Platform

Contents

AWS CLOUD & NETWORK SECURITY

ADITYA

ENLIGHTENS THE NESCIENCE

Under the Esteemed Guidance of
P Bala Srinivas, Asst Professor

Presented by
Y. Kranthi (16A95a0436)
N. Sudha (15A91A04G1)
B. Amit (15A91A04C3)
G.Indrani (16A95A0429)

Platform

CONTENTS

- Introduction
- Issues in implementation
- Objective
- S/W,H/W and services requirements
- Advantages of proposed approach
- Block Diagram
- Applications
- Conclusion
- Future work
- References

Contents

AWS

Amazon Web Services

IoT

Internet of Things

N/w SEC

Newtork Security

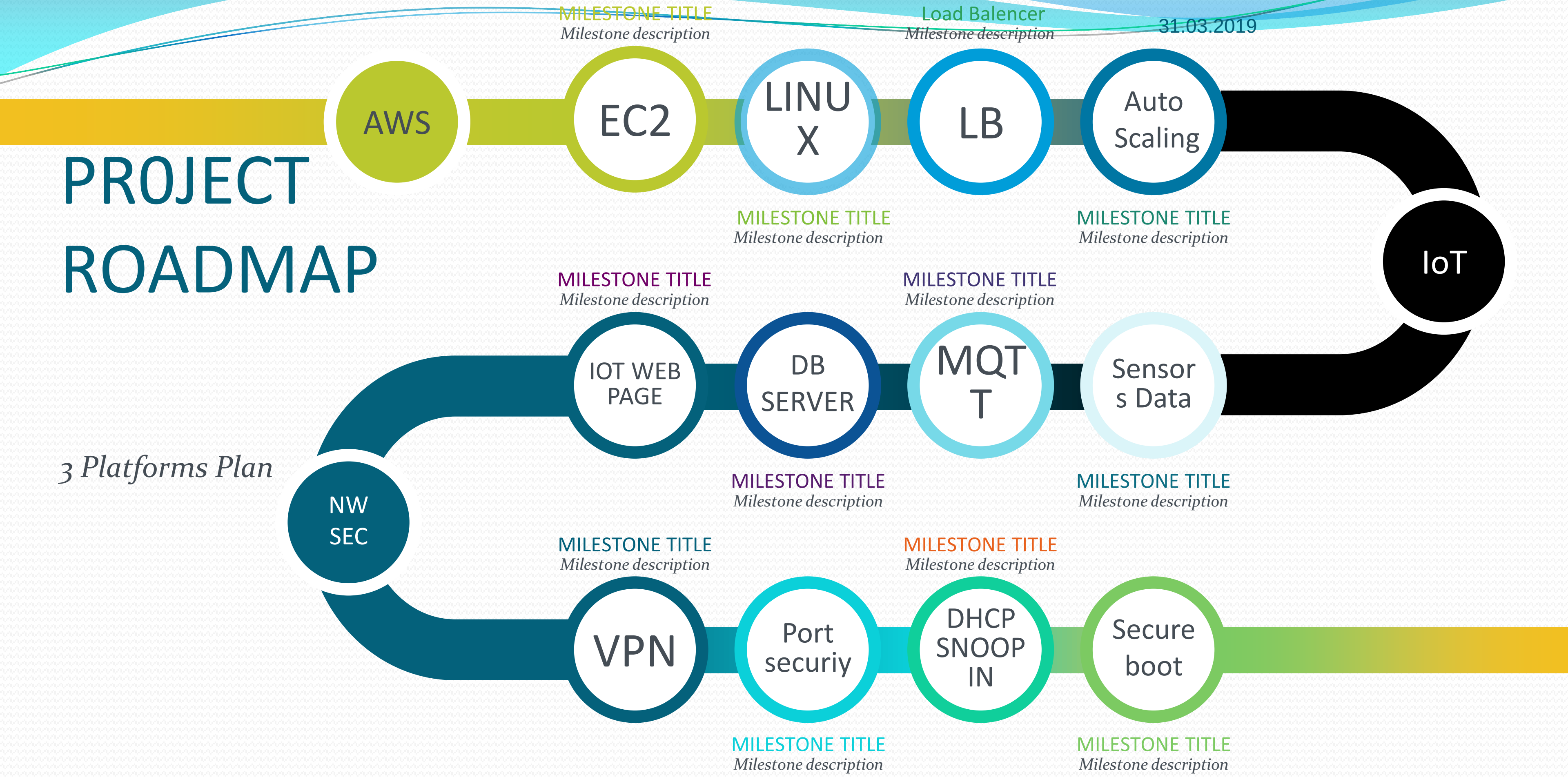
Platforms

Content

PROJECT ROADMAP

3 Platforms Plan

31.03.2019



AWS

MILESTONE TITLE
Milestone description
EC2

LINUX
MILESTONE TITLE
Milestone description

Load Balencer
Milestone description
LB

Auto Scaling
MILESTONE TITLE
Milestone description

IoT

MILESTONE TITLE
Milestone description
IOT WEB PAGE

DB SERVER
MILESTONE TITLE
Milestone description

MILESTONE TITLE
Milestone description
MQTT

Sensors Data
MILESTONE TITLE
Milestone description

NW SEC

MILESTONE TITLE
Milestone description
VPN

Port securiy
MILESTONE TITLE
Milestone description

MILESTONE TITLE
Milestone description
DHCP SNOOPIN

Secure boot
MILESTONE TITLE
Milestone description

Introduction:

- This project main aim is to handle thousands of requests(IOT and Web traffic load) on a web portal. When the user hits on a certain url and if the requests are more on the url the traffic load will be more. There will be lagging of the site and can’t be accessed.

- Due to this in commercial sites, there will be unavailability of the url, to avoid this problem we are going to change the existing policies in AWS Cloud, and create virtual data servers by using AWS Service. When the usage is normal we are going to reduce the created virtual servers but the existence of the url will not be lost.

cont

- Network security consists of the policies and practices to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.

- Only Network security can protect you from Trojan horse viruses. Network security involves the authorization of access to data in a system, controlled by the network administrator.

Issues in implementation:

- Unavailability of the website when the requests from users increases on the website.
- It costs more for maintaining physical servers so creating virtual servers using AWS services costs low.
- Security is low for networking devices.

Objective

- Nowadays, the E-commerce website is top-rated, the Online shopping sites are increased. These websites requesting (or) accessing data will be different day today. For suppose from monday-friday these sites will get approximately 10,000 requests.
- Only on weekends, the requests may increase to 50,000, on festivals and big billion days, they will get lakhs of requests. We have to maintain servers, applications, storage, etc for these sites.
- On weekdays load will be normal, So it may require 2 or 3 servers and on weekends we need 10 to 100 servers besides. On offer's day, we have to maintain thousands of servers.
- Mainatinence of servers is dificult. This much of infra of websites building and managing, it is challenging. To overcome this issue, we are moving to the cloud. That is **AWS CLOUD**, and it is providing a feature called load balancing and Auto scaling.

Hardware ,Software,Services used:

- AWS(Cloud Watch,VPC,EC2,LINUX,S3,SSH)
- Scripting Languages (Json)
- Cisco Networking devices (Router, Switch)
- Load Balancing provided by AWS.
- Auto Scaling provided by AWS.

Advantages of proposed approach:

- Handling millions of requests without any down time.
- Automatic server allocation will be possible without user interaction.
- Maintenance cost will be reduced with AWS.
- Layer 2 attacks like ARP SPOOFING, MAC FLOODING, and DHCP SPOOFING will be prevented.
- To connect different branches with security, we are implementing SITE TO SITE VPN.

Elastic Load Balancing

Elastic Load Balancing

- Distributes traffic across multiple EC2 instances, in multiple Availability Zones
- Supports health checks to detect unhealthy Amazon EC2 instances
- Supports the routing and load balancing of HTTP, HTTPS, SSL, and TCP traffic to Amazon EC2 instances

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Amazon CloudWatch

Amazon CloudWatch

- A monitoring service for AWS cloud resources and the applications you run on AWS
- Visibility into resource utilization, operational performance, and overall demand patterns
- Custom application-specific metrics of your own
- Accessible via AWS Management Console, APIs, SDK, or CLI

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Auto Scaling

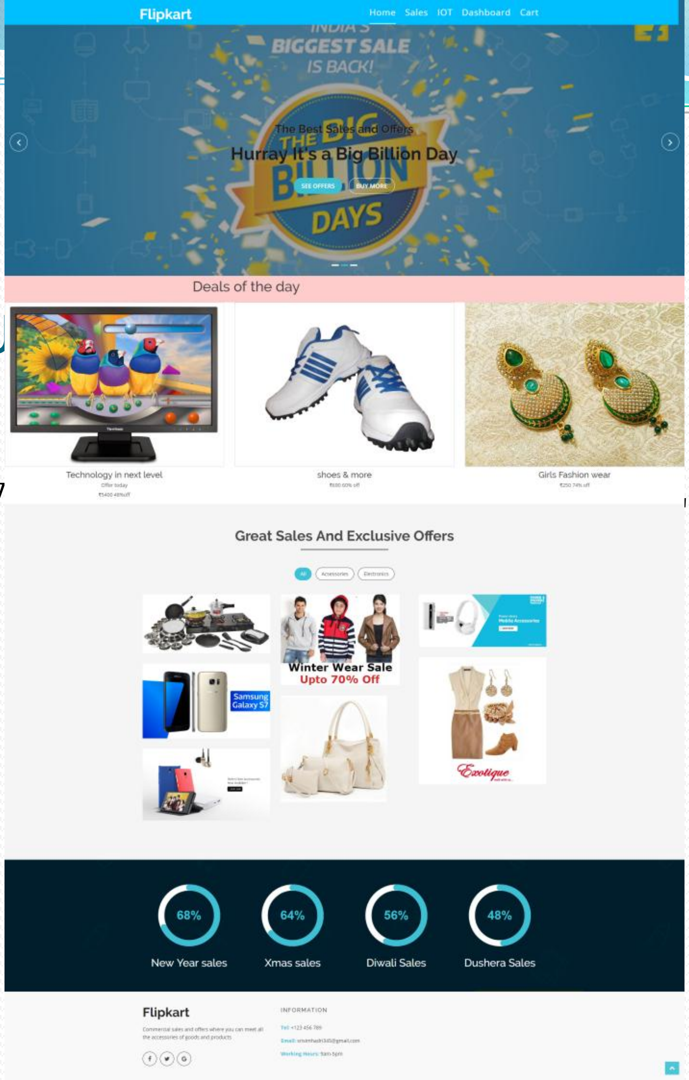
Auto Scalin g

- Scale your Amazon EC2 capacity automatically
- Well-suited for applications that experience variability in usage
- Available at no additional charge

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

WEB PAGE OUTPU

- Web page that w C2 instance:



The Best Sales and Offers

Hurray It's a Big Billion Day

Deals of the day

Technology in next level
Offer today
₹5400 40%off

shoes & more
₹600 60% off

Girls Fashion wear
₹250 74% off

Great Sales And Exclusive Offers

New Year sales

Xmas sales

Diwali Sales

Dushera Sales

Flipkart

Commercial sales and offers where you can meet all the accessories of goods and products

INFORMATION

Tel: +123 456 789

Email: srisimhadri345@gmail.com

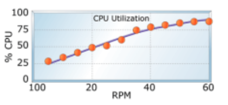
Working Hours: 9am-5pm

Auto Scaling Flow

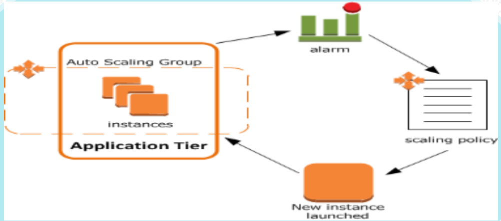
Load Balancer URL

Web page

More Requests are hitting on a web page



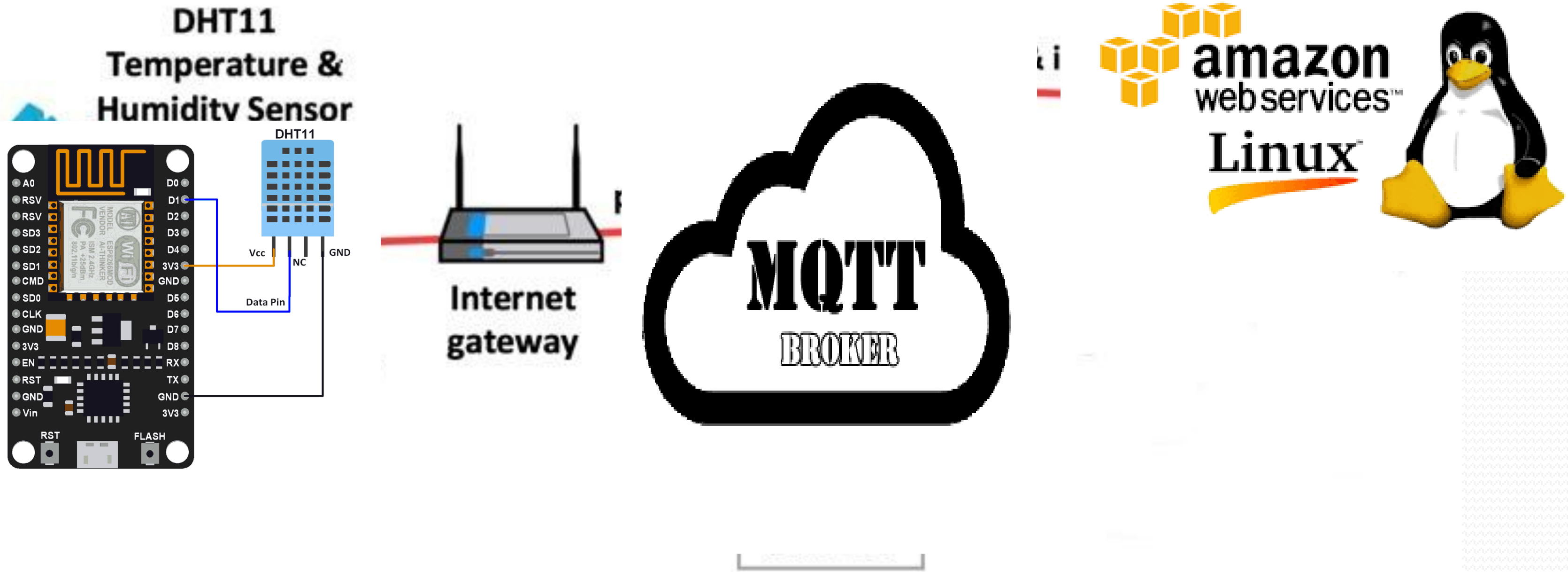
C.P.U load increases
Then automatic allocation
Of web servers



Auto Scaling and cloud watch triggers based on alarms

Web servers are created under the same load balancer

IOT BLOCK DIAGRAM



❑MQTT PROTOCOL

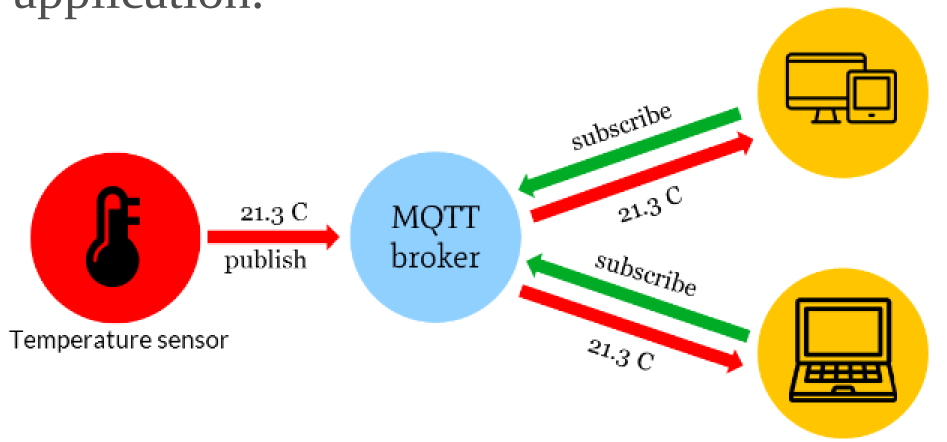
- MQTT means Message Queuing Telemetry Transport. It is small size, light weight, low power usage, minimized data packets and ease of implementation .it is used for “machine-to-machine” connection.

Working:

- MQTT is based on clients and a server. The server is the one who is responsible for handling the client’s requests of receiving or sending data between each other. MQTT server is called a broker and the clients are simply the connected devices.
- When a device (a client) wants to send data to the broker, we call this operation a “publish”.
- When a device (a client) wants to receive data from the broker, we call this operation a “subscribe”.
- Publish, is the process a device does to send its message to the broker.
- Subscribe, where a device does to retrieve a message from the broker.

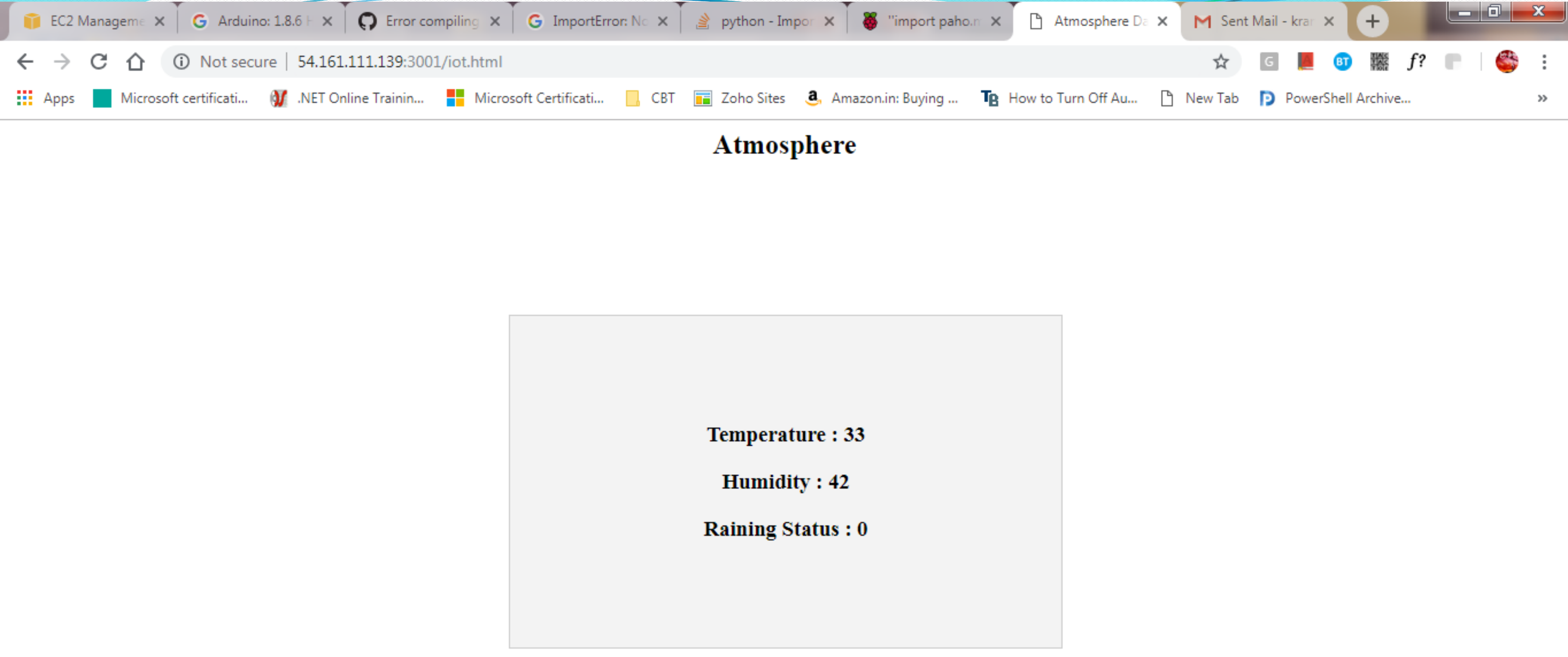
Sending sensor data to client through MQTT protocol:

The data such as temperature and humidity values from publisher is send to the **mqtt broker** . The broker role here is to take the message “temperature value” and deliver through a message to the subscriber phone or application.



Schematic data flow from sensor (machine) to devise (machine)

IOT page :



Atmosphere

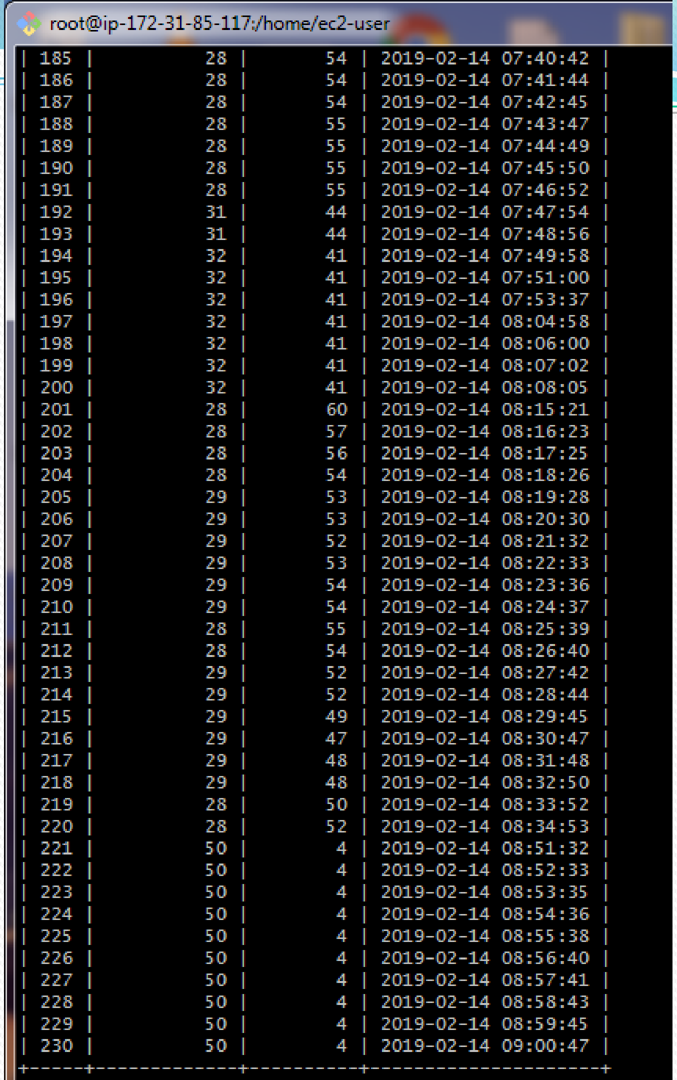
Temperature : 33

Humidity : 42

Raining Status : 0

Cont

- DB OUTPUT

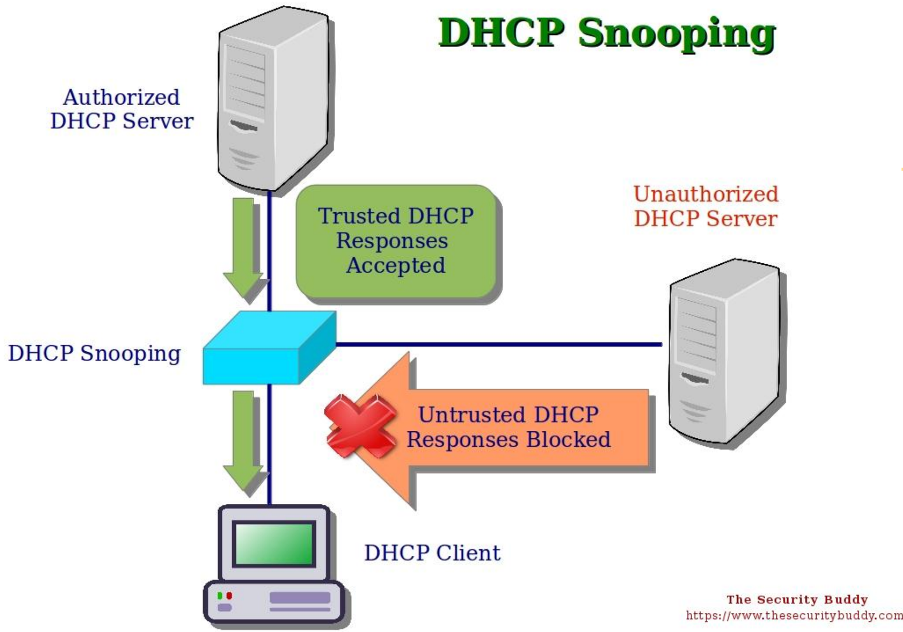


root@ip-172-31-85-117:/home/ec2-user

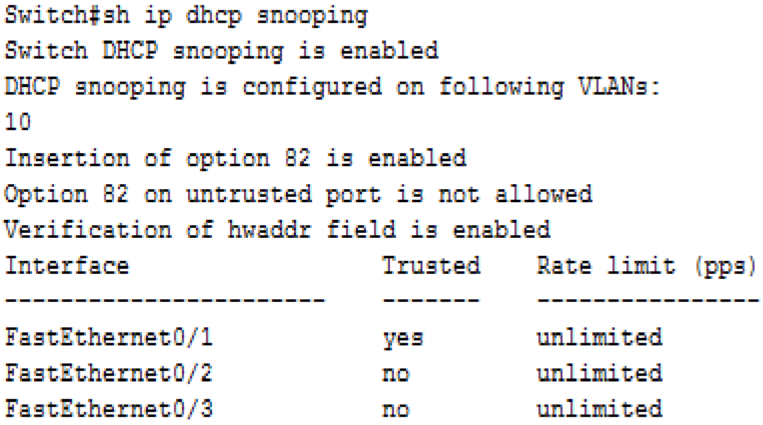
```
| 185 |           28 |        54 | 2019-02-14 07:40:42 |
| 186 |           28 |        54 | 2019-02-14 07:41:44 |
| 187 |           28 |        54 | 2019-02-14 07:42:45 |
| 188 |           28 |        55 | 2019-02-14 07:43:47 |
| 189 |           28 |        55 | 2019-02-14 07:44:49 |
| 190 |           28 |        55 | 2019-02-14 07:45:50 |
| 191 |           28 |        55 | 2019-02-14 07:46:52 |
| 192 |           31 |        44 | 2019-02-14 07:47:54 |
| 193 |           31 |        44 | 2019-02-14 07:48:56 |
| 194 |           32 |        41 | 2019-02-14 07:49:58 |
| 195 |           32 |        41 | 2019-02-14 07:51:00 |
| 196 |           32 |        41 | 2019-02-14 07:53:37 |
| 197 |           32 |        41 | 2019-02-14 08:04:58 |
| 198 |           32 |        41 | 2019-02-14 08:06:00 |
| 199 |           32 |        41 | 2019-02-14 08:07:02 |
| 200 |           32 |        41 | 2019-02-14 08:08:05 |
| 201 |           28 |        60 | 2019-02-14 08:15:21 |
| 202 |           28 |        57 | 2019-02-14 08:16:23 |
| 203 |           28 |        56 | 2019-02-14 08:17:25 |
| 204 |           28 |        54 | 2019-02-14 08:18:26 |
| 205 |           29 |        53 | 2019-02-14 08:19:28 |
| 206 |           29 |        53 | 2019-02-14 08:20:30 |
| 207 |           29 |        52 | 2019-02-14 08:21:32 |
| 208 |           29 |        53 | 2019-02-14 08:22:33 |
| 209 |           29 |        54 | 2019-02-14 08:23:36 |
| 210 |           29 |        54 | 2019-02-14 08:24:37 |
| 211 |           28 |        55 | 2019-02-14 08:25:39 |
| 212 |           28 |        54 | 2019-02-14 08:26:40 |
| 213 |           29 |        52 | 2019-02-14 08:27:42 |
| 214 |           29 |        52 | 2019-02-14 08:28:44 |
| 215 |           29 |        49 | 2019-02-14 08:29:45 |
| 216 |           29 |        47 | 2019-02-14 08:30:47 |
| 217 |           29 |        48 | 2019-02-14 08:31:48 |
| 218 |           29 |        48 | 2019-02-14 08:32:50 |
| 219 |           28 |        50 | 2019-02-14 08:33:52 |
| 220 |           28 |        52 | 2019-02-14 08:34:53 |
| 221 |           50 |         4 | 2019-02-14 08:51:32 |
| 222 |           50 |         4 | 2019-02-14 08:52:33 |
| 223 |           50 |         4 | 2019-02-14 08:53:35 |
| 224 |           50 |         4 | 2019-02-14 08:54:36 |
| 225 |           50 |         4 | 2019-02-14 08:55:38 |
| 226 |           50 |         4 | 2019-02-14 08:56:40 |
| 227 |           50 |         4 | 2019-02-14 08:57:41 |
| 228 |           50 |         4 | 2019-02-14 08:58:43 |
| 229 |           50 |         4 | 2019-02-14 08:59:45 |
| 230 |           50 |         4 | 2019-02-14 09:00:47 |
+-----+-------------+----------+---------------------+
```

Network Security

- Dhcp Snooping



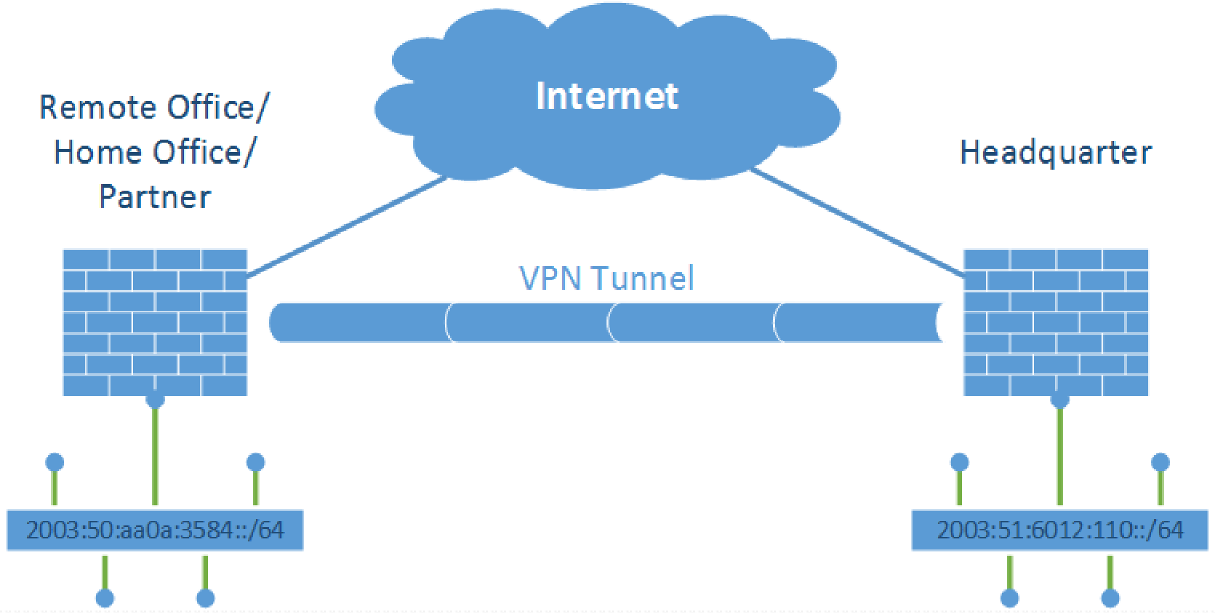
The Security Buddy
https://www.thesecuritybuddy.com/



```
Switch#sh ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
-----------------------    -------    ----------------
FastEthernet0/1            yes        unlimited
FastEthernet0/2            no         unlimited
FastEthernet0/3            no         unlimited
```

Cont

- **Site to Site VPN**



Cont

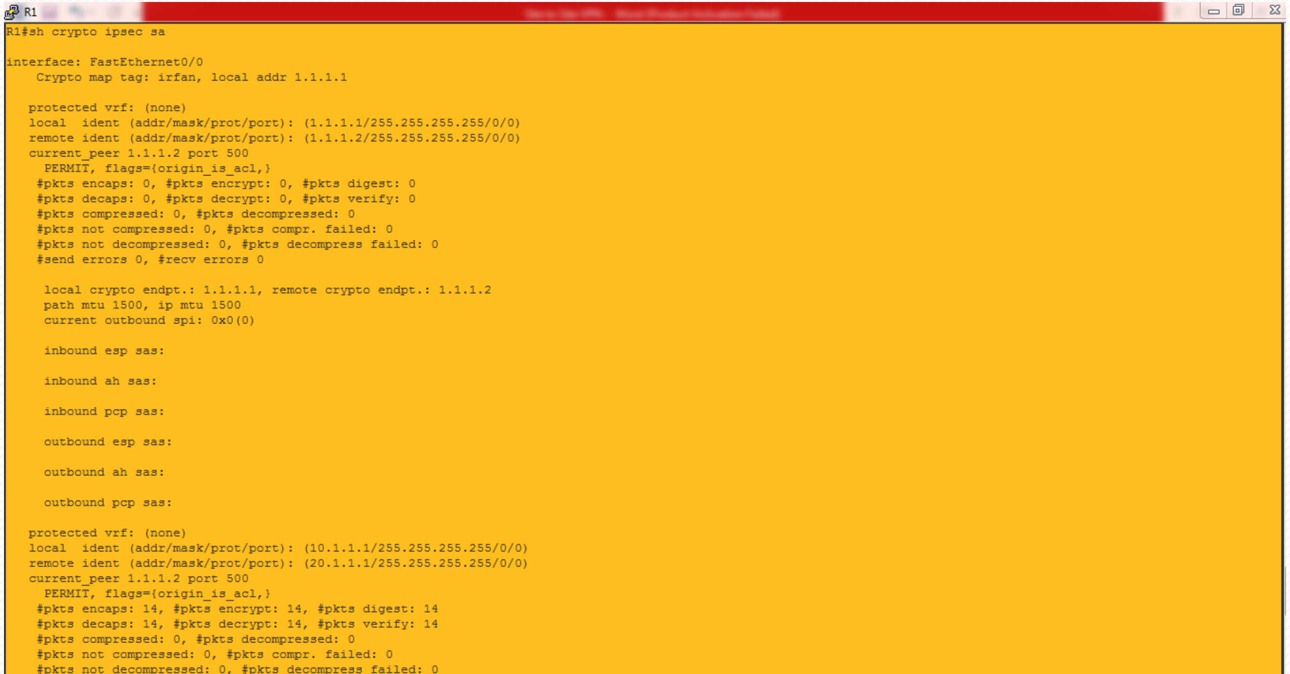
- Site-to-Site IPSec VPN Tunnels are used to allow the secure transmission of data, voice and video between two sites (e.g offices or branches).

- The VPN tunnel is created over the Internet public network and encrypted using a number of advanced encryption algorithms to provide confidentiality of the data transmitted between the two sites.

- These steps are: □ (1) Configure ISAKMP (ISAKMP Phase 1) □ (2) Configure IPSec (ISAKMP Phase 2, ACLs, Crypto MAP)

Cont

VPN OUTPUT



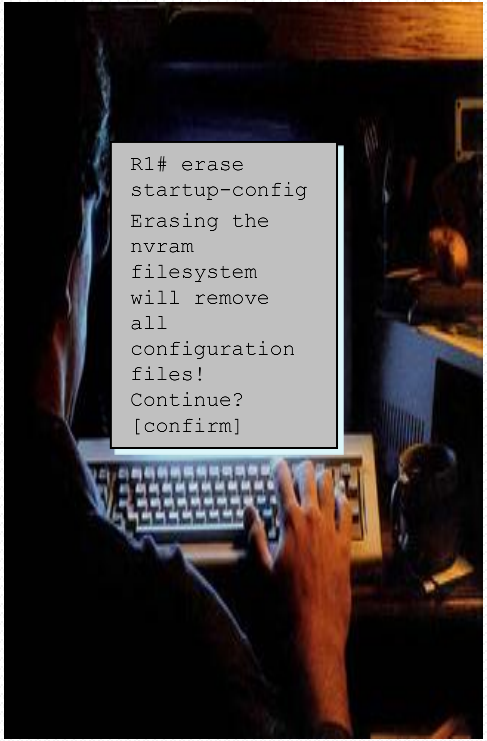
```
R1#sh crypto ipsec sa

interface: FastEthernet0/0
    Crypto map tag: irfan, local addr 1.1.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (1.1.1.1/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (1.1.1.2/255.255.255.255/0/0)
   current_peer 1.1.1.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 1.1.1.1, remote crypto endpt.: 1.1.1.2
     path mtu 1500, ip mtu 1500
     current outbound spi: 0x0(0)

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:

     outbound pcp sas:

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.1.1.1/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (20.1.1.1/255.255.255.255/0/0)
   current_peer 1.1.1.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 14, #pkts encrypt: 14, #pkts digest: 14
    #pkts decaps: 14, #pkts decrypt: 14, #pkts verify: 14
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
```

Cont

- **Secure Boot Sequence**
- The configuration file in the primary boot set is a copy of the running configuration that was in the router when the feature was first enabled
- D The feature secures the smallest working set of files to preserve persistent storage space. No extra space is required to secure the primary IOS image file.

The feature automatically detects image or configuration version mismatch. Only local storage is used for securing files

The feature can be disabled only through a console session



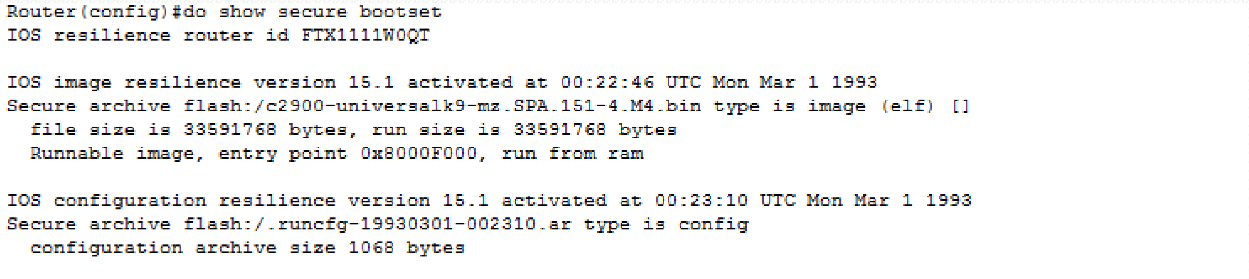
```
R1# erase
startup-config
Erasing the
nvram
filesystem
will remove
all
configuration
files!
Continue?
[confirm]
```

Cont..

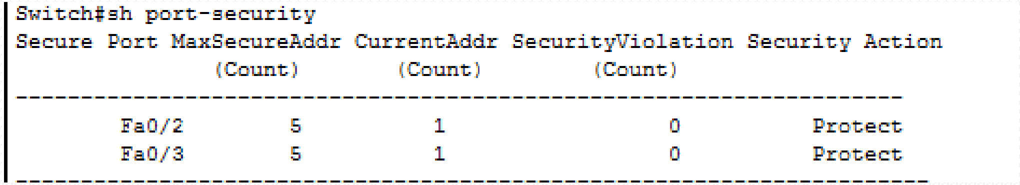
- **Port Security**
- Port security controls how many MAC addresses can be learned on a single switch port.This also protects against malicious applications that may be sending thousands of frames
- into the network, with a different bogus MAC address for each frame.
- **Dynamic Arp Spoofing**
- ARP provides IP communication within a Layer 2 broadcast domain by mapping an IP address to a MAC address.
- DAI is a security feature that validates ARP packets in a network. DAI intercepts, logs, and discards ARP packets with invalid IP-t o -MAC address bindings.
- This capability protects the network from some man-in-the-middle attacks.

Cont

SECURED BOOT AND PORT SECURITY OUPTUT



```
Router(config)#do show secure bootset
IOS resilience router id FTX1111W0QT

IOS image resilience version 15.1 activated at 00:22:46 UTC Mon Mar 1 1993
Secure archive flash:/c2900-universalk9-mz.SPA.151-4.M4.bin type is image (elf) []
  file size is 33591768 bytes, run size is 33591768 bytes
  Runnable image, entry point 0x8000F000, run from ram

IOS configuration resilience version 15.1 activated at 00:23:10 UTC Mon Mar 1 1993
Secure archive flash:/.runcfg-19930301-002310.ar type is config
  configuration archive size 1068 bytes
```



```
Switch#sh port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)          (Count)
--------------------------------------------------------------------
        Fa0/2          5           1                 0           Protect
        Fa0/3          5           1                 0           Protect
----------------------------------------------------------------------
```

APPLICATIONS

- Browser(To access AWS web Console)
- Putty
- Filezilla
- Packet Tracer
- GNS
- Ardunio IDE

CONCLUSION

- Website will be handled billion and million request with out any latency and unviability issue.
- By the help of Scaling feature.
- Atmosphere details of particular location are obtained by the help of IoT.
- On premises network secured by using principles, VPN, firewall.

FUTURE SCOPE

- IPS
- DB Migration to Cloud

REFERENCES

- AWS DOCUMENTATION from aws website
- CISCO DOCUMENTATION form cisco website

Thank you!