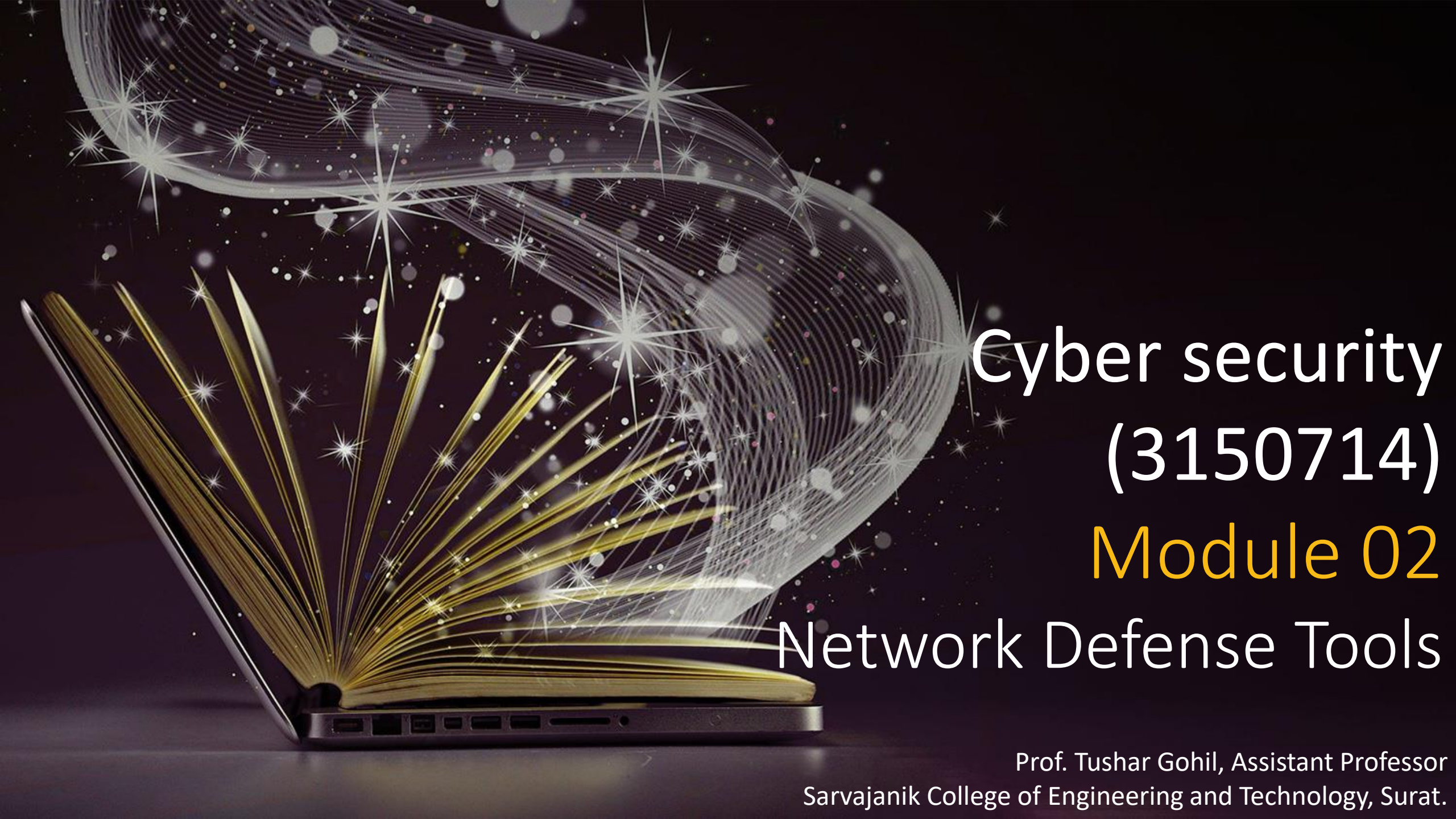


Cyber security (3150714)

Module 02

Network Defense Tools

Prof. Tushar Gohil, Assistant Professor
Sarvajanik College of Engineering and Technology, Surat.

Agenda

01 Firewalls and Packet Filters

Firewall Basics, Packet Filter Vs Firewall, Packet Characteristic to Filter, Stateless Vs Stateful Firewalls, Network Address Translation (NAT) and Port Forwarding

02 Snort

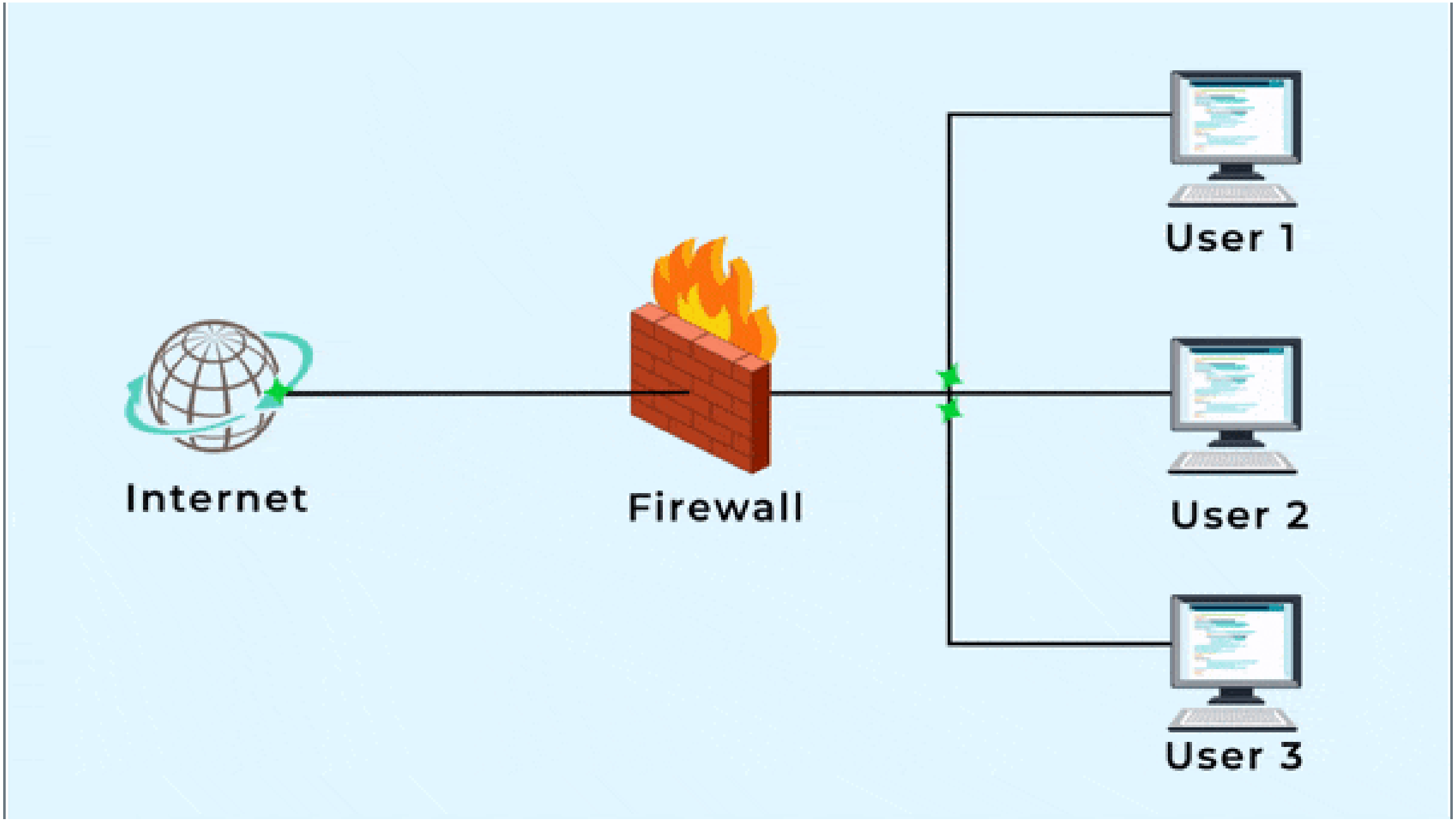
Intrusion Detection System

Firewalls and Packet Filters

Firewall Basics, Packet Filter Vs Firewall, Packet Characteristic to Filter, Stateless Vs Stateful Firewalls, Network Address Translation (NAT) and Port Forwarding

Overview

- One of the most notorious excuses, used by many and accepted by few, is the passive rhetoric of “Mistakes were made.” Even when accompanied by context, when “bad things happen” we rarely know what the specific mistake was or who made the mistake. Mistakes, apparently, just happen. In network security, one of the biggest mistakes you can make that exposes your system to attack is ***forgetting to turn on a firewall***.
- Firewalls aren’t magic; using one doesn’t afford perfect protection to your system(s).
- However, not using a firewall potentially exposes the data and vulnerable services on a system for which access should be restricted.


User 1
Internet
Firewall
User 2
User 3

Firewalls and Packet Filters : Basics

- 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. At its core, firewall software examines traffic on a network interface to determine whether packets should be allowed to enter or leave the interface.
- 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 and limit the potential damage of downloading an infected file.

Firewalls and Packet Filters : Basics

- Firewalls may also manage traffic between two or more different networks.
- In this scenario, traffic is inspected on an interface serving one network (say, the Internet), then transformed or modified if the device determines the packet is allowed to be passed onto an interface serving another network (say, your television).
- It's also how multiple devices behind a network device may all appear to share the same public IP when they are distinct systems on your internal network.
- Firewalls help keep internal traffic internal and safe from malicious external traffic.
- Firewalls take the direction of traffic into consideration when filtering packets.
- An ***ingress 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 ***egress filter*** affects packets that leave the interface.

  For a web site, this would be responses to incoming HTTP requests.

Firewalls and Packet Filters : Basics

- Two common network security software components that you can equate to firewall like functionality are :
  - **Personal firewalls :** Modern operating systems 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; it's another to take it from home to work to an airport to a cafe and connect to each of those networks. These firewalls primarily protect a system's services or file sharing from unauthorized access. Of course, the firewalls' rules must be in effect in order to block unauthorized access.
  - **Parental control software :** 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.
- 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.

Packet Filter vs. Firewall

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), whereas 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.

Firewalls and Packet Filters : Basics

- Sometimes you may also hear the phrase ***intrusion-prevention system (IPS).***
- This usually 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.
- Before you resort to trying to tackle a commercial IPS, determine whether using a firewall, keeping your systems fully patched on a regular basis, and perhaps using an IDS such as **Snort** provides sufficient protection for your system.

Firewalls and Packet Filters : **How a Firewall Protects a Network**

- Firewalls are only as effective as the rules they're configured to enforce.
- As mentioned previously, firewalls examine 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 acknowledgment to the sender. This provides explicit feedback that such traffic is not permitted through the firewall.
  - ***Drop*** the packet without any acknowledgment. This ends the packet's life on the network. No information is sent to the packet's sender. This method minimizes the sender's ability to deduce information about the protected network, but it may also adversely impact network performance for certain types of traffic. For example, a client may repeatedly attempt to connect to a service because it hasn't received an explicit message that the service isn't available.

Firewalls and Packet Filters : **How a Firewall Protects a Network**

- Most firewalls drop packets as their default policy for traffic that isn’t permitted.
- When building a ruleset, start with the concept of *least privilege* or *deny all*.
- It’s safer to start with a firewall that rejects every incoming connection and open only the necessary services you want to expose, rather than to start with an open firewall that exposes all your network’s resources.

Firewalls and Packet Filters : **Packet Characteristics to Filter**

- Most firewalls and packet filters can examine the following characteristics of network traffic:
  - ❖ Type of protocol (IP, TCP, UDP, ICMP, IPSec, etc.)
  - ❖ Source IP address and port
  - ❖ Destination IP address and port
  - ❖ ICMP message type and code
  - ❖ TCP flags (ACK, FIN, SYN, etc.)
  - ❖ Network interface on which the packet arrives
- For example, if you wanted to block incoming ping packets (ICMP echo requests) to your home network of 192.168.1.0/24, you could write something like the following rule.

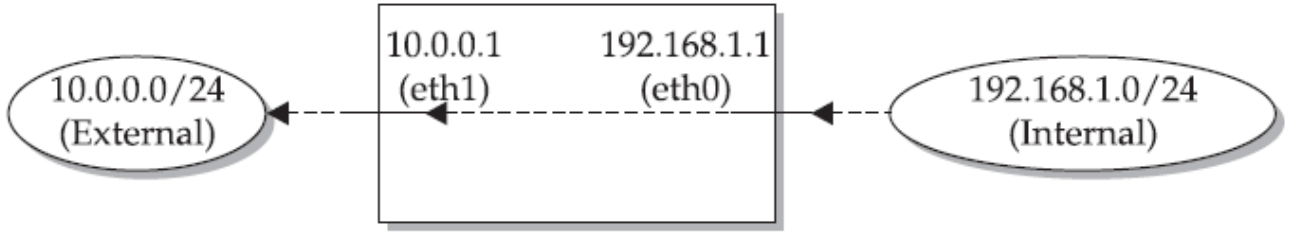
```
deny proto icmp type 8:0 from any to 192.168.1.0/24
```

- Or if you wanted to allow incoming web traffic to 192.168.1.50 but deny everything else, you would create two rules.

```
allow proto tcp from any:any to 192.168.1.50:80
deny proto all from any to 192.168.1.0/24
```

Firewalls and Packet Filters : **Packet Characteristics to Filter**

- You can also use a firewall to protect your network from IP spoofing.
- For example, 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, as shown here :



- Conversely, traffic from the 10.0.0.0/24 network destined for the 192.168.1.0/24 network will come in to the eth1 interface and go out of the eth0 interface.
- Therefore, you should never see traffic with a source address in the 192.168.1.0/24 range coming inbound on the eth1 interface.
- If you do, it means someone on the external 10.0.0.0/24 network is attempting to spoof an address in your local IP range. Your firewall can stop this kind of activity by using a rule like the following:

```
deny proto any from 192.168.1.0/24 to any on eth1
```

Firewalls and Packet Filters : **Stateless vs. Stateful Firewalls**

- 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 can 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.

Firewalls and Packet Filters : **Network Address Translation (NAT) and Port Forwarding**

- Networking devices, whether a consumer-level wireless access point or an enterprise grade firewall, are the ***gateways*** between networks.
- They separate external networks like the Internet from private networks like those used by the systems in your home.
- 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.
- Internal networks, on the other hand, *use "nonroutable" IP addresses*, referred to as private or RFC 1918 addresses.

Firewalls and Packet Filters : **Network Address Translation (NAT) and Port Forwarding**

- RFC 1918 refers to the document that explicitly defines the address space of the following networks :
  - **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.
- 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.
- 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
- The ability for organizations to independently use the same private network addresses reduces the risk of running out of unique addresses for the millions and millions of devices on modern networks.

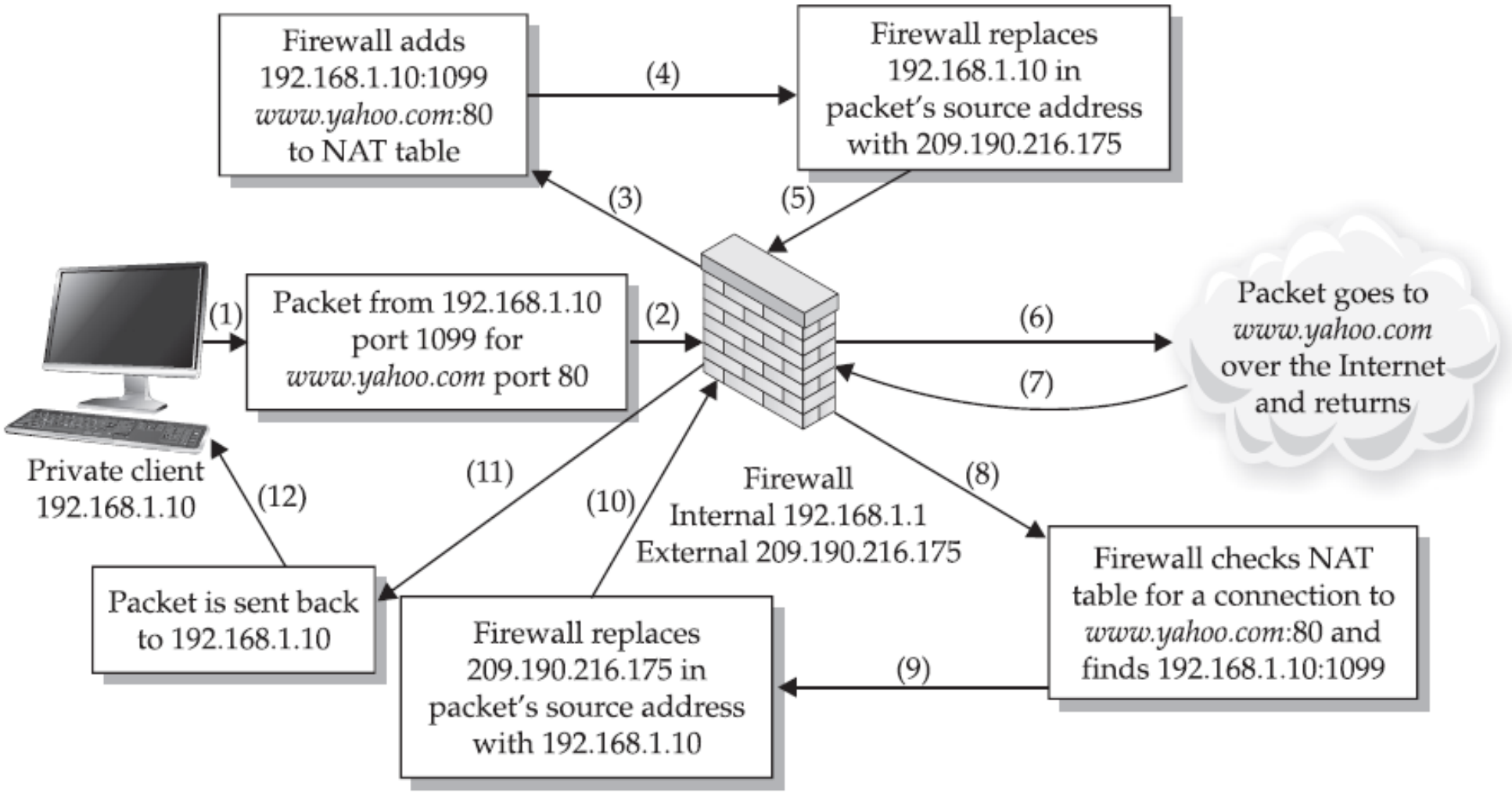
Firewalls and Packet Filters : **Network Address Translation (NAT) and Port Forwarding**

- 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 won’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 private IP address on their private network.
- ***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.
- 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.

Firewalls and Packet Filters : **Network Address Translation (NAT) and Port Forwarding**

- Then the device sends the packet to the destination IP address.
- From the destination system's point of view, the packet appears to have come directly from the NAT device.
- The destination system responds as necessary to the packet, sending it back to the NAT device's IP address.
- When the NAT device receives the response packet, it checks its address translation table to see if the address and port information of the packet match any of the packets that had been sent out.
- If no match is found, the packet is dropped or handled according to any firewall rules operating on the device.
- If a match is found, the NAT device rewrites the packet's destination IP address with the private IP address of the system that originally sent the packet.
- Finally, the NAT device sends the packet to its internal destination.
- The network address translation is completely transparent to the systems on the internal, private IP address and the Internet destination.
- *The private system can access the Internet, but an Internet system cannot directly address it.*

Firewalls and Packet Filters : **Network Address Translation (NAT) and Port Forwarding**



Firewalls and Packet Filters : **Network Address Translation (NAT) and Port Forwarding**

- But what happens if you decide you'd like to expose a particular service on your private network to the Internet?
- What if you wanted someone across the country to be able to look at something you had posted on your internal web server?
- For this, you can use a technique called ***port forwarding***.
- The NAT device may forward traffic received on a particular port on the device's external interface to a port on a system on the private, internal network.
- A remote system on the Internet that connects to the NAT device on this port effectively connects to the port on the internal system and only needs to know the public IP address of the NAT device.
- This is all well and good, but now you've made your private network a little less private by exposing the service listening on that port.
- Now anyone on the Internet can access your internal web server by connecting to the port on your NAT device.

Firewalls and Packet Filters : **PIX Firewall**

- A PIX firewall is a popular IP firewall that includes a network address translation appliance. It works in much the same way as an ordinary firewall by blocking attacks to the system from hackers, viruses, and worms.
- It is also used to hide multiple IP addresses behind one or multiple other IP addresses. Its objective was to help solve the shortage issue of available IP addresses. The PIX has had major security flaws and in 2013 an upgrade and fix to this issue was released by the manufacturer Cisco.
- The PIX became the first commercially available firewall product to allow protocol specific filtering. This allows for a much tighter security setting. This also allows the PIX to be very flexible scrutiny of web-based traffic using HTTP.
- The PIX can be managed and told what to do with packages that come from HTTP or any web-based point of origin. Security policies can be set up to monitor and react to instant messaging, peer-to-peer file sharing, and tunnelling applications.
- It can also be directed to inspect and preform deep packet inspection on applications such as FTP, ESMTP, and mobile tunnelling traffic.

Snort

Intrusion Detection System

Snort : An Intrusion-Detection System

- Firewalls block traffic that we know beforehand shouldn't be traversing a protected network.
- However, we must let some traffic into the network, and, of course, traffic needs to go out.
- A competent administrator creates a robust ruleset to prevent malicious traffic from bypassing a firewall.
- ***Snort*** is a network monitoring tool that watches traffic for signs of malicious activity (e.g., buffer overflows being executed against a service, command and control traffic from malware), suspicious activity (e.g., port scans and service enumeration), and anything else that you wish to look out for.
- At its core, 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.
- Network administrators place these systems where they can best monitor traffic, such as a point where they can see all traffic through a firewall or see all traffic between network segments with different security contexts.
- 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 : An Intrusion-Detection System : Modes

- Snort can be configured to run in three modes:
  - ***Sniffer mode,*** *which simply reads the packets off of the network and displays them for you in a continuous stream on the console (screen).*
  - ***Packet Logger mode****, which logs the packets to disk.*
  - ***Network Intrusion Detection System (NIDS) mode****, which performs detection and analysis on network traffic. This is the most complex and configurable mode.*

Snort : An Intrusion-Detection System : Modes : Sniffer mode

- If you just want to print out the TCP/IP packet headers to the screen (i.e. sniffer mode), try this:
  - snort -v
- This command will run Snort and just show the IP and TCP/UDP/ICMP headers, nothing else.
- If you want to see the application data in transit, try the following:
  - snort -vd
- This instructs Snort to display the packet data as well as the headers.
- If you want an even more descriptive display, showing the data link layer headers, do this:
  - snort -vde

Snort : An Intrusion-Detection System : Modes : Packet Logger mode

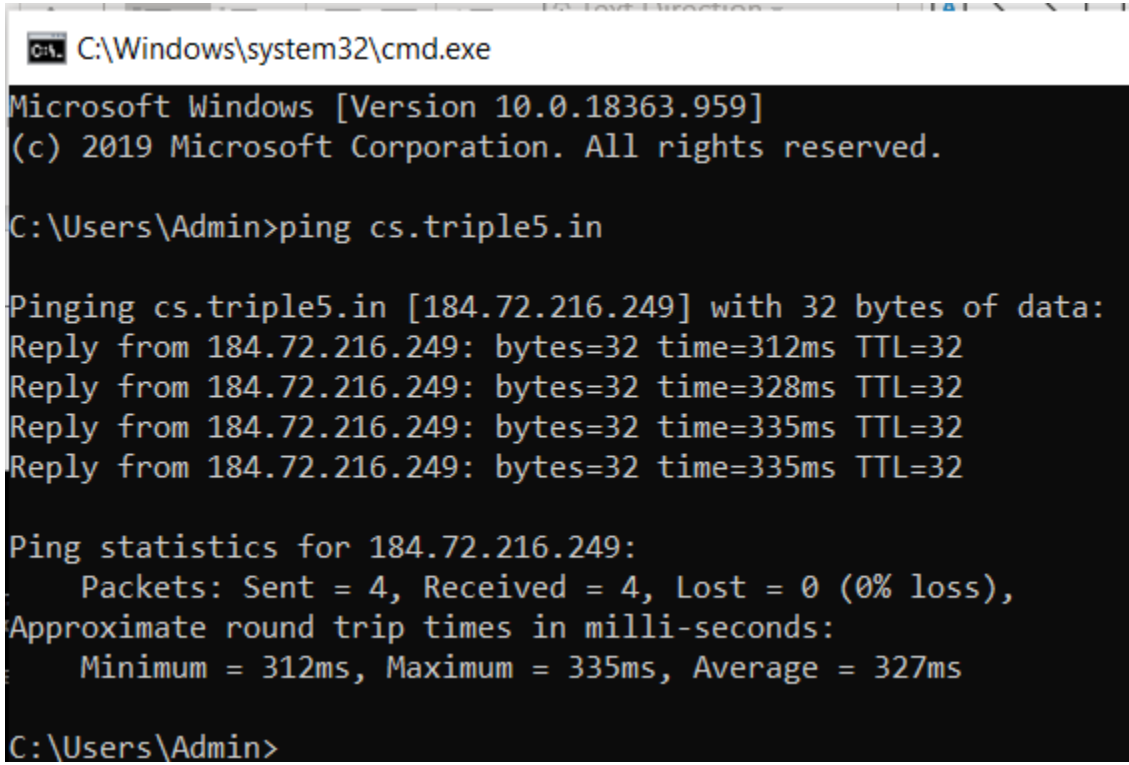
- if you want to record the packets to the disk, you need to specify a logging directory and Snort will automatically know to go into packet logger mode:
  - snort -dev -l ./log
- Of course, this assumes you have a directory named log in the current directory.
- If you don't, Snort will exit with an error message. When Snort runs in this mode, it collects every packet it sees and places it in a directory hierarchy based upon the IP address of one of the hosts in the datagram.

Snort : An Intrusion-Detection System : Modes : ***Network Intrusion Detection System***

- To enable Network Intrusion Detection System (NIDS) mode so that you don't record every single packet sent down the wire, try this:

```
nano /etc/snort/rules/local.rules

alert icmp any any -> $HOME_NET any (msg :"ICMP test"; sid:10000001; rev:001;)

sudo snort -A console -i eth0 -u snort -g snort -c /etc/snort/snort.conf
```

```
      --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.16 GRE (Build 118)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2020 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.9.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: appid  Version 1.1  <Build 5>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
Commencing packet processing (pid=763484)
07/20-04:11:00.608605  [**] [1:10000001:1] ICMP test [**] [Priority: 0] {ICMP} 61.177.172.61 -> 172.31.56.233
07/20-04:11:14.527762  [**] [1:10000001:1] ICMP test [**] [Priority: 0] {ICMP} 123.201.156.20 -> 172.31.56.233
07/20-04:11:14.527787  [**] [1:10000001:1] ICMP test [**] [Priority: 0] {ICMP} 172.31.56.233 -> 123.201.156.20
07/20-04:11:15.538996  [**] [1:10000001:1] ICMP test [**] [Priority: 0] {ICMP} 123.201.156.20 -> 172.31.56.233
07/20-04:11:15.539020  [**] [1:10000001:1] ICMP test [**] [Priority: 0] {ICMP} 172.31.56.233 -> 123.201.156.20
07/20-04:11:16.554117  [**] [1:10000001:1] ICMP test [**] [Priority: 0] {ICMP} 123.201.156.20 -> 172.31.56.233
07/20-04:11:16.554141  [**] [1:10000001:1] ICMP test [**] [Priority: 0] {ICMP} 172.31.56.233 -> 123.201.156.20
07/20-04:11:17.575465  [**] [1:10000001:1] ICMP test [**] [Priority: 0] {ICMP} 123.201.156.20 -> 172.31.56.233
07/20-04:11:17.575490  [**] [1:10000001:1] ICMP test [**] [Priority: 0] {ICMP} 172.31.56.233 -> 123.201.156.20
07/20-04:11:24.966052  [**] [1:10000001:1] ICMP test [**] [Priority: 0] {ICMP} 61.177.172.61 -> 172.31.56.233
```



THANK YOU