



Network Defense Tools,

Social Engineering Toolkit,

Network Security Monitoring tools

Firewalls and Packet Filters

Network Address Translation (NAT) and Port Forwarding

VPN

Ethical Hacking

Security Frameworks and Foundations: National Institute of Standards and Technology (NIST) Framework

Cloud Security Alliance (CSA),

Cloud Controls Matrix (CCM),

MITRE ATTACK,

OWASP Foundation

OSINT framework.



Network Defense

3

11/8/2021

MONITORING NETWORK SECURITY IS AN ESSENTIAL TASK AND REQUIRES SPECIALIZED TOOLS IN ADDITION TO NETWORK PERFORMANCE MONITORS.

Old security tools that just compare packet content to a list of known strategies quickly become outdated and need to be updated constantly. Smarter network security tools assess regular activities on a network and then lookout for anything that is different, which is called an **anomaly**. **Network Defense AI-based tools are more sustainable in the ever-changing landscape of cybersecurity.**



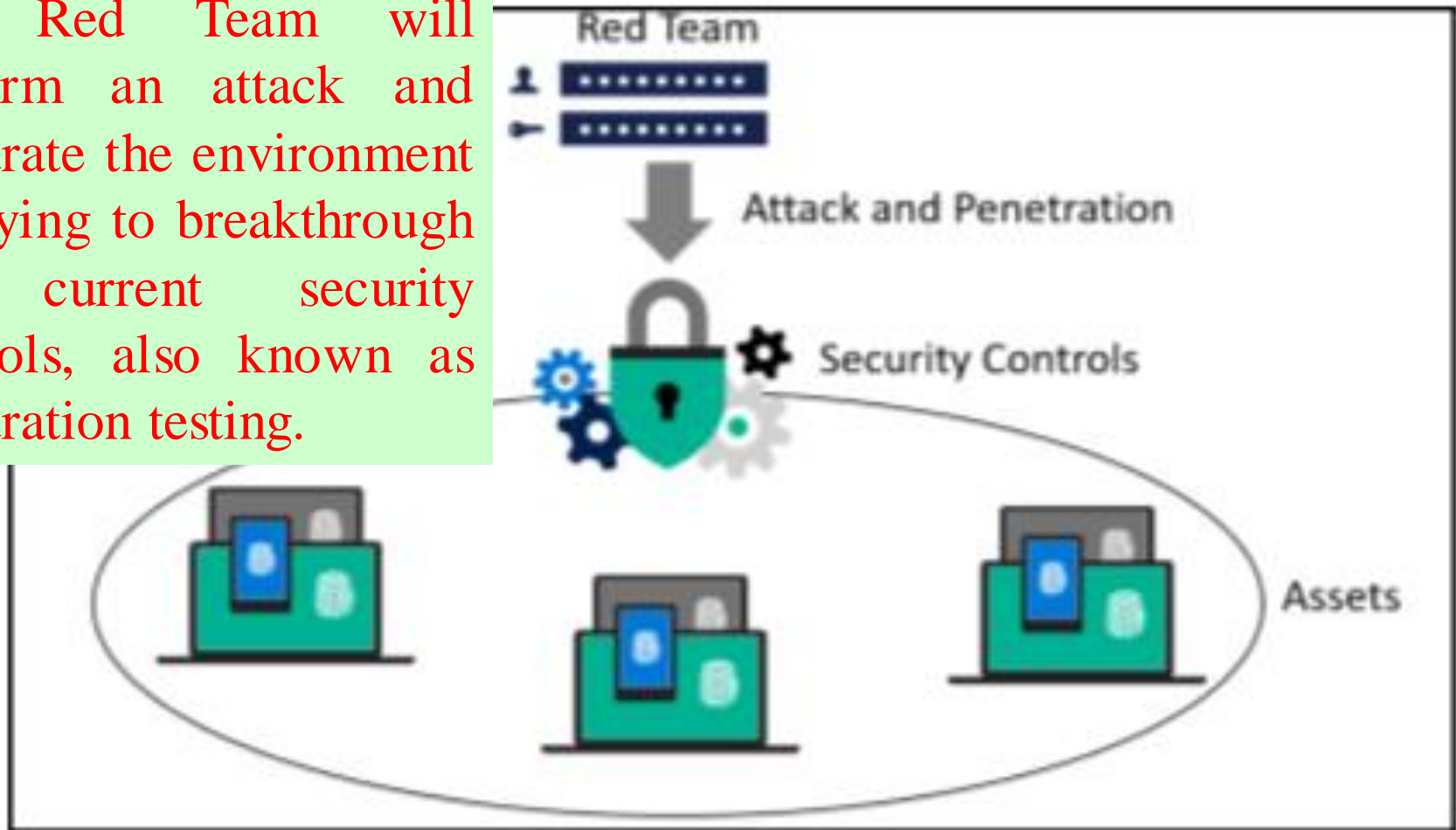
- NETWORK SECURITY MEASURES ARE THE SECURITY CONTROLS YOU ADD TO YOUR NETWORKS TO PROTECT CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY.
- NETWORK SECURITY MEASURES ARE THE TOOLS AND TECHNOLOGIES SUCH AS FIREWALLS AND INTRUSION PREVENTION SYSTEMS (IPS) THAT ARE ADDED TO A NETWORK TO SECURE STORED OR TRANSMITTED DATA, VOICE, AND VIDEO.

What is Network Detection and Response?

Network detection and response (NDR) products detect abnormal system behaviors by applying behavioral analytics to network traffic data. They continuously analyze raw network packets or traffic metadata between internal networks (east-west) and public networks (north-south). NDR can be delivered as a combination of hardware and software appliances for sensors, and a management and orchestration console in the form of an on-premises software or SaaS.

T Red Team workflow takes place using the following approach:

The Red Team will perform an attack and penetrate the environment by trying to breakthrough the current security controls, also known as penetration testing.





The Penetration Tester's job is to determine the success of the attack by identifying the exploit.

The main goals are as follows:

11/8/2023

Mean Time to Compromise (MTTC): This is the expected time for an attacker to compromise the target. It is the time from the first successful exploit to the point where the attacker is able to compromise the target.

Mean Time to Privilege Escalation (MTTP): This is the time from the point where the attacker has gained access to the system to the point where the attacker is able to compromise the target. It is the time from the first successful exploit to the point where the attacker is able to compromise the target.



The Blue Team needs to ensure that the assets are secure and in case the Red Team finds a vulnerability and exploits it, they need to rapidly remediate and document it as part of the lessons learned.

The following are some examples of tasks done by the Blue Team when an adversary (in this case the Red Team) is able to breach the system:

- **Save evidence:** It is imperative to save evidence during these incidents to ensure you have tangible information to analyze, rationalize, and take action to mitigate in the future.
- **Validate the evidence:** Not every single alert, or in this case evidence, will lead you to a valid attempt to breach the system. But if it does, it needs to be cataloged as an **Indication of Compromise (IOC)**.
- **Engage whoever is necessary to engage:** At this point, the Blue Team must know what to do with this IOC, and which team should be aware of this compromise. Engage all relevant teams, which may vary according to the organization.
- **Triage the incident:** Sometimes the Blue Team may need to engage law enforcement, or they may need a warrant in order to perform the further investigation, a proper triage will help on this process.
- **Scope the breach:** At this point, the Blue Team has enough information to scope the breach.
- **Create a remediation plan:** The Blue Team should put together a remediation plan to either isolate or evict the adversary.
- **Execute the plan:** Once the plan is finished, the Blue Team needs to execute it and recover from the breach.



The Blue Team members should also have a wide variety of skill sets and should be composed of professionals from different departments.

Some companies do have a dedicated Red/Blue Team, while others do not.

Estimated Time to Recover (ETDR)
Estimated Time to Recover (ETDR)

- The Blue Team and the Red Team's work doesn't finish when the Red Team is able to compromise the system.
- There is a lot more to do at this point, which will require full collaboration among these teams.
- A final report must be created to highlight the details regarding how the breach occurred, provide a documented timeline of the attack, the details of the vulnerabilities that were exploited in order to gain access and to elevate privileges (if applicable), and the business impact to the company.



Network Security Monitoring tools

- Network monitoring tools are tools that constantly track, analyze, and

11/8/2023



SNMP - The Simple Network Management

4 CATEGORIES OF NETWORK MONITORING

- **AVAILABILITY MONITORING. AVAILABILITY MONITORING IS THE SIMPLEST WAY FOR NETWORK TEAMS TO KNOW IF A DEVICE IS UP AND OPERATIONAL. ...**
- **CONFIGURATION MONITORING. ...**
- **PERFORMANCE MONITORING. ...**
- **CLOUD INFRASTRUCTURE MONITORING.**

most common



- **SolarWinds ipMonitor**- A combined network and server monitor that will discover all of your network assets automatically and continuously monitor them.
- **Paessler PRTG Network Monitor** -All-in-one network, server, and application monitor that is a collection of sensors. You customize the tool by deciding which sensors to turn on.
- **Site24x7 Server Monitoring** - A cut-down version of the Site24x7 Infrastructure plan that is limited to uptime monitoring. This is a cloud-based service.
- **ManageEngine OpManager** - A package of network and server monitoring services that is available in free and paid versions. Installs on Windows Server and Linux.
- **Domotz** - This cloud-based network monitoring service offers a full management and monitoring platform for a fixed price per site.
- **Zabbix** - A free infrastructure monitor that runs on Linux.
- **Nagios Core**.- An infrastructure monitor that can be extended by community-created extensions. A free version is called Nagios Core.
- **Icinga 2** - A free network monitor that is a fork of Nagios Core. Can be enhanced with Nagios extensions.

Note: Many more available in the market, based on organizational requirements suitable appropriate tools will be used.



Social Engineering Toolkit (SET)

Social Engineering Toolkit (SET) is **an integrated set of tools designed specifically to perform advanced attacks against the human element**, and is the most advanced if not the only toolkit of such kind that is. According to the **InfoSec Institute**, the following five techniques are among the most commonly used **social engineering attacks**.

Phishing. ...

Scareware. ...

Watering hole. ...

Spear phishing or whaling attack. ...

Cache poisoning or DNS spoofing. ...

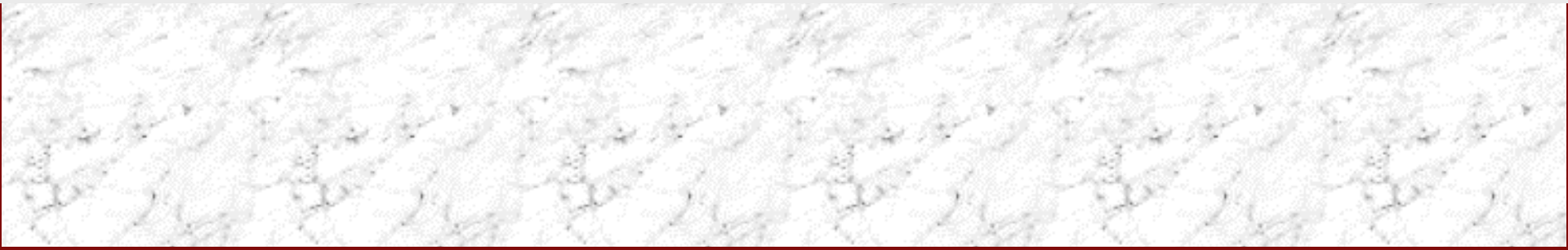
Pretexting. ...

Baiting and "quid pro quo" attacks



Social engineering prevention

- Don't open emails and attachments from suspicious sources
- Use multifactor authentication
- Be wary of tempting offers
- Keep your antivirus/antimalware software updated





Firewalls and Packet Filters

Mistake:

In Network Security, one of the biggest mistakes you can make that exposes your system to attack is forgetting to turn on a firewall.

11/8/2023

Need:

The organizations push toward securing their systems, they're working to reduce the risks (financial, data, reputation, etc.) associated with a compromise.

Challenge:

In fact, many network topologies become increasingly complex and difficult to manage over time. Add to this a great variety of systems with different patch levels and different configurations. Then, mix in ephemeral devices added by users.

In the face of all these systems to defend, organizations must consider how to react when they are compromised by hackers, not just blindly believe that they'll never be visited by malicious activity.

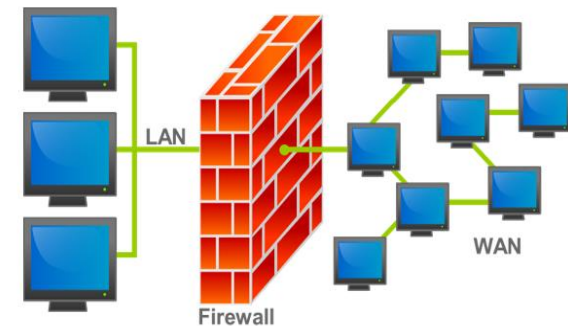
Network monitoring helps organizations to track down and eliminate or, at least, investigate suspicious activity. The SNORT network monitoring tool help identify activity when a firewall's defenses inevitably break down.

Firewalls and Packet Filters: The

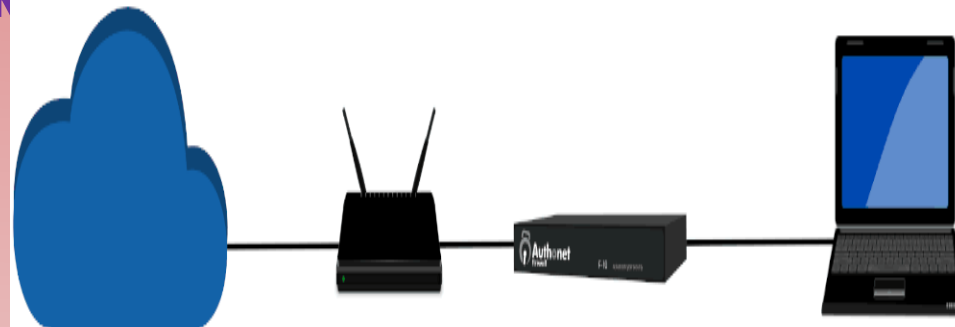
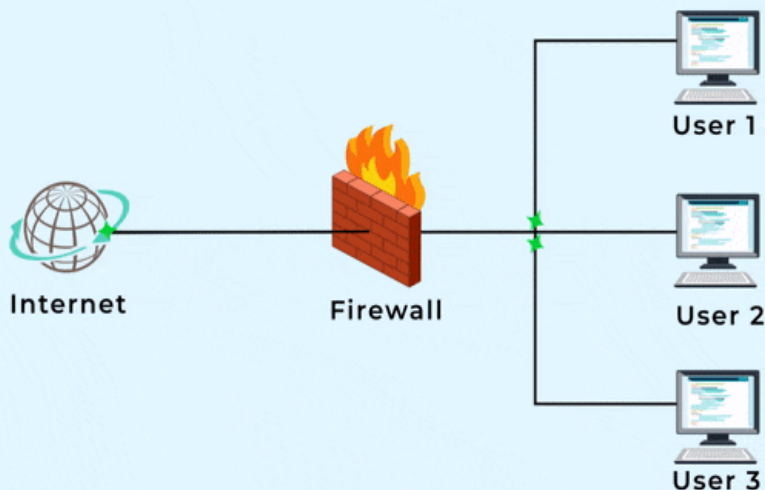
- NETWORK SECURITY DEVICES LIKE FIREWALLS CAN PROTECT ONE SYSTEM OR ONE MILLION SYSTEMS.
- WHAT IS A FIREWALL?
 - Firewalls are not strictly hardware devices. The capability of a firewall, to deny or accept traffic, is often built into devices like wireless access points and cable and DSL modems. It's also a part of almost all operating systems.
 - Firewall software examines traffic on a network interface to determine whether packets should be allowed to enter or leave the interface.



Firewall



- **THUS, FIREWALL SOFTWARE BLOCKS INBOUND CONNECTIONS TO A SYSTEM'S SERVICES THAT SHOULDN'T BE EXPOSED TO OTHER SYSTEMS ON A PUBLIC WI-FI NETWORK.**
- **THIS IS A USUAL CASE FOR PERSONAL FIREWALLS ON LAPTOPS WE CONNECT TO PUBLIC NETWORKS.**
- **BUT FIREWALL SOFTWARE CAN ALSO BE USED TO BLOCK OUTBOUND TRAFFIC FROM A SYSTEM TO A NETWORK.**
- **FOR EXAMPLE,**
YOU MIGHT WISH TO BLOCK TRAFFIC TO KNOWN MALWARE SITES TO TRY





- FIREWALLS HELP KEEP INTERNAL TRAFFIC INTERNAL AND SAFE FROM MALICIOUS EXTERNAL TRAFFIC.

17

NOTE: IF A DEVICE JUST ROUTES TRAFFIC BETWEEN NETWORKS AND IS UNABLE TO APPLY SECURITY RULES BASED ON THE TRAFFIC IT OBSERVES, IT IS JUST A ROUTER.

11/18/2023

- FIREWALLS TAKE THE DIRECTION OF TRAFFIC INTO CONSIDERATION WHEN FILTERING PACKETS. IT'S IMPORTANT TO KEEP A PERSPECTIVE ON WHAT ARE CONSIDERED INTERNAL OR EXTERNAL SYSTEMS WHEN CREATING RULES.
- AN INGRESS (INBOUND) FILTER AFFECTS PACKETS THAT ARRIVE ON A PROTECTED INTERFACE (OR NETWORK, SYSTEM, ETC). FOR A FIREWALL THAT PROTECTS A WEB SITE, THIS WOULD BE INBOUND TRAFFIC SUCH AS HTTP REQUESTS FROM ANYWHERE ON THE INTERNET TO THE WEB SERVER. AN INGRESS FILTER MIGHT ENSURE THAT ONLY HTTP TRAFFIC COMES INTO THE WEB SERVER.
- AN EGRESS (OUTBOUND) FILTER AFFECTS PACKETS THAT LEAVE THE INTERFACE. FOR A WEB SITE, THIS WOULD BE RESPONSES TO INCOMING HTTP REQUESTS. AN EGRESS FILTER MIGHT ENSURE THAT NO TRAFFIC IS INITIATED FROM THE WEB SERVER TO THE INTERNET. (THIS IS A COMMON COUNTERMEASURE TO MITIGATE CERTAIN WAYS A HACKER MIGHT CREATE A BACKDOOR TO ACCESS THE SYSTEM IN CASE IT'S COMPROMISED).



TWO COMMON NETWORK SECURITY SOFTWARE COMPONENTS THAT YOU CAN EQUATE TO FIREWALL LIKE FUNCTIONALITY ARE

11/18/2023

PERSONAL FIREWALLS: MODERN OSS INCLUDE FIREWALL CAPABILITIES BOTH BECAUSE FIREWALLS ARE AN IMPORTANT PIECE OF NETWORK SECURITY AND BECAUSE SYSTEMS MAY BE CONNECTED TO MANY DIFFERENT NETWORKS DURING THEIR LIFETIME. IT'S ONE THING TO HAVE YOUR LAPTOP PROTECTED BY A DSL OR CABLE MODEM THESE FIREWALLS PRIMARILY PROTECT A SYSTEM'S SERVICES OR FILE SHARING FROM UNAUTHORIZED ACCESS. OF, COURSE, THE FIREWALLS' RULES HAVE TO BE IN EFFECT IN ORDER TO BLOCK UNAUTHORIZED ACCESS.

PARENTAL CONTROL SOFTWARE: BLOCKS OUTBOUND TRAFFIC (USUALLY WEB) TO SITES EXCLUDED FROM ACCESS BASED ON APPROPRIATENESS (E.G., PORN), IDEOLOGY (E.G., POLITICS), SAFETY (E.G., MALWARE) OR OTHER REASONS. THIS REQUIRES A PRIVILEGED ACCOUNT (SUCH AS ROOT OR ADMINISTRATOR) TO DEFINE THE CONTROLS FOR A LOWER-PRIVILEGE ACCOUNT.

OTHER FILTERING SOFTWARE TOOLS SUCH AS **SPAM BLOCKERS** AND **VIRUS SCANNERS** ARE SIMILAR TO FIREWALLS IN THE SENSE THAT THEY ACCEPT OR DENY TRAFFIC BASED ON CONTENT INSPECTION.



- SPAM BLOCKERS AND VIRUS SCANNERS OPERATE “HIGHER UP THE STACK” ON APPLICATION LAYER CONTENT SUCH AS E-MAIL OR WEB TRAFFIC, WHEREAS FIREWALLS TYPICALLY OPERATE AT THE LEVEL OF IP ADDRESS AND PORT NUMBERS IN PACKET HEADERS.
- THERE IS CLEARLY AN ADVANTAGE TO BEING ABLE TO CONTROL TRAFFIC BASED ON APPLICATION LAYER CHARACTERISTICS.
- FOR EXAMPLE, INSTEAD OF BLOCKING ALL HTTP CONNECTIONS, YOU MAY WANT TO BLOCK ONLY THOSE THAT APPEAR TO BE SERVING MALWARE.
- A PACKET-LEVEL FILTER MIGHT ONLY BE ABLE TO FILTER BASED ON SOURCE OR DESTINATION PROPERTIES (E.G., PORT 80).
- THE APPLICATION LAYER (OR “DEEP INSPECTION”) FIREWALL MIGHT BE ABLE TO TELL THE DIFFERENCE BETWEEN VALID AND SPOOFED E-MAIL.
- TO MOST FIREWALLS, AN HTTPS CONNECTION JUST LOOKS LIKE RANDOM TRAFFIC OVER PORT 443.



PACKET FILTER VS. FIREWALL:

20

11/8/2023

- FIREWALLS AND PACKET FILTERS GENERALLY PERFORM THE SAME FUNCTION.
- PACKET FILTERS INSPECT TRAFFIC BASED ON CHARACTERISTICS SUCH AS PROTOCOL, SOURCE OR DESTINATION ADDRESSES, AND OTHER FIELDS IN THE TCP/IP (OR OTHER PROTOCOL) PACKET HEADER.
- FIREWALLS ARE PACKET FILTERS, BUT APPLICATION LAYER FIREWALLS MAY EXAMINE MORE THAN JUST PACKET HEADERS, THEY MAY EXAMINE PACKET DATA (OR PAYLOADS) AS WELL.
- FOR EXAMPLE, A PACKET FILTER MAY MONITOR CONNECTIONS TO PORTS 20 AND 21 (FTP PORTS)



- **A FIREWALL MAY BE ABLE TO ESTABLISH CRITERIA BASED ON THE FTP PORT NUMBERS AS WELL AS FTP PAYLOADS, SUCH AS THE PORT COMMAND OR FILENAMES THAT INCLUDE THE TEXT PASSWD.**
- **A WEB APPLICATION FIREWALL (WAF) WATCHES INCOMING CONNECTIONS FOR TELL-TALE SIGNS OF SQL INJECTION ATTACKS AND OUTBOUND TRAFFIC FOR SENSITIVE INFORMATION BEING LEAKED FROM THE WEB APP.**
- **THE TERM PACKET FILTER REFERS TO SOFTWARE THAT MAKES DECISIONS BASED ON PROTOCOL ATTRIBUTES: ADDRESSES, PORTS, AND FLAGS.**
- **PACKET FILTERING PROVIDES SECURITY TO A NETWORK ROUTING DEVICE.**
- **THE TERM FIREWALL IS USUALLY RESERVED FOR SOFTWARE OR DEVICES WHOSE PRIMARY PURPOSE IS TO APPLY SECURITY DECISIONS TO NETWORK TRAFFIC.**



- **INTRUSION-PREVENTION SYSTEM (IPS): THIS REFERS TO HARDWARE AND SOFTWARE THAT COMBINES PACKET FILTERING, CONTENT FILTERING, INTRUSION-DETECTION SYSTEM (IDS) CAPABILITIES, AND OTHER SECURITY FUNCTIONS.**
- **FOR EXAMPLE,**
ALERTS FROM AN IDS WOULD AUTOMATICALLY TRIGGER CERTAIN FIREWALL RULES.
- **NOTE: ALWAYS KEEPING YOUR SYSTEMS FULLY PATCHED ON A REGULAR BASIS, AND PERHAPS USING AN IDS SUCH AS SNORT PROVIDES SUFFICIENT PROTECTION FOR YOUR SYSTEM. IF YOU FIND THAT YOU NEED EXTRA SECURITY MEASURES, THEN LOOK INTO A COMMERCIAL IPS.**



HOW A FIREWALL PROTECTS A NETWORK:

- FIREWALLS ARE ONLY AS EFFECTIVE AS THE RULES THEY'RE CONFIGURED TO ENFORCE.
- FIREWALLS EXAMINE PARTICULAR CHARACTERISTICS OF NETWORK TRAFFIC AND DECIDE WHICH TRAFFIC TO ALLOW AND DENY BASED ON SOME CRITERIA.
- IT IS THE ADMINISTRATOR'S JOB TO DEFINE RULES SO THAT THE FIREWALL SUFFICIENTLY PROTECTS THE NETWORKS AND INFORMATION BEHIND IT WITHOUT NEGATIVELY IMPACTING LEGITIMATE TRAFFIC.
- MOST FIREWALLS HAVE THREE WAYS TO ENFORCE A RULE FOR NETWORK TRAFFIC::
 - **Accept the packet** and pass it on to its intended destination
 - **Deny the packet** and indicate the denial with an Internet Control Message Protocol (ICMP) message or similar acknowledgement to the sender. This provides explicit feedback that such traffic is not permitted through the firewall.
 - **Drop the packet** without any acknowledgement.

NOTE: It's safer to start with a firewall that rejects every incoming connection and open only the necessary holes for services you want to expose.



PACKET CHARACTERISTICS TO FILTER:

24

11/8/2023

MOST FIREWALLS AND PACKET FILTERS HAVE THE ABILITY TO EXAMINE THE FOLLOWING CHARACTERISTICS OF NETWORK TRAFFIC.

- Protocol – TCP / IP, FTP, UDP, ICMP, IPSec, etc
- Source IP Address & Port-
- Destination IP Address & Port
- ICMP message type and code
- TCP flags (ACK, FIN, SYN, etc)
- Network interface (DSL modem, or Cable (Lan), WI-FI) on which the packet arrives.



FOR EXAMPLE,

25

1. IF YOU WANTED TO BLOCK INCOMING PING PACKETS (ICMP ECHO REQUESTS) TO YOUR HOME NETWORK OF 192.168.1.0/24 -

11/8/2023

THE FOLLOWING RULES TO BE FOLLOWED:

- a. THE IMPORTANT COMPONENTS OF THE RULE ARE THE ACTION , I.E., DENY
- b. THE PACKET ATTRIBUTES (ICMP PROTOCOL SPECIFICALLY "PING" TYPES)
- c. THE DIRECTION OF THE RULE (PACKETS "FROM" ONE SOURCE "TO" ANOTHER) AND
- d. THE TYPE OF SOURCE (A NETWORK ADDRESS RANGE LIKE 192.168.1.0/24)

APPROPRIATE SYNTAX:

DENY PROTO ICMP TYPE 8:0 FROM ANY TO 192.168.1.0/24

FOR EXAMPLE,

26

11/8/2023

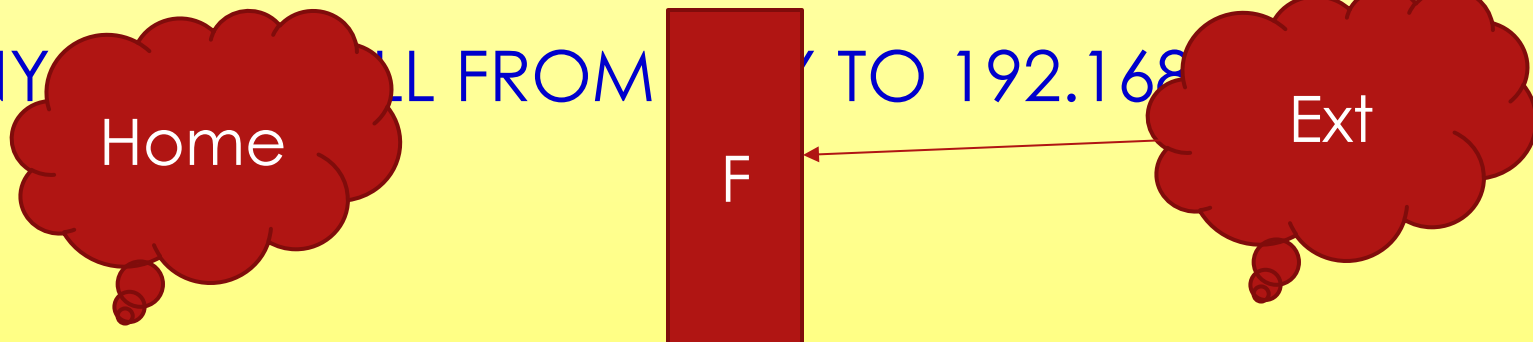
2. IF YOU WANTED TO ALLOW INCOMING WEB TRAFFIC TO 192.168.1.50 BUT DENY EVERYTHING ELSE, YOU WOULD CREATE TWO RULES.

- a. SPECIFY THE DIRECTION OF WEB TRAFFIC TO A SPECIFIC TCP PORT ON A SPECIAL HOST.
- b. MAKE SURE ALL OTHER TRAFFIC IS DENIED.

APPROPRIATE SYNTAX:

ALLOW PROTO TCP FROM ANY: ANY TO 192.168.1.50:80

DENY ALL FROM ANY: ANY TO 192.168.1.50





FOR SPOOFING EXAMPLE,

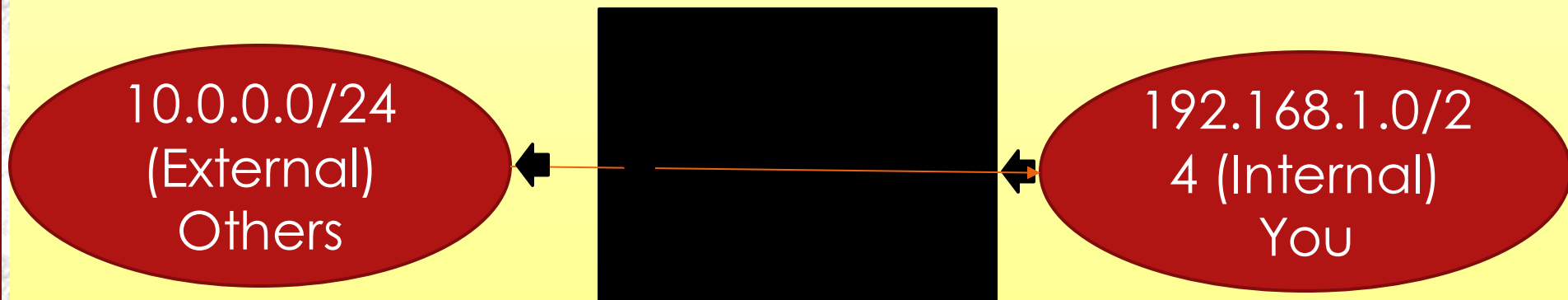
3. YOU CAN ALSO USE A FIREWALL TO PROTECT YOUR NETWORK FROM IP SPOOFING.

IMAGINE,

YOUR FIREWALL'S EXTERNAL INTERFACE (CALLED ETH1) HAS AN IP ADDRESS OF 10.0.0.1 WITH A NETMASK OF 255.255.255.0.

YOUR FIREWALL'S INTERNAL INTERFACE (CALLED ETH0) HAS AN IP ADDRESS OF 192.168.1.1 WITH A NETMASK OF 255.255.255.0.

ANY TRAFFIC FROM THE 192.168.1.0 NETWORK DESTINED TO THE 10.0.0.0 NETWORK WILL COME IN TO THE ETH0 INTERFACE AND GO OUT OF THE ETH1 INTERFACE



APPROPRIATE SYNTAX:

DENY PROTO ANY FROM 192.168.1.0/24 TO ANY ON ETH1



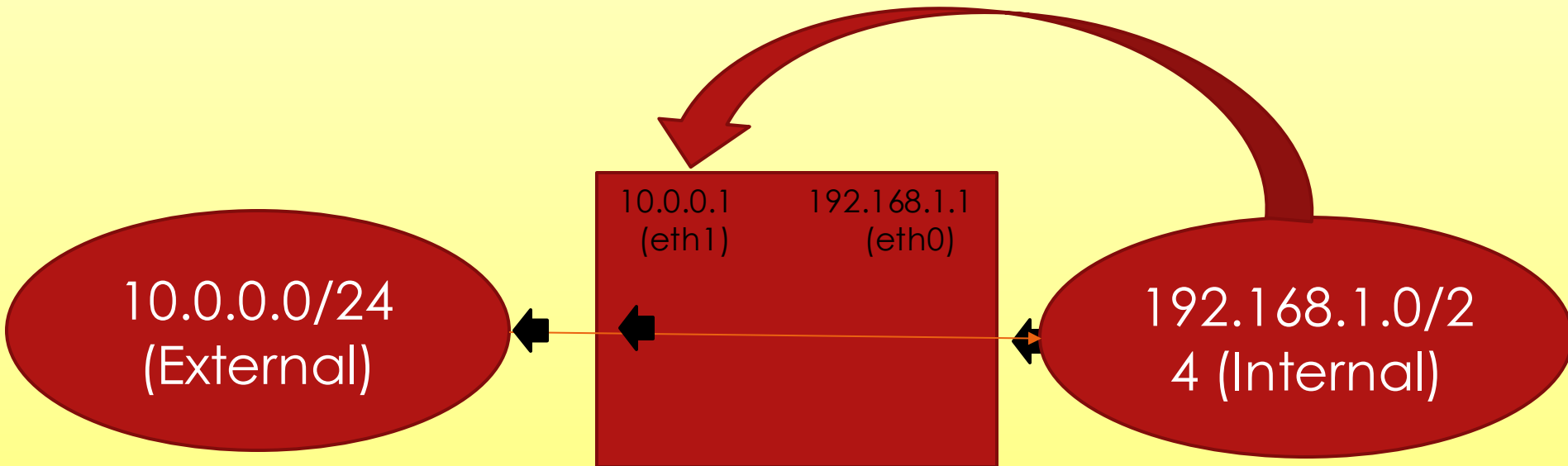
FOR ANTI-SPOOFING EXAMPLE,

4. WE REWRITE THE RULE WITH LESS AMBIGUITY BY SPECIFYING THE NETWORK INTERFACE ON WHICH IT SHOULD BE APPLIED.

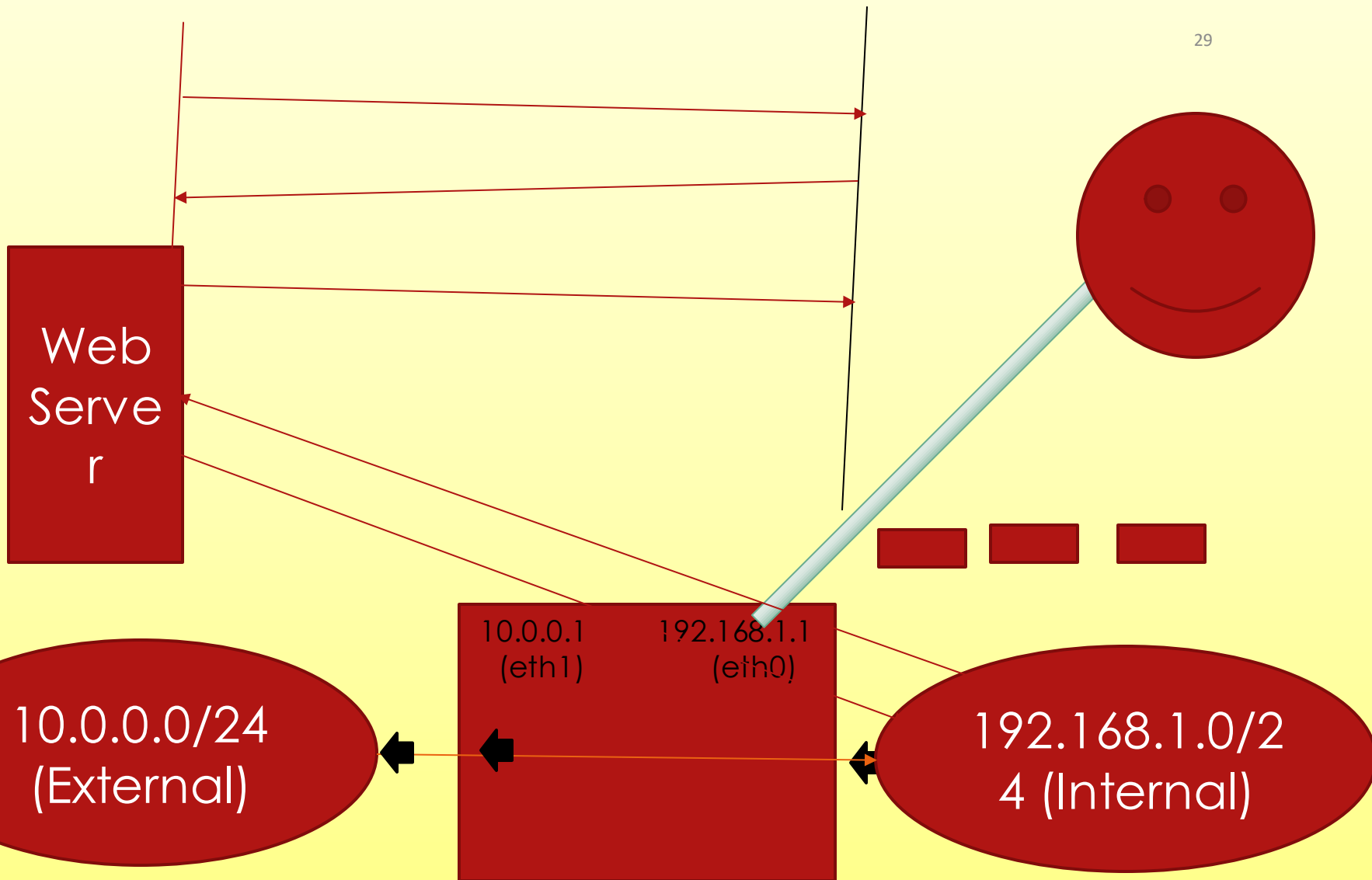
APPROPRIATE SYNTAX:

DENY PROTO ANY FROM 192.168.1.0/24 TO ANY IN ON ETH1

ALLOW PROTO ANY FROM 192.168.1.0/24 TO ANY OUT ON ETH1



* THE COMBINATION OF THESE TWO RULES CLEARLY INDICATES OUR INTENTION.





STATELESS VS. STATEFUL FIREWALLS:

THROUGH NMAP TOOL WE CAN DETERMINE WHETHER A FIREWALL IS STATEFUL OR NOT.

A STATELESS FIREWALL EXAMINES INDIVIDUAL PACKETS IN ISOLATION FROM EACH OTHER; IT DOESN'T TRACK WHETHER RELATED PACKETS HAVE ARRIVED BEFORE OR ARE COMING AFTER.

A STATEFUL FIREWALL PLACES THAT PACKET IN THE CONTEXT OF RELATED TRAFFIC AND WITHIN A PARTICULAR PROTOCOL, SUCH AS TCP / IP OR FTP. THIS ENABLES STATEFUL FIREWALLS TO GROUP INDIVIDUAL PACKETS TOGETHER INTO CONCEPTS LIKE CONNECTIONS, SESSIONS, OR CONVERSATIONS.

CONSEQUENTLY, A STATEFUL FIREWALL IS ABLE TO FILTER TRAFFIC BASED NOT ONLY ON A PACKET'S CHARACTERISTICS, BUT ALSO ON THE CONTEXT OF A PACKET ACCORDING TO A SESSION OR CONVERSATION.

FOR EXAMPLE, A TCP ACK PACKET WILL BE DENIED IF THE PROTECTED SERVICE HASN'T SET UP THE SYN AND SYN-ACK HANDSHAKE TO ESTABLISH A CONNECTION.



STATEFUL FIREWALLS ALSO ALLOW FOR MORE DYNAMIC RULESETS.

FOR EXAMPLE, SUPPOSE A SYSTEM ON THE INTERNAL 192.168.1.0/24 NETWORK WANTED TO CONNECT TO A WEBSERVER ON THE INTERNET.

11/8/2023

THE FOLLOWING STEPS DEMONSTRATE THE DRAWBACKS OF TRYING TO APPLY SIMPLE PACKET INSPECTION TO THE TRAFFIC.

STEP-1: ESTABLISHES A RULE FOR TCP TRAFFIC FROM THE 192.168.1.0/24 NETWORK TO PORT 80 ON ANY IP ADDRESS.

APPROPRIATE SYNTAX:

ALLOW PROTO TCP FROM 192.168.1.0/24: ANY TO ANY:80 OUT ON ETH1

SO FAR, SO GOOD.

BUT WHAT HAPPENS WHEN THE WEB SERVER RESPONDS?

WE NEED TO MAKE SURE THE RESPONSE PACKET GETS ACCEPTED BY OUR FIREWALL.



UNFORTUNATELY, SINCE THE WEB BROWSER'S SYSTEM CHOOSES A PORT AT RANDOM TO RECEIVE TRAFFIC, WE WON'T KNOW WHICH DESTINATION PORT TO OPEN FOR THE RESPONSE UNTIL AFTER THE CONNECTION STARTS.

32

11/8/2023

THE ONLY THING WE KNOW FOR CERTAIN IS THAT THE WEB SERVER'S RESPONSE PACKET WILL HAVE A SOURCE PORT OF 80.

CONSEQUENTLY, WE MIGHT TRY A RULE THAT ALLOWS ANY WEB TRAFFIC (E.G., TCP PORT 80) FROM THE INTERNET TO REACH OUR INTERNAL NETWORK.

APPROPRIATE SYNTAX:

ALLOW PROTO TCP FROM ANY:80 TO 192.168.1.0/24: ANY IN ON ETH1

THIS ALLOWS THE WEB SERVER'S RESPONSE TO REACH ANY HOST ON THE INTERNAL NETWORK AT THE EXPENSE OF OPENING A GAPPING HOLE IN THE FIREWALL.

THE RULE ASSUMES THAT ONLY RETURN WEB TRAFFIC WOULD BE USING A SOURCE PORT OF 80.



- IF A HACKER WERE AWARE THAT ANY PACKET WITH A SOURCE PORT OF 80 COULD PASS THROUGH THE FIREWALL, THEY COULD USE PORT REDIRECTION TO SET UP A TUNNEL TO DO SOMETHING AS SIMPLE AS SCAN FOR PORTS OR AS SIMPLE AS TUNNEL TRAFFIC FOR A REMOTE SHELL.
- THE TUNNEL WOULD FORWARD ANY TRAFFIC IT RECEIVED TO A MACHINE ON THE 192.168.1.0 NETWORK, SUBSTITUTING 80 FOR THE PACKET'S SOURCE PORT IN ORDER TO TRAVERSE THE FIREWALL RULE.
- FOR A STATELESS FIREWALL, A RATHER WEAK PROTECTION AGAINST THIS SCENARIO IS TO RESTRICT INCOMING TRAFFIC TO THE EPHEMERAL PORTS USED BY TCP CLIENTS, AS FOLLOWS

APPROPRIATE SYNTAX:

**ALLOW PROTO TCP FROM ANY:80 TO
192.168.1.0/24: 1024-65535 IN ON ETH1**



- **THE OPERATING SYSTEM'S NETWORK STACK CHOOSES A RANDOM PORT AS THE SOURCE OF ITS TRAFFIC, WHEREAS THE DESTINATION PORT FOR SOMETHING LIKE AN HTTP SERVICE IS 80 BY DEFAULT.**
- **THIS RULE IMPROVES ON THE STATELESS PROTECTION, BUT IT STILL LEAVES A LARGE, UNNECESSARY HOLE IN THE FIREWALL.**

QUESTION YOURSELF:

WOULDN'T IT BE BETTER IF THE FIREWALL COULD INSTEAD REMEMBER THE DETAILS OF OUR OUTGOING CONNECTION?

IF THE INITIAL OUTGOING PACKET IS ALLOWED BY THE FIREWALL, ANY OTHER PACKETS THAT ARE PART OF THAT SESSION SHOULD ALSO BE ALLOWED.

THIS DYNAMIC RULE PREVENTS US FROM HAVING TO POKE POTENTIALLY EXPLOITABLE HOLES IN OUR FIREWALL.

THIS IS THE ADVANTAGE OF STATEFUL FIREWALLS.

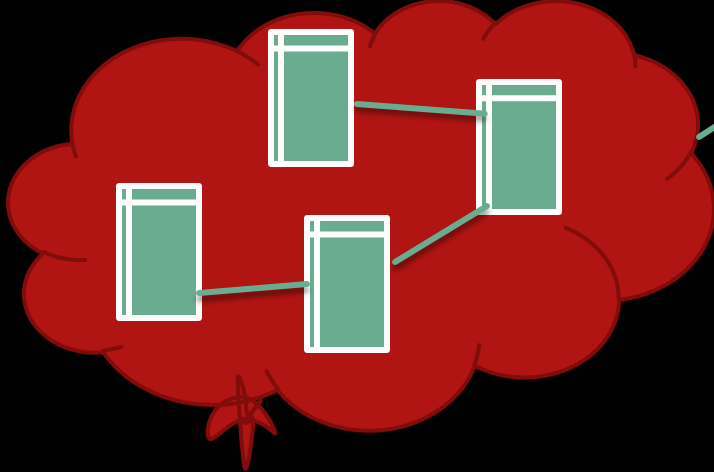
Network Address Translation (NAT) and Port

- NETWORKING DEVICES SUCH AS WAP OR FIREWALL, ARE THE GATEWAYS BETWEEN NETWORKS.
- THEY SEPARATE EXTERNAL NETWORKS LIKE THE INTERNET FROM PRIVATE NETWORKS

cs2028/11

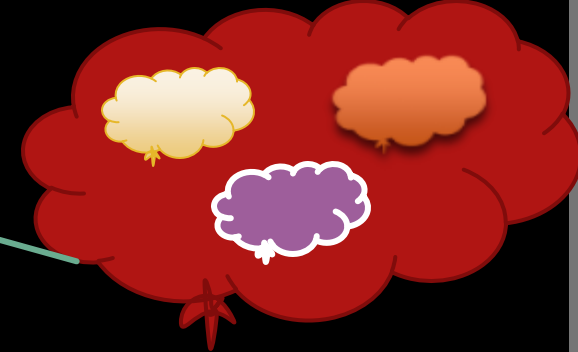
35

Internal Network



Firewal
I/
WAP

external Network





- SYSTEMS ON THE INTERNET MUST HAVE UNIQUE, PUBLIC (I.E., ROUTABLE) IP ADDRESSES.
- THIS ENSURES THAT PACKETS FOR A WEB SITE OR A GAMING SERVER ALWAYS GO TO THE RIGHT DESTINATION.
- IF THE SAME PUBLIC IP ADDRESS WERE PERMITTED TO BE USED FOR DIFFERENT, UNRELATED SERVERS, THEN TRAFFIC CONTROL WOULD BE A NIGHTMARE OF CONGESTION AND SECURITY PROBLEMS.

NOTE: INTERNAL NETWORKS, USE “NON-ROUTABLE” IP ADDRESSES, REFERRED TO AS PRIVATE OR RFC 1918 ADDRESSES.

- FOR EXAMPLE, 192.168.0.0 THROUGH 192.168.255.255 (WRITTEN 192.168.0.0/16 OR 192.168.0.0/255.255.0.0)
- 172.16.0.0 THROUGH 172.31.255.255 (WRITTEN 172.16.0.0/12 OR 172.16.0.0/255.240.0.0)
- 10.0.0.0 THROUGH 10.255.255.255 (WRITTEN 10.0.0.0/8 OR 10.0.0.0/255.0.0.0)

THE INTERNET ASSIGNED NUMBERS AUTHORITY (IANA) RESERVED THOSE IP ADDRESS BLOCKS FOR PRIVATE NETWORKS.



11/8/2022

- THIS ENABLES ORGANIZATIONS LARGE AND SMALL TO BUILD NETWORKS WHOSE TRAFFIC WILL NOT LEAK ONTO THE INTERNET UNLESS IT PASSES THROUGH A GATEWAY DEVICE LIKE A ROUTER OR FIREWALL.
- INTERNET TRAFFIC SHOULD NEVER ACCOMMODATE PACKETS WHOSE SOURCE CONTAINS AN RFC 1918 ADDRESS.
- IT ALSO MEANS THAT ORGANIZATIONS ARE FREE TO USE ADDRESSES WITHIN THESE NETWORKS WITHOUT WORRYING ABOUT WHETHER OTHER NETWORKS ARE USING THE SAME IP ADDRESSES.

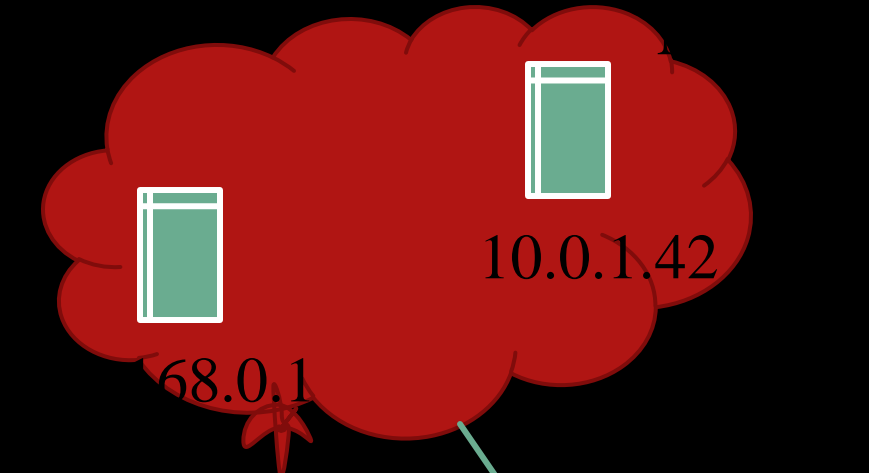
NOTE:

- IPV4 SUPPORTS ABOUT 4 BILLION DEVICES
- IPV6 SUPPORTS ABOUT 3.4×10^{38} UNIQUE DEVICES
- THE “NONROUTABLE” NATURE OF PRIVATE ADDRESS SPACES POSES A PROBLEM ONCE A DEVICE NEEDS TO ACCESS THE INTERNET.
- THE ADDRESSES ARE FINE FOR SYNCING YOUR STEREO WITH YOUR MUSIC COLLECTION STORED ON THE LOCAL NETWORK, BUT THEY DON'T WORK WHEN YOUR DEVICE WITH ADDRESS 10.0.1.42 NEEDS TO RETRIEVE MUSIC FROM STORAGE ON THE INTERNET.



- THE MUSIC STORAGE SERVICE NEEDS TO KNOW THE DIFFERENCE BETWEEN YOUR DEVICE USING THE 10.0.1.42 ADDRESS AND SOMEONE ELSE'S DEVICE USING THE SAME THEIR PRIVATE NETWORK. Music Collection Server

Internal Network

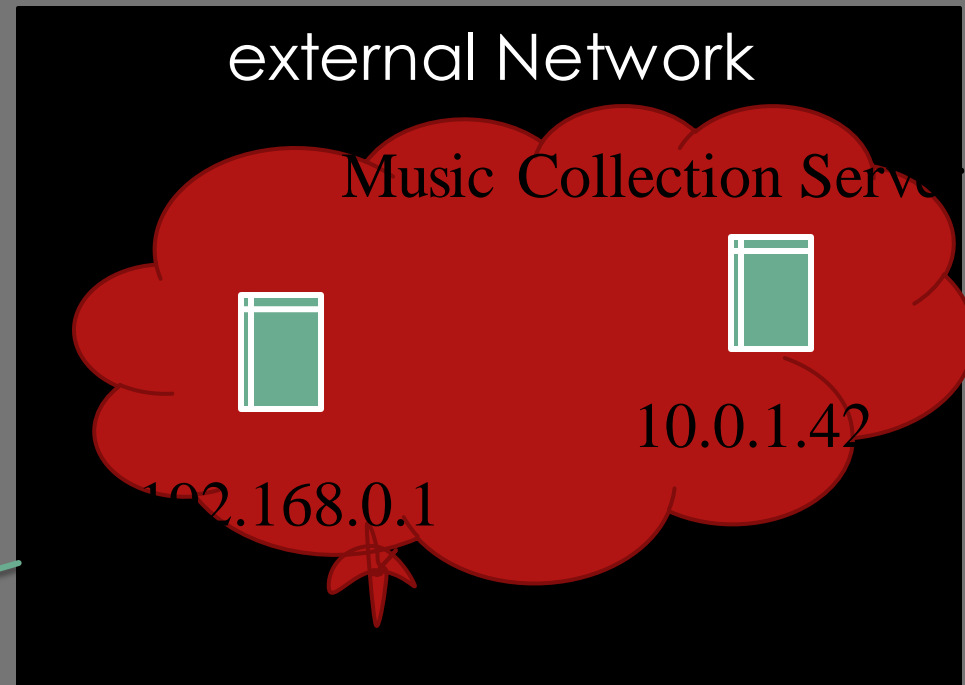


Storage
Machine



Firewall
/
WAP /
NAT /
VPN

external Network

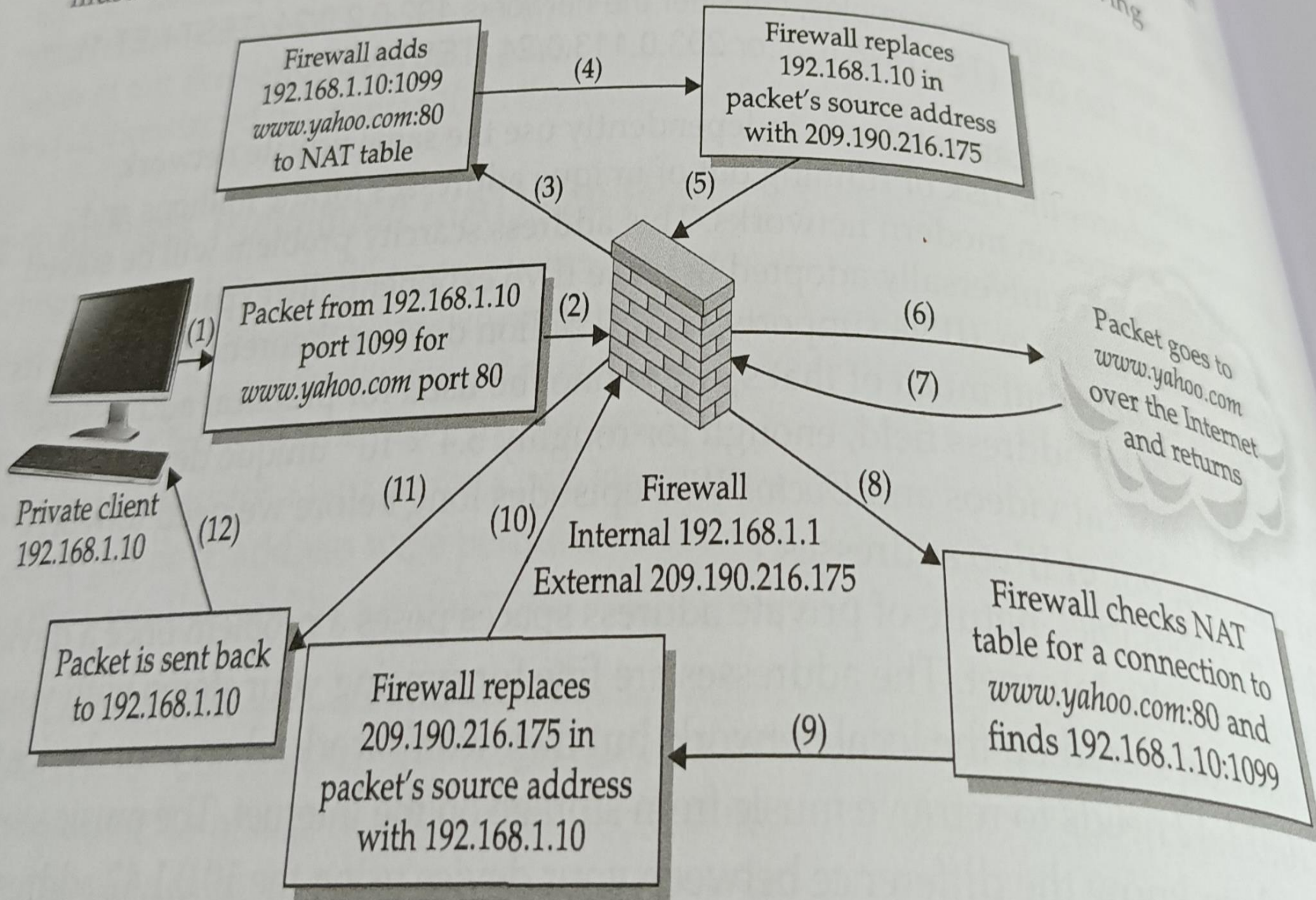


Music Collection Server

10.0.1.42

192.168.0.1

209,190.216.175 – External IP





- NETWORK ADDRESS TRANSLATION (NAT) SOLVES THIS ROUTING PROBLEM BY TRANSLATING PACKETS FROM PRIVATE TO PUBLIC ADDRESSES.
- NAT IS USUALLY PERFORMED BY A NETWORKING DEVICE ON ITS EXTERNAL INTERFACE FOR THE BENEFIT OF THE SYSTEMS ON ITS INTERNAL INTERFACE.
- A NAT DEVICE ALLOWS MACHINES ON ITS PRIVATE, INTERNAL NETWORK TO MASQUERADE AS THE IP ADDRESS ASSIGNED TO THE NAT DEVICE.
- PRIVATE SYSTEMS CAN COMMUNICATE WITH THE INTERNET USING THE ROUTABLE, PUBLICLY ACCESSIBLE IP ADDRESS ON THE NAT DEVICE'S EXTERNAL INTERFACE.
- WHEN A NAT DEVICE RECEIVES TRAFFIC FROM THE PRIVATE NETWORK DESTINED FOR THE EXTERNAL NETWORK (INTERNET), IT RECORDS THE PACKET'S SOURCE AND DESTINATION DETAILS.
- THE DEVICE THEN REWRITES THE PACKET'S HEADER SUCH THAT THE PRIVATE SOURCE IP ADDRESS IS REPLACED WITH THE DEVICE'S EXTERNAL, PUBLIC IP ADDRESS.



The basic of Virtual Private Networks (VPN)

41

→ VPNs are a complex subject in terms of identity, authentication, and encryption.

11/8/2023

→ So many firewall and networking devices provide some degree of VPN capability

→ A VPN establishes an encrypted channel between two networks (or single systems, or a combination) that is overlaid on a public network.

→ VPNs designed to mitigate the impact of using a hostile network like a public WI-FI connection where data may be sniffed or intercepted by an attacker.

→ The VPN's encrypted traffic is meant to be opaque to anyone who tries to monitor or interfere with it.

→ The VPN provides confidentiality and integrity.



→ A VPN server requires a remote client to authenticate to it before it will connect the remote client to the protected network.

→ A VPN extends the boundaries of a network, which creates a mixed sense of security

→ VPNs usually forward all traffic between the networks over a single set of ports.

→ By combining the capabilities of a firewall, a NAT device, and a VPN in one network device, you can greatly improve the external security of your internal network without losing convenience or productivity.



Linux Firewall

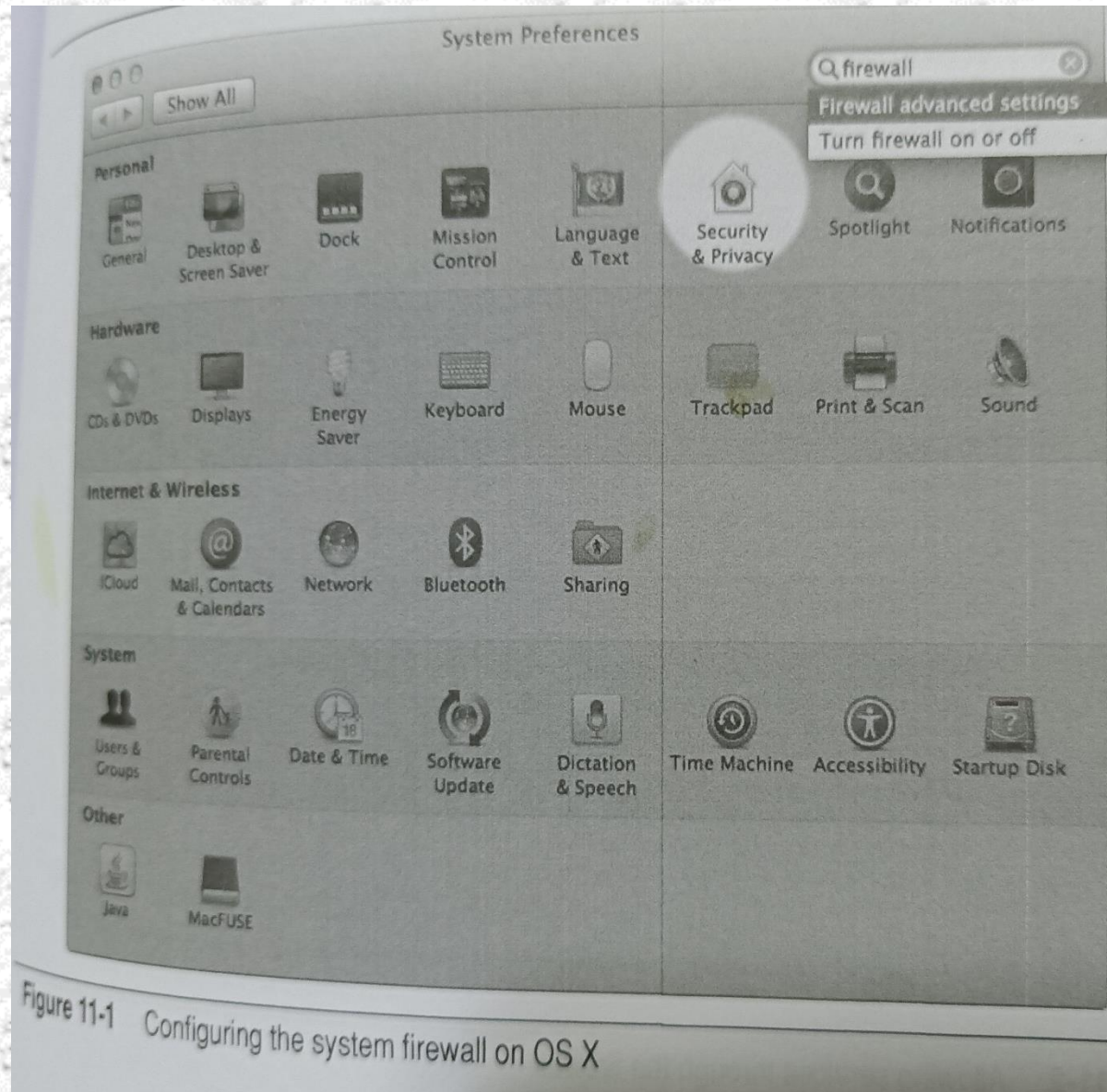


Figure 11-1 Configuring the system firewall on OS X



Control Panel > All Control Panel Items > Windows Firewall

[Control Panel Home](#)

[Allow an app or feature through Windows Firewall](#)

[Change notification settings](#)

[Turn Windows Firewall on or off](#)





[Restore defaults](#)

[Advanced settings](#)

[Troubleshoot my network](#)

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

 Private networks		Not connected 
Networks at home or work where you know and trust the people and devices on the network		
Windows Firewall state:	On	
Incoming connections:	Block all connections to apps that are not on the list of allowed apps	
Active private networks:	None	
Notification state:	Notify me when Windows Firewall blocks a new app	
 Guest or public networks		Connected 
Networks in public places such as airports or coffee shops		
Windows Firewall state:	On	
Incoming connections:	Block all connections to apps that are not on the list of allowed apps	
Active public networks:	 bmsit.net	
Notification state:	Notify me when Windows Firewall blocks a new app	

See also

[Action Center](#)

[Network and Sharing Center](#)



Control Panel > All Control Panel Items > Windows Firewall

[Control Panel Home](#)

[Allow an app or feature through Windows Firewall](#)

[Change notification settings](#)

[Turn Windows Firewall on or off](#)





[Restore defaults](#)

[Advanced settings](#)

[Troubleshoot my network](#)

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

 Private networks		Not connected 
Networks at home or work where you know and trust the people and devices on the network		
Windows Firewall state:	On	
Incoming connections:	Block all connections to apps that are not on the list of allowed apps	
Active private networks:	None	
Notification state:	Notify me when Windows Firewall blocks a new app	
 Guest or public networks		Connected 
Networks in public places such as airports or coffee shops		
Windows Firewall state:	On	
Incoming connections:	Block all connections to apps that are not on the list of allowed apps	
Active public networks:	 bmsit.net	
Notification state:	Notify me when Windows Firewall blocks a new app	

See also

[Action Center](#)

[Network and Sharing Center](#)



Snort: Intrusion Detection System Introduction

- FIREWALLS BLOCK TRAFFIC THAT WE KNOW BEFOREHAND SHOULDN'T BE TRAVERSING A PROTECTED NETWORK. HOWEVER, WE HAVE TO LET SOME TRAFFIC INTO THE NETWORK AND, TRAFFIC NEEDS TO GO OUT.
- A COMPETENT ADMINISTRATOR CREATES A ROBUST RULESET TO PREVENT MALICIOUS TRAFFIC FROM BYPASSING A FIREWALL.
- A SAVVY ADMINISTRATOR PREPARES FOR SCENARIOS IN WHICH MALICIOUS TRAFFIC MANAGES TO BYPASS THE FIREWALL. THIS IS WHERE NETWORK MONITORING COMES IN



Snort: Intrusion Detection System

- SNORT ([WWW.SNORT.ORG](http://www.snort.org)) IS A NETWORK MONITORING TOOL THAT WATCHES TRAFFIC FOR SIGNS OF MALICIOUS ACTIVITY.
- FOR EXAMPLE,
 - monitor buffer overflows being executed against a service,
 - command control traffic from malware,
 - suspicious activity – port scans and service enumeration etc.



Snort Modes

48

MODE-1: SNORT RUNS AS AN AD HOC SNIFFER (SIMILAR TO TCPDUMP),

MODE-2: A PACKET LOGGER (CONTINUOUS RECORDING OF NETWORK TRAFFIC), OR

MODE-3: AN IDS (TRIGGERS ALARMS BASED ON SUSPICIOUS ACTIVITY).

NOTE: SNORT USES A RULE CONFIGURATION FILE NAMED SNORT.CONF TO CONTROL HOW IT FILTERS TRAFFIC



- AN INTRUSION-DETECTION SYSTEM (IDS) IS A SNIFFER LIKE TCPDUMP OR WIRESHARK, BUT WITH SPECIALIZED FILTERS THAT ATTEMPT TO IDENTIFY MALICIOUS ACTIVITY.
- A GOOD IDS CAN FIND ANYTHING FROM A BUFFER OVERFLOW ATTACK AGAINST AN SSH SERVER TO THE TRANSMISSION OF /ETC/PASSWORD FILES OVER FTP.
- THE IDS EXAMINES PACKETS, LOOKING FOR PARTICULAR **SIGNATURES OR PATTERNS** THAT ARE ASSOCIATED WITH SUSPICIOUS OR PROHIBITED ACTIVITY.
- THE IDS THEN REPORTS ON ALL TRAFFIC THAT MATCHES THOSE SIGNATURES.
- SNORT IS A ROBUST IDS THAT RUNS ON UNIX-BASED AND WINDOWS SYSTEMS. IT IS FREE AND OPEN SOURCE.



Snort Rules

Alert Rule Log packets where the details of a match are of interest. A suspicious event may be generated by a common rule (looking for a port scan) or a strong indicator of a cyber event (web attack) or custom rules that monitor packets you define to be important factors (detectable intrusion, file transfer, malware, etc.).

Pass Rules Explicitly ignore packets. Traffic that matches these rules will not be logged.

Log Rule Record a packet but do not generate an alert. This would be useful for logging and forensic analysis of traffic that is not critical or monitored sensitive systems so that traffic can be analyzed in case a compromise is detected.

Activate Rules Generate an alert for traffic that matches this rule's trigger, then activate a subsequent dynamic rule.

Dynamic Rule Triggered by activation rules. This enables you to chain rules together in a way that makes it possible to make an efficient path through rules (no useless) and a more efficient (create



Here are a few examples of how a firewall could operate⁵¹ at different layers:

- **Layer 2 – data link** – it could make a block or forward decision based on the media access control (MAC) address of the frame.
- **Layer 3 – network** – it could make a block or forward decision based on the Internet Protocol (IP) address within the packet.
- **Layer 4 – transport** – it could make a block or forward decision based on the transmission control protocol (TCP) port number in the datagram.
- **Layer 5 – session** – it could make a block or forward decision based on the real-time protocol (RTP) information.
- **Layer 7 – data** – it could make a block or forward decision based on application or application service.



Ethical Hacking

<https://youtu.be/fNzpcB7ODxQ>



Security Frameworks and Foundations:

seven common cybersecurity frameworks.

- NIST Cybersecurity Framework.
- ISO 27001 and ISO 27002.
- SOC2.
- NERC-CIP.
- HIPAA.
- GDPR.
- FISMA.



National Institute of Standards and Technology (NIST) Framework



Cloud Security Alliance (CSA),

/2023



Cloud Controls Matrix (CCM),



MITRE ATTACK,



OWASP Foundation



OSINT framework.



References:

<https://www.comparitech.com/net-admin/network>