# SECURITY ANALYST
# AUDI MUMBAI WEST

Thesis submitted in partial fulfilment

of the requirements of the degree of

**Masters in Science with Specialization in Cybersecurity**

by

Sanket keny

Under the Supervision of

**Prof. Rashid Patel**

**April 2023**

**Nagindas Khandwala College(Autonomous)**
**Malad, Mumbai 400064**

# CERTIFICATE

This is to certify that the dissertation entitled **“SECURITY ANALYST AT AUDI MUMBAI WEST”** is a bonafide work of “**SANKET KENY” (ROLL NO: 4 AND GR NO:3511434)** submitted to the Nagindas Khandwala College(Autonomous),Mumbai in partial fulfillment of the requirement for the award of the degree of **“Masters in Science with Specialization in Cybersecurity”**.

**Prof. Rashid patel**
Internal-Examiner

External Examiner

# Supervisor’s Certificate

This is to certify that the dissertation entitled **“SECURITY ANALYST AT AUDI MUMBAI WEST”** submitted by **SANKET KENY, (ROLL NO: 4 AND GR NO:3511434)** is a record of original work carried out by him/her under my supervision and guidance in partial fulfillment of the requirements of the degree of **Masters in Science with Specialization in Cybersecurity** at Nagindas Khandwala College(Autonomous),Mumbai 400064 . Neither this dissertation nor any part of it has been submitted earlier for any degree or diploma to any institute or university in India or abroad.

**Prof. Rashid Patel**

Internal Examiner

# Declaration of Originality

I, **Sanket keny, Roll no : 04 GR NO (3511434)**, hereby declare that this dissertation entitled “**SECURTIY ANALYST AT AUDI MUMBAI WEST*”*** presents my original work carried out as a Master Student of Nagindas Khandwala College(Autonomous),Mumbai 400064. To the best of my knowledge, this dissertation contains no material previously published or written by another person, nor any material presented by me for the award of any degree or diploma of Nagindas Khandwala College(Autonomous),Mumbai or any other institution. Any contribution made to this research by others, with whom I have worked at Ajeenkya D Y Patil University, Pune or elsewhere, is explicitly acknowledged in the dissertation. Works of other authors cited in this dissertation have been duly acknowledged under the sections “Reference” or “Bibliography”. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission.

I am fully aware that in case of any non-compliance detected in future, the Academic Council of Nagindas Khandwala College(Autonomous),Mumbai may withdraw the degree awarded to me on the basis of the present dissertation.

**Date:**

**Place:**

**Sanket keny**

# Acknowledgement

I remain immensely obliged to **Prof. Rashid Patel** for providing me with the idea of this topic, and for his invaluable support in garnering resources for me either by way of information or computers also his guidance and supervision which made this Internship happen.

Date : 10th December, 2022

Audi
Mumbai West

Ground Floor Neo Vikram, New Link R
Opp. Star Bazzar, Sahakar Nagar,
Azad Nagar, Andheri West,
Mumbai - 400 053
Ph: +91 80808 01342
sales@audimumbaiwest.in
https://mumbaiwest.myaudi.in

To,
Sanket Keny,
Mumbai.

**Subject: Internship Confirmation Letter**

Dear Sanket,

This is in reference to your application for a Security Analyst Internship at Modi Motor Agencies Pvt. Ltd.

We can confirm your internship for the duration of three months starting from 12th December 2022 till 11th March, 2023. Please note you will be paid **INR 6,000 /-** as a monthly stipend (Rupees Six thousand only) and you will have to report to undersigned on **12th December, 2022** at Modi Motor Agencies Pvt. Ltd. for your joining formalities and induction. The project head and mentor will be assigned to you once you have completed these formalities.

Please note on successful completion of your internship, you will be required to submit a Project Report and bases your performance an internship completion certificate shall be issued.

We welcome you on board and wish you all the best for your assignments.

For Modi Motor Agencies Pvt. Ltd.

Authorised Signatory

MODI MOTORS AGENCIES PVT. LTD.
THANE

# Abstract

A Sonic Firewall is a network security device that is designed to protect computer networks from unauthorized access and malicious attacks. It is a hardware-based firewall that is used to secure both small and large networks.

Sonic Firewall offers various features such as intrusion prevention, malware protection, content filtering, VPN connectivity, and more.

It can also be configured to perform other security functions such as load balancing, bandwidth management, and application control. Sonic Firewall is widely used in organizations to secure their network infrastructure and ensure data privacy and integrity.

Its ability to detect and prevent network-based threats makes it an essential tool for network security.

Overall, Sonic Firewall is an effective network security solution that helps organizations protect their valuable data and assets from cyber threats.

# Contents

# CHAPTER 1

# INTRODUCTION

### 1.1 Problem Statement

Sonic Firewall is used to enhance network security and protect computer networks from unauthorized access and malicious attacks. It serves as a barrier between a private internal network and the external internet or other untrusted networks. Sonic Firewall provides advanced features such as intrusion prevention, malware protection, content filtering

Also it enables us to give access to what mode of stream is required in which department
Such as marketing , insurance, sales and many more.

Having a grouped challenged in a bandwidth issue in multiple locations across Mumbai and make them up and running

VPN connectivity, and more. It can also be used to perform other security functions such as load balancing, bandwidth management, and application control.

> By implementing Sonic Firewall, organizations can secure their network infrastructure and ensure data privacy and integrity. It helps to prevent cyber attacks such as viruses, spyware, phishing, and hacking attempts, which can cause damage to network resources and compromise sensitive information.

Sonic Firewall can also help organizations comply with regulatory requirements and industry standards by providing advanced security features and logging capabilities.

Overall, Sonic Firewall is used to protect networks and sensitive data from cyber threats and to ensure the confidentiality, integrity, and availability of network resources.

## 1.2 **Scope of Project**

The scope of Sonic Firewall is to provide network security for computer networks, both small and large. It is designed to be scalable and can be deployed in various network environments, including enterprise networks, branch offices, and remote locations.

The Sonic Firewall provides a range of security features, including intrusion prevention, malware protection, content filtering, VPN connectivity, and more. It can also be used to perform other security functions such as load balancing, bandwidth management, and application control.

Sonic Firewall can be configured to meet specific security requirements and compliance regulations, making it suitable for various industries, including healthcare, finance, retail, and education. It can also integrate with other security solutions, such as endpoint security, to provide comprehensive protection against cyber threats.

In summary, the scope of Sonic Firewall is to provide network security for organizations of all sizes and across various industries. It offers a range of security features and can be customized to meet specific security requirements and compliance regulations

## 1.3 Objective of Project

The main objective of Sonic Firewall is to enhance network security and protect computer networks from unauthorized access and malicious attacks. It serves as a barrier between a private internal network and the external internet or other untrusted networks.
The Sonic Firewall achieves this objective by providing a range of security features, including intrusion prevention, malware protection, content filtering, VPN connectivity, and more.

In addition to protecting network infrastructure and sensitive data, the objectives of Sonic Firewall include:

Providing real-time threat prevention: Sonic Firewall is designed to detect and prevent network-based threats in real-time, ensuring that network resources and data are protected from cyber attacks.

Offering high availability and reliability: Sonic Firewall is designed to be highly available and reliable, ensuring that network resources are always accessible and protected.

Simplifying network management: Sonic Firewall provides a centralized management console that enables network administrators to monitor and manage network security from a single location.

Enhancing compliance: Sonic Firewall can help organizations comply with regulatory requirements and industry standards by providing advanced security features and logging capabilities.

Overall, the objective of Sonic Firewall is to provide comprehensive network security that ensures the confidentiality, integrity, and availability of network resources while simplifying network management and enhancing compliance.

## 1.4 Proposed System

The purpose of Sonic Firewall is to provide network security and protect computer networks from cyber threats. Sonic Firewall serves as a barrier between a private internal network and the external internet or other untrusted networks, preventing unauthorized access and malicious attacks.

Sonic Firewall achieves this purpose by providing a range of security features, including intrusion prevention, malware protection, content filtering, VPN connectivity, and more. It can also be used to perform other security functions such as load balancing, bandwidth management, and application control.

The purpose of Sonic Firewall is to:
Protect network infrastructure and sensitive data: Sonic Firewall is designed to detect and prevent network-based threats, ensuring that network resources and data are protected from cyber attacks.

Ensure the confidentiality, integrity, and availability of network resources: Sonic Firewall prevents unauthorized access to network resources, ensuring that sensitive information remains confidential, and that network resources are always available.

Provide comprehensive network security: Sonic Firewall offers a range of security features that can be customized to meet specific security requirements and compliance regulations, making it suitable for various industries and organizations of all sizes.

Simplify network management: Sonic Firewall provides a centralized management console that enables network administrators to monitor and manage network security from a single location, simplifying network management and reducing administrative overhead.

Overall, the purpose of Sonic Firewall is to provide network security and protect computer networks from cyber threats while ensuring the confidentiality, integrity, and availability of network resources.

# CHAPTER 2

## LITERATURE SURVEY

A survey brief about Sonic Firewall could include the following information:
Purpose: To understand the level of awareness and usage of Sonic Firewall among organizations and IT professionals.

Target Audience: The survey would target IT professionals and decision-makers responsible for network security within organizations.

Objectives: The objectives of the survey would include assessing the level of awareness and usage of Sonic Firewall, understanding the factors that influence the adoption of Sonic Firewall, and identifying the key features and benefits of Sonic Firewall that are most valued by users.

Survey Questions: Sample survey questions could include:
Are you familiar with Sonic Firewall?
Have you ever used Sonic Firewall in your organization?
What factors influenced your decision to adopt Sonic Firewall?
What are the key features and benefits of Sonic Firewall that are most important to you?
How effective do you find Sonic Firewall in protecting your network against cyber threats?
Would you recommend Sonic Firewall to other organizations looking for network security solutions?

Data Analysis: The survey results would be analyzed to identify patterns and trends in the level of awareness and usage of Sonic Firewall, as well as the factors that influence its adoption and the key features and benefits that users value the most.

Overall, a survey brief about Sonic Firewall would aim to provide insights into the level of awareness and usage of the solution, as well as the factors that influence its adoption and the key features and benefits that are most valued by users.

## 2.1 Literature Review

Sonic Firewall is a network security solution that provides protection against a range of cyber threats, including malware, phishing, and ransomware. The solution offers advanced threat detection and prevention capabilities, as well as a range of other security features such as intrusion prevention, content filtering, and VPN connectivity.

Here are some of the key findings from literature on Sonic Firewall:

Sonic Firewall is effective in detecting and preventing cyber threats: A study published in the International Journal of Computer Science and Mobile Computing (January 2018) compared the features and performance of Sonic Firewall and Fortinet Firewall. The study found that Sonic Firewall was effective in detecting and preventing cyber threats, including malware and phishing attacks.

Sonic Firewall offers a range of advanced security features: According to an article published in Help Net Security (April 2021), Sonic Firewall provides a comprehensive range of advanced security features that can be customized to meet specific security requirements and compliance regulations. These features include intrusion prevention, content filtering, and VPN connectivity.

Sonic Firewall is suitable for SMBs: An article published in Enterprise Tech (January 2021) states that Sonic Firewall is an ideal solution for small and medium-sized businesses (SMBs) looking for comprehensive network security. The solution offers enterprise-level security features at a reasonable cost and can be easily managed by SMBs with limited IT resources.

Sonic Firewall provides centralized management and monitoring: According to a review published in Infosec Resources (January 2021), Sonic Firewall provides a centralized management console that enables network administrators to monitor and manage network security from a single location. This simplifies network management and reduces administrative overhead.

Sonic Firewall is constantly evolving: An article published in Techwarn (August 2021) notes that Sonic Firewall is constantly evolving to keep up with the latest cyber threats and security trends. The solution is regularly updated with new features and capabilities to ensure that it remains effective in protecting against emerging threats.

Overall, the literature suggests that Sonic Firewall is an effective network security solution that provides a comprehensive range of advanced security features. The solution is suitable for SMBs and can be easily managed and monitored from a centralized console. Sonic Firewall is also constantly evolving to keep up with the latest cyber threats and security trends.

# CHAPTER 3

## METHODOLODY

The methodology for implementing Sonic Firewall in an organization would typically involve the following steps:
Network Assessment: The first step in implementing Sonic Firewall would be to conduct a network assessment to identify the existing network infrastructure, security vulnerabilities, and potential threats. This would involve a review of the network architecture, hardware and software configurations, and security policies and procedures.

Sonic Firewall Deployment: Once the network assessment is complete, the next step would be to deploy Sonic Firewall on the network. This would involve installing the hardware or virtual appliance on the network and configuring it according to the organization's security requirements and policies.

Configuration and Optimization: After the Sonic Firewall is deployed, it would need to be configured and optimized to provide the best possible protection against cyber threats. This would involve setting up rules and policies to manage network traffic, configuring intrusion prevention settings, and optimizing content filtering and VPN connectivity.

Testing and Evaluation: Once the Sonic Firewall is configured and optimized, it would need to be tested and evaluated to ensure that it is functioning properly and providing adequate protection against cyber threats. This would involve conducting penetration testing and vulnerability assessments to identify any security gaps or weaknesses in the network.

Maintenance and Monitoring: Finally, Sonic Firewall would need to be regularly maintained and monitored to ensure that it continues to provide effective protection against cyber threats. This would involve applying software updates and security patches, monitoring network traffic for suspicious activity, and conducting regular security audits.

Overall, the methodology for implementing Sonic Firewall would involve a comprehensive approach that includes network assessment, deployment, configuration and optimization, testing and evaluation, and ongoing maintenance and monitoring. This approach would help ensure that the organization's network is secure and protected against a range of cyber threats.

## 3.1 Description

Sonic Firewall is a network security solution designed to protect organizations from a wide range of cyber threats, including malware, viruses, ransomware, and other cyber attacks. It is a hardware or virtual appliance that is installed on the network and is designed to provide comprehensive protection against cyber threats, while also providing advanced security features such as intrusion prevention, content filtering, and VPN connectivity.

Sonic Firewall is designed to be easy to deploy and manage, with a centralized management console that enables network administrators to monitor and manage network security from a single location. It is also customizable, allowing organizations to configure and optimize the solution to meet their specific security requirements and compliance regulations.

Sonic Firewall uses a range of advanced security technologies to protect against cyber threats, including:
Intrusion Prevention: Sonic Firewall uses intrusion prevention technology to detect and prevent network attacks, including known and unknown threats.
Content Filtering: Sonic Firewall provides content filtering capabilities that enable organizations to block access to specific websites or applications, as well as filter web content based on categories or keywords.
VPN Connectivity: Sonic Firewall provides secure VPN connectivity that enables remote workers to connect to the network securely, while also providing a secure connection for branch offices and partners.
Threat Intelligence: Sonic Firewall uses threat intelligence to identify and block known threats, as well as to detect and prevent new and emerging threats.

Overall, Sonic Firewall is a comprehensive network security solution that provides organizations with advanced protection against a wide range of cyber threats. It is designed to be easy to deploy and manage, customizable to meet specific security requirements, and constantly evolving to keep up with the latest cyber threats and security trends.

## 3.2 Operating Environment - Hardware And Software

### Hardware:

A computer with a processor that supports virtualization (recommended at least a quad-core CPU)

Sufficient amount of RAM (recommended at least 8GB)

An internet connection to install required packages and libraries

### Software:

Operating System: Windows 10 or later version, or Linux

## 3.3 Technology used

Sonic Firewall uses a range of advanced security technologies to protect against cyber threats, including:

Intrusion Prevention: Sonic Firewall uses intrusion prevention technology to detect and prevent network attacks, including known and unknown threats. It monitors network traffic for suspicious activity and blocks malicious traffic before it can reach its destination.

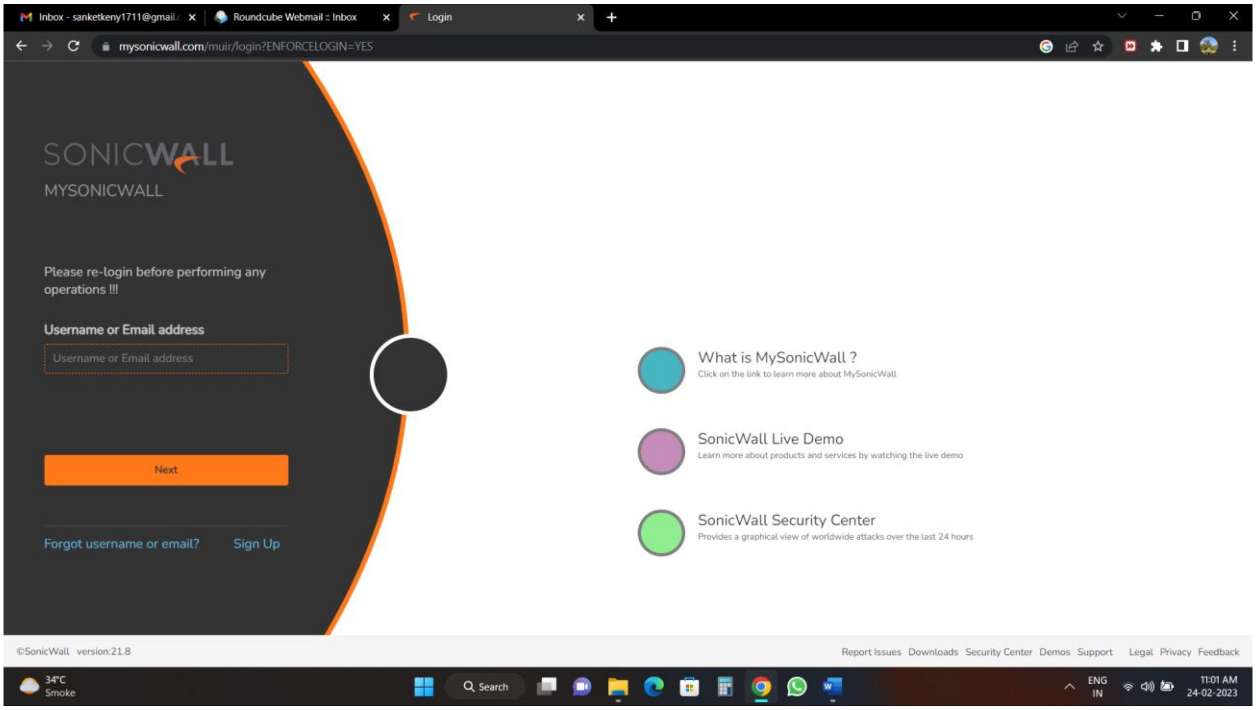
Content Filtering: Sonic Firewall provides content filtering capabilities that enable organizations to block access to specific websites or applications, as well as filter web content based on categories or keywords. This helps to prevent employees from accessing inappropriate content or downloading malicious files.

Virtual Private Network (VPN) Connectivity: Sonic Firewall provides secure VPN connectivity that enables remote workers to connect to the network securely, while also providing a secure connection for branch offices and partners. This helps to ensure that sensitive data is transmitted securely over the network.

Threat Intelligence: Sonic Firewall uses threat intelligence to identify and block known threats, as well as to detect and prevent new and emerging threats. This includes the use of machine learning algorithms and artificial intelligence to analyze network traffic and identify potential threats.

Deep Packet Inspection: Sonic Firewall uses deep packet inspection (DPI) to examine network traffic at the packet level. This enables it to identify and block advanced threats that may be hidden in encrypted traffic.

Analyzing and checking the ports of Sonic Firewall Of All Audi Mumbai Based Showrooms
Here I have attached a few screenshots of the image Here we analyze all the network in its port and the traffic of our organistation


Inbox - sanketkeny1711@gmail.
Roundcube Webmail :: Inbox
Login
mysonicwall.com/muir/login?ENFORCELOGIN=YES
SONICWALL
MYSONICWALL
Username or Email address
Next
Forgot username or email?
Sign Up
What is MySonicWall ?
SonicWall Live Demo
SonicWall Security Center
©SonicWall version:21.8
Report Issues Downloads Security Center Demos Support Legal Privacy Feedback
34°C Smoke
Search
ENG IN
11:01 AM 24-02-2023

Please re-login before performing any operations !!!

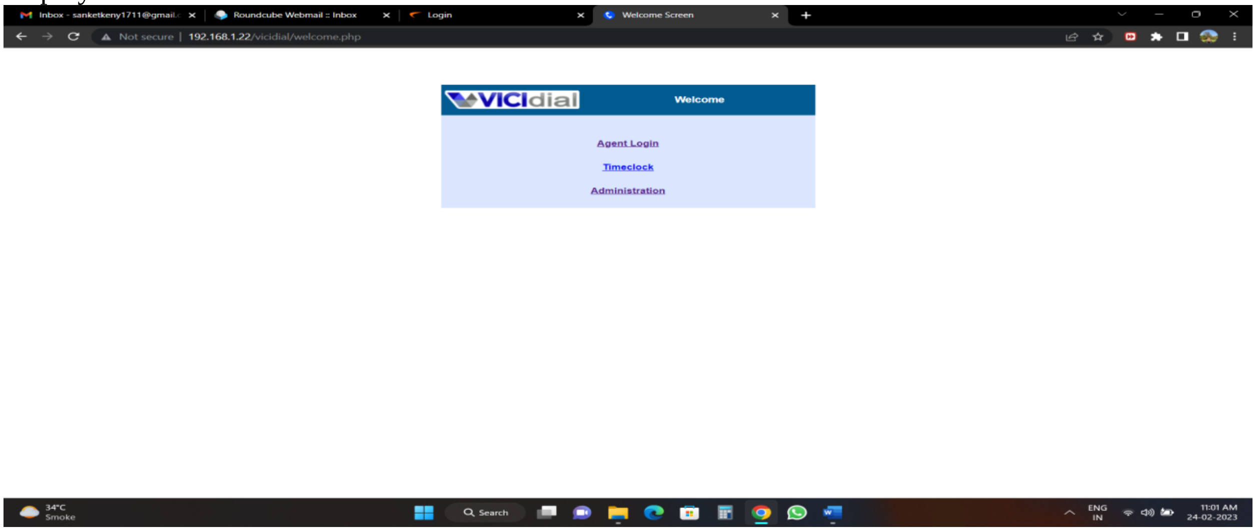
Username or Email address

Click on the link to learn more about MySonicWall

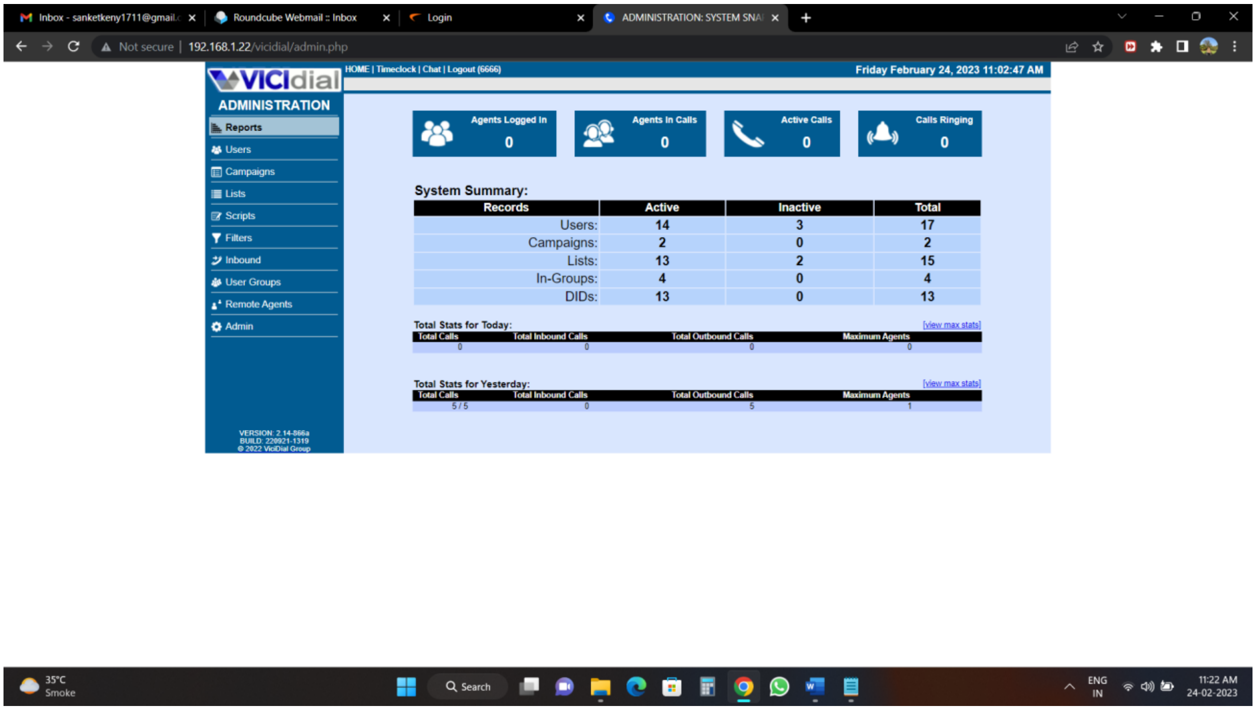
Learn more about products and services by watching the live demo

Provides a graphical view of worldwide attacks over the last 24 hours

Setting Up the ViCi Dialler for the company adding user in it as used for the telecaller of the company employes



Here we check the users are logged in or not in the system and in What campaings are the performing



Friday February 24, 2023 11:02:47 AM

| Agents Logged In | Agents In Calls | Active Calls | Calls Ringing |
|---|---|---|---|
| 0 | 0 | 0 | 0 |

System Summary:

| Records | Active | Inactive | Total |
|---|---|---|---|
| Users: | 14 | 3 | 17 |
| Campaigns: | 2 | 0 | 2 |
| Lists: | 13 | 2 | 15 |
| In-Groups: | 4 | 0 | 4 |
| DIDs: | 13 | 0 | 13 |

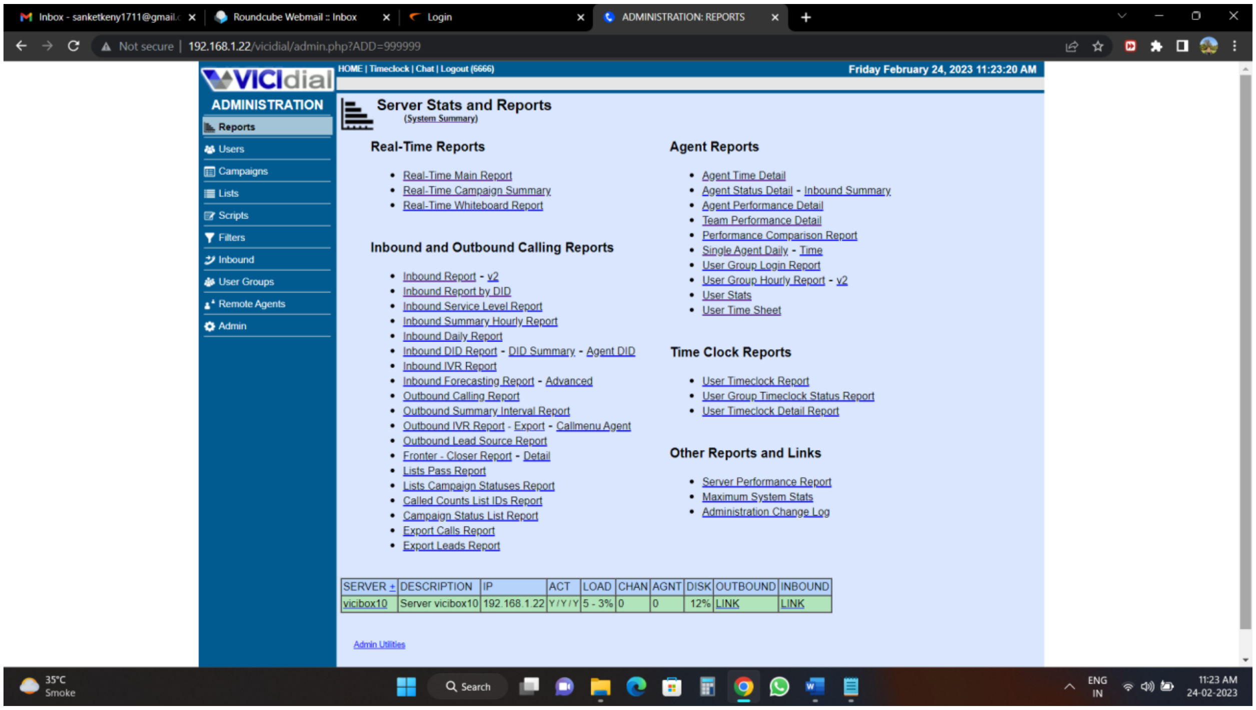
Total Stats for Today: [view max stats]

| Total Calls | Total Inbound Calls | Total Outbound Calls | Maximum Agents |
|---|---|---|---|
| 0 | 0 | 0 | 0 |

Total Stats for Yesterday: [view max stats]

| Total Calls | Total Inbound Calls | Total Outbound Calls | Maximum Agents |
|---|---|---|---|
| 5 / 5 | 0 | 5 | 1 |

Here we get the overall report of the work and what client is based in what system



Friday February 24, 2023 11:23:20 AM

Server Stats and Reports
(System Summary)

Real-Time Reports

- Real-Time Main Report
- Real-Time Campaign Summary
- Real-Time Whiteboard Report

Inbound and Outbound Calling Reports

- Inbound Report - v2
- Inbound Report by DID
- Inbound Service Level Report
- Inbound Summary Hourly Report
- Inbound Daily Report
- Inbound DID Report - DID Summary - Agent DID
- Inbound IVR Report
- Inbound Forecasting Report - Advanced
- Outbound Calling Report
- Outbound Summary Interval Report
- Outbound IVR Report - Export - Callmenu Agent
- Outbound Lead Source Report
- Fronter - Closer Report - Detail
- Lists Pass Report
- Lists Campaign Statuses Report
- Called Counts List IDs Report
- Campaign Status List Report
- Export Calls Report
- Export Leads Report

Agent Reports

- Agent Time Detail
- Agent Status Detail - Inbound Summary
- Agent Performance Detail
- Team Performance Detail
- Performance Comparison Report
- Single Agent Daily - Time
- User Group Login Report
- User Group Hourly Report - v2
- User Stats
- User Time Sheet

Time Clock Reports

- User Timeclock Report
- User Group Timeclock Status Report
- User Timeclock Detail Report

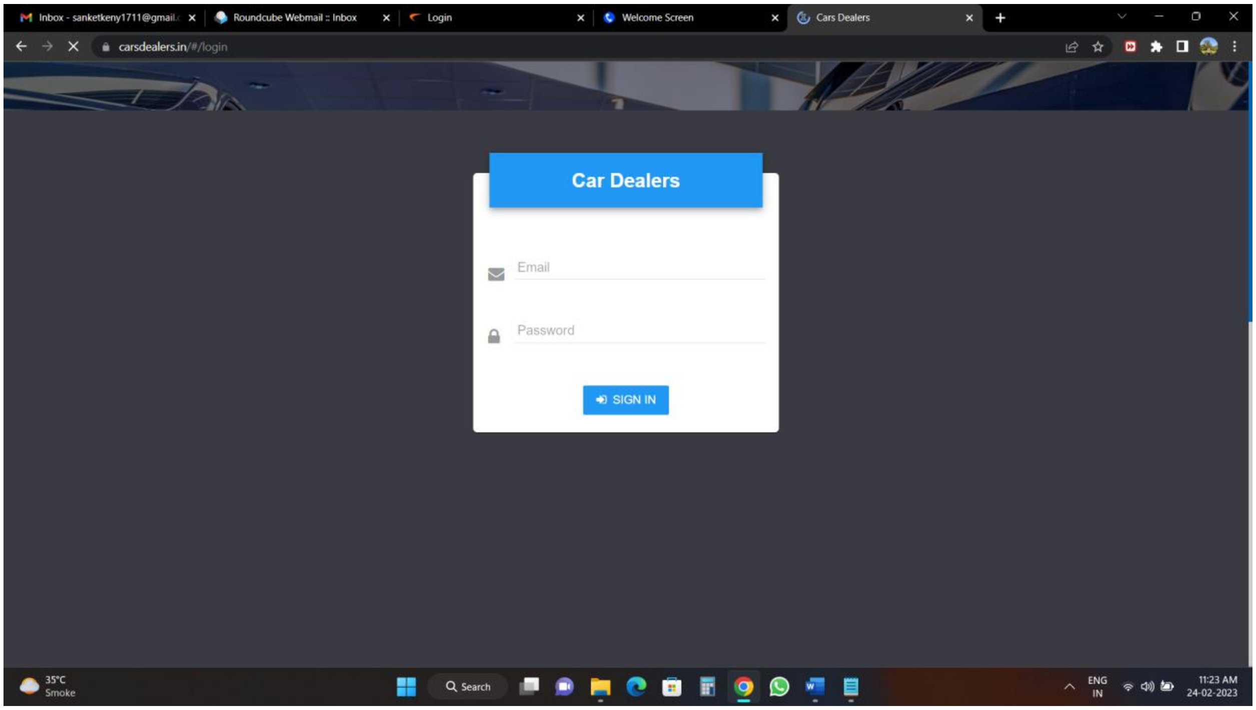
Other Reports and Links

- Server Performance Report
- Maximum System Stats
- Administration Change Log

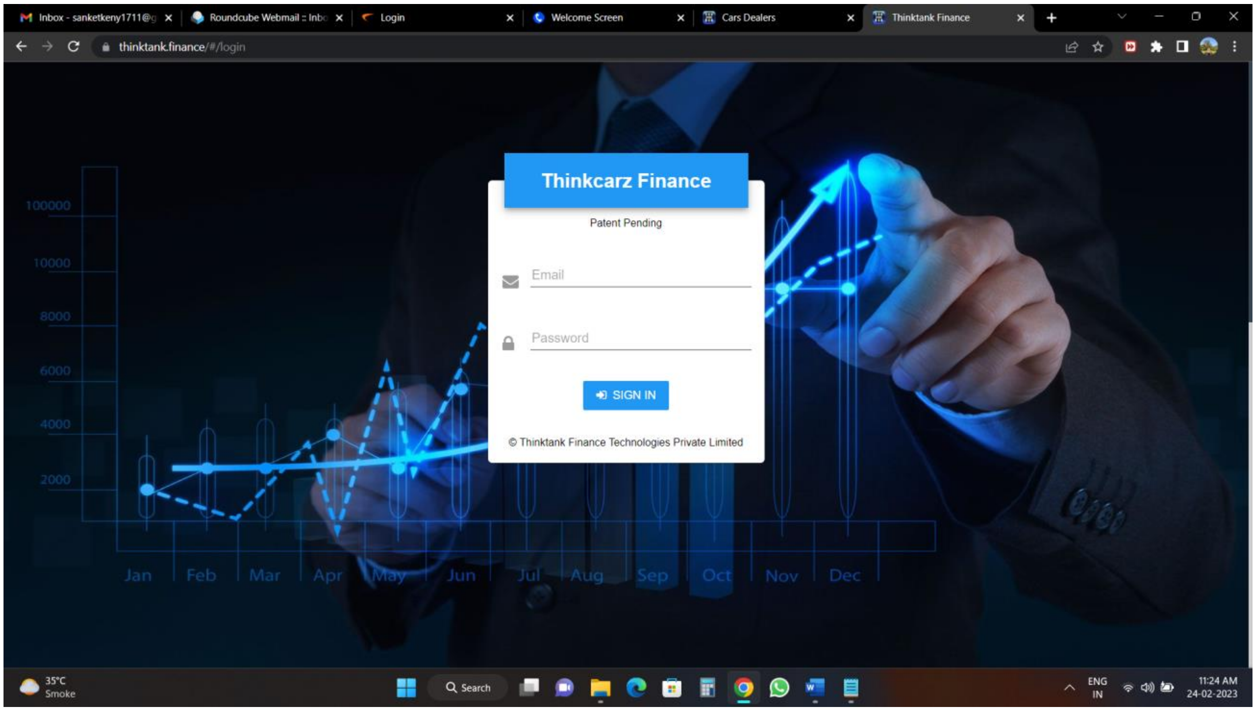
| SERVER + | DESCRIPTION | IP | ACT | LOAD | CHAN | AGNT | DISK | OUTBOUND | INBOUND |
|---|---|---|---|---|---|---|---|---|---|
| vicibox10 | Server vicibox10 | 192.168.1.22 | Y / Y / Y | 5 - 3% | 0 | 0 | 12% | LINK | LINK |

Admin Utilities

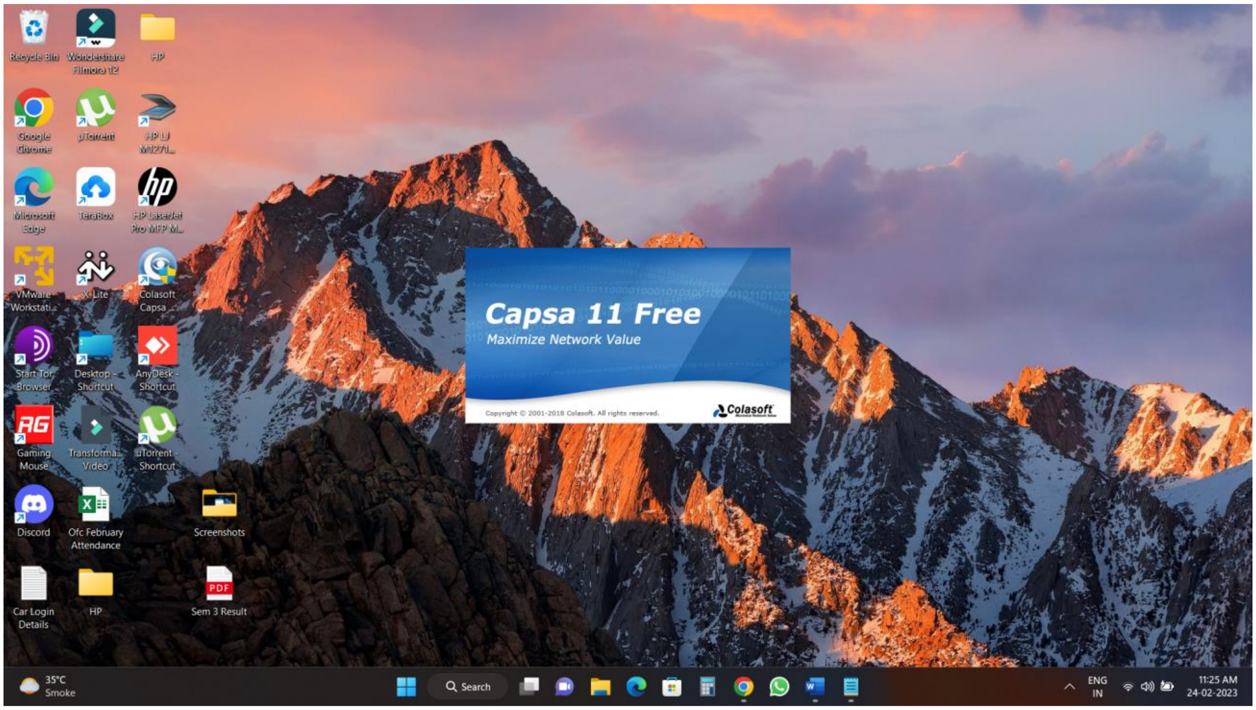
This is the Car dealer portal where we have added the car configuration and its specification which is directly linked with our other website such as ThinkTank finance



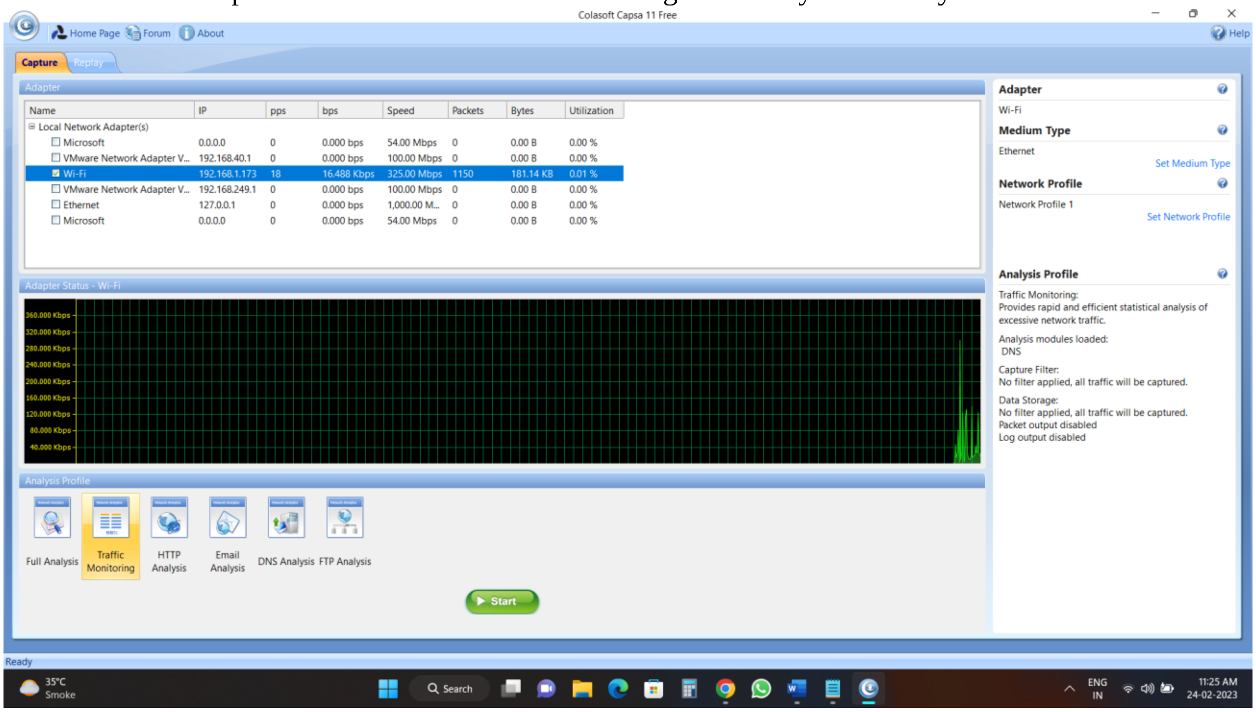
This Is the thinktank finance portal where we give financial value of each car and its listing is done .This is app is beneficial for the Car disbursement loan



This is Capsa 11 Software which we use to manage Baance loading of network in all our audi Mumbai Showrooms and workshop .It Helps us to find which regin uses what type of data and how much is consumed



There are various options to choose from which we can get the analysis of the system



| Name | IP | pps | bps | Speed | Packets | Bytes | Utilization |
|---|---|---|---|---|---|---|---|
| ⊟ Local Network Adapter(s) | | | | | | | |
| □ Microsoft | 0.0.0.0 | 0 | 0.000 bps | 54.00 Mbps | 0 | 0.00 B | 0.00 % |
| □ VMware Network Adapter V... | 192.168.40.1 | 0 | 0.000 bps | 100.00 Mbps | 0 | 0.00 B | 0.00 % |
| ☑ Wi-Fi | 192.168.1.173 | 18 | 16.488 Kbps | 325.00 Mbps | 1150 | 181.14 KB | 0.01 % |
| □ VMware Network Adapter V... | 192.168.249.1 | 0 | 0.000 bps | 100.00 Mbps | 0 | 0.00 B | 0.00 % |
| □ Ethernet | 127.0.0.1 | 0 | 0.000 bps | 1,000.00 M... | 0 | 0.00 B | 0.00 % |
| □ Microsoft | 0.0.0.0 | 0 | 0.000 bps | 54.00 Mbps | 0 | 0.00 B | 0.00 % |

**Adapter**
Wi-Fi

**Medium Type**
Ethernet
Set Medium Type

**Network Profile**
Network Profile 1
Set Network Profile

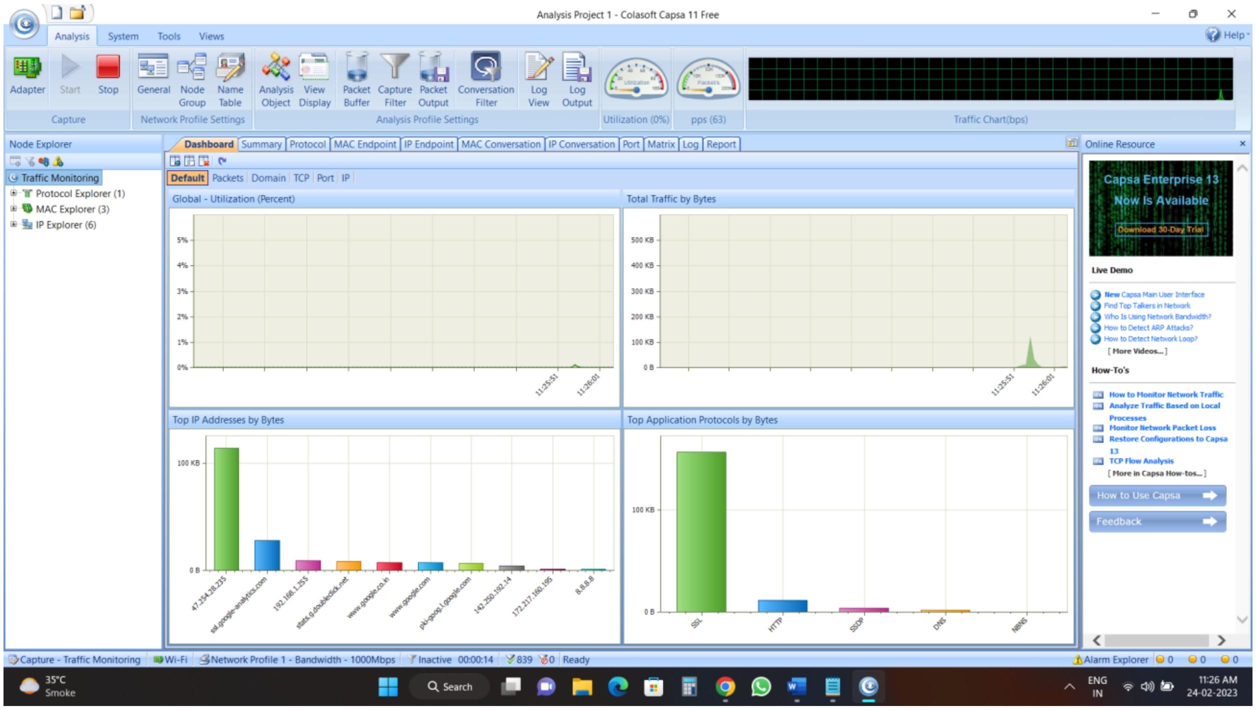
**Analysis Profile**
Traffic Monitoring:
Provides rapid and efficient statistical analysis of excessive network traffic.

Analysis modules loaded:
DNS

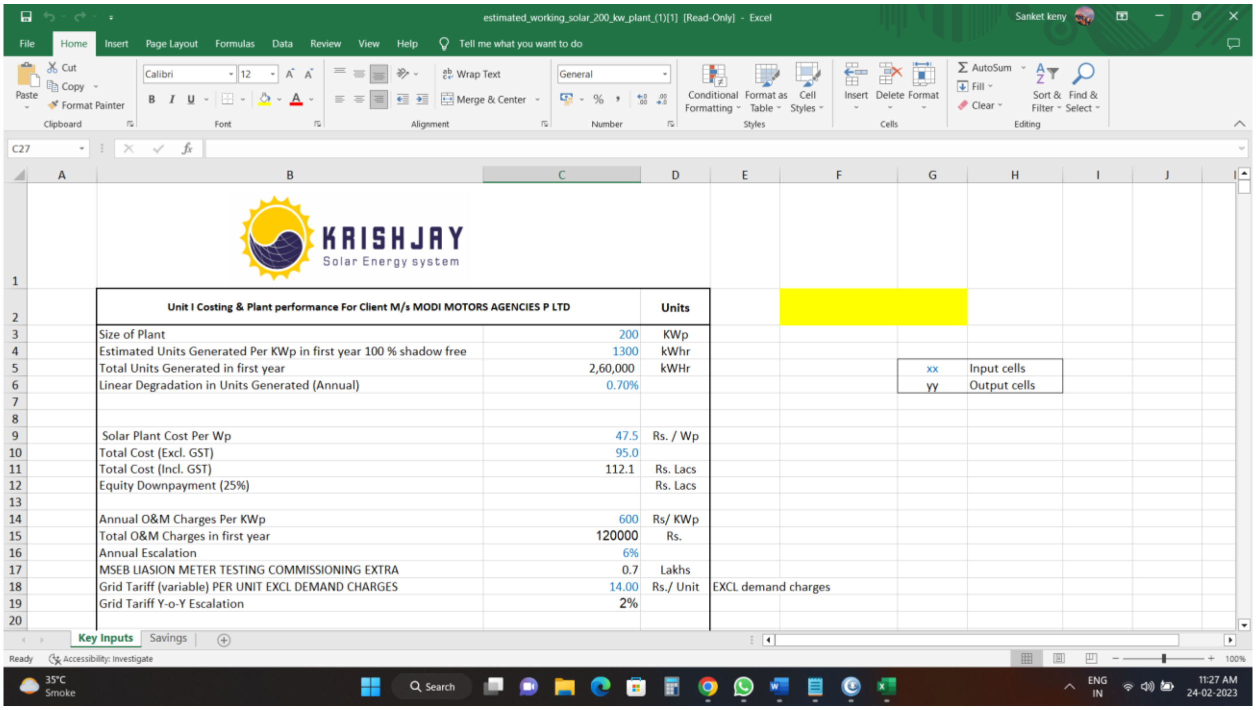
Capture Filter:
No filter applied, all traffic will be captured.

Data Storage:
No filter applied, all traffic will be captured.
Packet output disabled
Log output disabled

It gives us a detailed review of each of it



Setting up of solar panel in overall Showroom and reviewing it And its Configuration and budgeting

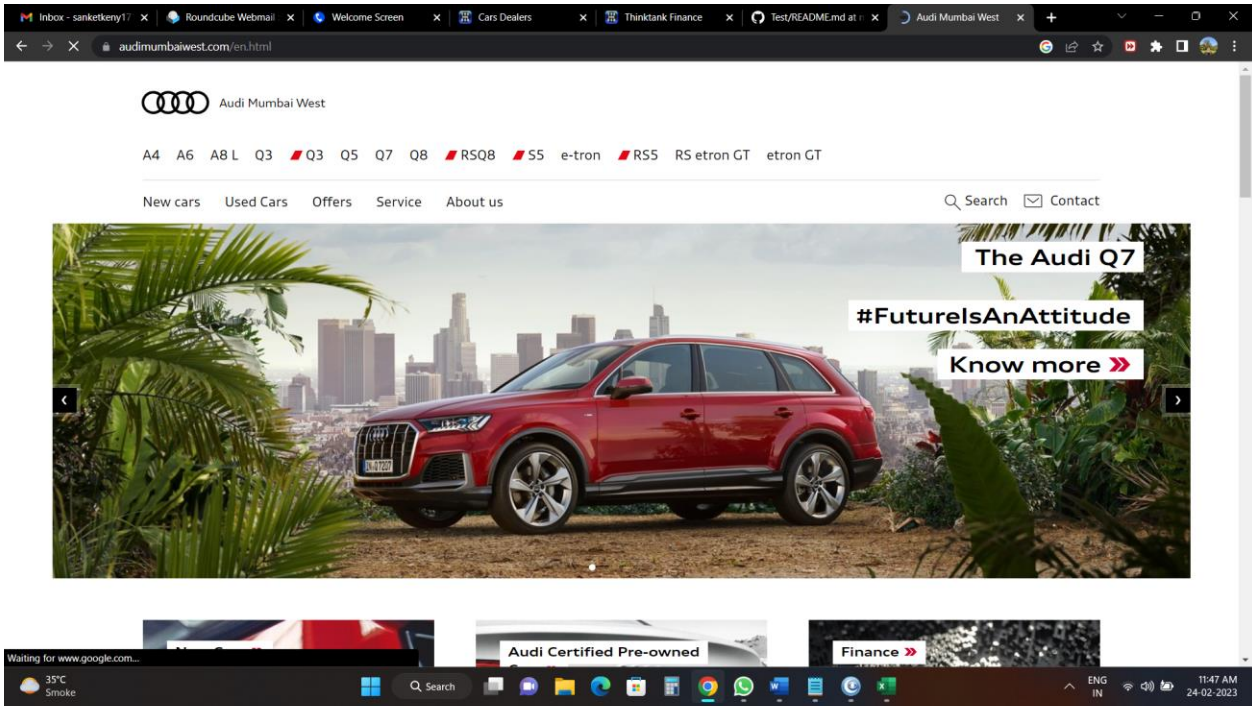


| Unit I Costing & Plant performance For Client M/s MODI MOTORS AGENCIES P LTD | | Units |
|---|---|---|
| Size of Plant | 200 | KWp |
| Estimated Units Generated Per KWp in first year 100 % shadow free | 1300 | kWhr |
| Total Units Generated in first year | 2,60,000 | kWHr |
| Linear Degradation in Units Generated (Annual) | 0.70% | |
| | | |
| | | |
| Solar Plant Cost Per Wp | 47.5 | Rs. / Wp |
| Total Cost (Excl. GST) | 95.0 | |
| Total Cost (Incl. GST) | 112.1 | Rs. Lacs |
| Equity Downpayment (25%) | | Rs. Lacs |
| | | |
| Annual O&M Charges Per KWp | 600 | Rs/ KWp |
| Total O&M Charges in first year | 120000 | Rs. |
| Annual Escalation | 6% | |
| MSEB LIASION METER TESTING COMMISSIONING EXTRA | 0.7 | Lakhs |
| Grid Tariff (variable) PER UNIT EXCL DEMAND CHARGES | 14.00 | Rs./ Unit |
| Grid Tariff Y-o-Y Escalation | 2% | |

EXCL demand charges

| | |
|---|---|
| xx | Input cells |
| yy | Output cells |

This is Audi Mumbai West website we need to monitor it and check its working and if it contains any glitches



Working on Various Inhouse applications such as work mail and powerpoint ,Tally and keeping it upto date on virtual servers As I don’t have the permission to share the screen shot of the server room or any other software as I could get this amount of screenshot for representation of the data

Our future projects Contains of :
finalizing of  Solar network  and panels
Vici Dialer Configuration to be enhanced
Audi Mumbai West Website to enhance
Some more Website creations and its technical survey to be done

# CHAPTER 4

## Conclusion and Future Scope

In conclusion, Sonic Firewall is a powerful network security solution that offers a range of advanced security technologies to protect organizations from a wide range of cyber threats. It is designed to be easy to deploy and manage, with a centralized management console that enables network administrators to monitor and manage network security from a single location.

Sonic Firewall provides features such as intrusion prevention, content filtering, VPN connectivity, threat intelligence, deep packet inspection, and advanced encryption to ensure comprehensive protection against cyber attacks.

Looking to the future, Sonic Firewall will likely continue to evolve and improve to keep up with the ever-changing landscape of cyber threats. This may include the integration of new security technologies such as artificial intelligence and machine learning, as well as enhancements to existing features to provide even greater protection against cyber attacks.

Additionally, Sonic Firewall may expand its capabilities to provide enhanced protection for emerging technologies such as cloud-based applications and the Internet of Things (IoT).

Overall, Sonic Firewall is a powerful and flexible network security solution that is well-positioned to continue providing comprehensive protection against cyber threats for organizations of all sizes in the years to come.

# CHAPTER 5

## REFERENCES

SonicWall: https://www.sonicwall.com/
SonicWall TZ series: https://www.sonicwall.com/products/firewalls/tz-series