Perl Scripting, Automation and UNIX

Project report submitted in partial fulfillment of the requirement for the degree of Bachelor of Technology

in

Information Technology

By

Aayushi Gupta (151472)

Under the supervision of

Mr. Sarthak Gupta

To

Department of Computer Science & Engineering and Information Technology
Jaypee University of Information Technology Waknaghat, Solan-173234, Himachal Pradesh

Candidate's Declaration

I hereby declare that the work presented in this report entitled **"Networking, Perl Scripting, Automation and UNIX"** in partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology** in **Computer Science and Engineering/Information Technology** submitted in the department of Computer Science & Engineering and Information Technology**,** Jaypee University of Information Technology Waknaghat is an authentic record of my own work carried out over a period from Feb 2019 to June 2019 under the supervision of **Mr. Sarthak Gupta** (Software Engineer-QA).

The matter embodied in the report has not been submitted for the award of any other degree or diploma.

(Student Signature)
Aayushi Gupta, 151472.

This is to certify that the above statement made by the candidate is true to the best of my knowledge.

(Supervisor Signature)
Mr. Sarthak Gupta
Sr. Software Engineer
SMSM-QA

Dated: 15th May,2019

ACKNOWLEDGEMENT

I take this opportunity to express my profound gratitude and deep regards to my mentor Mr. Sarthak Gupta for his exemplary guidance, monitoring and constant encouragement throughout the course of this thesis. The blessing, help and guidance given by him time to time shall carry me a long way in the journey of life on which I am about to embark.

I also take this opportunity to express a deep sense of gratitude to Mr. Alok Kushwaha, Director, Engineering QA, Zscaler, for his cordial support, valuable information and guidance, which helped me in completing this task through various stages.

I am obliged to staff members of Zscaler, for the valuable information provided by them in their respective fields. I am grateful for their cooperation during the period of my assignment.

Lastly, I thank almighty, my parents for their constant encouragement without which this assignment would not bepossible.

Aayushi Gupta

TABLE OF CONTENTS

CHAPTER-1

INTRODUCTION

1.1 Introduction

The company was founded in 2008 by Chief Executive Officer Jay Chaudhry. Zscaler is headquartered in San Jose, California, and has offices around the world. Zscaler is an exciting and fast growing technology company. The most innovative enterprise in the security market, valued at $ 35 billion, the company is working to integrate cloud computing with Internet security. Just as Salesforce has transformed the CRM market, Zscaler is revolutionizing the world of Internet security. Today, Zscaler protects more than 15 million users of more than 5,000 of the world's largest corporations and government organizations against cyber attacks and data breaches, while remaining fully compliant with corporate and regulatory policies. Global 1000 brands such as GE, Nestle, ExxonMobil, Schneider Electric, as well as government and military organizations such as the US Marines, NATO and the UK National Health Services rely on Zscaler to provide secure and productive Internet experience for all their users. , from any device and from any place in the world.

1.2 Problem Statement

Cloud is the differentiator. Zscaler deploy all its services 100% from the cloud.

- No software installation needed.
- No hardware setup required.
- Just subscribe and be secure everywhere.
- Can customize policies for different users,groups and locations.
- Very fast multitenant architecture which enforces approx. zero latency.
- Highly scalable architecture. Beside this Zscaler has 100+ data centers,processes 25B+ transactions everyday,blocks 105M+ threats everyday and has 100K+ security updates every day.

1.3 Objectives

Objectives of this company and services provided by it are:

- Access control cloud firewall. url filtering. bandwidth control.
- Threat prevention antivirus. intrusion prevention. advanced protection. cloud sandboxing.
- Data protection forensics. DLP
- Logging for real time analysis

1.4 Methodology

When a new connection request is hit at sme,it will generate the user login page and the filled information is then forwarded to the CA.CA then checks if it is a valid user name by checking into its cache.In case of valid user the authentication request is forwarded to the AA(authentication agent) or AD,which performs the final authentication. Above is the case of nonhosted DB. In case of hosted DB, CA stores the user credentials itself.So CA performs the final authentication and no AA/AD are involved.
Zscaler provides cloud-based information security delivered through what would be the world's largest security cloud with more than 100 global data centers. Localized datacenters store security policies that can be distributed worldwide in seconds, tracking users as they travel around the world to apply these strategies without latency. Zscaler serves as a web proxy, routing all traffic in its software to enforce corporate and security policies, eliminating the time and money companies spend managing Web filtering and security on their own servers .

1.5 Organization

1.5.1 Zscaler for APTs

Zscaler saves us from from zero-day attacks and advanced threats by providing proactive protection against severe threats, file-based behavior and security threats such as threat intelligence feeds. Zscaler gives us a comprehensive solution that consolidates the existing features of security appliances to save, detect and protect from advanced security threats.

1.5.2 Zscaler Mobile Security

Zscaler Mobile Security provides its real-time protection and analysis to mobile devices in BYOD environments by distributing mobile traffic through its centralized cloud. Mobile Security makes us able to see into mobile application traffic, saves us from from web-based threats, risky applications and application of policy on mobile devices.

1.6 Partnerships

Zscaler joins hands with many internet providers including RSA, Okta, OneLogin and Ping Identity to provide its customers with simple cloud security. Zscaler joins hands with mobile management (MDM) vendors, including AirWatch and MobileIron to enhance MDM with mobile security. Zscaler takes help from security information event management (SIEM) service providers, including HP ArcSight, IBM QRadar and Splunk, enabling data detection, digital security analysis and combination with industry and governmental rules and regulations.

..

CHAPTER-2

LITERATURE SURVEY

2.1 Recognization

I.6.1. 2008

"InformationWeek named Zscaler "Startup of the Week".

I.6.2. 2009

Is was named as"Cool Vendors in Software-as-a-Service Security, 2009" by Gartner.

I.7.3 2011

It was named as "Cool Vendors in Cloud Security Services, 2011" by Gartner. Zscaler was named a "Leader" in the Gartner "Magic Quadrant for Secure Web Gateway." Zscaler was named an "Emerging Vendor 2011: Security Vendors" by CRN. Zscaler was named a "Best Web Content Management Finalist" in the SC Magazine.

I.7.4. 2012

It was named as "Leader" in the Gartner "Magic Quadrant for Secure Web Gateways." Zscaler was named an "Emerging Vendor 2012: Security Vendors" by CRN. Zscaler CEO Jay Chaudhry was named a "The Top 25 Disrupters Of 2012" by CRN.

I.7.5. 2013

It was named as "Leader" in the Gartner "Magic Quadrant for Secure Web Gateways." Zscaler was named an "Emerging Vendor 2013: Security Vendors" by CRN. Zscaler was named a "Tech 10: Hot Antivirus Alternatives For 2013" by CRN. Zscaler was named a Red Herring "2013 Top 100 North America: Winners."

I.7.6. 2014

It was named as "Leader" in the Gartner "Magic Quadrant for Secure Web Gateways." It is voted as the top 50 best places to work at in private sector. Zscaler was named an "Emerging Vendor 2014: Security Vendors" by CRN. It was named "Tech 10: Hot Antivirus Alternatives For 2014" by CRN. Was named as a Red Herring "2014 Top 100 North America: Winners."

2.2 Customers

Today Zscaler leads the market in providing its customers with the largest threats possible.Globally there are 1000 of brands such as such as GE, Nestlé, ExxonMobil, Schneider Electric, United Airlines, including government enterprises and military related organisations like United States Marines, NATO and the National Health Services of the UK rely on. Zscaler always try to provide its clients with maximum possible security so that there is no complaints from the user.It always tries to help it clients by applying various kinds of policies such as bandwidth control, firewall filtering, DNS rules etc.

2.3 The Zscaler Difference

In today's world major big companies are struggling to provide maximum security to their fellow colleagues, security is encompassed to highest possible level so that there are no breaches.

The major difference that Zscaler provides is by providing maximum possible authentication provided by ensuring all policies are strictly applied without any chance of being decoded. All the information in stored in id format in encrypted way so that it is difficult to decode. Also results of policies such as sandbox reports are again verified so that it is ensured that result provided by sandbox is correct.

.

2.4 Zscaler Outreach

Zscaler has the world's largest footprint for any security vendor. Every day, Zscaler protects more than 12 million users in more than 200 countries around the world.

CHAPTER-3

SYSTEM DEVELOPMENT AND ARCHITECTURE

Zscaler Development Process:

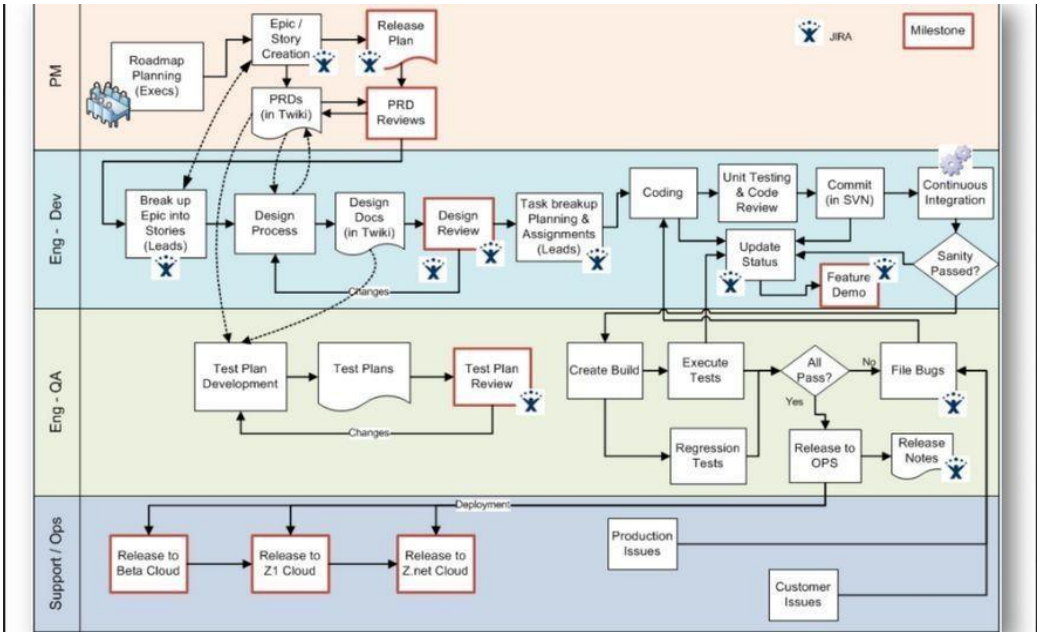
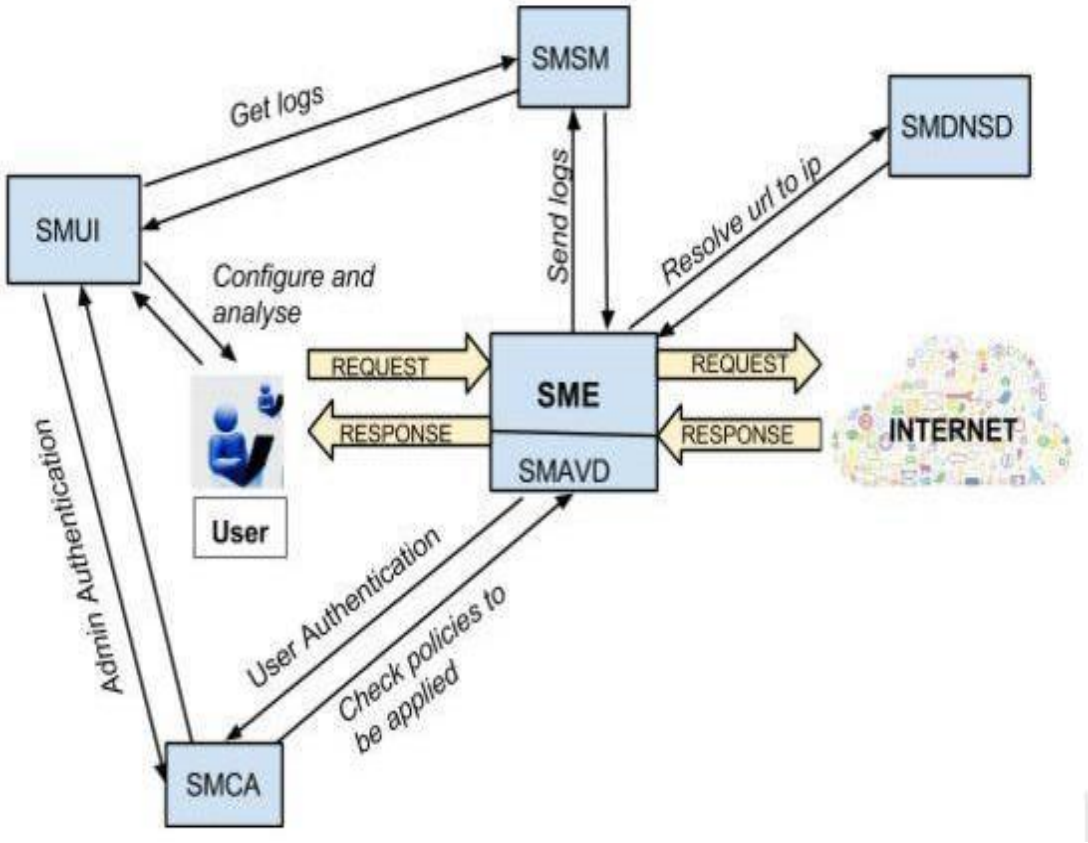


Fig: Steps followed for development in Zscaler

Zscaler's architecture is made from ground without any prior knowledge. Zscaler architecture is developed in a very easy manner so that it is easier to communicate with all nodes.The architecture consists of various components like SMCA, SME, SMSM, SMUI. All these nodes are connected to each other and and work together to provide a overall smooth experience.SMCA is the central authority which consists of the complete database. All the requests go to SMCA for authentication of users and their passwords. SME acts as a gateway as all transaction requests goes through SME with the help of cookies. The SMSM is the Nanolog team which logs all the transactions so that we are able to present different types of charts on UI where users can check which sites are accessed by the users what are the number of blocked and non blocked transactions.

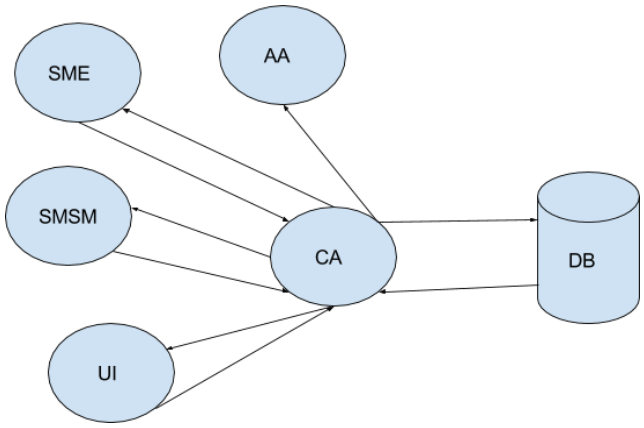
Zscaler Cloud Architecture:



Zscaler Cloud Architecture's Components

1. Central Authority (SMCA)

CA is the brain of the whole cloud architecture where all the control and configuration informations are stored.CA ties the entire cloud together.One CA cluster(primary CA + secondary CA) is present for each Zscaler cloud.



Functions of CA :

1.1 Data repository

● Stores informations of all the nodes present in the cloud like systemids of all the nodes,primary node of a cluster.

● Holds the lists of organisations,users, groups and departments along with all the policies and configurations of the company.

● No user credentials are stored in the zen or nanolog.They are stored at AA/AD of the organisation(in case of nonhosted DB) or at CA(in case of hosted DB).

● It assigns unique id to company,location and user and stores them in a fast memory. Zen and Nanolog are only aware of these token ids.

1.2 Health Monitoring

- Passive Health Monitoring:In this method CA sends health request message to all the nodes and the nodes send reply messages containing information regarding their health (e.g. memory and cpu usages). Above information is used in load balancing also.
- Active Health Monitoring:In this method CA sends node specific requests to the various nodes, e.g. for Smsm node some log retrieval request is sent and for Sme a request having real time traffic is sent.If the node replies as expected then the node is working great otherwise it is marked as down.

1.3 Authentication

When a new connection request is hit at sme,it will generate the user login page and the filled information is then forwarded to the CA.CA then checks if it is a valid user name by checking into its cache.In case of valid user the authentication request is forwarded to the AA(authentication agent) or AD,which performs the final authentication. Above is the case of nonhosted DB. In case of hosted DB, CA stores the user credentials itself.So CA performs the final authentication and no AA/AD are involved.

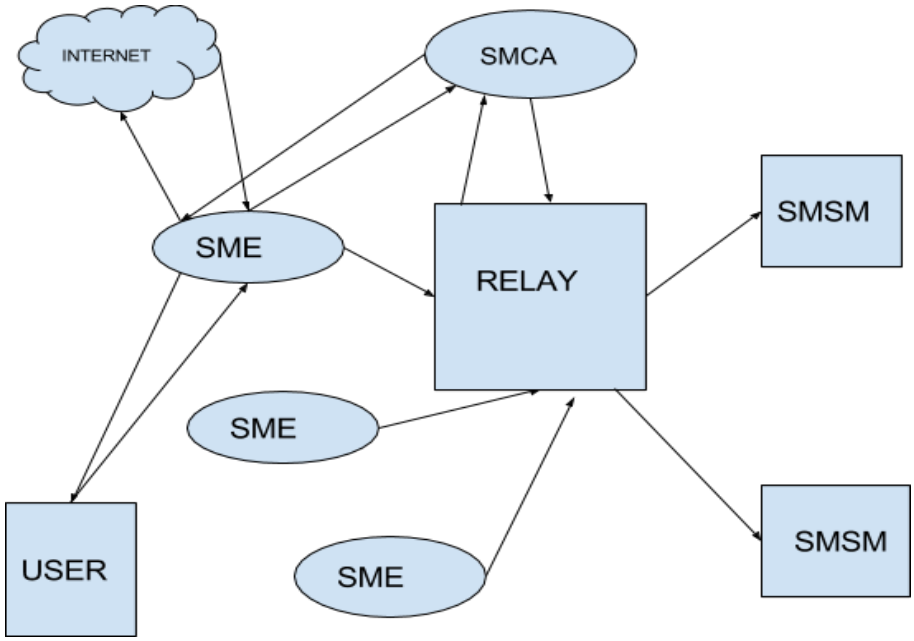
1.4 Does Load Balancing For SMSM

By analysing the health status of the nodes in the smsm cluster. Selects The New Primary Node Of the Smsm Cluster If the Existing Primary Goes Down: The most updated secondary is chosen as the new primary. And many more… as mentioned earlier CA is the brain of the cloud,so its functions are quite crucial for the well functioning of the cloud.If CA goes down then the whole cloud will go down.

2. ZEN -Zscaler Enterprise Node

These nodes are actually connected to the end user. These nodes are responsible for enforcing the policies on the end-point user. The session is initiated here by forwarding the traffic to the CA to check which policies are applicable. It is also called as SME. An enterprise forwards it traffic to the nearest ZEN which first tells the users to add his username. The ZEN first authenticates ths username by sending it to SMCA which authenticates the user. SME sends this username to SMCA through smca_aw cookie which contains the username.When the SMCA authenticates the username by checking it into database it sends it back to the user which is then asked to add password. After entering the password the request is again send to SMCA which authenticates this and tells the SME which policies need to be applied. SME applies this policies and provides the user with the desired action that whether it can view a site or not.

When traffic is hitting the enforcement node. We need to make the policy decision as fast as possible. So the proxy and the entire software stack was written from scratch that could handle the proxy latency with a few micro seconds. The data comes into memory and leaves from memory. It never touches the hard disk until it reaches the nanolog cluster.



2.1 SME MAIN FUNCTIONS

- SME also referred as Zen, the gateway to which the user's network traffic will be redirected to.
- SME asks SMCA for the policies to be applied, once user getsauthenticated.
- SME verifies the incoming traffic against the policies to decide whether to allow it or block it.
- SME also has anti virus detection engines that matches for the signatures in incoming traffic to identify malicious links.
- SME also performs sandbox testing when required to analyse the behaviour of suspect code.
- All the users will be redirected to their nearest zen servers by number of techniques like tunneling, PAC or proxy chaining.
- SME captures the logs and sends it to SMSM.

2.2 Traffic Forwarding Methods

2.2.1 PAC FILE HOSTING

- Fully supported traffic forwarding method for roaming users.
- A javascript which tells the browser which proxy to connect over which tcp port and can also instruct the browser to bypass the proxy for certain destinations and protocols.
- The PAC File is hosted on the Pac server of the Zscaler cloud.
- Each customer can create his own PAC file and host it in their profile in the Zscaler cloud.
- Advantage of hosting on the server is the availabilty of variables - GATEWAY and SECONDARY_GATEWAY, this instructs the pac server to insert the IP addresses of the closes ZENs based on the IP address of the customer.

2.2.2 GRE

- Establishing a GRE tunnel between the edge device andZen.
- GRE requirements:
    - Static routable IP.
    - GRE compatible device.

- If above requirements are met the customer needs to contact the zscaler support to enable their IP address for GRE tunneling.
- Each IP address can connect to up to 2 separate ZENs for GRE.
- GRE routers have to be configured to send all the internet bound traffic through these GRE tunnels.

VPN IPSEC

- VPN helps to protect users and secure public and private networks. Unsecured networks are also secured by various encryption and decryption techniques.
- Zscaler supports aggressive mode and main mode VPN access. In order to use main mode VPN, you need to have a static and routable IP address associated to your VPN edge device.
- If your site is using dynamic IP addressing and your edge device supports it you can use aggressive mode. This does not require you to have support provision your IP address in the system.

PROXY CHAINING

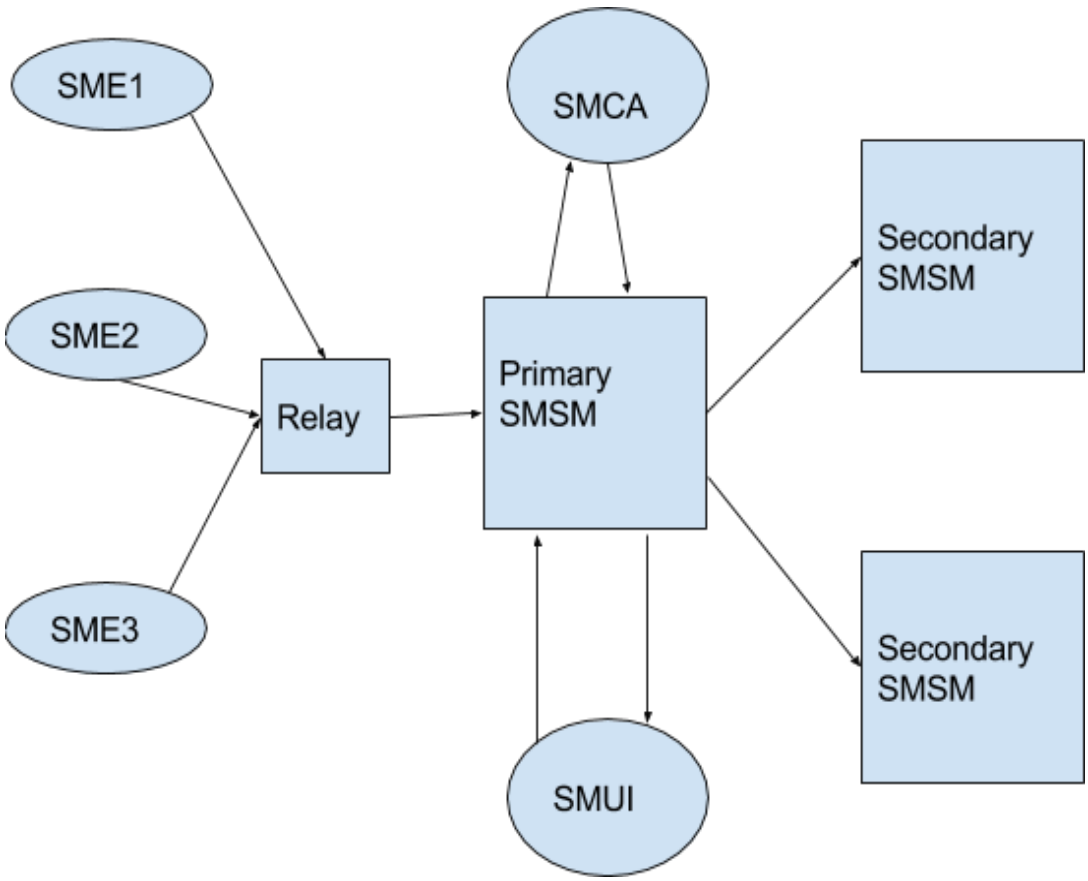
- Proxy chaining is a very useful deployment option where you already have a proxy solution deployed.
- This enables you to realize the value of Zscaler without any significant configuration changes. For instance, you can setup a BlueCoat proxy to forward all traffic for a certain subnet, users, or category to Zscaler.
- You can send all uncategorized traffic to Zscaler and begin to immediately use its superior threat analysis engine.

PORT FORWARDING

- In the browser, you configure the forwarding port and the proxy is set as the IP of a ZEN.
- The port could be 443 or some other port assigned by Zscaler.

3. SMSM (SafeMarch Statistical Manager)

SMSM which is Safe march Stastical Manager helps to store the logs of all the transactions which pass through the SME. Logs are stored in two ways one which stores complete transactions in id format and other stores the counters. These logs are provided to the user and the charts that we see on UI are also generated through these logs stored by SMSM.



- The logs generated by Zen are stored in the nanolog clusters. Only the traffic meta data is stored and not the actual data.
- The logs of an http request or response are approximately 2000 bytes long. We are generating 30000 of these requests per second from every Zen. So we are generating 2000 * 30000 bytes of data per second from every zen. So the data needs to be compressed.
- Log routers have the mapping of a user id to the nanolog cluster where its logs needs to be stored. The nanolog cluster is located in the geographical location of the customer's choice.
- NSS(Nanolog streaming service) is a virtual machine located in the user's premises. It establishes a secure connection with the nanolog cluster storing the company's data and the nanolog cluster can directly stream the nanolog data to it.
- 370k counters are logged every second. So these need to be stored in the compressed format.

Every transaction that comes on the smsm node for logging contains around 30 fields but all of them may not be needed to be stored and this point is kept in mind for compressing the transaction logs.

CHAPTER-4

TEST PLAN

4.1 Writing Test Plans

4.1.1 Goal- To prepare ourselves to think through the efforts needed to validate the feature.

4.2 Introduction to SMUI

4.2.1 Goal- To understand the user interface portal of Zscaler that how logs are stored so as to test each feature.

4.3 Networking Fundamentals

4.3.1 Goal- to take advantage of prior knowledge of network fundamentals and practical knowledge of concepts such as telnet, initial UDP sessions, traceroute, ssl connections, advanced proxy application, self-signed ssl agent, and so on.

4.4 Introduction to Linux Commands

4.4.1Goal- For basic Linux commands and text editors usage and learning.

4.5 Configuration of the Setup

4.5.1 Goal- To configure the setup for manual testing of the feature assigned.

4.6 SMCA

4.6.1 Goal- To understand the role, working and monitoring of SMCA in the Zscaler's cloud architecture.

4.7 SAML

4.7.1 Goal- To get familiar with the security assertion markup language (SAML) and use it for feature testing on the client side.

4.8 Manual Testing

4.8.1 Goal- To make sure that the feature under testing is bug free and as per the requirement of the program requirements document(P.R.D.).

4.9 Automation

4.9.1 Goal- To automate the various test cases with the help of Perl scripting to increase the effectiveness, efficiency and coverage oftesting.

4.10 Script Debugging

4.10.1 Goal- To make the scripts failing after upgrade error free by setting breakpoints.

4.11 Verifying Regression and Bugs

4.11.1 Goal- To verify the results of the non automated test cases and client side issues.

4.12 Migration Testing

4.12.1 Goal- To test the components of the clone of the production cloud before and after migration.

4.1 Writing Test Plans

To write the test plan the for the feature assigned we need to understand the feature in detail with help of the PRD and understanding the feature from the developer. Writing test plan is necessity before beginning any project because of the following reasons;-

IV.7.1 We need to make a test plan before starting any project because it tells us how much effort is required so that our software is accepted by the end users..

IV.7.2 We need to make a test plan because it makes it easier for the end users to understand the project and makes it easier for them to validate.

IV.7.3 We need to make a test plan because it is a necessity in a cooperative world.

IV.7.4 We need to make a test plan because it helps us find errors easily.

IV.7.5 We need to make a test plan because it provides us with a written document where scope, project objective everything is mentioned.

IV.7.6 We need to create a test plan because in this all test cases are written, we know the count of pass and fail cases.

IV.7.7 We need to make a test plan because it provides us with strategies that helps us improvise our project

IV.7.8 We need to make a test plan because the software testing process is a 3 step process, of which first part is testing plan making.

IV.7.9 We need to make a test plan because it helps us review our project with our fellow team mates and colleagues.

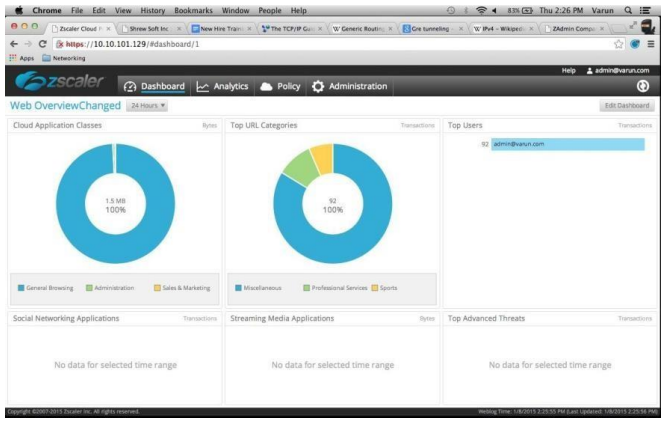
IV.7.10 We need to create a test plan in a documented way because it provides us with basic knowledge.

4.2 Zscaler Admin UI

Zscaler admin UI allows admin to have wide observation on the traffic of different users, some configure policies are also applicable on the users, management of user accounts, shows engagement of any transaction for analytics on SME.

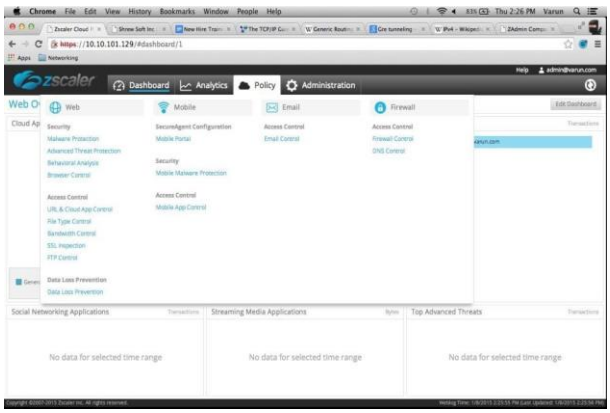
4.2.1 Dashboard

It gives the detailed description of traffic on the cloaud application and url traffic from various users in the form of pie charts.



4.2.2 Policy

You can set different policies on various individual,groups or even departments based on your requirement.

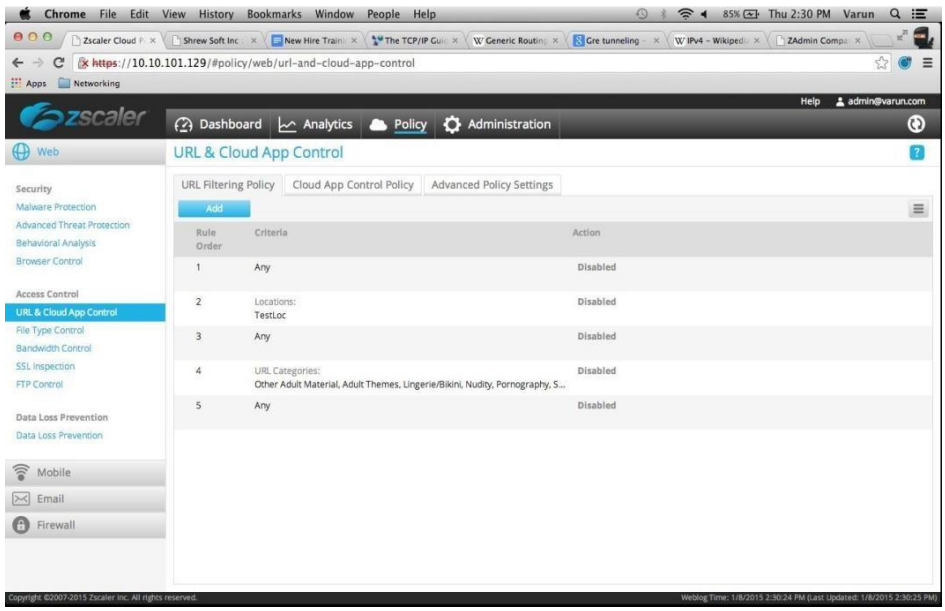


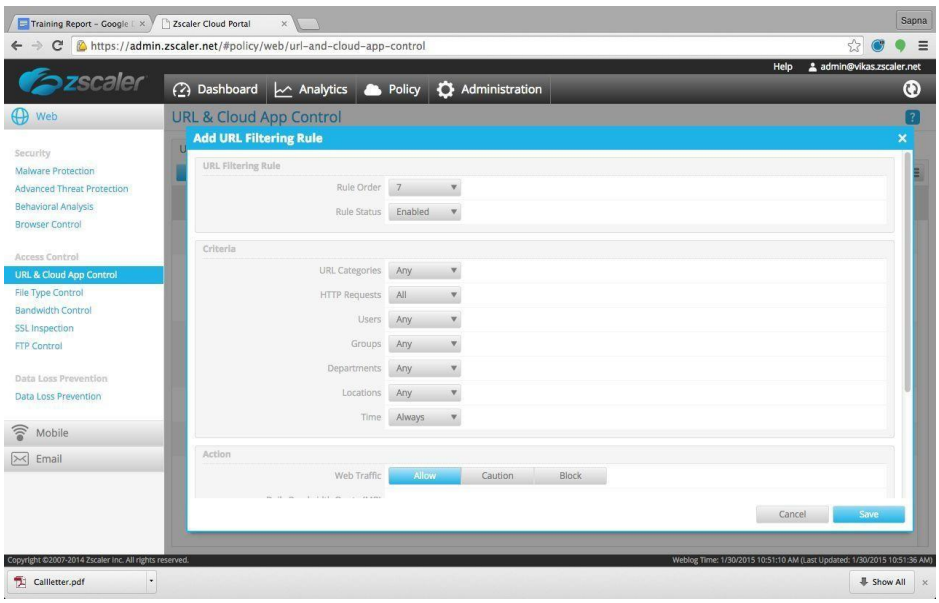
Web policies

Behavioral analysis, browser control, advanced threat protection and malware protection are used to provide maximum security.

Access Control

It can be used on certain file types and urls to block those content that should not be accessed by the user.





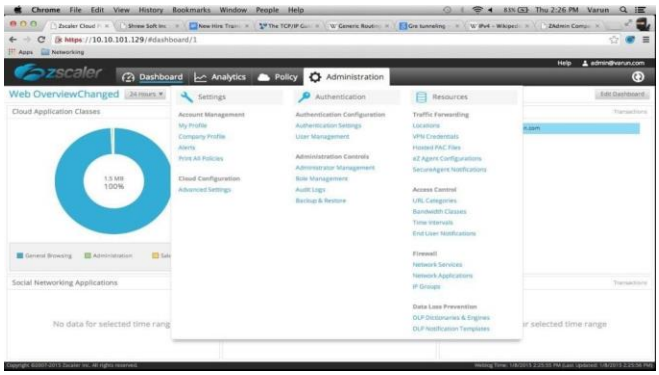
Bandwidth control

Bandwidth policy is applied to users on a site-only basis and not on road warriors. It can be of two types either on a session basis or a minimum limit and maximum bandwidth.

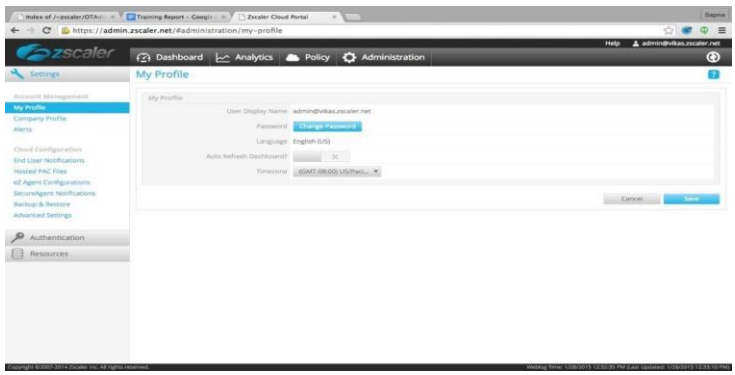
Follow these steps to change bandwidth policy:

1. ZA is used to change the static ip of computer.
2. Location is added in SMUI under administration tab,ssl scanning is enabled and download and upload limit is specified.
3. On particular location bandwidth control can be applied from policy tab.

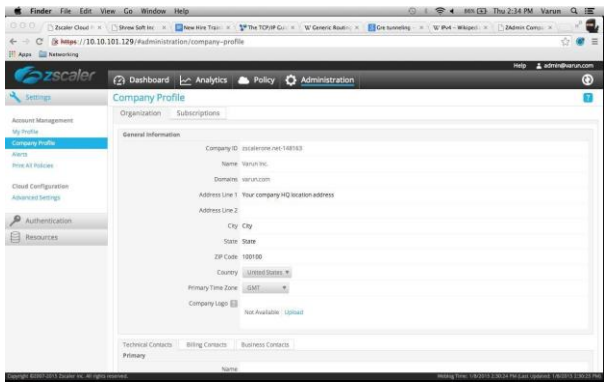
4.2.3 Administration



Account Management:



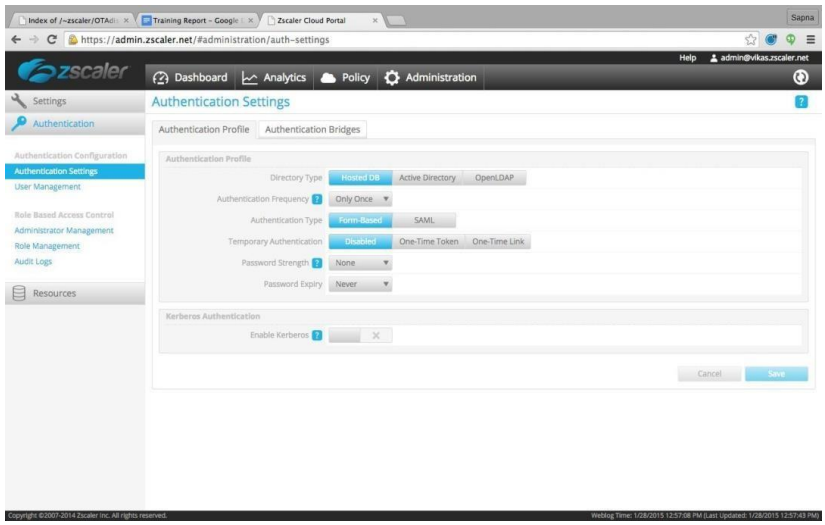
Admin can manage his own account.

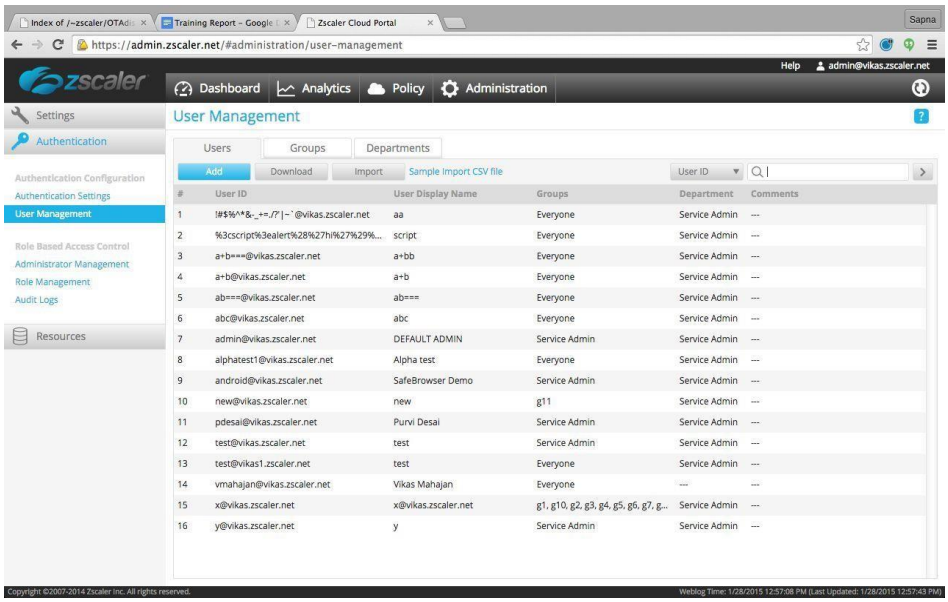


Admin can set company's profile.

Authentication configuration

Admin can specify the authentication profile

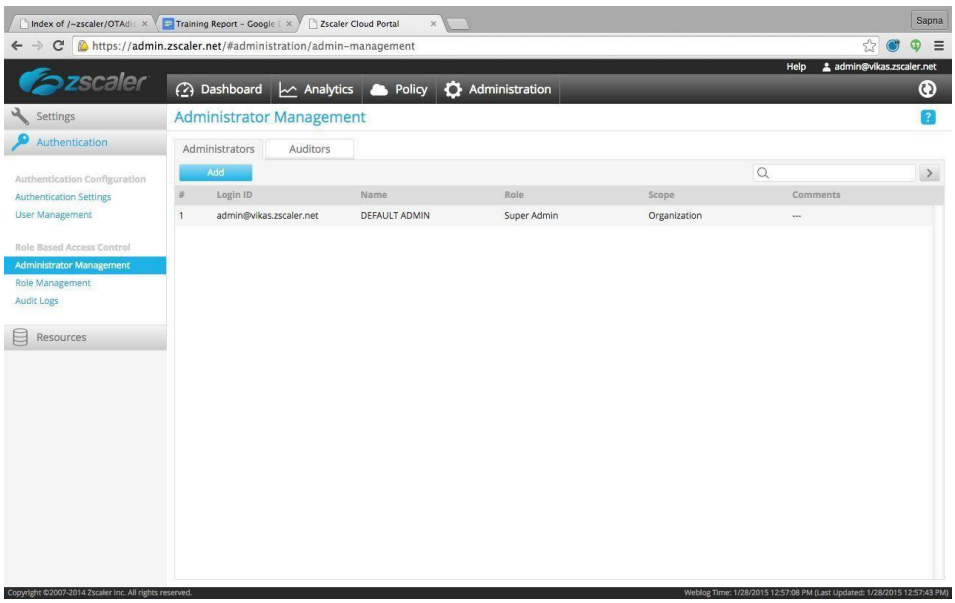




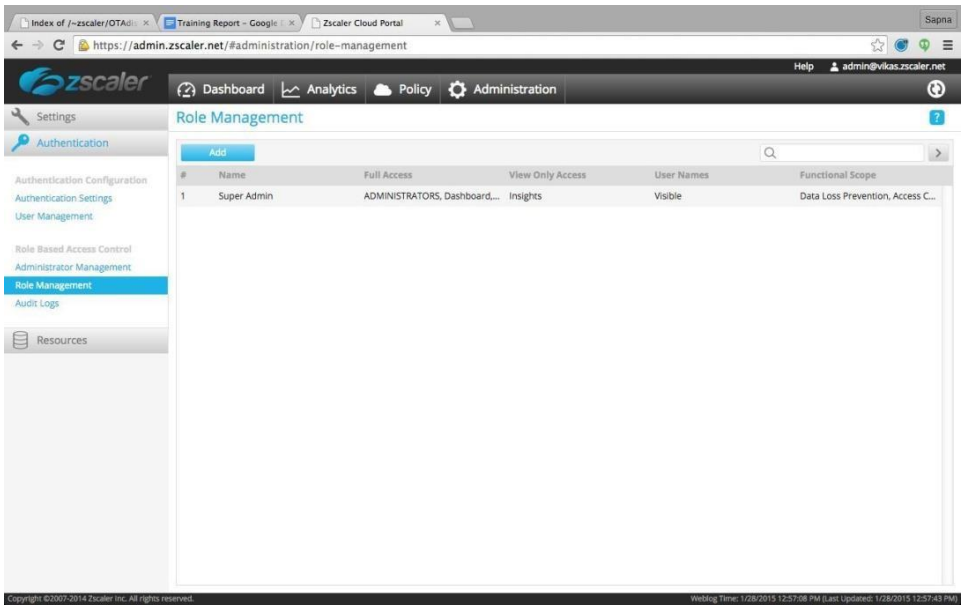
Admin can manage users, groups and departments.

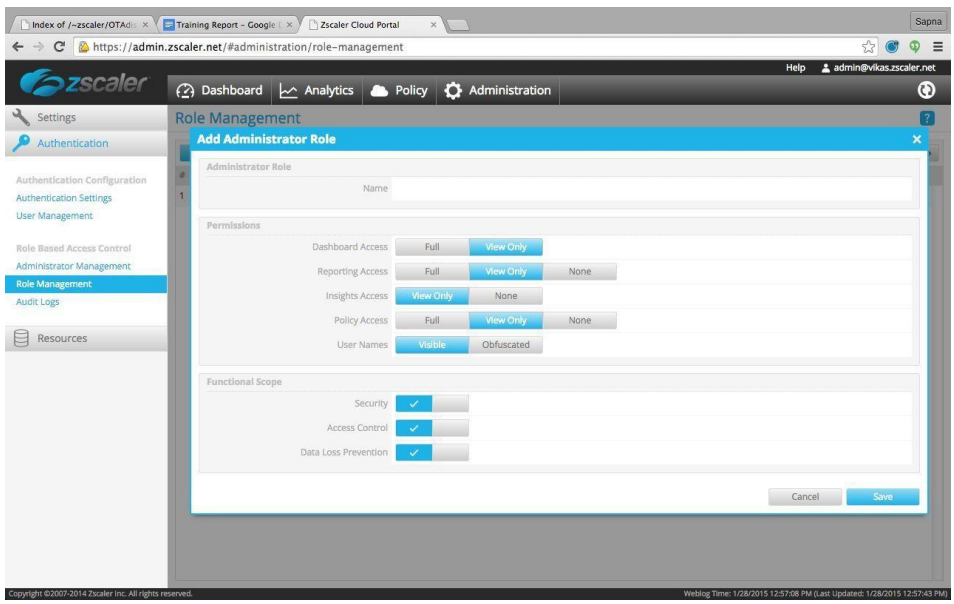
Role based access control

Administrator Management



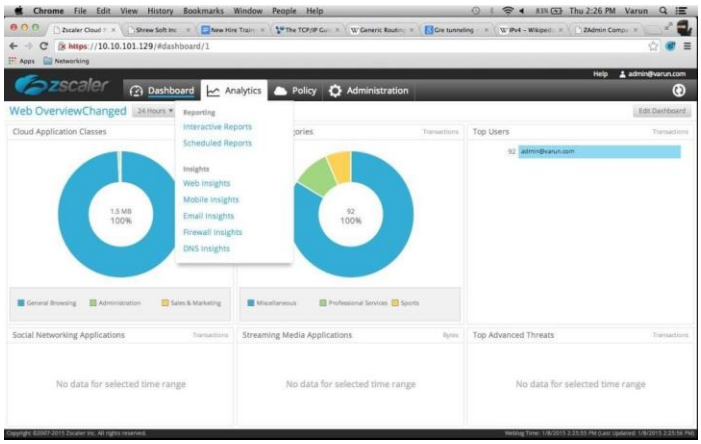
The administrator can manage the roles of different users such as superadmin and admin and provide access permissions





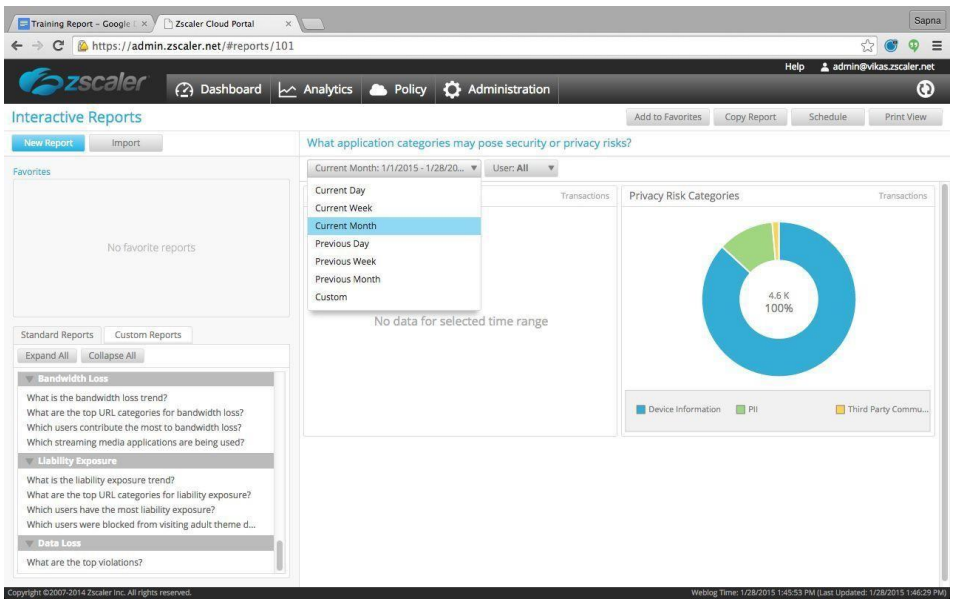
4. Analytics

SMSM has two ways to access reports. One is based on the counter that is stored in the RAM. The administrator can get interactive reports and insights from here (faster). While records are fetched from secondary memory (slower than interactive reports and insights)

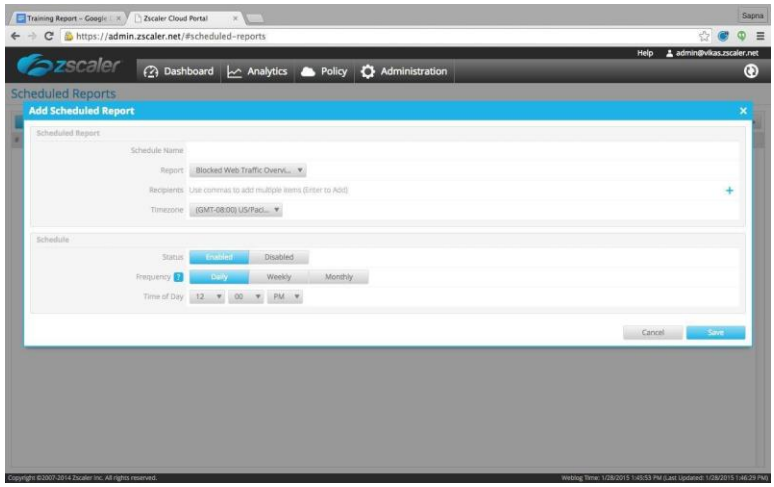


5. Reporting

Interactive reports - The administrator can view standard reports as well as provide custom reports. It can also specify the time frame for viewing reports.



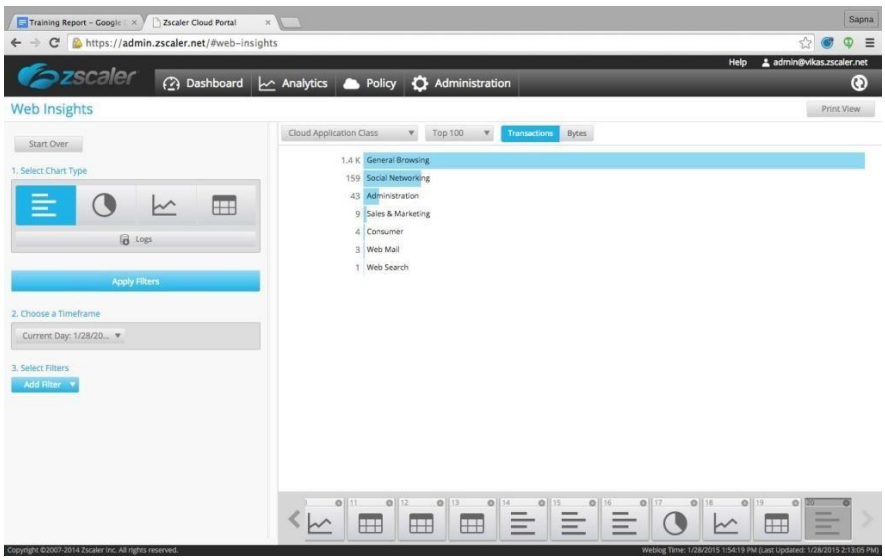
Scheduled Reports - Reports can be scheduled by the admin.



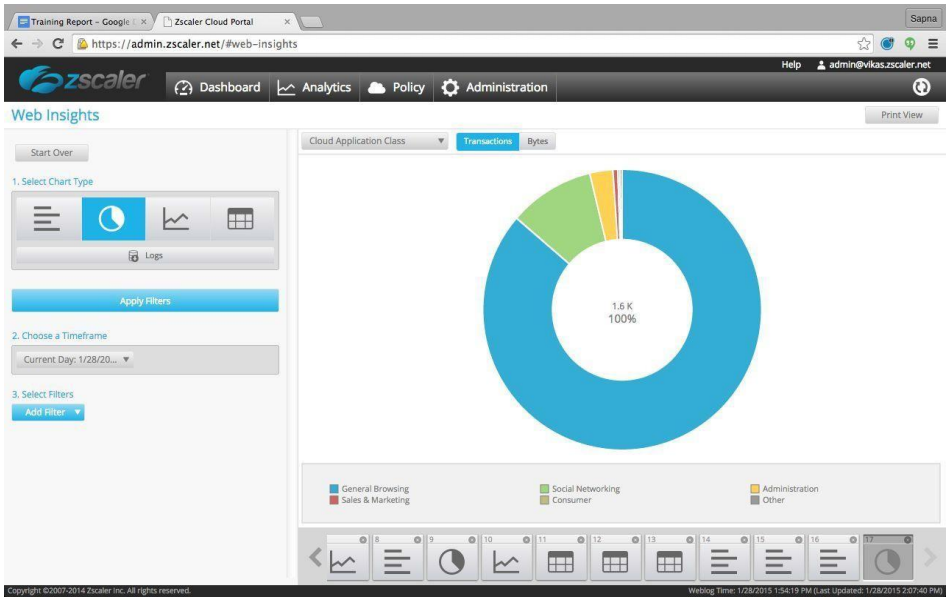
3 Insights

The administrator can view Web insights, mobile phone views, e-mail views, firewall views, and DNS views. These can be viewed in the form of a graph bar, pie chart, graph line, or table. The administrator can choose the time frame and apply filters to view these ideas.

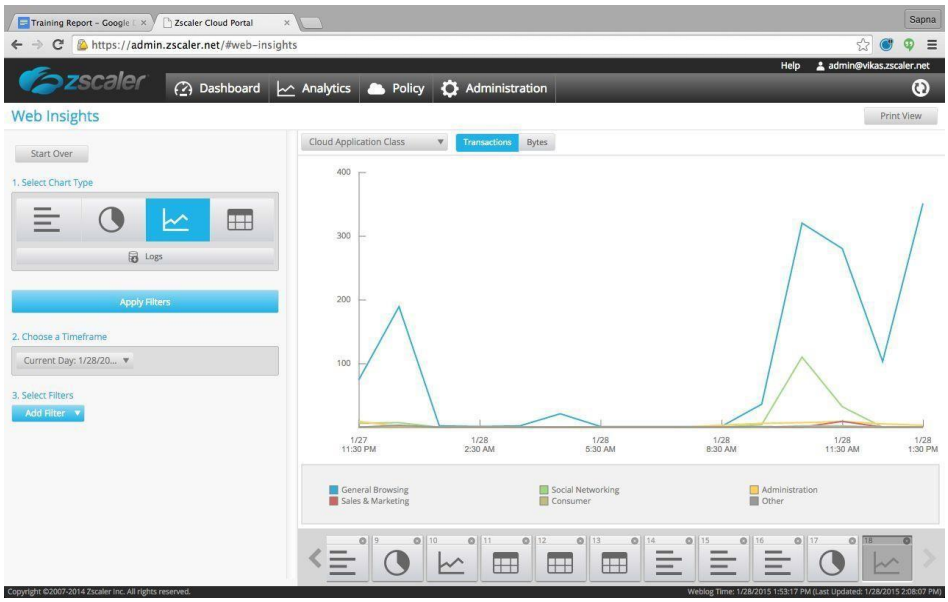
Web insights - bar graph



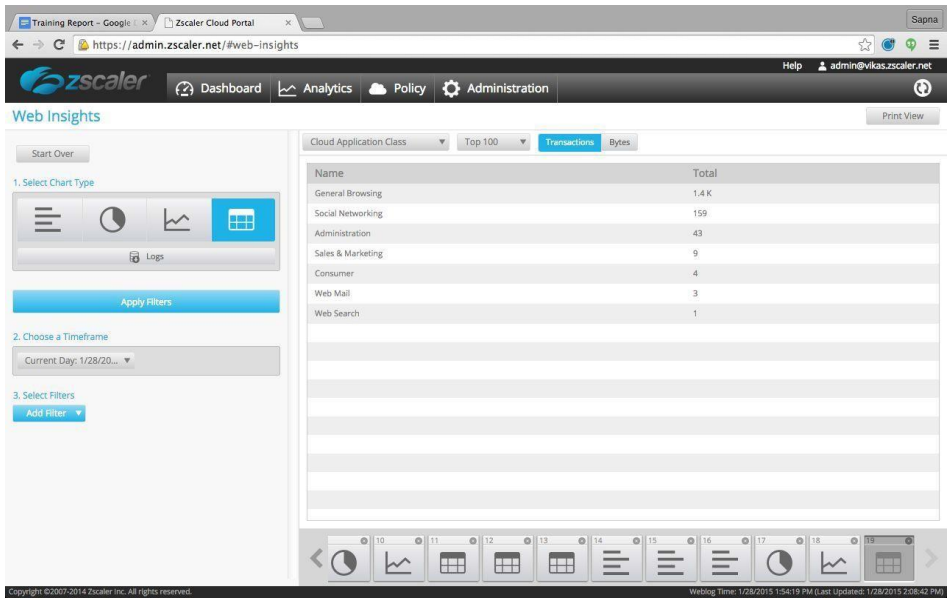
Web insights - pie chart

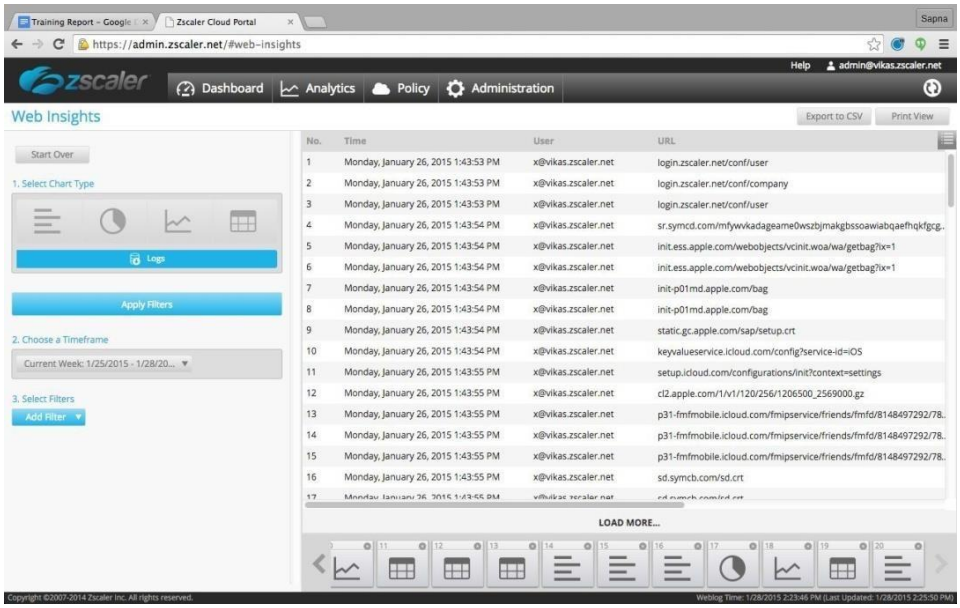


Web insights - line graph



Web insights – Table

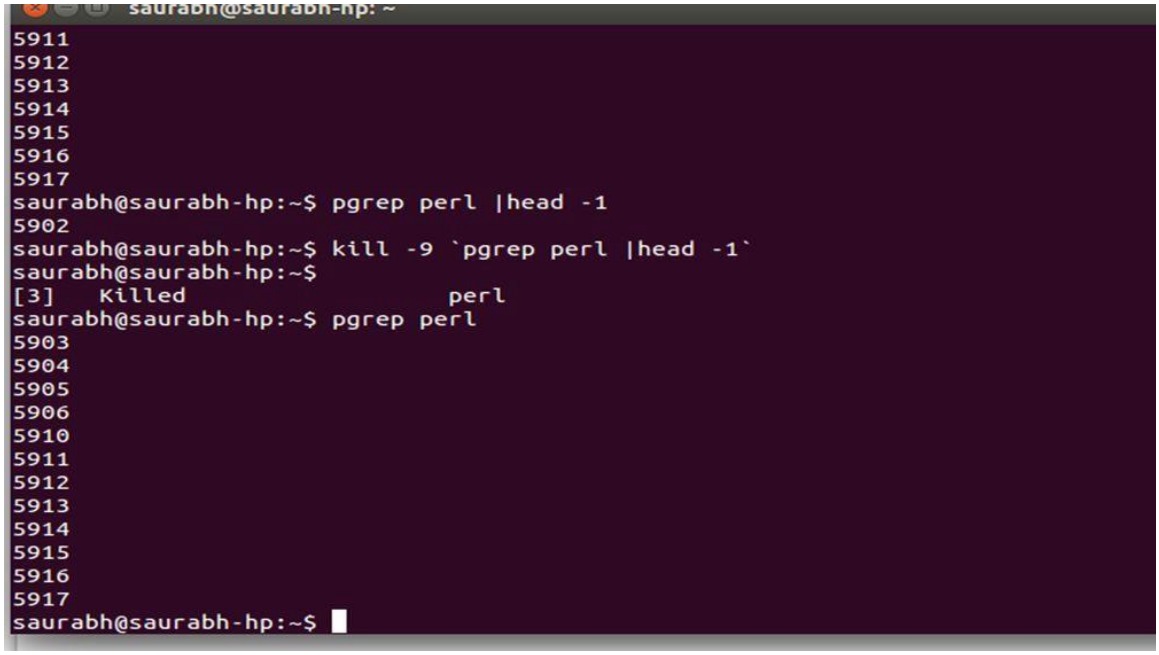




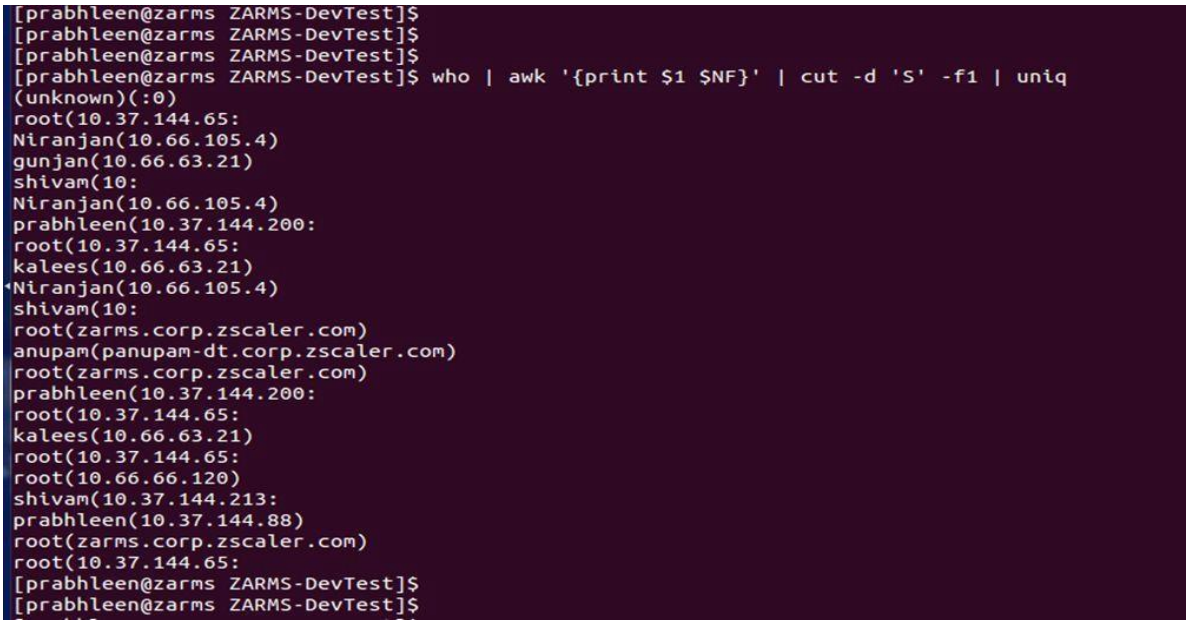
Logs

4.3 Basics of Linux

Following is the command to fork multiple processes and kill a specific process.



Following is the command to check other users who are logged into system and helps check their Ip address, port number etc.



Following are the vi editor commands:

1-search a keyword on any line. (/pattern)

2-Jump to a

specific line.

(:line no:)

3-Command to delete,copy,cut and paste a

line or particular word (dd, yy, p)(yw)(v

for selecting then y/d)

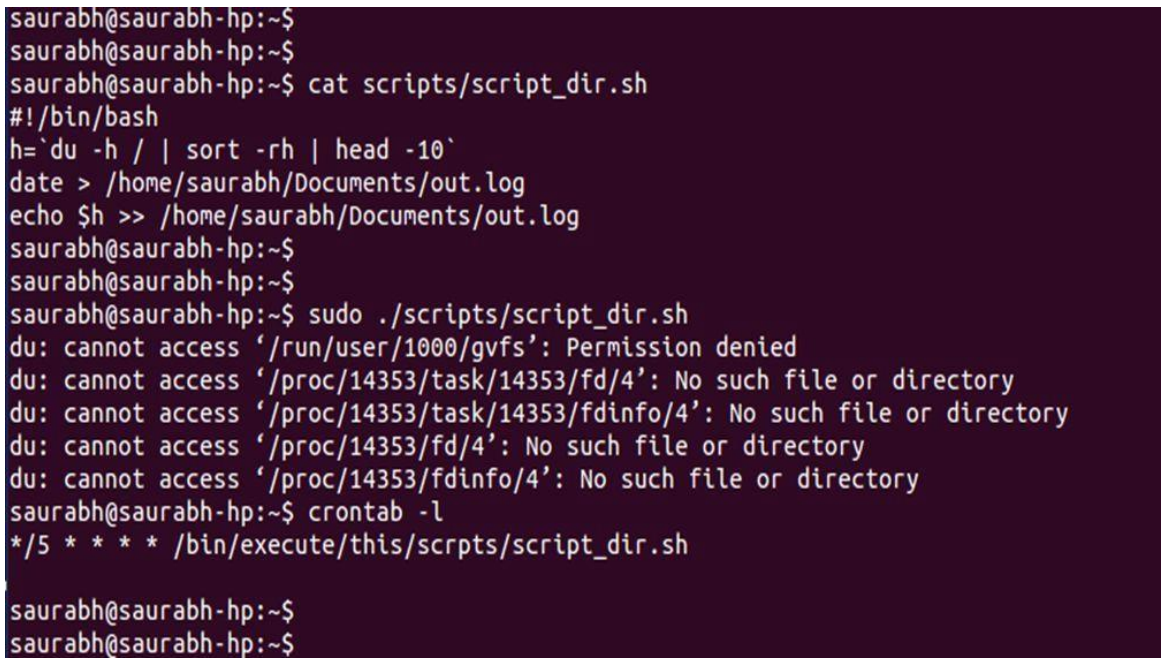
4-Select and replace a particular word in vim file

:s/pattern1/pattern2/(single word), /g for whole line ,%s for whole paragarph

5-Paste :set paste then paste

This command helps us in replacing a word without even opening the file

Here we create a script which helps us check disk usage of all directories and list the top 10 directories with maximum disk usage.



- This is command which help us in downloading file through command prompt.

CHAPTER-5

RESULT AND PERFORMANCE ANALYSIS

Ways to do performance analysis:

5.1 Manual Test Scenario

This type of testing is carried out before automated testing application. Test cases are created in this case which are targeting the comprehensive features of the product. The product rigorously tested manually beforehand to find defective components. It is also responsible to check feasibility of the features in the product. It is not so complicated instead very simple in nature. All tester needs to do is sit like an end user and check for the given test cases.

Being manual in nature this testing technique doesn't include any kind of automation techniques or tools. End user is imitated by tester find any kind of bug which can interrupt the end user. Any unwanted software behavior in this case is also checked by this testing techniques.

The test lead plan out the complete procedure of how shall the testing techniques shall be applied in test plan document. In this document the complete workflow of the script is understood and testing plan is inscribed accordingly. All scenarios are considered in this type testing to cover each kind of possible bug.

In testing process the test cases made are applied and executed and difference between actual and expected values are corrected. After fixing all the bugs the document is retested. This complete procedure mainly targets to deliver a quality product.

5.2 Automation

Automation was done by me under two different perspectives mentioned following.

5.2.1 Automation test cases using perl to increase the efficiency, effectiveness and coverage of testing. Some of the test cases automated by me are as follows

SAML Cert testing test cases

test_QA_13571_UI_Has_Multiple_SAML_Certs

test_QA_13415_Old_customers_should_have_old_saml_cert_selected_on_Migration

test_QA_13417_Migrating_Old_customers_to_new_cert

test_QA_13411_saml_auth_with_ap_and_Single_sign_on_disabled

test_QA_13410_saml_auth_without_ap

test_QA_13409_saml_auth_with_ap

test_QA_13408_saml_auth_with_new_cert

test_QA_13407_saml_auth_with_old_cert

test_idp_initiated_test_cases

test_QA_13405_XML_Validation_for_this_cloud

test_QA_13403_Download_XML

test_QA_13402_Download_SP_Certs_from_UI

test_QA_13401_Existing_SAML_cert_Available_And_Marked_Deprecated

test_QA_13399_SAML_Certs_Seprated_From_Gateway_Certs

5.2.2 Automation of Migration testing to reduce the manual effort and to increase the efficiency, effectiveness and coverage of the migration testing.

5.2.3 Steps to implement the automation of migration testing

5.2.3.1.1 Making design docs about how to achieve this task and reviewing it from the seniors

5.2.3.1.2 Writing algorithms for the task

5.2.3.1.3 Implementing the algorithm for writing the code for the task

5.2.3.1.4 Testing the written code intensively for any errors

5.2.4 Brief description of the logic of this automation

In the migration testing the user needed to verify that the settings of the client before the upgrade and after the upgrade are same unless some new feature is added. To test this

manually the user used to take screenshots of the client setting before and after the upgrade. This takes a lot of manual effort and the testing is also not effective as it's next to impossible to verify each every setting of the client as each setting contains thousands of entries. To automate this we decided to save the Api responses of each and every client for every settings. We made get request to each and every API for each and every client and stored it in json format before and after the upgrade and then matched these two json objects.

5.3 Script Debugging

The main purpose of script debugging is to make the scripts failing after upgrade error free by setting breakpoints and debugging accordingly. This situation sometimes arises because of the cloud upgrade because in some cases after the cloud upgrade the complete environment changes on which script is running.

Sometimes what happens is script running very well turns to be in bad working state. This type of debugging technique is comes to rescue.

We perform this type of testing by line by line testing where actual output values are compared with the final output values. And then the product is finalized.

5.4 Verifying Regression and Bugs

The previous functionality test cases needed to be executed again on the every new build for verifying the overall functionality and stability of the product. This includes to verify the results of the non automated test cases of the previous functionality and to verify the bugs filed by the clients on the production. This cycle needs to be completed twice for each and every release so that previous functionality is not affected while adding new functionalities to the Product. This is the most important part of testing.

5.5 Migration Testing

The main purpose is the verify that after upgrade no changes have been made on the client side in the old configuration. This testing is done on the clone of the production cloud to ensure smooth running of the production cloud. To test the the client side configurations the user takes screenshots of each every configuration of the client both before and after the upgrade on the clone cloud and then matches the two screenshots manually. A lot of manual effort is needed for this. If any dissimilarity is seen than a bug is reported and the root cause ofthat bug is found and then this procedure is repeated again.

CHAPTER-6

CONCLUSION

Being an undergraduate of Jaypee University Of Information technology I am grateful for the training provided to me at Zscaler softech private Limited.

I would not have gained this much knowledge If I would have went straight into the corporate world without gaining knowledge from this training program. In this training program I got to know how to communicate and work and corporate world. The training provided to me at Zscaler Softech Limited helped me enhance my concepts that I learned in college.

Some challenges that I faced during this training program were how to adapt to the new environment, learning new technologies every day. The biggest challenge was handling pressure and this training made me learn how to work in pressure. I got to interact with people from different sphere of life with varying cultural background which help me gained a lot of knowledge.This training program also helped me in increasing me overall confidence and helped me develop an overall personality.

I would like to thank Zscaler Softech Pvt. Ltd and Jaypee University of Information Technology for providing me this opportunity to complete my industrial training and gain so much knowledge and overall experience.

In the end I would like to thank the readers for sparing their valuable time and going through my report. All types of suggestions, remarks are welcomed as they will be for my betterment and will also help in making this project a bigger success.

REFRENCES

- Stevens, W. Richard. *TCP/IP Illustrated Volume I: The Protocols*. Boston, Mass. : Addison-Wesley, 2004. ISBN 0-201-70245-2
- Wright G.R., Stevens, W. R. *TCP/IP Illustrated Volume II: The Implementation*. Boston,
  Mass. : Addison-Wesley, 1995. ISBN 0-201-63354-X
- Stevens, W. Richard. *Unix Network Programming Volume I: Network APIs*. Boston, Mass. : Addison-Wesley, 2004. ISBN 0-201-70245-2
- Marshall Kirk McKusick, George V. Neville-Neil *The Design and Implementation of the*
  FreeBSD Operating System. Boston, Mass. : Addison-Wesley, 2004. ISBN 0-201-70245-2
- Tanenbaum, A. S. *Modern Operating Systems*. Prentice Hall, 2001. ISBN 0-13-03358-0
- Comer, Douglas E. *Internetworking with TCP/IP Volume I: Principles, Protocols and Architecture*. Upper Saddle River, New Jersey. : Prentice Hall, 1995. ISBN 0-13-227836-7
- Herbert, Thomas F. *The Linux TCP/IP Stack: Networking for Embedded Systems*. Hingham,
  Massachusetts. : Charles River Media, 2005. ISBN 1-58450-284-3
- RAW IP FAQ: http://www.whitefang.com/rin/rawfaq.html
- SOCK_RAW Demystified http://sock-raw.org/papers/sock_raw