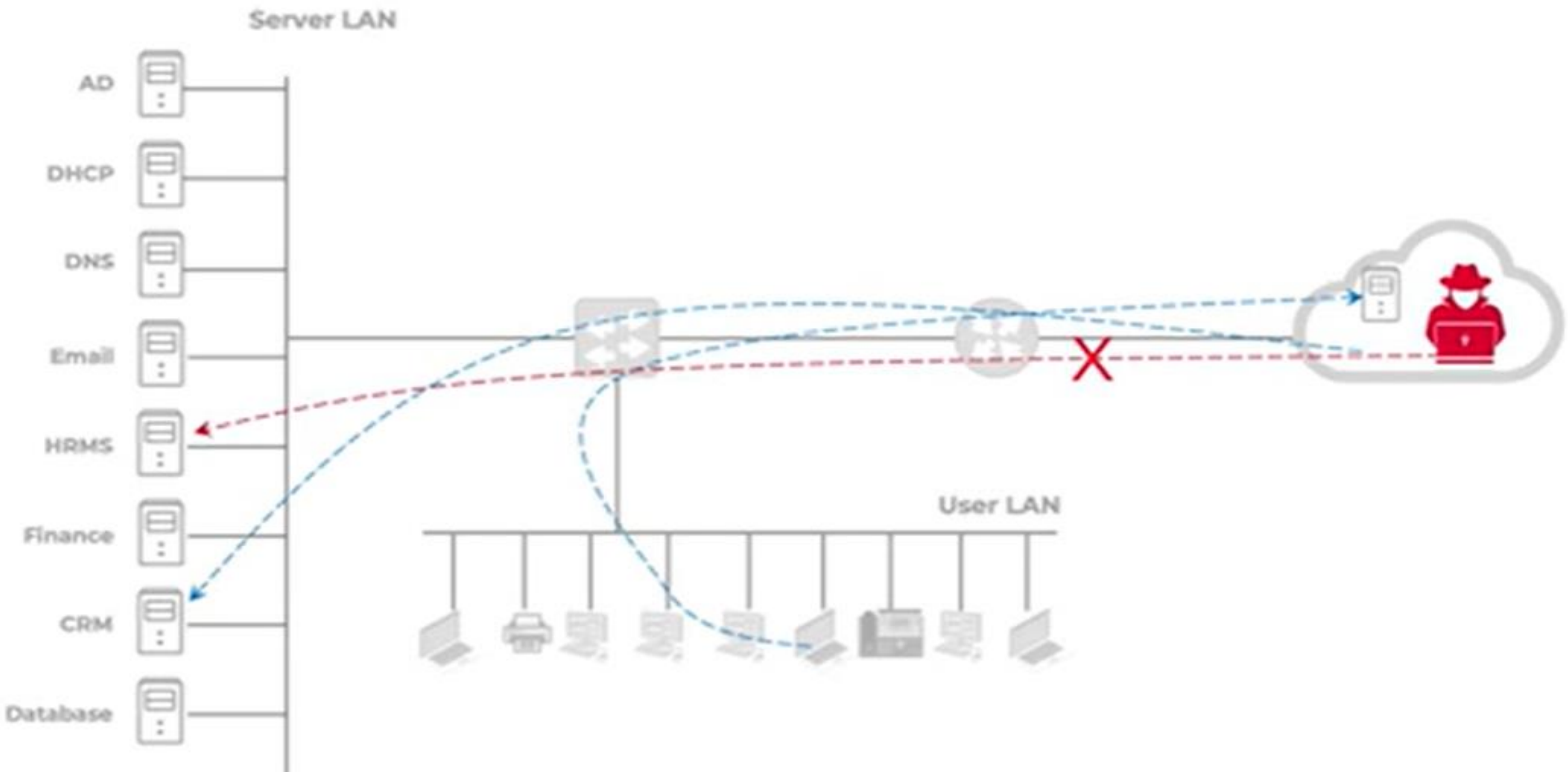
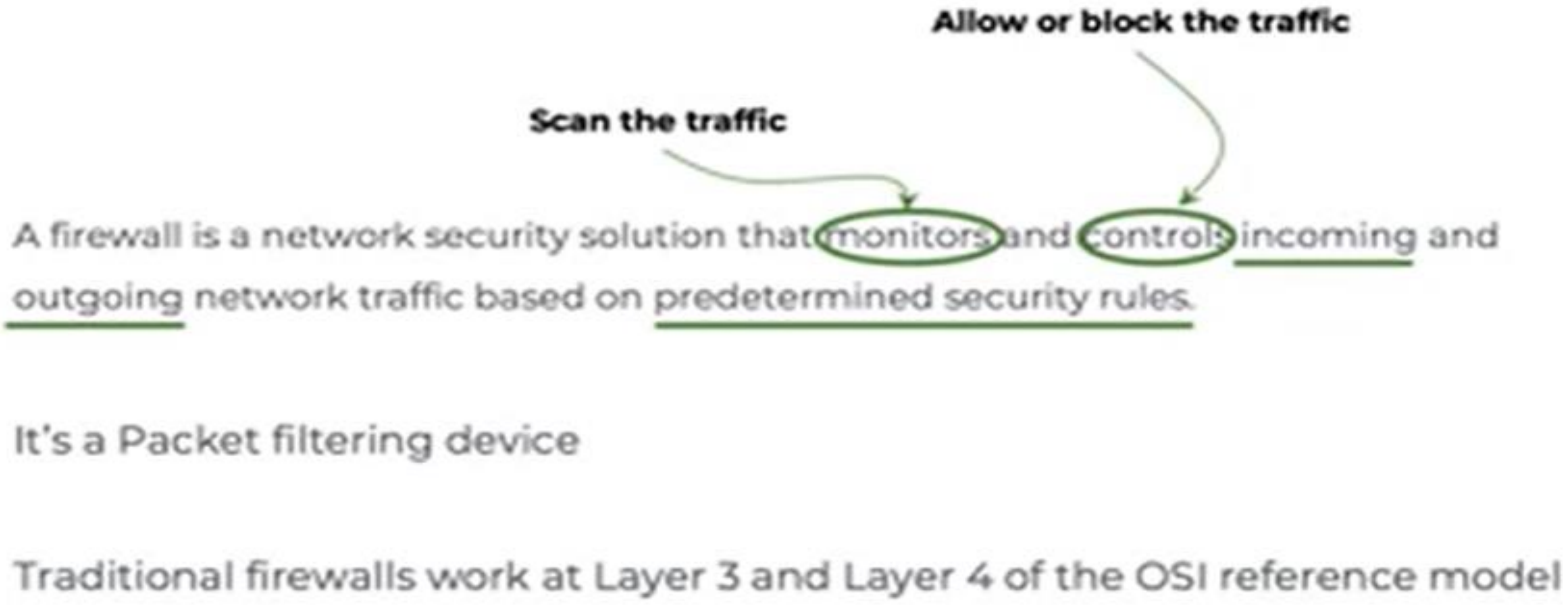
Firewall


Server LAN
AD
DHCP
DNS
Email
HRMS
Finance
CRM
Database
User LAN

What is a Firewall?



Allow or block the traffic

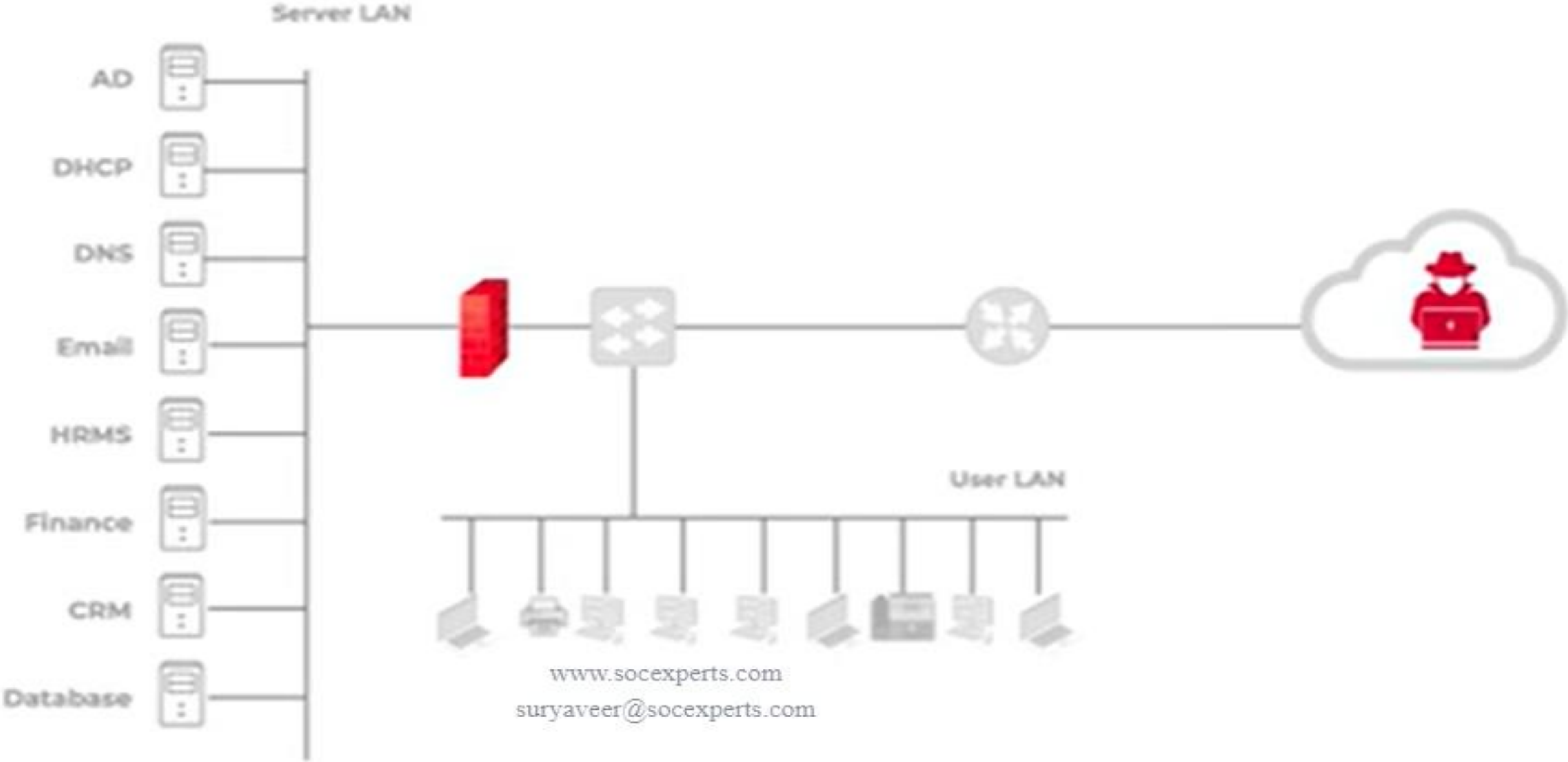
Scan the traffic

A firewall is a network security solution that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

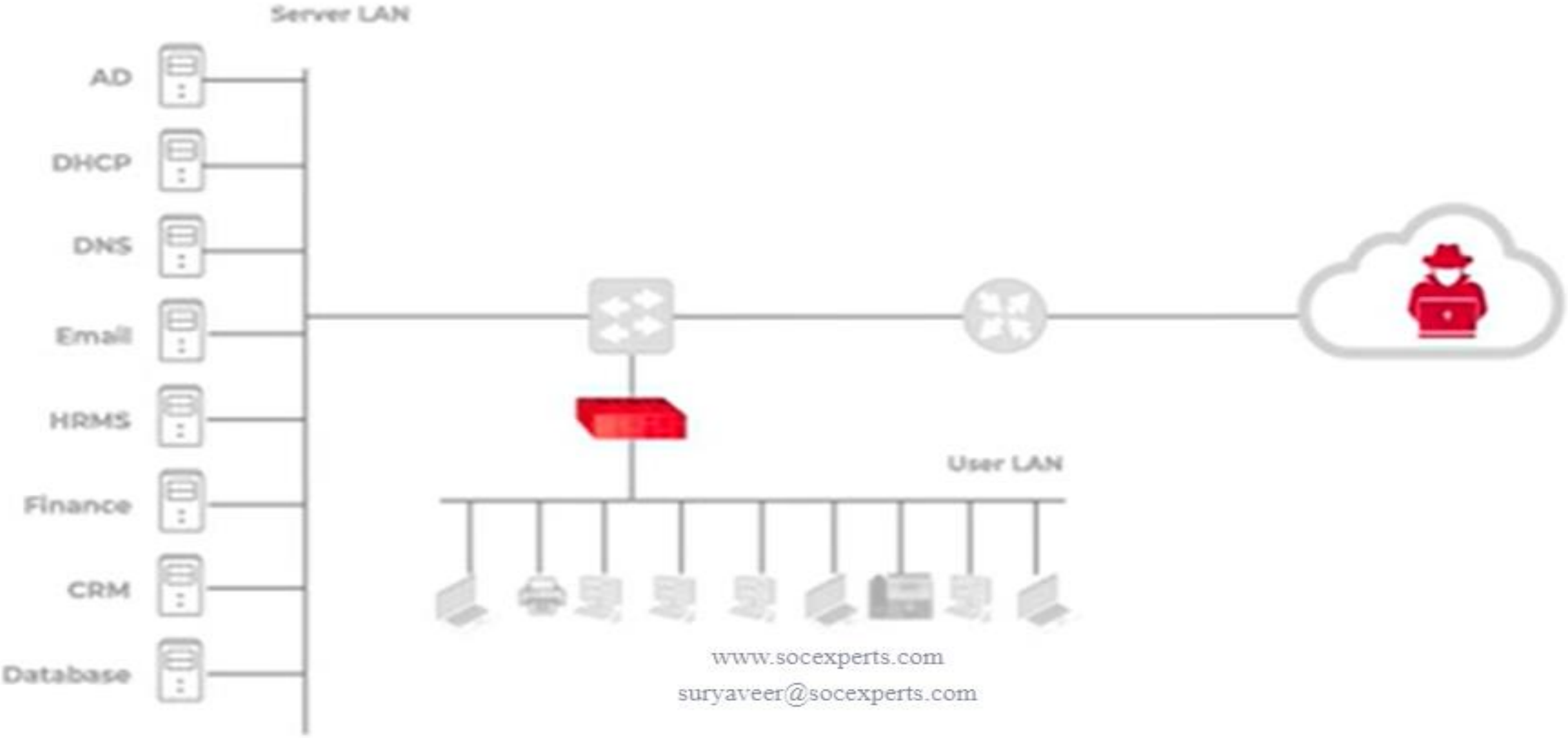
It's a Packet filtering device

Traditional firewalls work at Layer 3 and Layer 4 of the OSI reference model

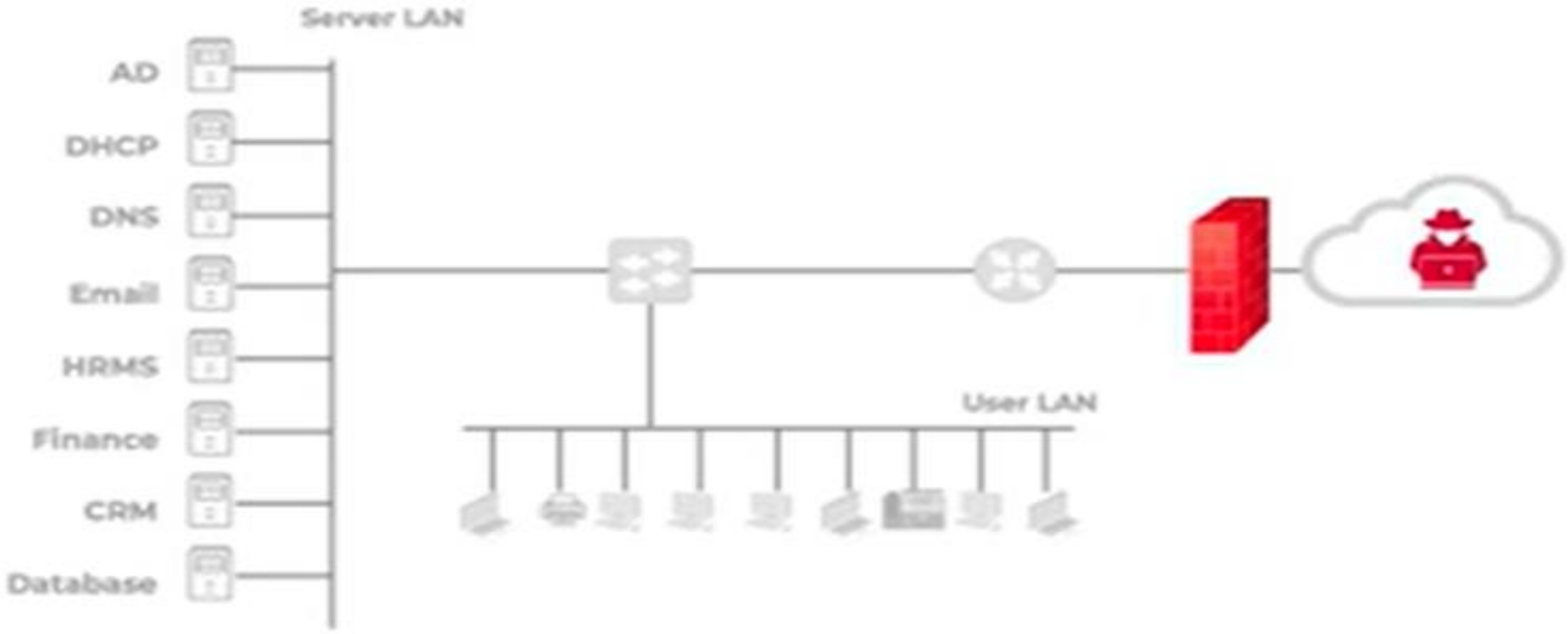
Firewall Placement



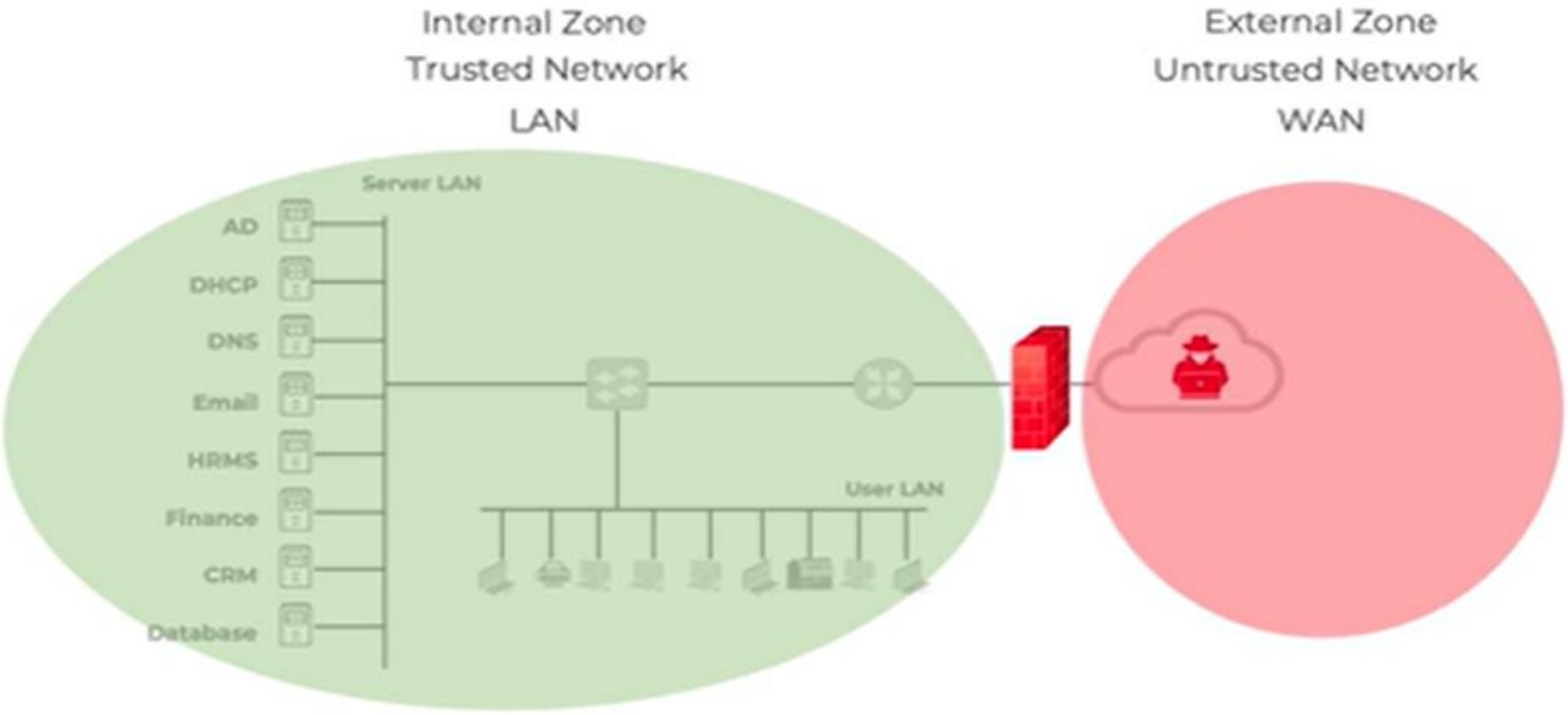
Firewall Placement



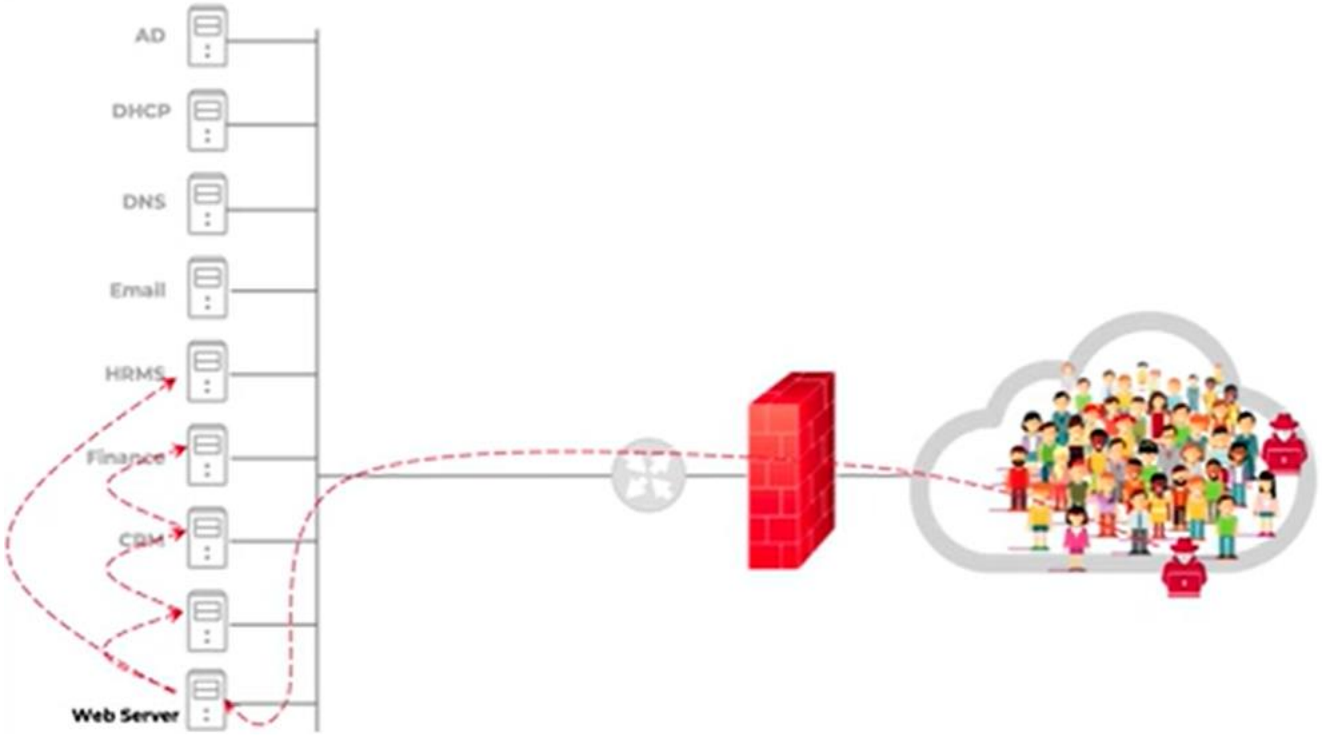
Firewall Placement



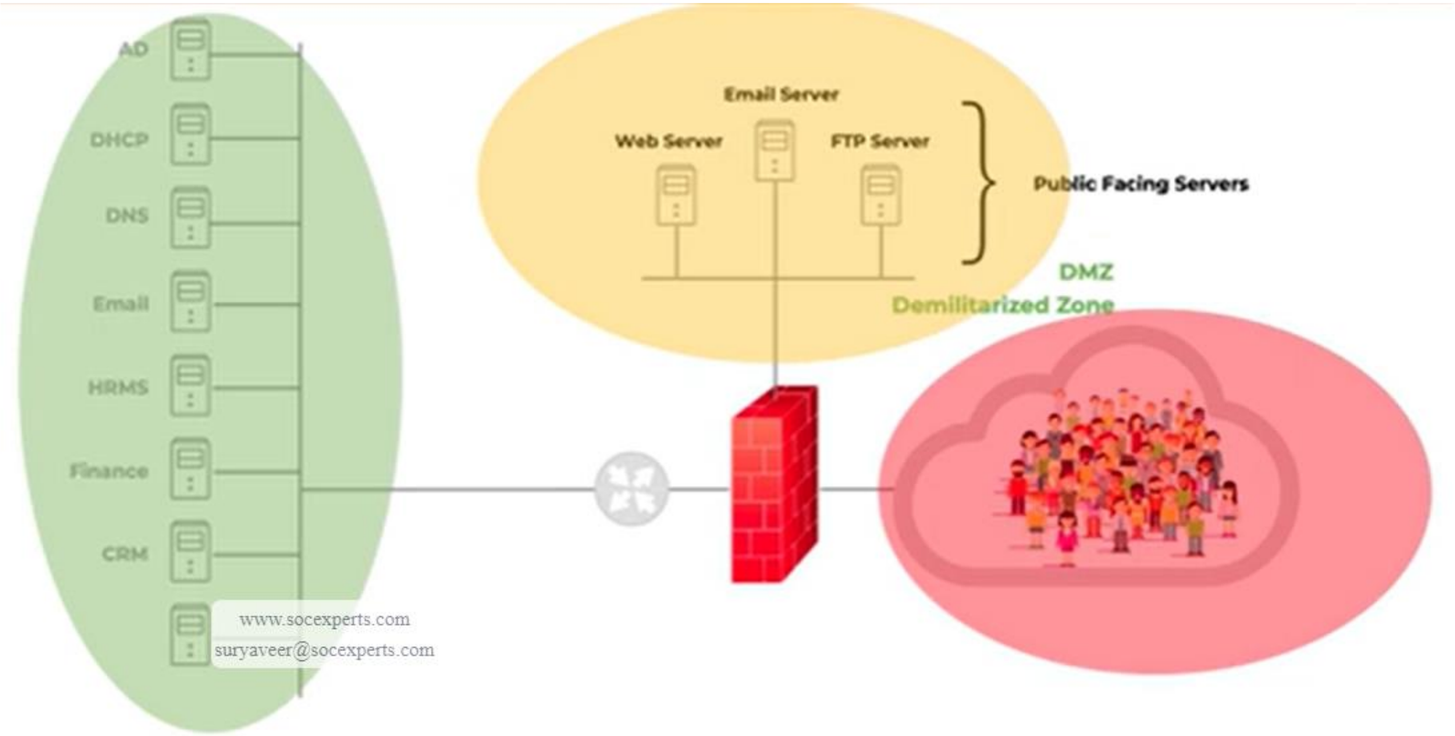
Firewall Zones



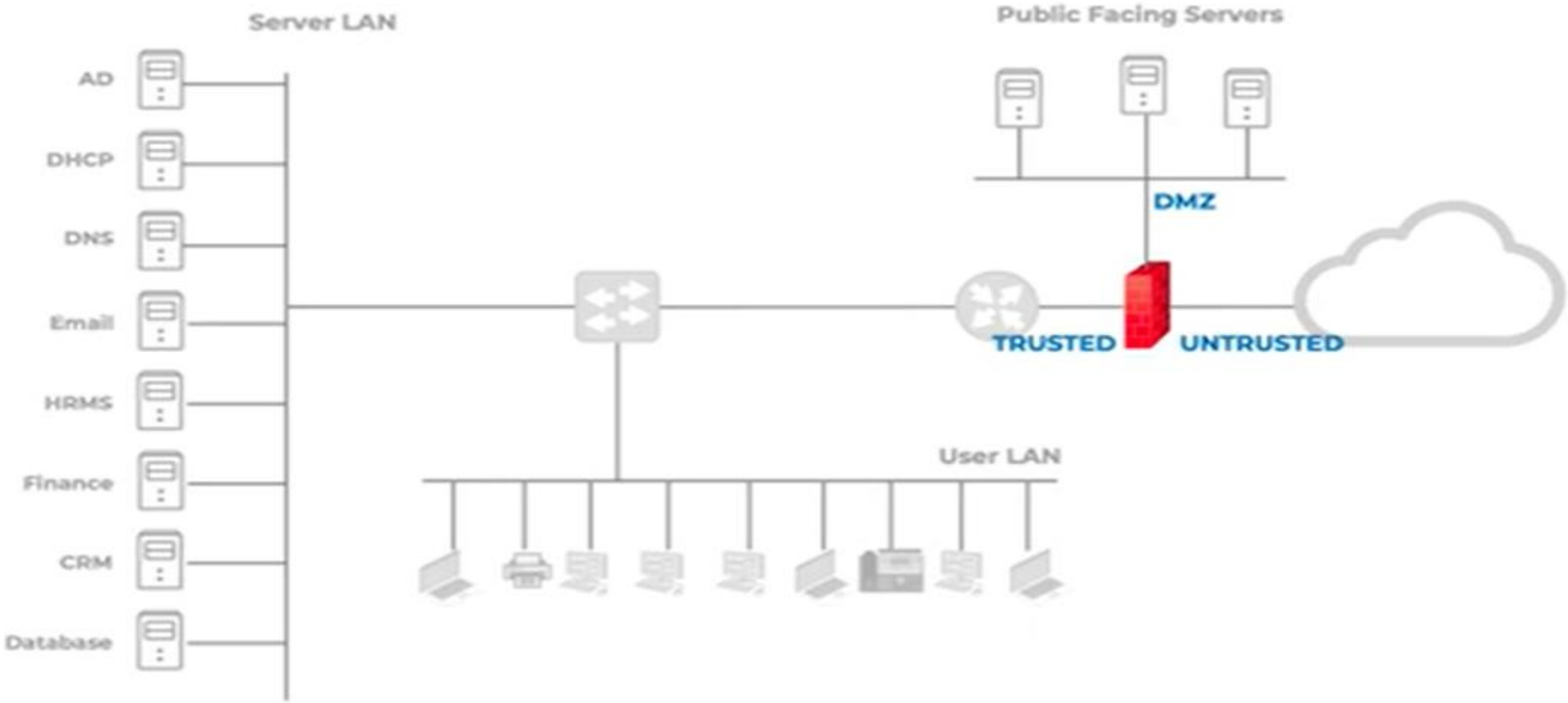
Without DMZ



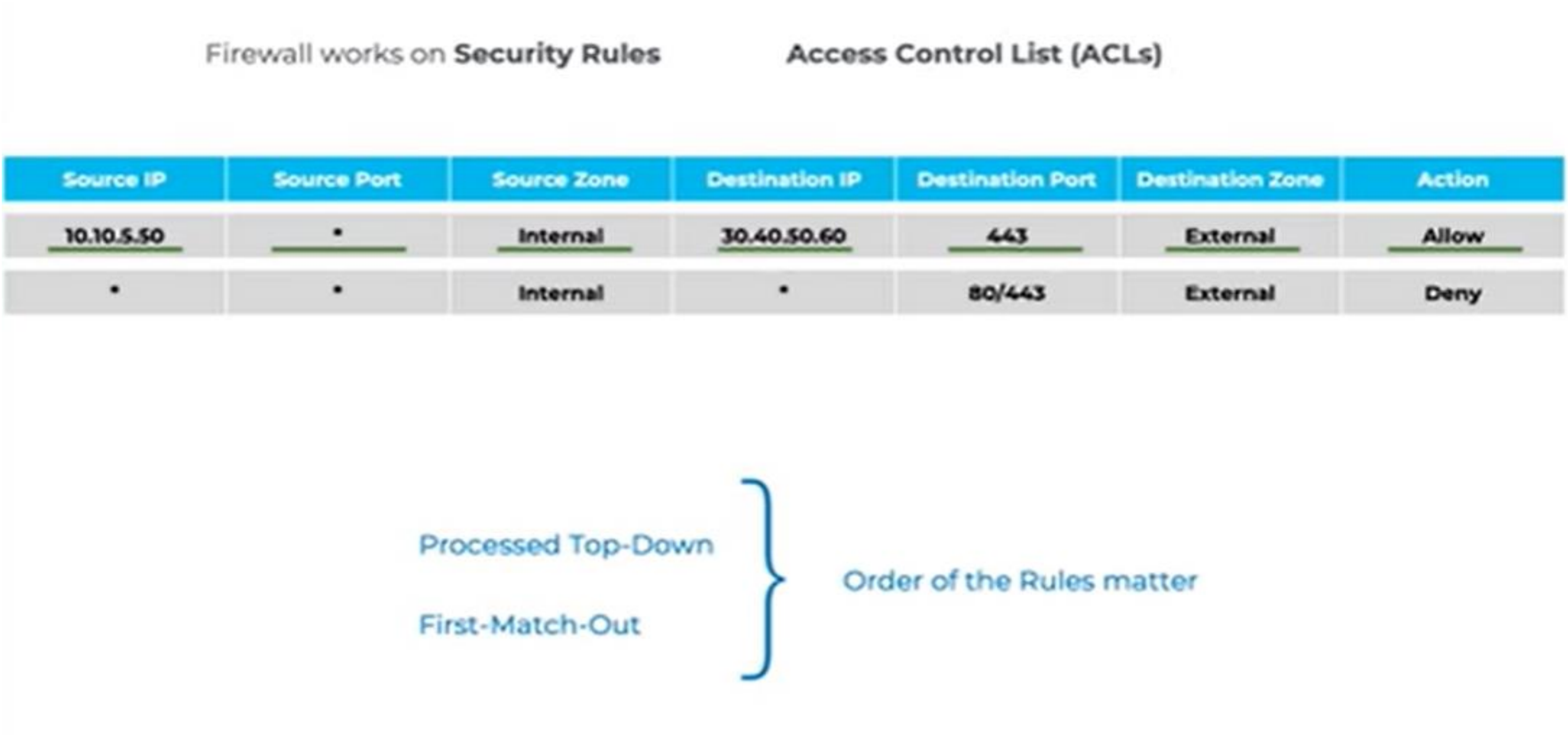
With DMZ


AD
DHCP
DNS
Email
HRMS
Finance
CRM
Email Server
Web Server
FTP Server
Public Facing Servers
DMZ
Demilitarized Zone

Final Network



How Does Firewall Work?



Firewall works on **Security Rules**

Access Control List (ACLs)

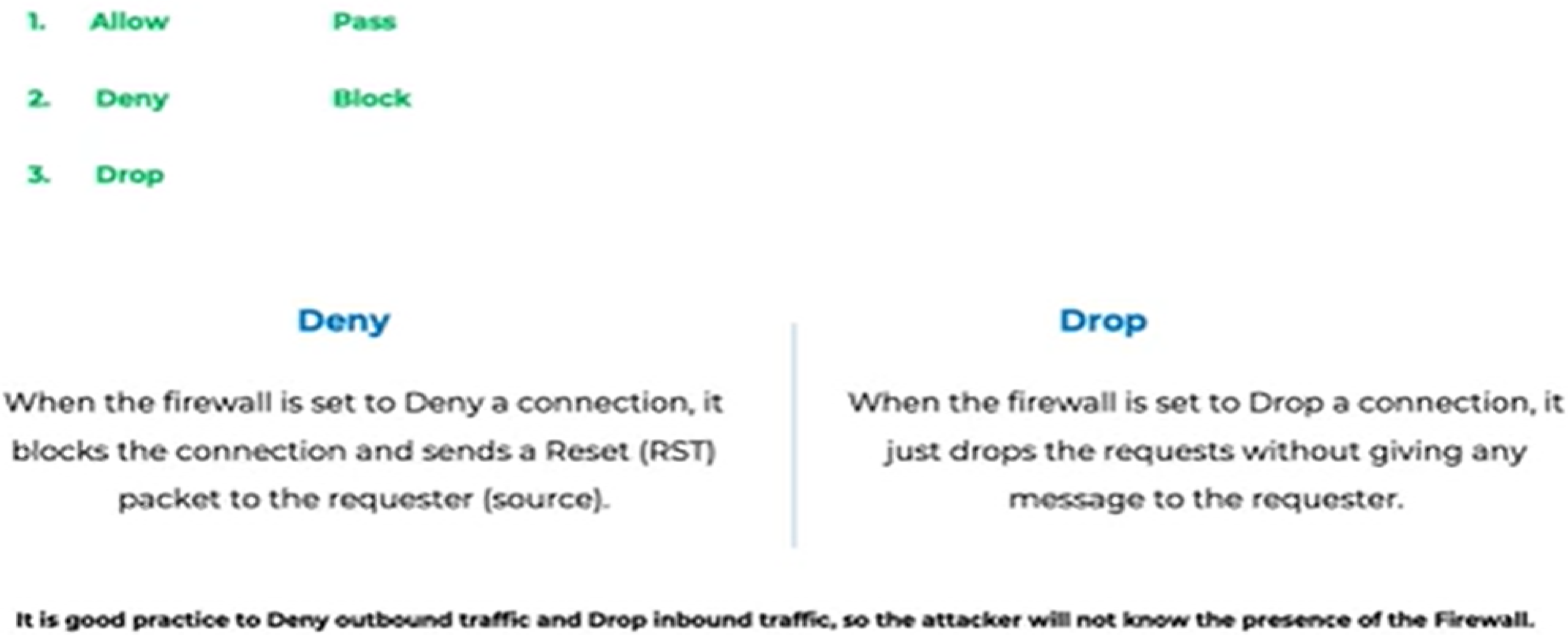
Source IP	Source Port	Source Zone	Destination IP	Destination Port	Destination Zone	Action
10.10.5.50	*	Internal	30.40.50.60	443	External	Allow
*	*	Internal	*	80/443	External	Deny

Processed Top-Down

First-Match-Out

Order of the Rules matter

Firewall Actions



1. Allow Pass
2. Deny Block
3. Drop

Deny

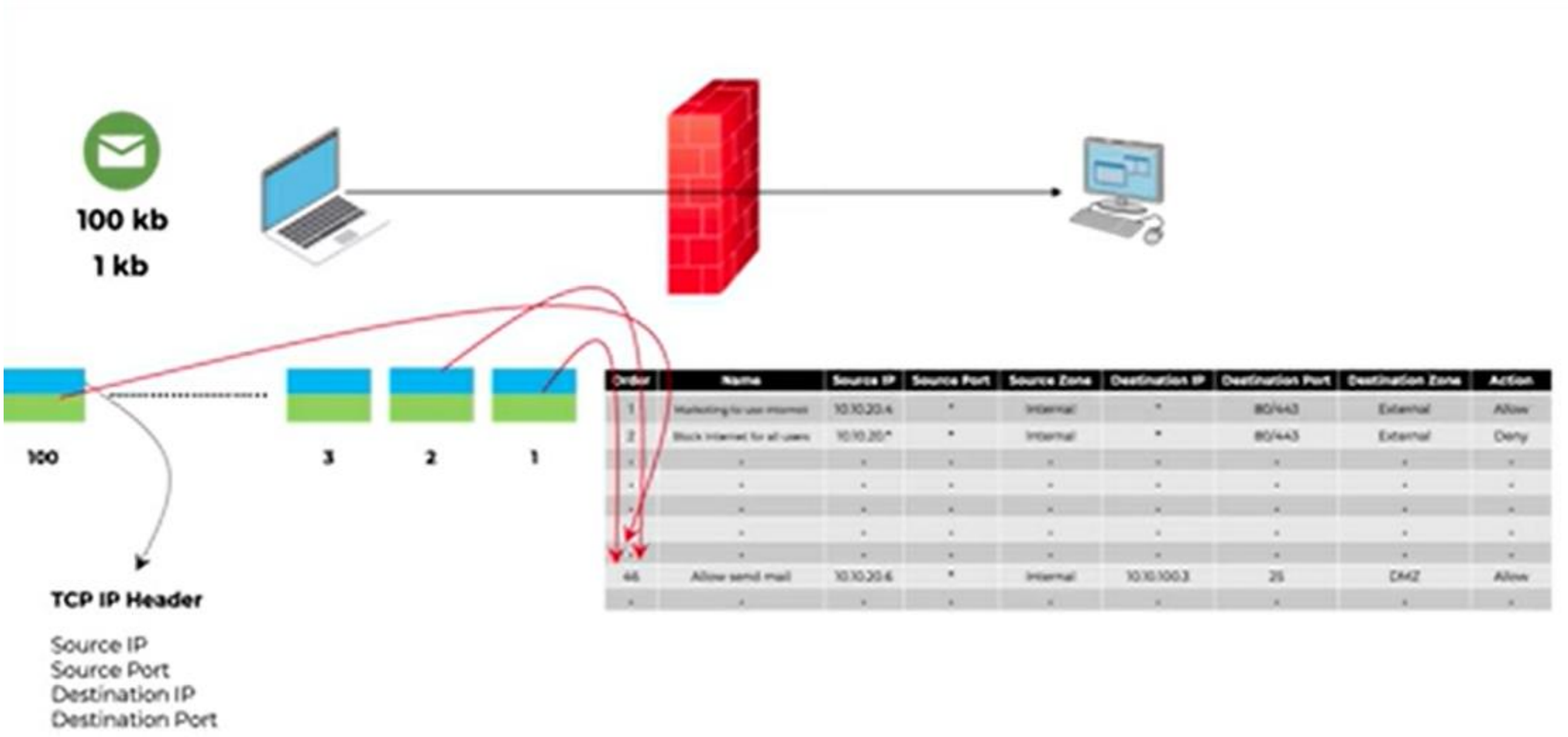
When the firewall is set to Deny a connection, it blocks the connection and sends a Reset (RST) packet to the requester (source).

Drop

When the firewall is set to Drop a connection, it just drops the requests without giving any message to the requester.

It is good practice to Deny outbound traffic and Drop inbound traffic, so the attacker will not know the presence of the Firewall.

Stateful Inspection

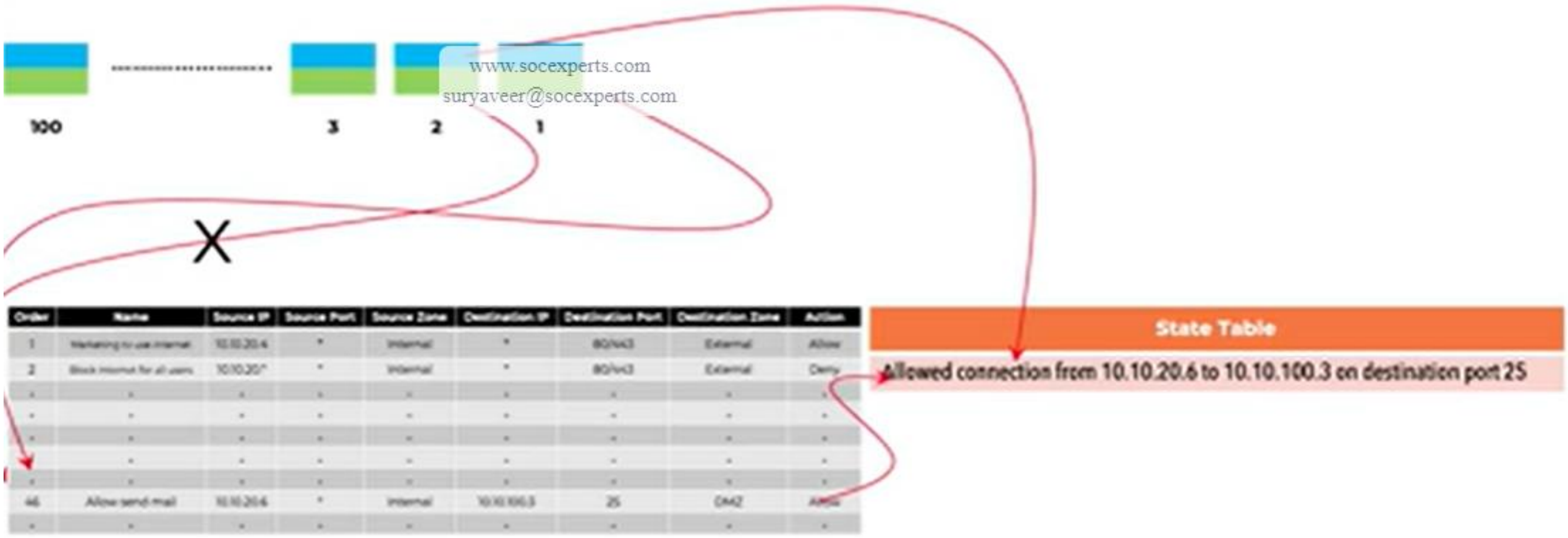


Order	Name	Source IP	Source Port	Source Zone	Destination IP	Destination Port	Destination Zone	Action
1	Marketing to use internet	10.10.20.4	*	Internal	*	80/443	External	Allow
2	Block internet for all users	10.10.20.*	*	Internal	*	80/443	External	Deny
·	·	·	·	·	·	·	·	·
·	·	·	·	·	·	·	·	·
·	·	·	·	·	·	·	·	·
·	·	·	·	·	·	·	·	·
·	·	·	·	·	·	·	·	·
46	Allow send mail	10.10.20.6	*	Internal	10.10.100.3	25	DMZ	Allow
·	·	·	·	·	·	·	·	·

TCP IP Header

Source IP
Source Port
Destination IP
Destination Port

Stateful Inspection



Order	Name	Source IP	Source Port	Source Zone	Destination IP	Destination Port	Destination Zone	Action
1	Marketing to use internet	10.10.20.6	*	Internal	*	80/443	External	Allow
2	Block internet for all users	10.10.20.*	*	Internal	*	80/443	External	Deny
·	·	·	·	·	·	·	·	·
·	·	·	·	·	·	·	·	·
·	·	·	·	·	·	·	·	·
	·	·	·	·	·	·	·	·
·	·	·	·	·	·	·	·	·
46	Allow send mail	10.10.20.6	*	Internal	10.10.100.3	25	DMZ	Allow
·	·	·	·	·	·	·	·	·

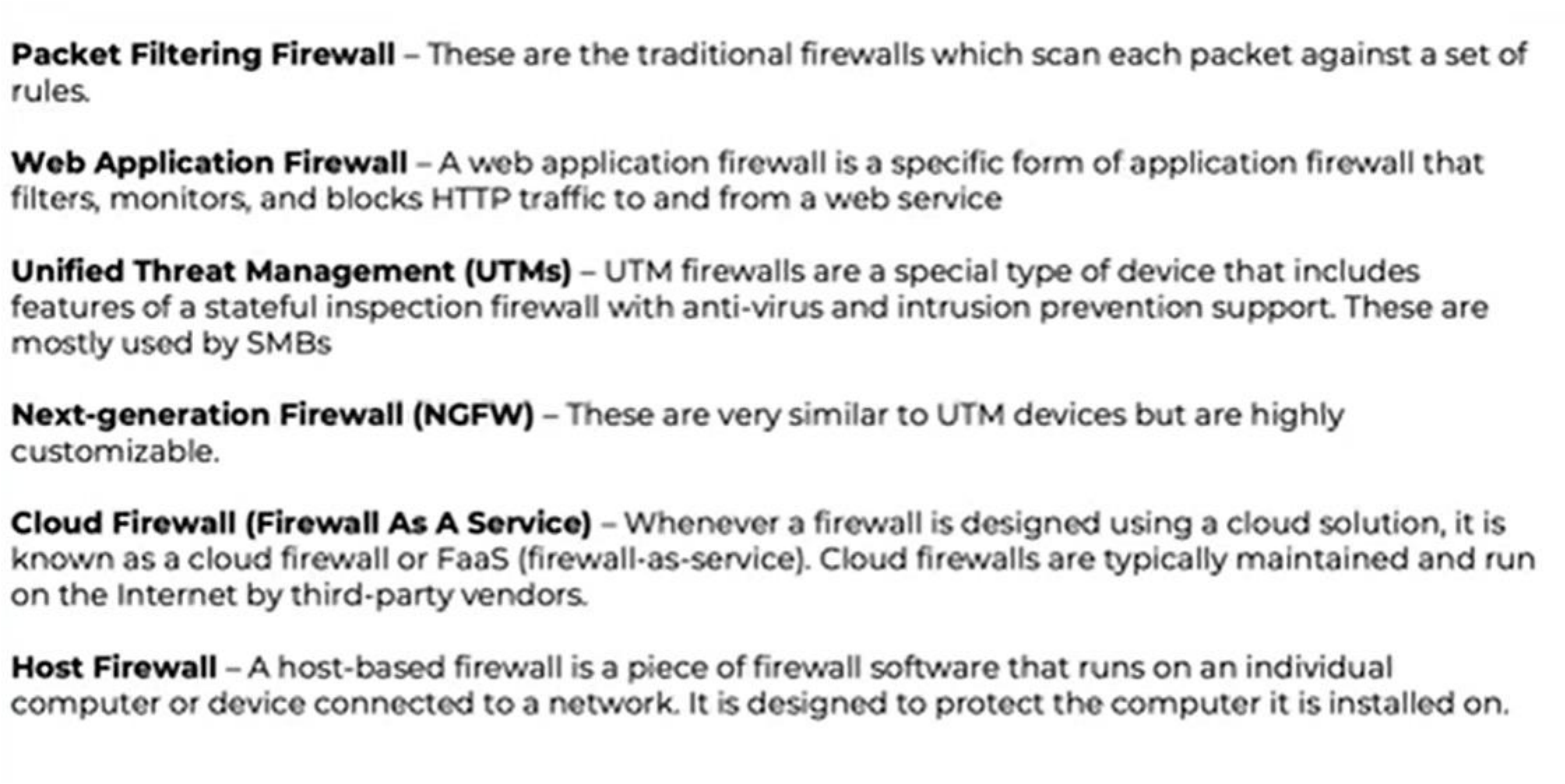
State Table
Allowed connection from 10.10.20.6 to 10.10.100.3 on destination port 25

or any allowed connection firewall will not process the rules after the first packet.

he connection will be removed form the state table for 2 reasons

- Once the firewall processes the **FIN** (end of connection)
- When the firewall sees a **RST** (connection is interrupted)

Types of Firewall



Packet Filtering Firewall – These are the traditional firewalls which scan each packet against a set of rules.

Web Application Firewall – A web application firewall is a specific form of application firewall that filters, monitors, and blocks HTTP traffic to and from a web service

Unified Threat Management (UTMs) – UTM firewalls are a special type of device that includes features of a stateful inspection firewall with anti-virus and intrusion prevention support. These are mostly used by SMBs

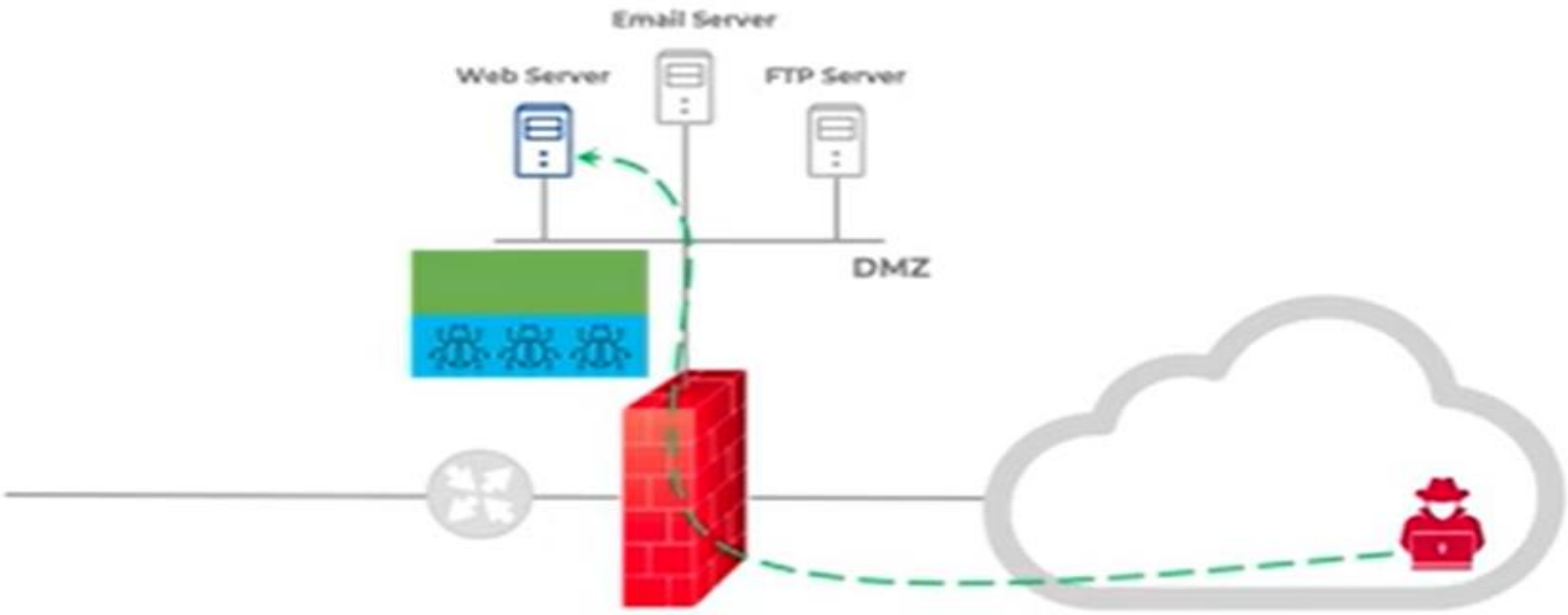
Next-generation Firewall (NGFW) – These are very similar to UTM devices but are highly customizable.

Cloud Firewall (Firewall As A Service) – Whenever a firewall is designed using a cloud solution, it is known as a cloud firewall or FaaS (firewall-as-service). Cloud firewalls are typically maintained and run on the Internet by third-party vendors.

Host Firewall – A host-based firewall is a piece of firewall software that runs on an individual computer or device connected to a network. It is designed to protect the computer it is installed on.

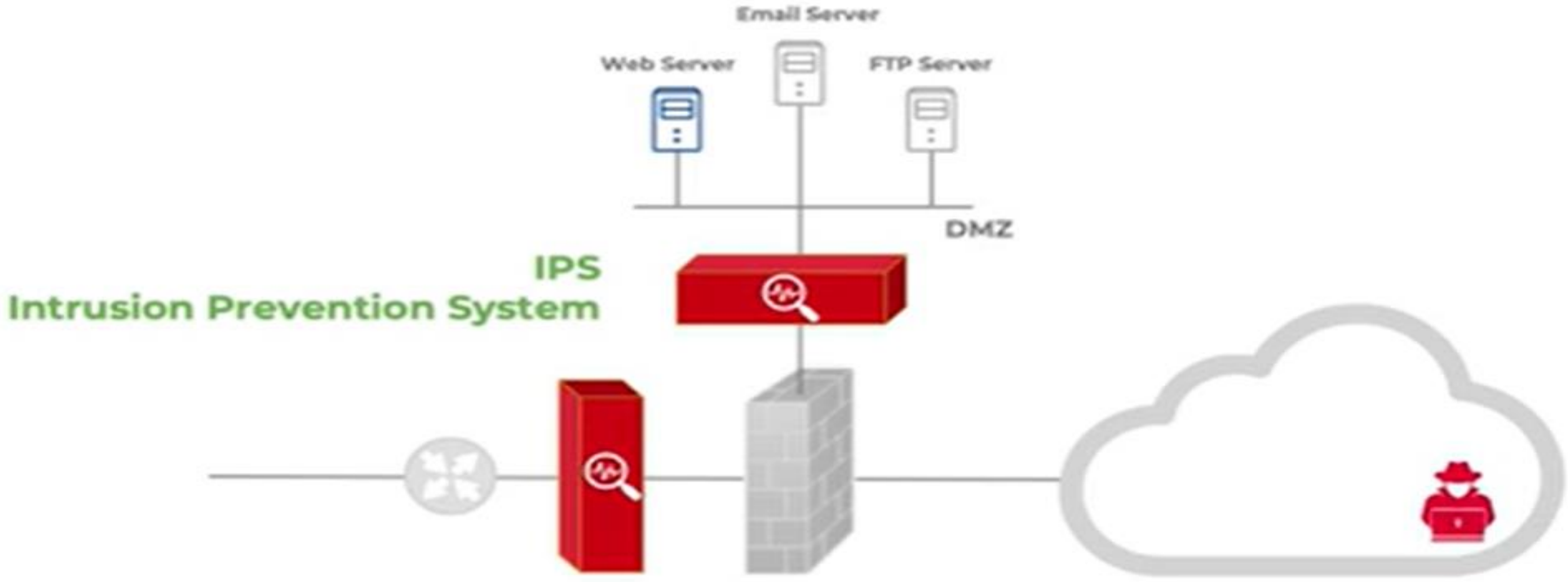
IPS

Firewall Limitation



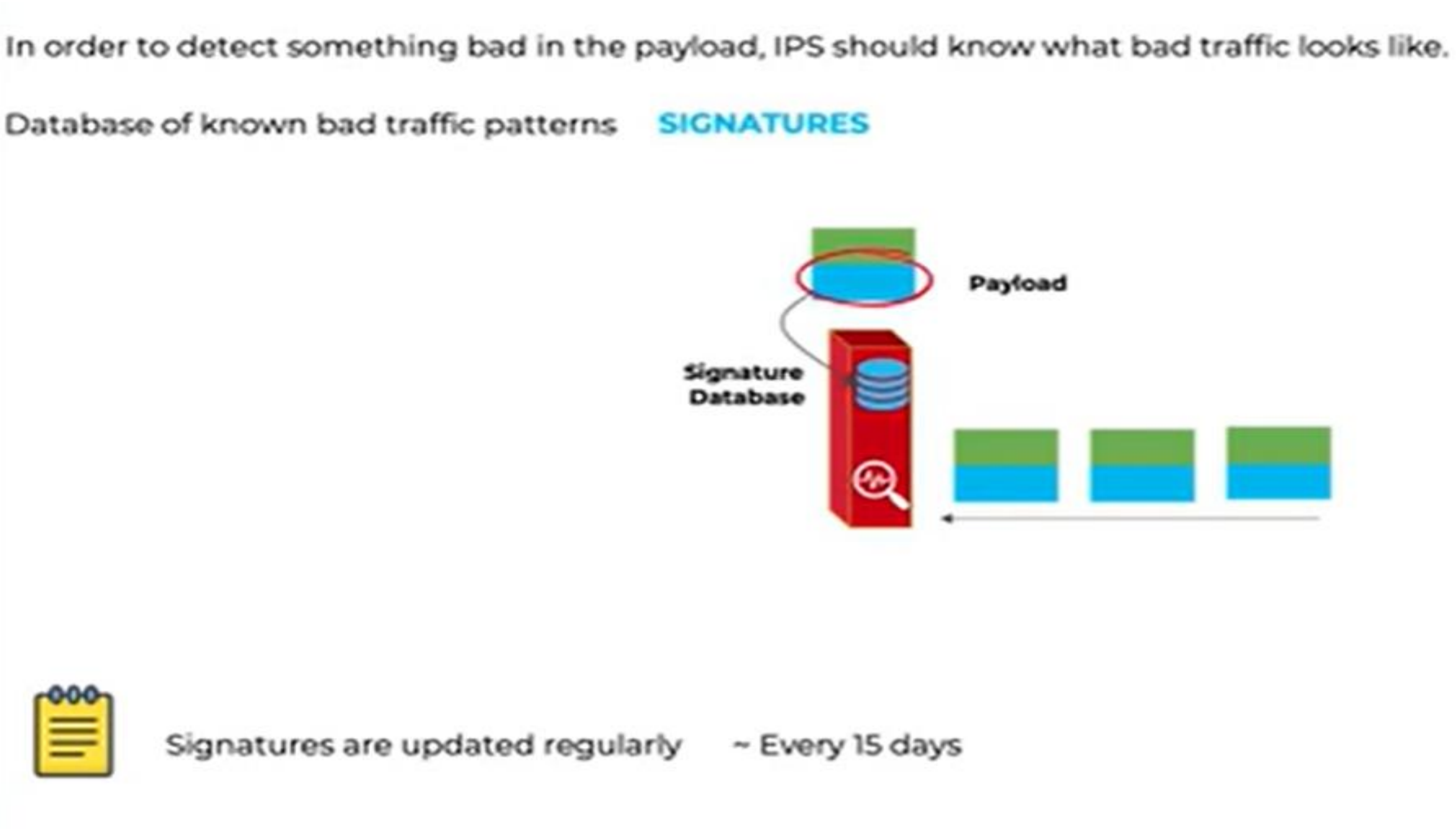
Source IP – Any
Source Port - Any
Destination IP – 50.60.70.80 (Public IP of Web Server)
Destination Port – 443
Allow

IPS



Deep Packet Inspection

How IPS Works?

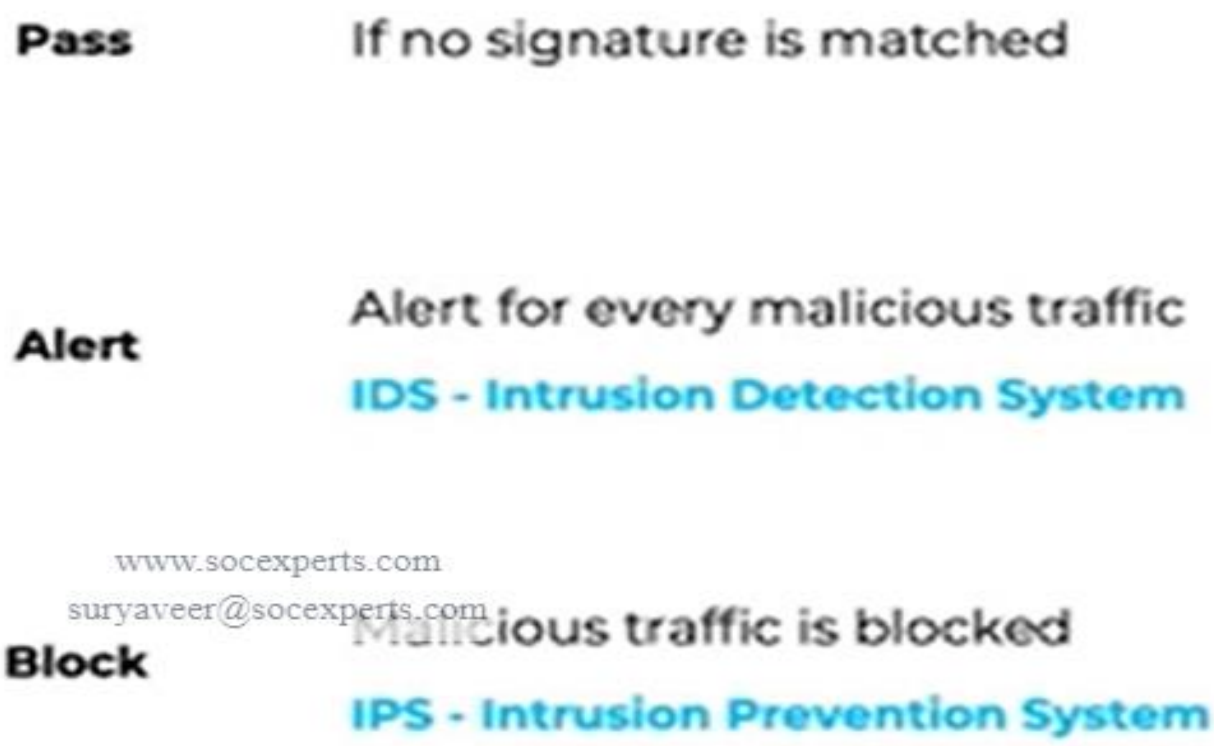


In order to detect something bad in the payload, IPS should know what bad traffic looks like.

Database of known bad traffic patterns SIGNATURES

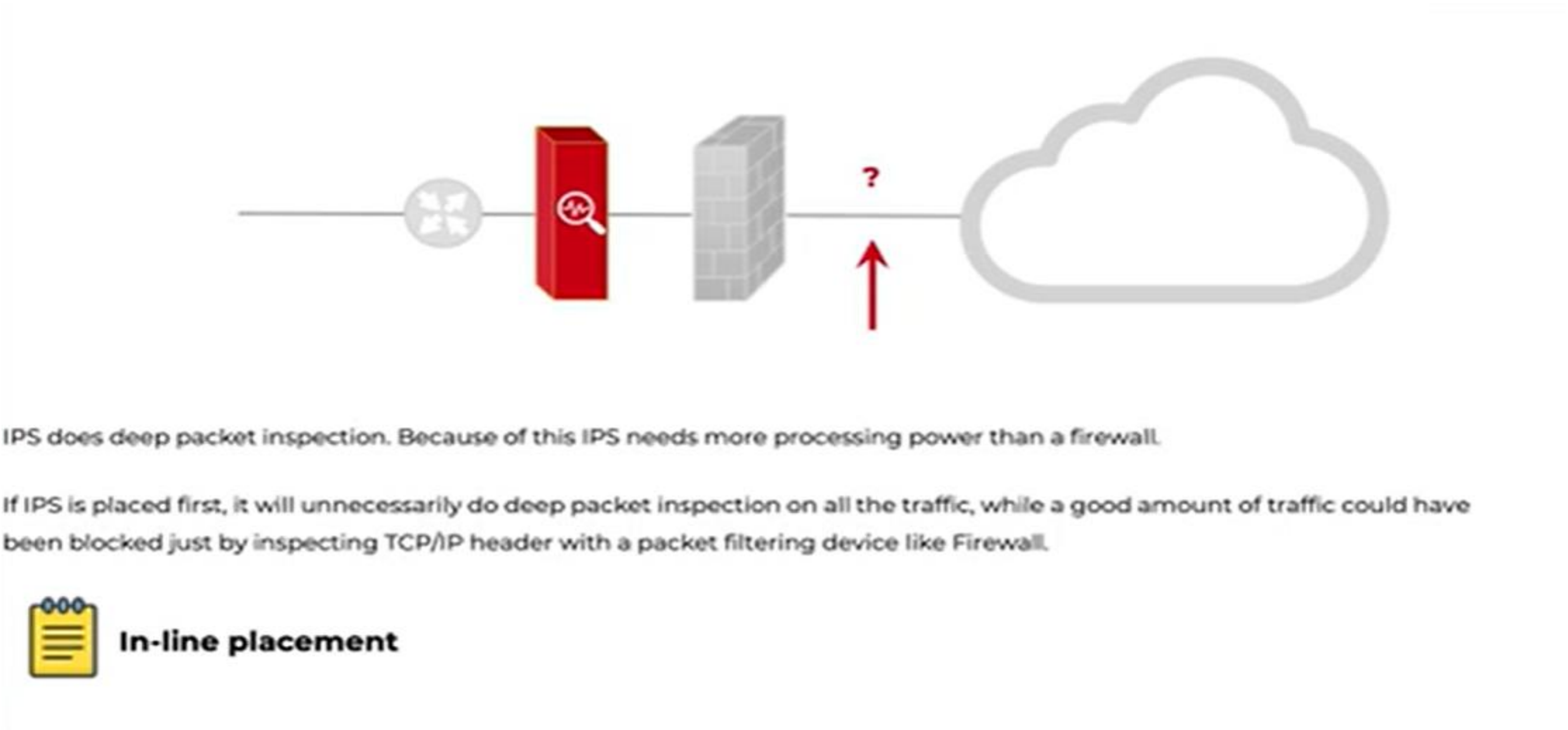
Signatures are updated regularly ~ Every 15 days

IPS Actions



Pass	If no signature is matched
Alert	Alert for every malicious traffic IDS - Intrusion Detection System
Block	Malicious traffic is blocked IPS - Intrusion Prevention System

IPS Placement

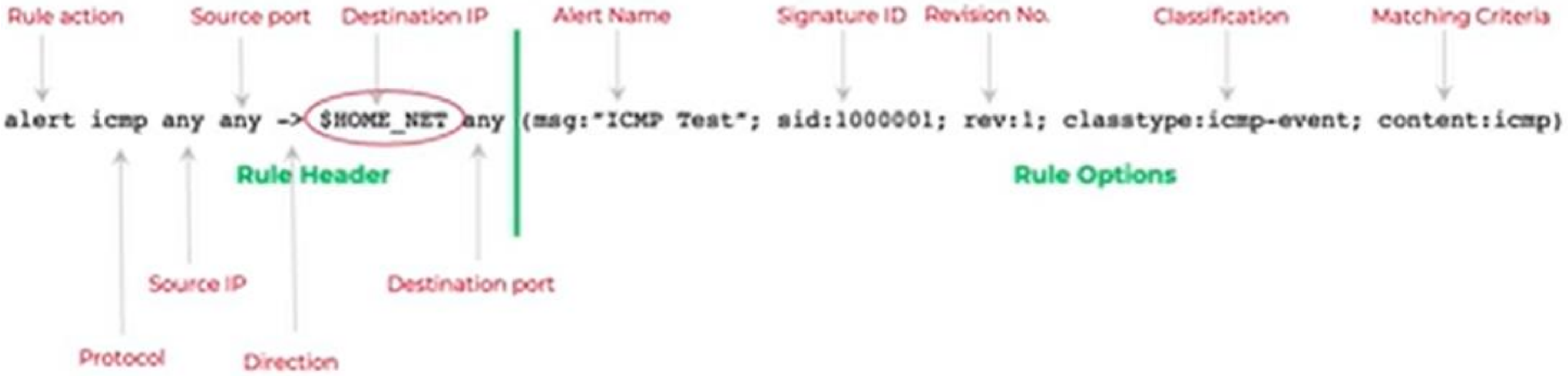


IPS does deep packet inspection. Because of this IPS needs more processing power than a firewall.

If IPS is placed first, it will unnecessarily do deep packet inspection on all the traffic, while a good amount of traffic could have been blocked just by inspecting TCP/IP header with a packet filtering device like Firewall.

In-line placement

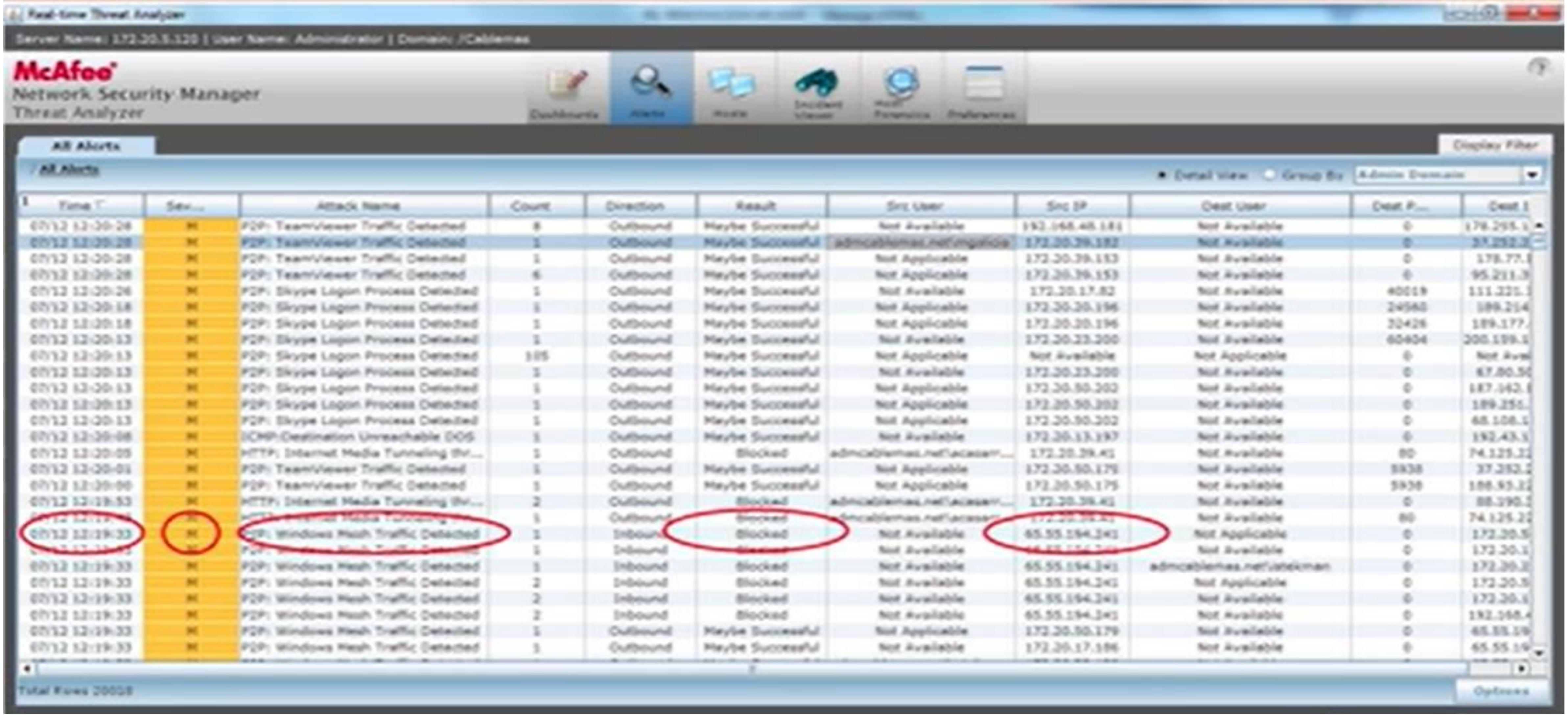
IPS Signature



```
alert icmp any any -> $HOME_NET any (msg:"ICMP Test"; sid:1000001; rev:1; classtype:icmp-event; content:icmp)
```

SNORT RULE STRUCTURE

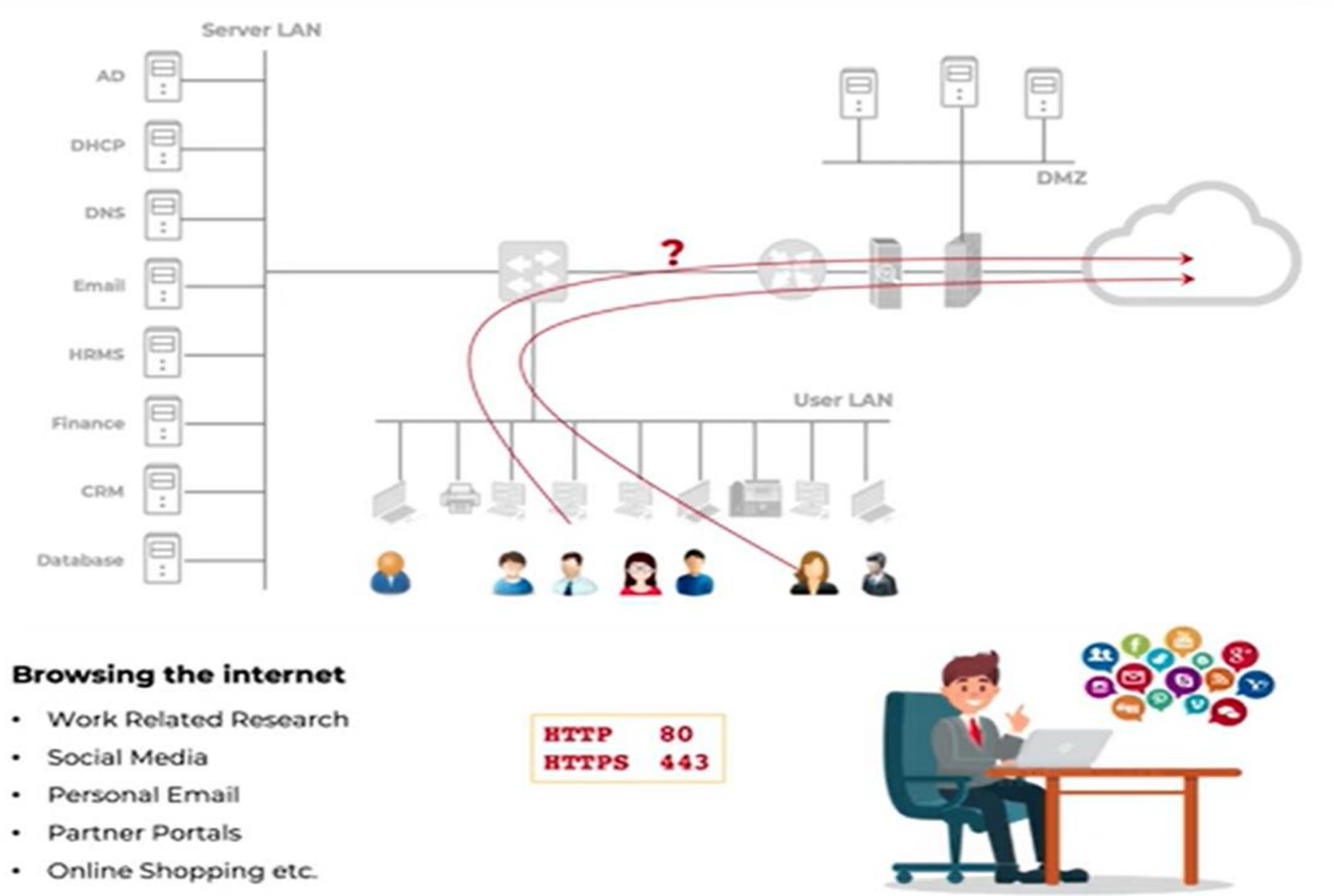
Sample Signature



Time	Sev...	Attack Name	Count	Direction	Result	Src User	Src IP	Dest User	Dest P...	Dest I
07/12 12:20:28	M	P2P: TeamViewer Traffic Detected	8	Outbound	Maybe Successful	Not Available	192.168.48.181	Not Available	0	178.255.1
07/12 12:20:28	M	P2P: TeamViewer Traffic Detected	1	Outbound	Maybe Successful	admcablemas.net\mgalicia	172.20.39.182	Not Available	0	37.252.2
07/12 12:20:28	M	P2P: TeamViewer Traffic Detected	1	Outbound	Maybe Successful	Not Applicable	172.20.39.153	Not Available	0	178.77.1
07/12 12:20:28	M	P2P: TeamViewer Traffic Detected	6	Outbound	Maybe Successful	Not Applicable	172.20.39.153	Not Available	0	95.211.3
07/12 12:20:26	M	P2P: Skype Logon Process Detected	1	Outbound	Maybe Successful	Not Available	172.20.17.82	Not Available	40019	111.221.1
07/12 12:20:18	M	P2P: Skype Logon Process Detected	1	Outbound	Maybe Successful	Not Applicable	172.20.20.196	Not Available	24560	189.214
07/12 12:20:18	M	P2P: Skype Logon Process Detected	1	Outbound	Maybe Successful	Not Applicable	172.20.20.196	Not Available	20426	189.177.
07/12 12:20:13	M	P2P: Skype Logon Process Detected	1	Outbound	Maybe Successful	Not Available	172.20.23.200	Not Available	60404	200.159.1
07/12 12:20:13	M	P2P: Skype Logon Process Detected	105	Outbound	Maybe Successful	Not Applicable	Not Available	Not Applicable	0	Not Ava
07/12 12:20:13	M	P2P: Skype Logon Process Detected	1	Outbound	Maybe Successful	Not Available	172.20.23.200	Not Available	0	67.80.5
07/12 12:20:13	M	P2P: Skype Logon Process Detected	1	Outbound	Maybe Successful	Not Applicable	172.20.50.202	Not Available	0	187.162.
07/12 12:20:13	M	P2P: Skype Logon Process Detected	1	Outbound	Maybe Successful	Not Applicable	172.20.50.202	Not Available	0	189.251.
07/12 12:20:13	M	P2P: Skype Logon Process Detected	1	Outbound	Maybe Successful	Not Applicable	172.20.50.202	Not Available	0	68.108.1
07/12 12:20:08	M	ICMP:Destination Unreachable DOS	1	Outbound	Maybe Successful	Not Available	172.20.13.197	Not Available	0	192.43.1
07/12 12:20:05	M	HTTP: Internet Media Tunneling thr...	1	Outbound	Blocked	admcablemas.net\acasar...	172.20.39.41	Not Available	80	74.125.22
07/12 12:20:01	M	P2P: TeamViewer Traffic Detected	1	Outbound	Maybe Successful	Not Applicable	172.20.50.175	Not Available	5938	37.252.2
07/12 12:20:00	M	P2P: TeamViewer Traffic Detected	1	Outbound	Maybe Successful	Not Applicable	172.20.50.175	Not Available	5938	188.93.12
07/12 12:19:53	M	HTTP: Internet Media Tunneling thr...	2	Outbound	Blocked	admcablemas.net\acasar...	172.20.39.41	Not Available	0	88.190.5
[illegible]	M	HTTP: Internet Media Tunneling	1	Outbound	Blocked	admcablemas.net\acasar...	172.20.39.41	Not Available	80	74.125.22
07/12 12:19:33	M	P2P: Windows Mesh Traffic Detected	1	Inbound	Blocked	Not Available	65.55.194.241	Not Applicable	0	172.20.5
[illegible]	M	P2P: Windows Mesh Traffic Detected	1	Inbound	Blocked	Not Available	65.55.194.241	Not Available	0	172.20.1
07/12 12:19:33	M	P2P: Windows Mesh Traffic Detected	1	Inbound	Blocked	Not Available	65.55.194.241	admcablemas.net\atekman	0	172.20.2
07/12 12:19:33	M	P2P: Windows Mesh Traffic Detected	2	Inbound	Blocked	Not Available	65.55.194.241	Not Applicable	0	172.20.5
07/12 12:19:33	M	P2P: Windows Mesh Traffic Detected	2	Inbound	Blocked	Not Available	65.55.194.241	Not Available	0	172.20.1
07/12 12:19:33	M	P2P: Windows Mesh Traffic Detected	2	Inbound	Blocked	Not Available	65.55.194.241	Not Available	0	192.168.4
07/12 12:19:33	M	P2P: Windows Mesh Traffic Detected	1	Outbound	Maybe Successful	Not Applicable	172.20.50.179	Not Available	0	65.55.19
07/12 12:19:33	M	P2P: Windows Mesh Traffic Detected	1	Outbound	Maybe Successful	Not Available	172.20.17.186	Not Available	0	65.55.19

WEB GATEWAY

Why Users visits Internet?

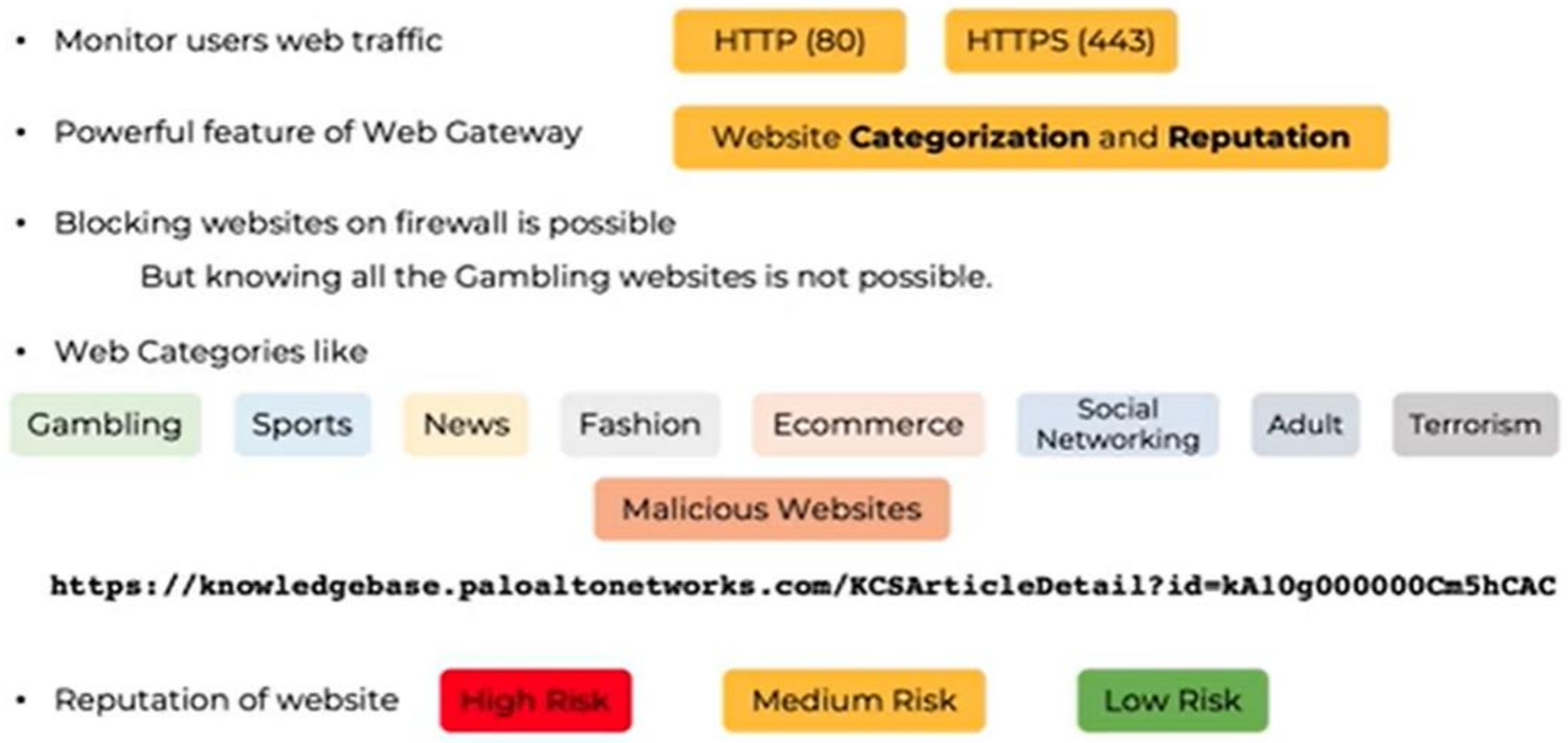


Browsing the internet

- Work Related Research
- Social Media
- Personal Email
- Partner Portals
- Online Shopping etc.

```
HTTP    80
HTTPS   443
```

Web Gateway Features



- Monitor users web traffic

HTTP (80) HTTPS (443)

- Powerful feature of Web Gateway

Website **Categorization** and **Reputation**

- Blocking websites on firewall is possible

    But knowing all the Gambling websites is not possible.

- Web Categories like

Gambling Sports News Fashion Ecommerce Social Networking Adult Terrorism

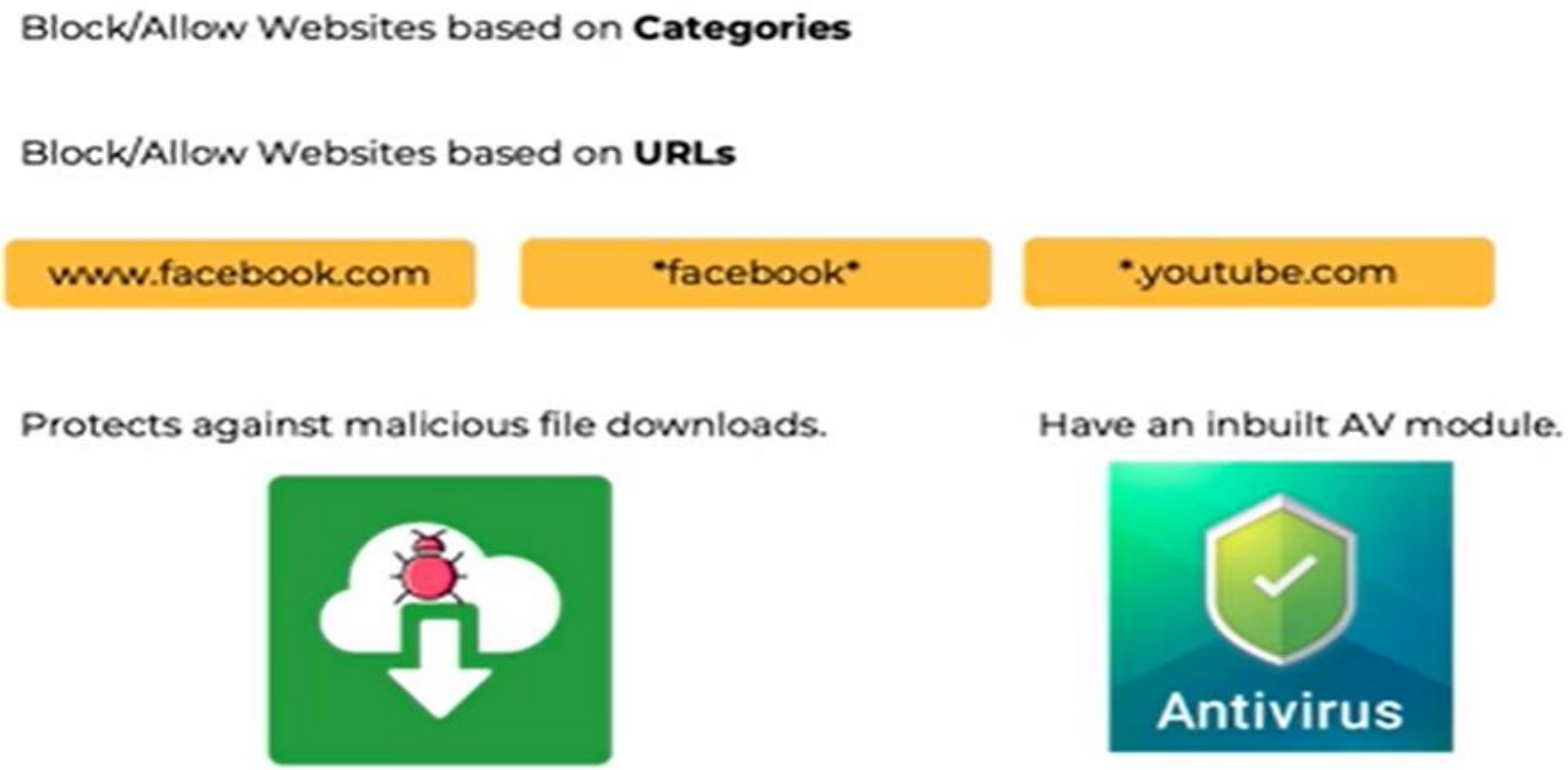
Malicious Websites

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm5hCAC

- Reputation of website

High Risk Medium Risk Low Risk

Web Gateway Features



Block/Allow Websites based on **Categories**

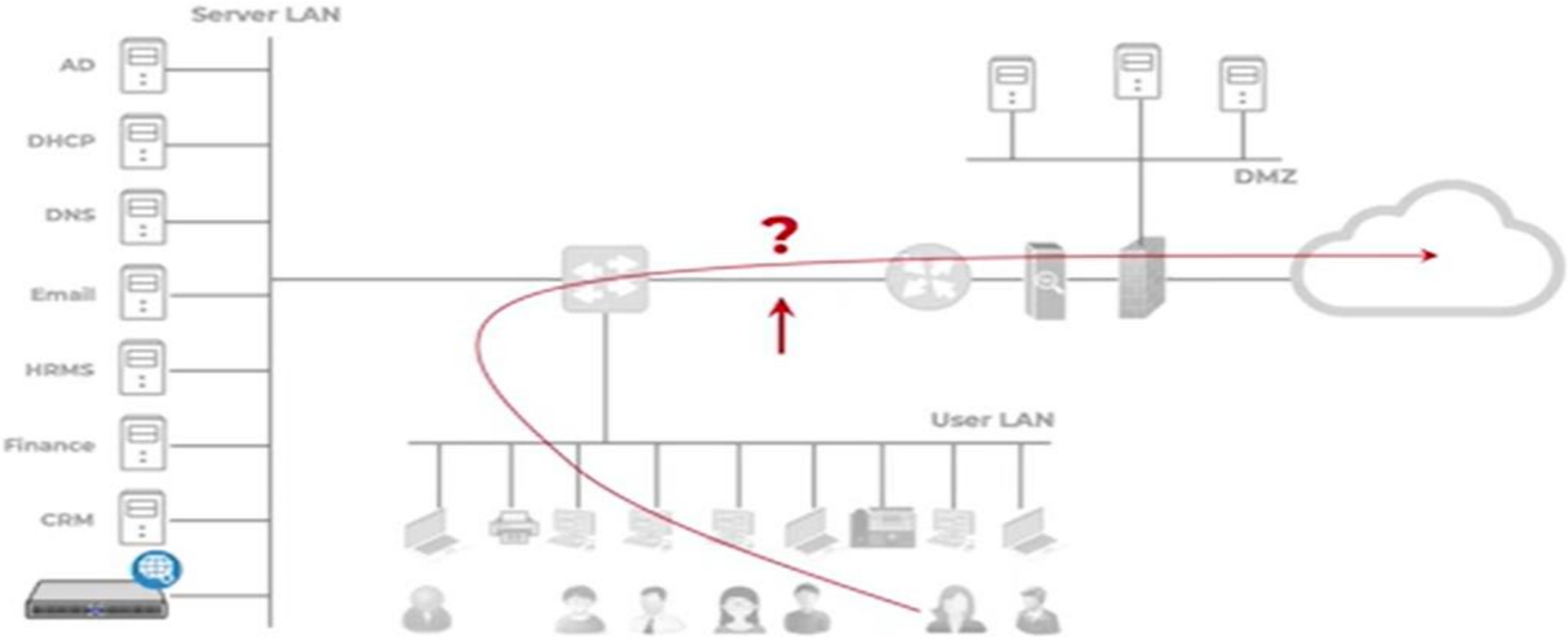
Block/Allow Websites based on **URLs**

www.facebook.com | *facebook* | *.youtube.com

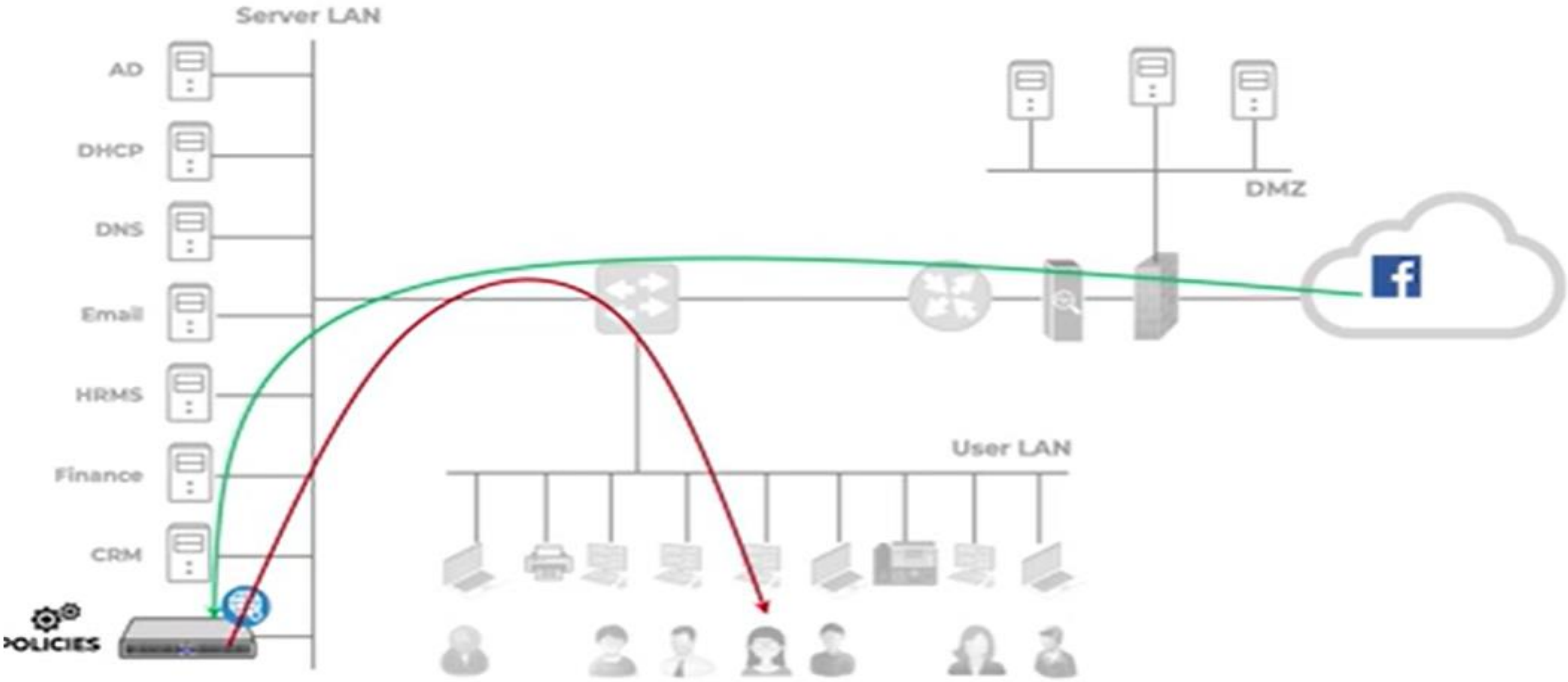
Protects against malicious file downloads.

Have an inbuilt AV module.

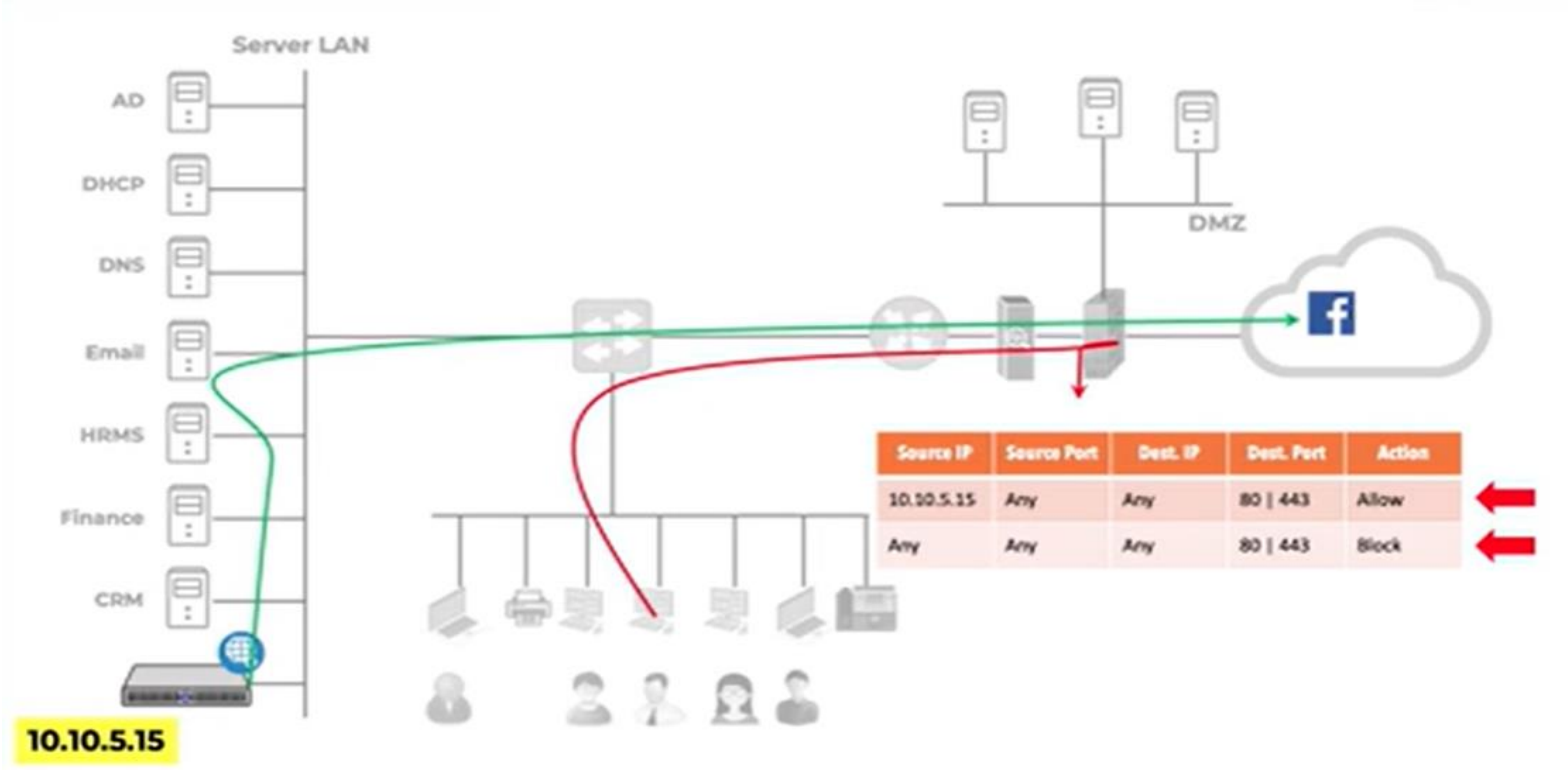
Web Gateway Placement



Web Gateway Working

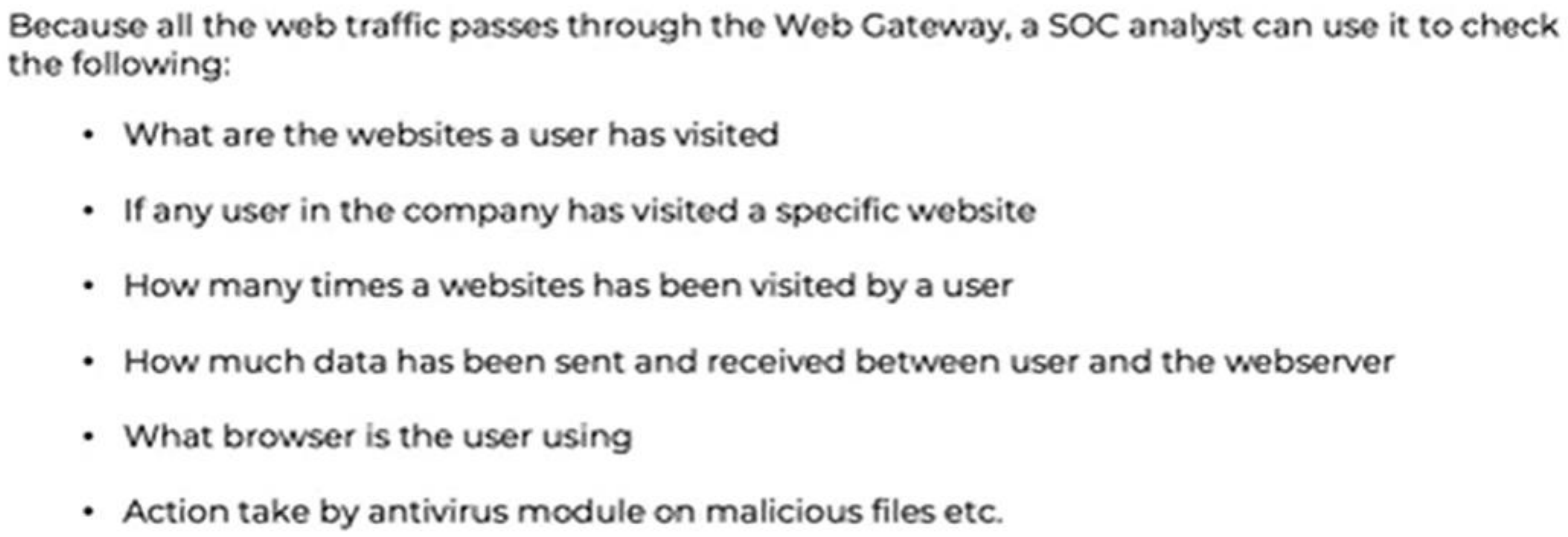


Web Gateway Working



Source IP	Source Port	Dest. IP	Dest. Port	Action
10.10.5.15	Any	Any	80 | 443	Allow
Any	Any	Any	80 | 443	Block

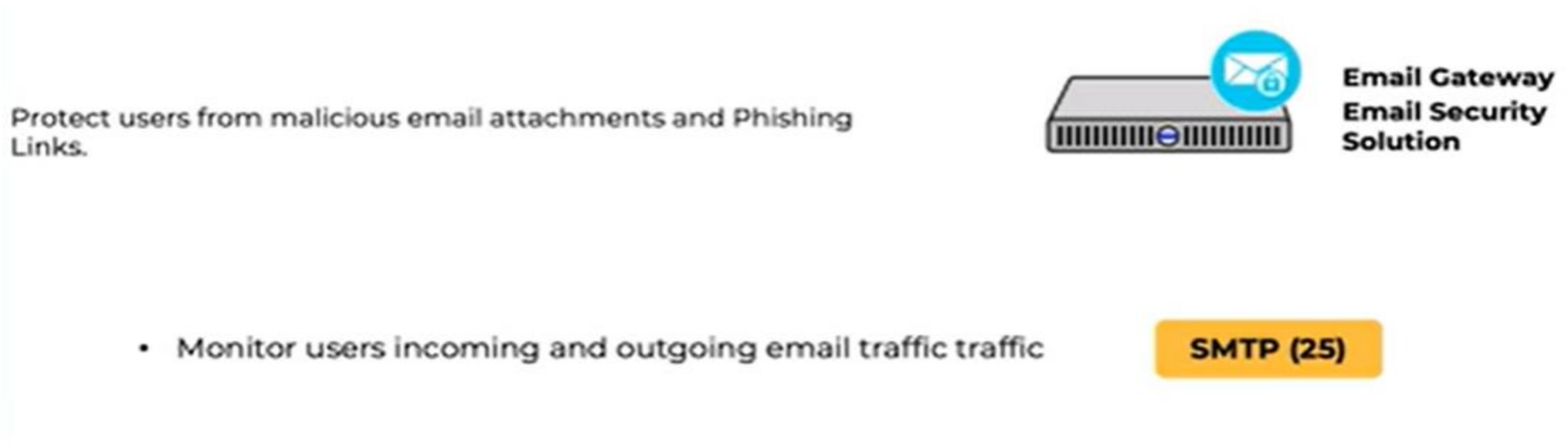
How Security Analyst Uses Web Gateway?



Because all the web traffic passes through the Web Gateway, a SOC analyst can use it to check the following:

- What are the websites a user has visited
- If any user in the company has visited a specific website
- How many times a websites has been visited by a user
- How much data has been sent and received between user and the webserver
- What browser is the user using
- Action take by antivirus module on malicious files etc.

Email Gateway



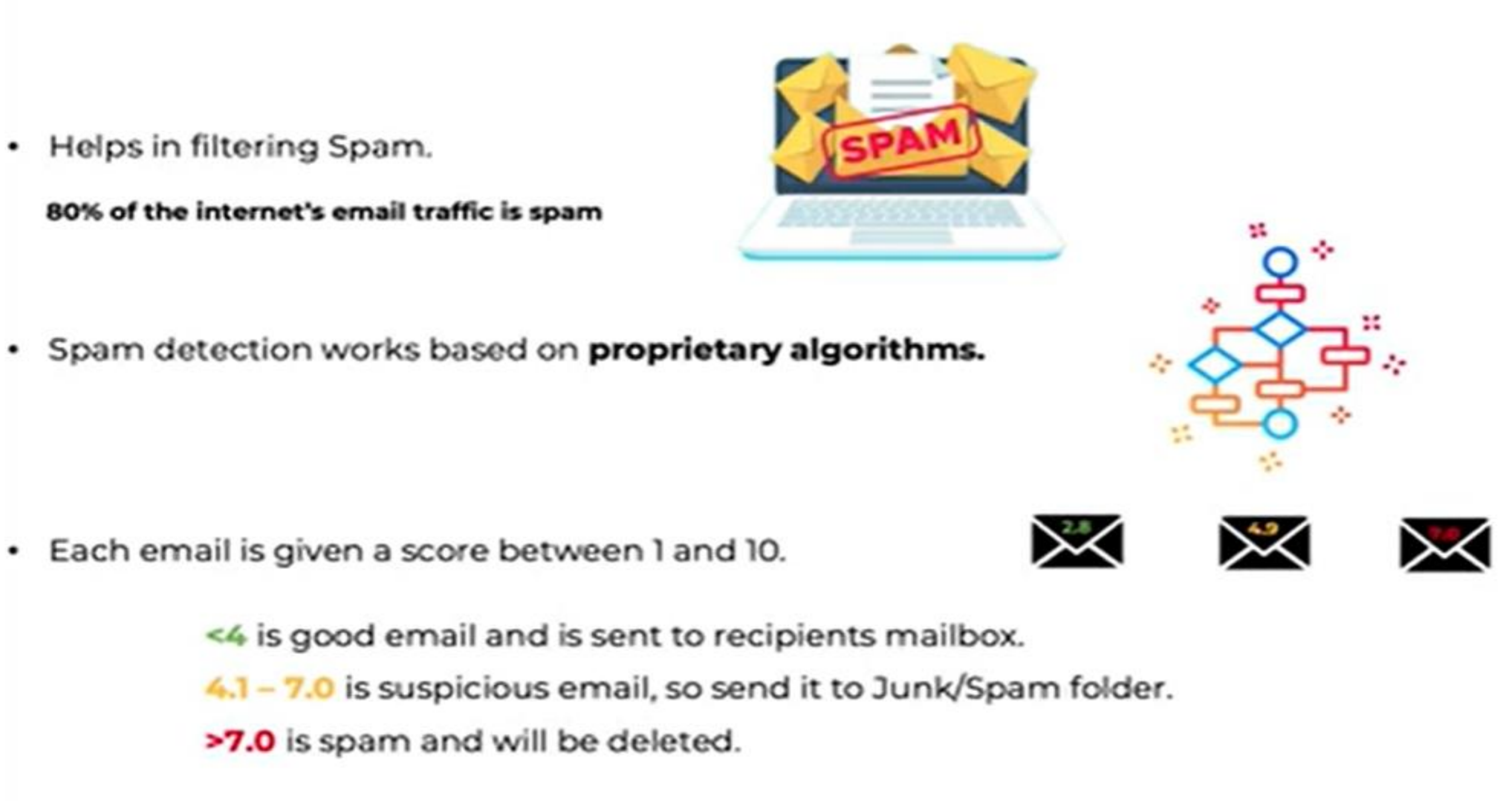
Protect users from malicious email attachments and Phishing Links.

Email Gateway
Email Security Solution

- Monitor users incoming and outgoing email traffic traffic

SMTP (25)

Features of Email Gateway—Spam Filtering



- Helps in filtering Spam.

80% of the internet's email traffic is spam

- Spam detection works based on **proprietary algorithms.**

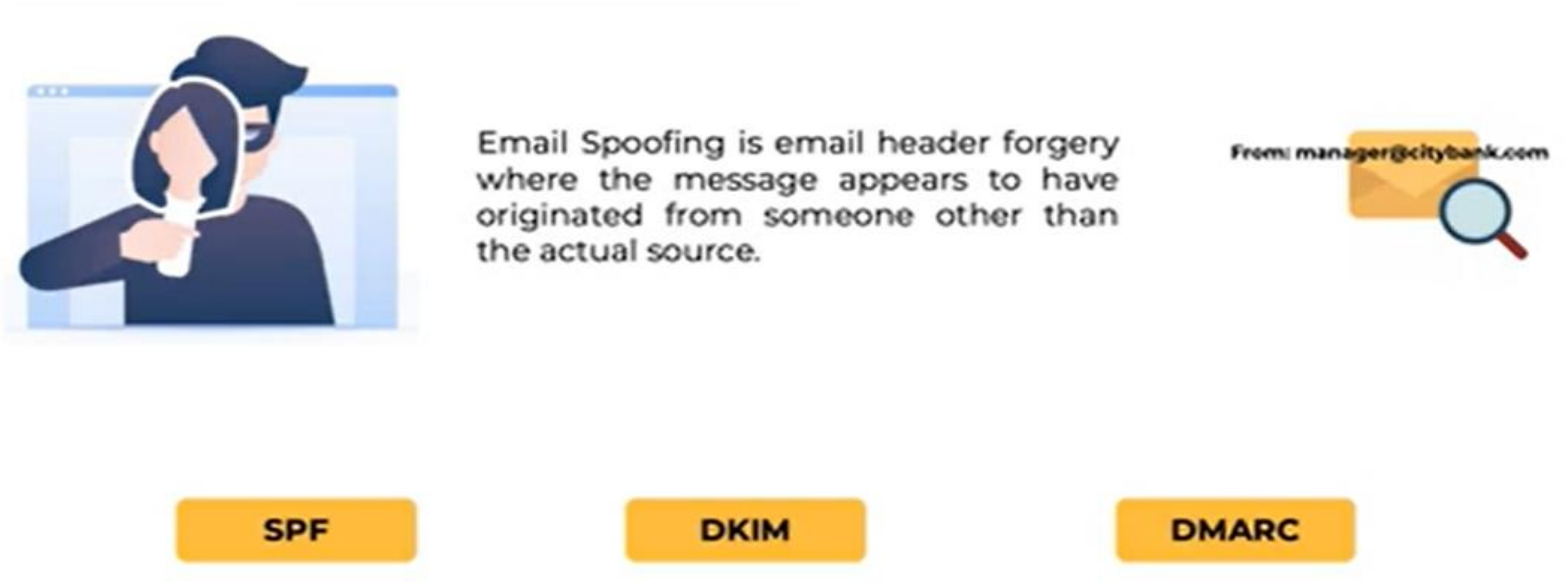
- Each email is given a score between 1 and 10.

  <4 is good email and is sent to recipients mailbox.

  4.1 – 7.0 is suspicious email, so send it to Junk/Spam folder.

  >7.0 is spam and will be deleted.

Features of Email Gateway—Anti Spoofing



Email Spoofing is email header forgery where the message appears to have originated from someone other than the actual source.

SPF

DKIM

DMARC

Features of Email Gateway-- Malware Defense

Email Gateway solution also does Malware defense.

Scan attachments using Built-in Antivirus module

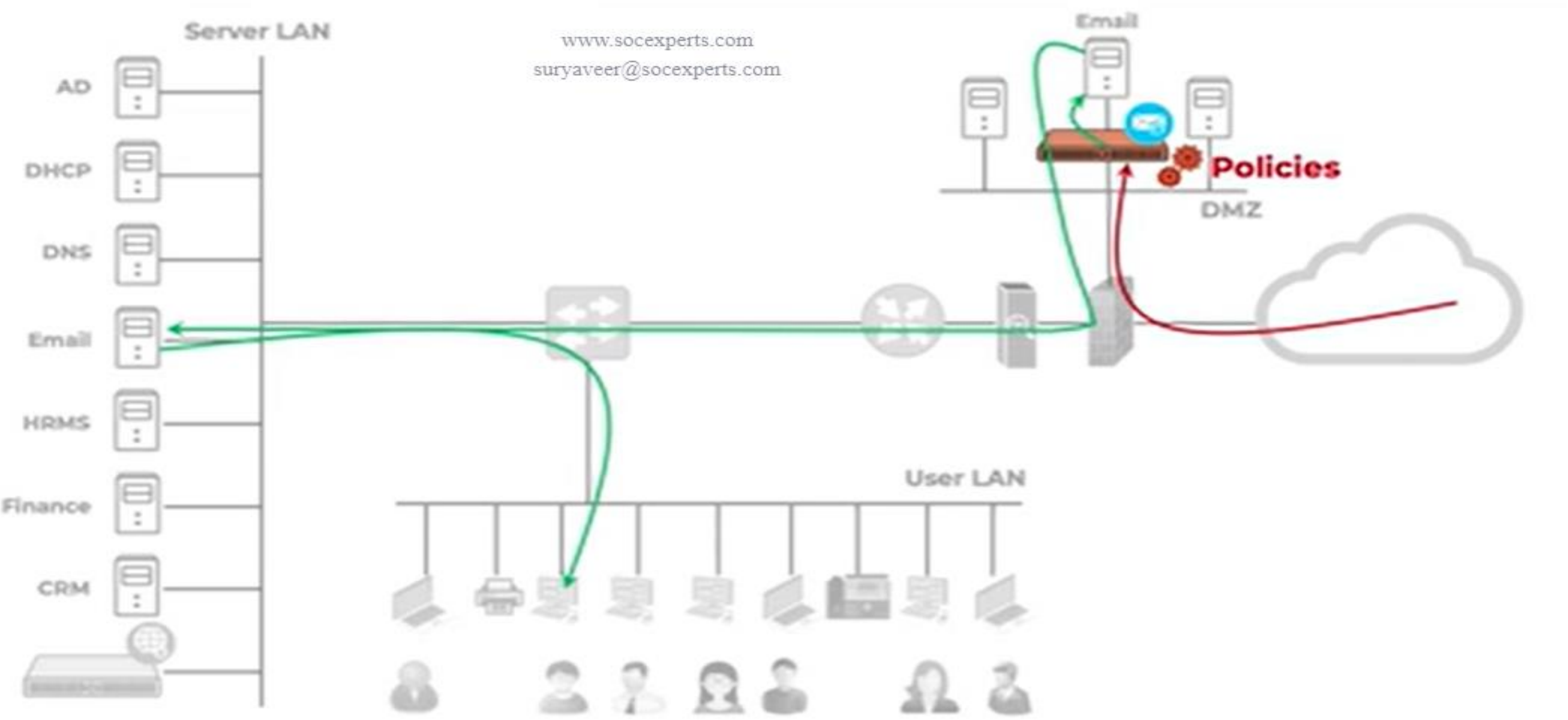
Features of Email Gateway– Anti Phishing

Phishing is a type of social engineering where an attacker sends a fraudulent message designed to trick a human victim into revealing sensitive information or to download malicious attachments.

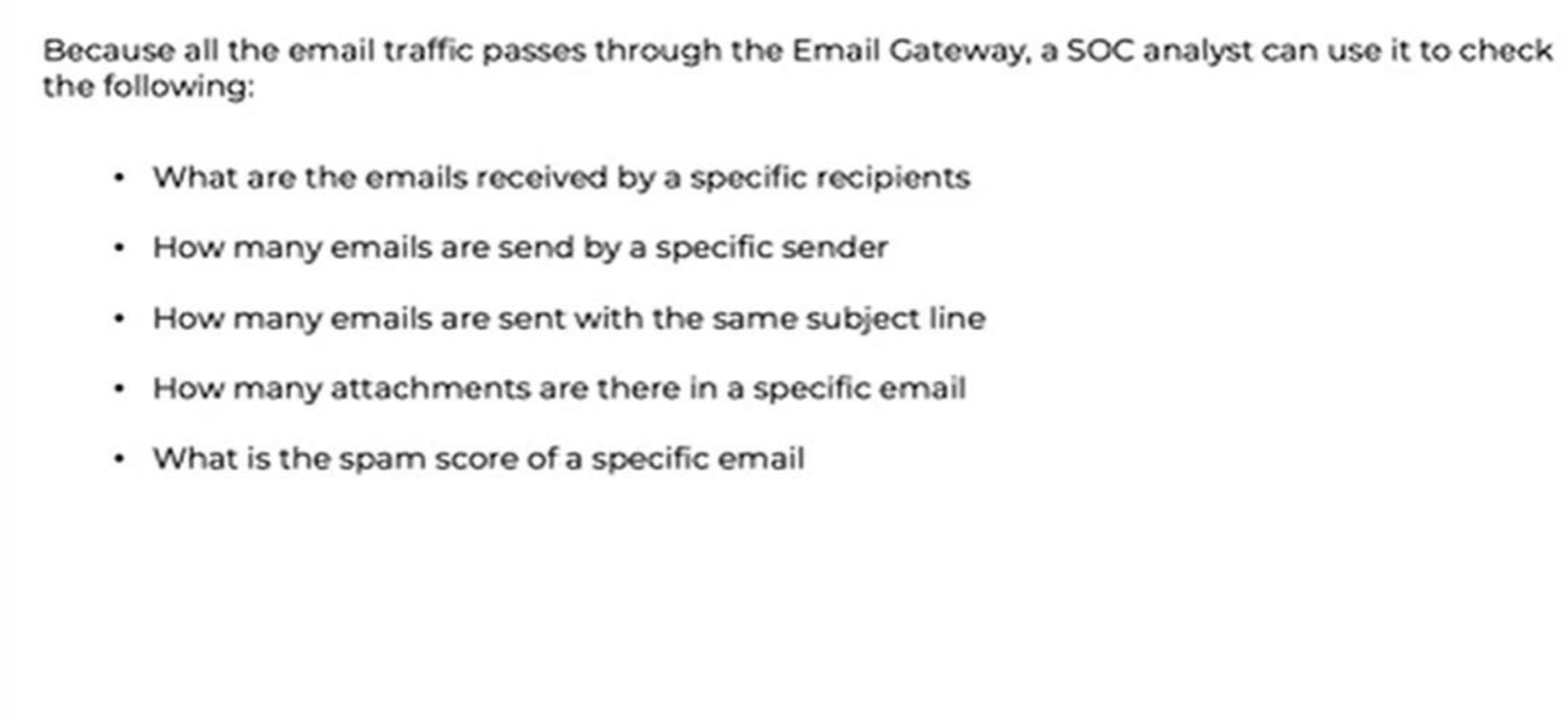
Threat Intelligence

Machine Learning Algorithms

Email Gateway Placement



How Security Analyst Uses Email Gateway?



Because all the email traffic passes through the Email Gateway, a SOC analyst can use it to check the following:

- What are the emails received by a specific recipients
- How many emails are send by a specific sender
- How many emails are sent with the same subject line
- How many attachments are there in a specific email
- What is the spam score of a specific email