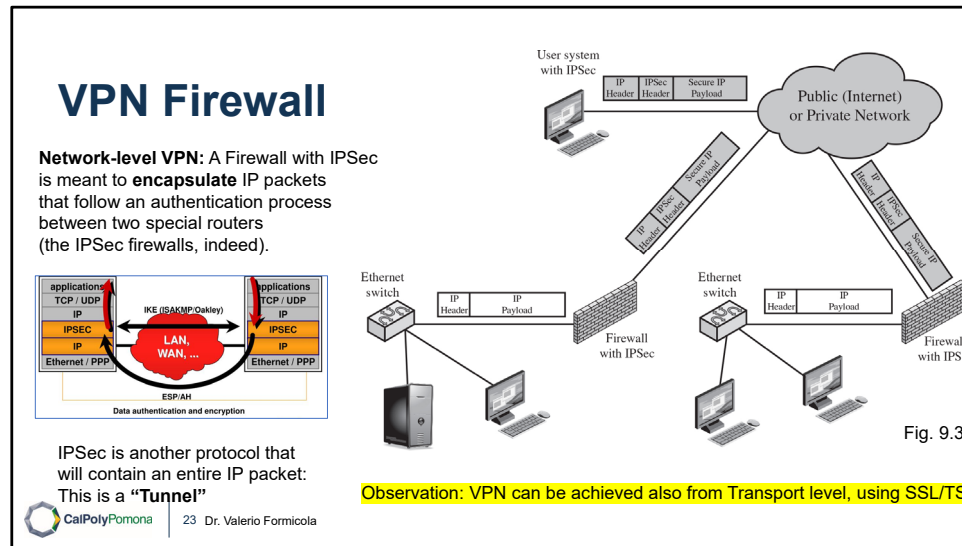
The external firewall provides a measure of access control and protection for the DMZ systems consistent with their need for external connectivity. The external firewall also provides a basic level of protection for the remainder of the enterprise network. In this type of configuration, internal firewalls serve three purposes:

1. The internal firewall adds more stringent filtering capability, compared to the external firewall, in order to protect enterprise servers and workstations from external attack.

2. The internal firewall provides two-way protection with respect to the DMZ. First, the internal firewall protects the remainder of the network from attacks launched from DMZ systems. Such attacks might originate from worms, rootkits, bots, or other malware lodged in a DMZ system. Second, an internal firewall can protect the DMZ systems from attack from the internal protected network.

3. Multiple internal firewalls can be used to protect portions of the internal network from each other. Figure 8.5 (Example of NIDS Sensor Deployment) shows a configuration in which the internal servers are protected from internal workstations and vice versa. It also illustrates the common practice of placing the DMZ on a different network interface on the external firewall from that used to access the internal networks.

The internal protected network consisting of workstations along with the application and database servers is connected to a LAN switch. The internal D M Z network consisting of Web servers, e mail server, and D N S server is connected to another LAN switch. The two LAN switches are connected by an internal firewall. The internal D M Z network LAN switch is then connected to a boundary router through an external firewall. The router is then connected to the internet.



In today's distributed computing environment, the virtual private network (VPN) offers an attractive solution to network managers. In essence, a VPN consists of a set of computers that interconnect by means of a relatively unsecure network and that make use of encryption and special protocols to provide security. At each corporate site, workstations, servers, and databases are linked by one or more local area networks (LANs). The Internet or some other public network can be used to interconnect sites, providing a cost savings over the use of a private network and offloading the wide area network management task to the public network provider. That same public network provides an access path for telecommuters and other mobile employees to log on to corporate systems from remote sites.

But the manager faces a fundamental requirement: security. Use of a public network exposes corporate traffic to eavesdropping and provides an entry point for unauthorized users. To counter this problem, a VPN is needed. In essence, a VPN uses encryption and authentication in the lower protocol layers to provide a secure connection through an otherwise insecure network, typically the Internet. VPNs are generally cheaper than real private networks using private lines but rely on having the same encryption and authentication system at both ends. The encryption may be performed by firewall software or possibly by routers. The most common protocol mechanism used for this purpose is at the IP level

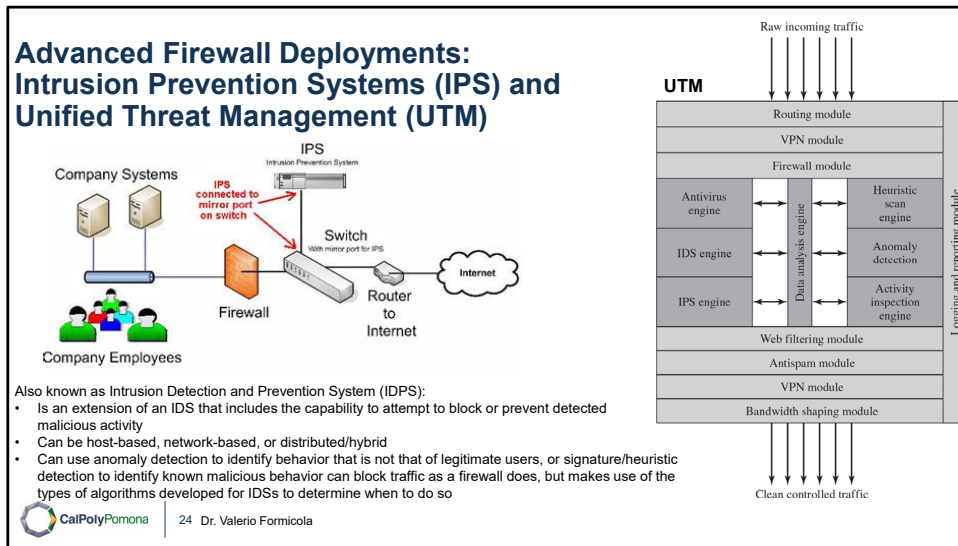
and is known as IPSec.

Figure 9.3 is a typical scenario of IPSec usage. An organization maintains LANs at dispersed locations. Nonsecure IP traffic is used on each LAN. For traffic off site, through some sort of private or public WAN, IPSec protocols are used. These protocols operate in networking devices, such as a router or firewall, that connect each LAN to the outside world. The IPSec networking device will typically encrypt and compress all traffic going into the WAN and decrypt and uncompress traffic coming from the WAN; authentication may also be provided. These operations are transparent to workstations and servers on the LAN. Secure transmission is also possible with individual users who dial into the WAN. Such user workstations must implement the IPSec protocols to provide security. They must also implement high levels of host security, as they are directly connected to the wider Internet. This makes them an attractive target for attackers attempting to access the corporate network.

A logical means of implementing an IPSec is in a firewall, as shown in Figure 9.3. If IPSec is implemented in a separate box behind (internal to) the firewall, then VPN traffic passing through the firewall in both directions is encrypted. In this case, the firewall is unable to perform its filtering function or other security functions, such as access control, logging, or scanning for viruses. IPSec could be implemented in the boundary router, outside the firewall. However, this device is likely to be less secure than the firewall and thus less desirable as an IPSec platform.

The workstations along with database servers are connected to Ethernet switches. The Ethernet switches are connected to the Firewall with I P Sec, with I P header, and I P payload tokens. The firewall is then connected to the Public, internet, or Private network through the I P header, I P S e c header, Secure I P Payload tokens. The Internet is then connected to the user system with I P S e c, through the I P header, I P S e c header, and Secure I P Payload tokens.

<https://www.cloudflare.com/learning/network-layer/what-is-ipsec/>



Intrusion prevention system (IPS):

A further addition to the range of security products is the intrusion prevention system (IPS), also known as intrusion detection and prevention system (IDPS). It is an extension of an IDS that includes the capability to attempt to block or prevent detected malicious activity. Like an IDS, an IPS can be host-based, network-based, or distributed/hybrid, as we discuss in Chapter 8. Similarly, it can use anomaly detection to identify behavior that is not that of legitimate users, or signature/heuristic detection to identify known malicious behavior.

Once an IDS has detected malicious activity, it can respond by modifying or blocking network packets across a perimeter or into a host, or by modifying or blocking system calls by programs running on a host. Thus, a network IPS can block traffic, as a firewall does, but makes use of the types of algorithms developed for IDSs to determine when to do so. It is a matter of terminology whether a network IPS is considered a separate, new type of product or simply another form of firewall.

Unified Threat Management (UTM):

In the past few chapters, we have reviewed a number of approaches to countering malicious software and network-based attacks, including antivirus and antiworm products, IPS and IDS, and firewalls. The implementation of all of these systems can provide an organization with a defense in depth using multiple layers of filters and defense mechanisms to thwart attacks. The downside of such a piecemeal implementation is the need to configure, deploy, and manage a range of devices and software packages. In addition, deploying a number of devices in sequence can reduce performance.

One approach to reducing the administrative and performance burden is to replace all inline network products (firewall, IPS, IDS, VPN, antispam, antispyware, and so on) with a single device that integrates a variety of approaches to dealing with network-based attacks. The market analyst firm IDC refers to such a device as a unified threat management (UTM) system and defines UTM as follows: “Products that include multiple security features integrated into one box. To be included in this category, [an appliance] must be able to perform network firewalling, network intrusion detection and prevention and gateway anti-virus. All of the capabilities in the appliance need not be used concurrently, but the functions must exist inherently in the appliance.”

A significant issue with a UTM device is performance, both throughput and latency. [MESS06] reports that typical throughput losses for current commercial devices is 50%. Thus, customers are advised to get very high-performance, high-throughput devices to minimize the apparent performance degradation.

Figure 9.6 is a typical UTM appliance architecture. The following functions are noteworthy:

1. Inbound traffic is decrypted if necessary before its initial inspection. If the device functions as a VPN boundary node, then IPSec decryption would take place here.
2. An initial firewall module filters traffic, discarding packets that violate rules and/or passing packets that conform to rules set in the firewall policy.
3. Beyond this point, a number of modules process individual packets and flows of packets at various protocols levels. In this particular configuration, a data analysis engine is responsible for keeping track of packet flows and coordinating the work of antivirus, IDS, and IPS engines.
4. The data analysis engine also reassembles multipacket payloads for content analysis by the antivirus engine and the Web filtering and antispam modules.

5. Some incoming traffic may need to be re-encrypted to maintain security of the flow within the enterprise network.
6. All detected threats are reported to the logging and reporting module, which is used to issue alerts for specified conditions and for forensic analysis.
7. The bandwidth-shaping module can use various priority and quality-of-service (QoS) algorithms to optimize performance.

Raw incoming traffic is given as input to the Logging and reporting module, which consists of 8 layers as follows. Routing module, V P N module, Firewall module, Data analysis engine, Web filtering module, Antispam module, V P N module, Bandwidth shaping module. The Data analysis engine has 3 layers of stacked rows on either side, with the layers from top to bottom as follows. Left stack, Antivirus engine, I D S engine, I P S engine. Right stack, Heuristic scan engine, Anomaly detection, Activity inspection engine. Double headed arrows extend from each stacked layer to the data analysis engine. The output is given to Clean controlled traffic.

Network segmentation

- Is the process of dividing a LAN in Segments, each with different kind of users, hosts, servers, risks and exposure to externals.
- Each segment might be separated by the others using router firewalls.
- A notable segmentation model for Industrial Control Systems is called *Purdue model*

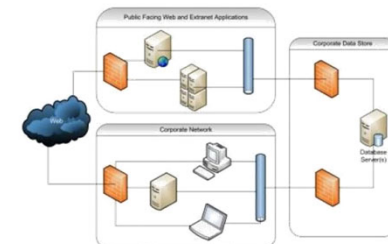


Figure 1: A secure network segmentation



25 Dr. Valerio Formicola

