Usage of OPNET IT tool to Simulate and Test the Security of Cloud under varying Firewall conditions

GRADUATE PROJECT REPORT

Submitted to the Faculty of
The School of Engineering & Computing Sciences
Texas A&M University-Corpus Christi
Corpus Christi, TX

in Partial Fulfillment of the Requirements for the Degree of
Master of Science in Computer Science

by

Ankush Veer Reddy Vee
Spring 2012

Committee Members

Dr. Mario Garcia
Committee Chairperson

Dr. Long zhuang Li
Committee Member

Dr. David Thomas
Committee Member
Abstract

Cloud computing is the key technology widely used across most of the organizations. The main advantage with cloud computing is that, the risk of infrastructure maintenance reduces a lot. Most of the service providers offer a wide range of services to their clients in the form of cloud services and the clients can use the same from a remote location. Apart from the list of advantages with cloud computing there are some limitations and security has a significant role among them. Providing security to the client’s information and data are the main challenge to the cloud service providers and there is lot research done in this context to provide the required security for the information and data. In general the services offered by the cloud service providers are accessible through the web and blocking the web traffic across the cloud access should be given top priority. The main aim of this project is to evaluate the cloud security against the firewall implementation under three different scenarios. OPNET IT guru is used as the simulation tool in this project and three scenarios are created in this context. First scenario has no security across the cloud, second scenario has the actual firewall implementation and this particular firewall allows all the required traffic, whereas the third scenario deals with the firewall implementation which discards the web traffic. Database and web applications are used as the required applications across the cloud to generate the traffic and now the firewalls will act on these applications. The performance of these applications is estimated against the firewall working conditions and the overall performance of the cloud is evaluated. All the three scenarios are compared against the metrics for the individual applications and also the performance of the cloud is estimated.
# Contents

1: Introduction .................................................................................................................. 1

1.1.1  Public cloud ........................................................................................................... 1

1.1.2  Private clouds ....................................................................................................... 2

1.1.3  Community clouds ............................................................................................... 2

1.1.4  Combined cloud .................................................................................................... 2

1.1.5  Hybrid clouds ....................................................................................................... 3

1.2  History ........................................................................................................................ 3

1.2.1  The Cloud cube model ....................................................................................... 3

1.2.2  Data Security model ........................................................................................... 4

1.3  Data storage example clouds .................................................................................. 5

1.4  Benefits with cloud computing ............................................................................... 6

1.5  Security issues with Cloud computing ................................................................. 7

1.5.1  Privacy issues ..................................................................................................... 7

1.5.2  Availability and backup ...................................................................................... 8

1.5.3  Access issues ...................................................................................................... 8

1.5.4  Trust .................................................................................................................... 8

1.5.5  Illegal secondary usage ...................................................................................... 9

1.5.6  Data proliferation issues ..................................................................................... 9

2: Narrative ....................................................................................................................... 10
2.1 Problem definition ........................................................................................................ 10
2.2 Aims and objectives .................................................................................................. 12
3. Design of proposed model ............................................................................................ 13

3.1 No firewall scenario ................................................................................................. 13
3.2 Firewall scenario ....................................................................................................... 16
3.3 Firewall scenario: Block web access .......................................................................... 16

4. Simulation procedure .................................................................................................. 17

4.1 OPNET IT guru as Simulation tool ........................................................................... 17
4.3 Simulation of No Firewalls scenario ......................................................................... 18

4.3.1 Application configuration settings ........................................................................ 21
4.3.2 Profile configuration settings ............................................................................... 23
4.3.3 Cloud configuration ............................................................................................... 24
4.3.4 West router and East router configuration .............................................................. 25
4.3.5 Home office configuration .................................................................................... 26
4.3.6 Server configurations .......................................................................................... 28
4.3.7 Performance metrics ............................................................................................ 30
4.4 Firewall scenario ...................................................................................................... 33

4.5 Firewall blocking scenario ....................................................................................... 35
4.6 Running the simulation ............................................................................................. 36

5. Results and Evaluation ............................................................................................... 38
5.1 Results for Database application ............................................................................. 38

5.2.1 Database query response time ............................................................................. 39

5.2.2 Server DB query load .......................................................................................... 40

5.2.3 Database Server point to point utilization .......................................................... 42

5.3 Results for web application ..................................................................................... 43

5.3.1 Page response time for no firewall scenario ....................................................... 43

5.3.2 Page response time across firewall scenarios .................................................... 44

5.4 Cloud performance .................................................................................................. 46

5.4.1 Point to point cloud utilization across west router ............................................ 46

6: Testing ....................................................................................................................... 49

6.1 First case: .................................................................................................................. 49

6.1.1 Database query response time: .......................................................................... 49

6.1.2 Server DB Query load: ....................................................................................... 50

6.1.3 Database server point to point utilization: ....................................................... 52

6.1.4 Point to point cloud utilization across west router .......................................... 53

6.2 Second case: ............................................................................................................ 54

6.2.1 Database query response time: .......................................................................... 54

6.2.2 Server DB query load .......................................................................................... 55

6.2.3 Database Server point to point utilization .......................................................... 56

6.2.4 Point to point cloud utilization across east router............................................. 58
7: Conclusion and future work........................................................................................................... 60

7.1 Conclusion.................................................................................................................................. 60

7.2 Future work ................................................................................................................................. 62
List of figures

Figure 1: OPNET Home screen ..........................................................................................14
Figure 2: New project creation ..........................................................................................15
Figure 3: OPNET IT guru object palette ..........................................................................18
Figure 4: New project creation using OPNET ...................................................................19
Figure 5: Basic workspace for the network .......................................................................20
Figure 6: Basic network setup ..........................................................................................21
Figure 7: Application configuration settings ......................................................................22
Figure 8: Database profile configuration ..........................................................................23
Figure 9: Web profile configuration ..................................................................................24
Figure 10: IP32 cloud configuration ................................................................................25
Figure 11: East and West router configuration ..................................................................26
Figure 12: Home office configuration .................................................................................27
Figure 13: Home office connection to Router west ..............................................................27
Figure 14: Database server configuration .........................................................................26
Figure 15: Web server configuration ................................................................................29
Figure 16: Server connections to Router east ....................................................................29
Figure 17: Three levels of performance metrics ................................................................30
Figure 18: Global statistics ...............................................................................................31
Figure 19: Node level statistics .......................................................................................32
Figure 20: Link level statistics ..........................................................................................32
Figure 21: Procedure to duplicate scenario

Figure 22: Firewall configuration

Figure 23: Firewall scenario setup

Figure 24: Web traffic block

Figure 25: Manage scenarios

Figure 26: Simulations run for one hour

Figure 27: Response time

Figure 28: Load on database server

Figure 29: Database server across router

Figure 30: Page response time across no firewall

Figure 31: Page response time across firewall

Figure 32: Point to point cloud utilization

Figure 33: Response time

Figure 34: Load on database server

Figure 35: Database server across router

Figure 36: Point to point cloud utilization

Figure 37: Response time

Figure 38: Load on database server

Figure 39: Database server across router

Figure 40: Point to point cloud utilization
1: Introduction

1.1 Introduction to Cloud computing

Most of the organizations are in need to some remote infrastructure to execute their process. The term process in this context can be varied in terms of server maintenance, database maintenance and some other key services like product optimizations. The main reasons for the organizations to choose a remote or third party services is mainly to reduce the of maintenance and also to reduce the cost burdens. Cloud computing is the right choice at this level and thus it has emerged quickly in the technology market and could have attracted the attention of most of the organizations. Cloud service providers are also increasing rapidly in the market and they are providing wide range of services. The key services include data server and typical file storage mechanisms. Clients in general register with the service providers to make use of the key services provided through the cloud. In general there are different types of clouds and they are discussed as below

1.1.1 Public cloud

Public clouds are simple internet based clouds and they are accessible publicly. Even public domain users can also use the services provided by the public clouds. The type of services provided by the public clouds includes some public documents, file sharing and database storing for normal users. Few public web services are provided across the public clouds and passing the required arguments will make the cloud accessible. Pay per usage process is followed across the
public clouds and there are many third parties available to provide the public access to these clouds.

### 1.1.2 Private clouds

Private networks are used across maintaining the private clouds. In general one or more organizations will make use of these private clouds and they need a separate network to access the same. Few access level restrictions are imposed over these private clouds and a perfect pass of these restrictions is required to access the private clouds. Private clouds are owned by a single organization and they use their own private network domains to provide the required services.

### 1.1.3 Community clouds

When two or more organizations are in need of similar requirements they form together and create the community cloud. These organizations will share the common infrastructure and computational power of the cloud. Community clouds are really useful when it comes to group level requirement for a group of organizations.

### 1.1.4 Combined cloud

Two or more clouds with different nature of operation are combined together and referred as combined clouds. When a single cloud can’t handle the client requirements, these combined
clouds are used to accomplish the required job. Integrated level of services is provided by this type of clouds and the level of integration is complex enough in this case.

1.1.5 Hybrid clouds

When a type of service can’t be provided by simple private or public clouds, hybrid clouds are used by the organizations. High end and complex tasks are accomplished by these hybrid clouds. Complex business needs of the organizations are solved by these hybrid clouds and the main limitation with this type of clouds is its complex nature.

1.2 History

Security is the main concern for cloud computing, there are many existing models that provide an idea towards the cloud security and they were discussed as below

1.2.1 The Cloud cube model

The cloud cube model identifies four different dimensions for providing security to the clouds. These dimensions can be categorized into two important types like the internal and external and these dimensions define the physical location of the data across the cloud. Organizational boundaries are considered as the internal and external dimensions for the cloud and it will be based on the cloud usage like from outside the organization or within the organization.
The other dimension is the propriety or open and this defines the ownership of the cloud against security. The degree of interoperability and data transportability is estimated across this dimension. The typical constraints on the data usage are estimated across this dimension. Propriety indicates the organization ownership and the control over the cloud remains with the organization, whereas the open indicates the public nature of the cloud. Based on these parameters the required security constraints are imposed.

The third dimension represents the Parameterized or De-Parameterized nature of the cloud. Parameterized indicates the architecture being followed across the cloud within the IT limits of the organization and the De-Parameterized indicates the IT architecture external to the organization. The entire internal network firewalls act across the Parameterized architecture, whereas the external firewalls acts across the De-Parameterized architecture.

The fourth dimension speaks about the Insourced or Outsourced nature of the cloud. In general Insourced dimension is maintained by own staff and the internal security policies are applied across the cloud. Outsourced dimension deals with the security policies provided by the third parties.

1.2.2 Data Security model

Protecting the data is the main concern across cloud computing and this model describes a famous model to protect the data. Three level defense system is used across providing security to the cloud data. User authentication can be considered as the first layer and on this layer all the users who are trying to access the cloud data need to be authenticated against their login credentials.
Second layer is responsible for data encryption process. The user’s data is protected using the typical data encryption models once the users are authenticated at the first layer. This can be considered as the important layer as encryption is always required to hide the actual data from the attackers. Third layer deals with the fast recovery of the data. If in case the data is lost the recovery mechanism is implemented across this layer.

The user authentication layer is used for protecting the data from unauthorized access and also to ensure that the data is not tampered. If the authentication layer fails in some cases, the second layer encrypts the data from misusage and this provides an upper layer of data protection. If the attacker can access the encryption keys and gain the data, the third layer has the key role to recover the data in a faster manner.

1.3 Data storage example clouds

Data storage can be considered as the primary services provided by most of the clouds and few examples are discussed in this section. Most of the data storage services provided by the clouds are completely based on internet. There are many websites created in this context and a detailed discussion is as given below

- Google docs can be considered as one of the important cloud data storage system. Different types of documents like the normal word documents, templates; PDF’s and presentations are uploaded to the Google server. Registered users can download the same from the remote locations. Users are also provided with an option to edit the documents and upload back based on their rights over the documents.
• Emailing servers can also be considered as an example of cloud data storage. Different email servers like Google, Yahoo and Hotmail provide some space across the mail access to the privileged users. Remote access to the mails is provided in this case and the corresponding attachments and data is stored on the remote email servers.

• Picasa is another good example of cloud storage. Users of Picasa can upload the photos and share the URLs and the corresponding photos are actually stored at a remote location. Separate data servers are provided in this case and the photos are stored on these servers which were actually maintained at the remote locations.

• YouTube is another good example of video storage at remote locations. Users can upload the videos and these videos are stored across a remote database server and they are accessed via the clouds.

• There are few storage websites, where some space is provided to the users to upload the files and folders. Some storage limit is given to the users and premium users provide unlimited storage space. The best example in this context is www.4shared.com and www.sendspace.com, where these websites provide remote database access to the registered users.

1.4 Benefits with cloud computing

A detailed discussion of different types of clouds and the corresponding examples is done in the previous section and the key benefits with cloud computing are given in this section. A simple benefit with cloud computing is that any device which can access the internet can also access the cloud services. Deployment of the cloud applications is very simple task and the users
need not worry about the compatibility and storage issues. All they need is a simple device and knowledge of the application being accessed from the remote locations. Version of the software is also automatically updated at the remote locations and users can simply access the latest versions. Following are other important benefits of cloud computing

- Data storage has increased a lot for the users, as the risk of maintaining local data servers is reduced
- Even the cost of infrastructure maintenance is reduced for the organizations
- The level of flexibility is more with cloud computing when compared to other computational aspects
- Mobility of usage is another best advantage with cloud computing

Apart from the listed benefits, there are many business and technology benefits with cloud computing.

1.5 Security issues with Cloud computing

The key benefits with cloud computing are discussed in the previous section and apart from this, there are some key security issues and they are as discussed below

1.5.1 Privacy issues

As all the cloud services are available at the remote locations, users can’t have the complete control over their data. But it is always their basic right to protect their data and they
have an intension to view all the database operations. Privacy is the main concern to be considered here, and if the cloud services can’t provide the level of privacy it can be considered as the main security threat. These privacy issues are mainly irritating across the public clouds, where the access to the clouds is through the public domains.

1.5.2 Availability and backup

In general most of the client software’s and databases are maintained across the remote locations across cloud computing. If the required resources are not available at peak times and even the backup failing across the clouds, this situation definitely leads to lots of security issues.

1.5.3 Access issues

Cloud computing has the threat of accessing the sensitive information. There are lots of chances where the information stored across the cloud may be lead to theft by the intruders and hackers.

1.5.4 Trust

Trust is always required across the cloud computing implementation. A mutual trust between the vendors and the clients is essential and if it is missing the overall security of the cloud is affected a lot.
1.5.5 Illegal secondary usage

There are lots of chances where the illegal secondary usage of information across clouds may happen. Most of the cloud business models reveal that, service providers can use the user’s data for the secondary usage and this may lead to serious security threats.

1.5.6 Data proliferation issues

Across most of the cloud service providers share the information or data to a group of organizations and this situation leads to data proliferation issues. It will be very easy to copy the data from different data centers and this finally leads to lots of security issues. There are some chances where the original copy of data can be deleted due to misuse of data proliferation.
2: Narrative

2.1 Problem definition

In general there are lots of security issues involved with cloud computing and they can be broadly categorized into two different types like the security issues faced by the cloud service providers and the security issues faced by the cloud customers. These two aspects should be considered while estimating the overall security requirements of cloud computing (Hamlen, 2010). Cloud service providers should ensure that their infrastructure is secure enough and their client information, data and other resources should be secure enough. Cloud customer security requirements will be on other lines, where they always ensure a safe and privileged access to their data which is located at the remote locations. Thus by considering all these requirements, the security of the cloud and the corresponding policies are designed.

Implementation of Virtualization across the cloud has become one of the successful and unique security policies being in practice these days by most of the cloud service providers. Virtualization adds a new and additional layer across the cloud and thus the data and information of the customers is much protected (WHITE, 2009). The actual concept of cloud computing was introduced in 2006 when the Amazon’s Elastic Computing cloud was proposed and since then many service providers has entered into the market. With the growth in the service providers equally the clients are increased and this has led to more security requirements across the cloud computing particularly in the aspects of customer data and information (Atayero, 2011). Data security is given the top most priority across the cloud security and there are some models proposed in this context as well. Risk coming with opportunity is the main issues to be considered against the cloud data security. The virtual machine concept was widely used by most
of the service providers like IBM blue cloud and Microsoft’s Window Azure. The main
difference between IBM blue cloud and Microsoft Windows’ Azure is that, blue cloud runs on
the Linux environment, whereas Azure runs on Windows operating system.

There are many advantages with the virtual machine implementation, where all the
required server operations are no more physical in nature and a group of virtual servers is used in
this context (Binning, 2011). The services provided by the service provider are not affected even
there are some physical changes to the virtual machine and thus the customers can enjoy the
uninterrupted services. However there are some limitations to the virtual machine concept as
well and the key among them are the attacks on the virtual server. In general these virtual servers
will form a separate group which is apart from the logical groups. In general the cloud
environment is dynamic in nature and the data operations between the remote data servers and
the client are prone to frequent updates (Andry, 2010). In this process any attacker can change
the read and write operations and thus a strict authentication policy implementation is required in
this context. Thus from this overall analysis it can be understood cloud security has a lot of scope
for research and thus interested in this area and would like to create a new security model that
can be used to block the unwanted web traffic across the cloud data access. OPNET IT guru is
used as the simulation tool and the actual implementation procedure is explained in the next
section. Following are the key aims, objectives and research questions identified in this context.
2.2 Aims and objectives

Aim: To evaluate the cloud performance under the secure firewall implementation and block the unwanted web traffic using the OPNET IT guru simulation.

Objectives

Following are the research objectives

- To critically review the cloud security issues and the current security models in the implementation
- To identify the key limitations with the current security models and propose a new security model for cloud data and information security
- To design the simulation using OPNET It guru and create three scenarios
- To create a normal scenario where there is no firewall implementation, create a firewall scenario for data security and finally to create a firewall scenario for web security
- To measure the performance of the cloud under these three scenarios using some performance metrics
- To compare the scenario results and corresponding graphs and to evaluate the performance of cloud and understand the level of security requirements.
3. Design of proposed model

As discussed the main aim of this project is to evaluate the cloud performance and estimate the security requirements OPNET IT guru is used as the simulation tool. Three scenarios are created in this context and a detailed description of the scenarios is as given below

3.1 No firewall scenario

In general OPNET IT guru provides an option to create scenarios and in this simulation three scenarios are created. The main objective of this scenario is to impose no firewall conditions across the network. An IP based cloud is used as the required cloud and this cloud acts as the internet cloud and connects two or more subnets, which represents the service providers. Two routers are used across the simulation process among those where one of the router act as the firewall routers. Two different applications are created across this scenario, one is the database application and the other is the web application. The required application traffic is created by configuring the applications at the application configuration and profile configuration level. A heavy database access application is used in this simulation such that imposes more database queries over the database server. Required configurations are done at the application and the profile config level and the performance of the cloud in terms of database applications and web application are studied. Figure 1 shows the basic workspace of OPNET It guru and the required simulations are done at this level
A new project is created using the file menu and the required scenarios are also created at this level and the corresponding process is as shown in Figure 2.
The cloud used across this simulation is done for 150 workstations and it is simulated in a way that all the 150 workstations access the database application and the web application. As mentioned there is no security provided in this scenario and the normal performance of the cloud is estimated. Following are the performance metrics used for the performance evaluation of cloud when there is no security across the cloud:

- HTTP page response time is estimated for the web application
- DB query time and response time for the database application are estimated
- Node level statistics like server DB query response time and load are also estimated for the database application
- Link level and utilization statistics are also estimated across the simulation process

Same list of performance metrics is used for the other two scenarios and the required description is as given below.
3.2 Firewall scenario

The first scenario is duplicated and the required firewall scenario is created. In this particular scenario a firewall router is created and a constant packet latency of 0.05 seconds are imposed for packet filtering. Similar performance metrics are used as in the first scenario.

3.3 Firewall scenario: Block web access

This scenario is created by duplicating the second scenario and the main aim of this scenario is to block the unauthorized web access.

Once the required three scenarios are created the simulation is run for one hour and the corresponding performance of the cloud is evaluated and the expected results are discussed in the next section.
4. Simulation procedure

As the main aim of these scenarios is to evaluate the performance of database and web application under three different scenarios like no firewall, firewall and firewall blocking the web traffic, OPNET IT guru is used as the simulation tool. As discussed in the previous section three scenarios are created using this simulation tool and simulation is run for one hour for the results evaluated. A detailed explanation of the simulation procedure followed and design metrics used is given in this chapter. Each and every scenario is explained in a detailed manner and the proposed model of blocking the web traffic is described as below

4.1 OPNET IT guru as Simulation tool

OPNET IT guru provides a rich user interface to create the required network models. Cloud is simulated in this project and it provides a wide range of models to create the required cloud model. OPNET It guru has an object palette and this holds different node models and user can use the same to create the required network model. A sample screen of object palette that holds the nodes for creating the cloud model is as shown below Figure 3.
All the required objects from the object palette are dragged across the workspace to create the required network. OPNET provides scope for comparing different scenarios and these scenarios can be created and duplicated accordingly. Few changes are made towards the duplicate scenarios and once the required number of scenarios is created, the actual performance evaluation is done. Performance evaluation of the required network can be done by choosing individual statics at three levels. Global level, node level and link level statistics are available across the simulation tool and the desired metrics can be chosen for the performance comparison. OPNET IT guru provides an option to run the simulation as per the requirements and once the simulation is run the actual results are evaluated. The detailed procedure followed to create the simulation of all the three scenarios is as given below

4.3 Simulation of No Firewalls scenario

A detailed explanation of the simulation procedure followed to create the no firewall scenario is given in this section. In general a firewall is a router that can impose some security policies over the network. Firewalls can monitor and regulate the traffic that passes across the
network and internet and such a firewall is used in this application. In this simulation a home office LAN network is used as the destination and the all the communication is done through the cloud and few routers. The actual steps followed to create the simulation is as given below

To create a basic network, a new project is created across the OPNET IT guru. Name of the project and the corresponding scenario are given and in this project, scenario name is given as No Firewalls and the corresponding is shown in Figure 4.

![Figure 4: New project creation using OPNET IT guru](image)

Once the required project name and scenario name are set, the following steps are used to create the basic network

- Create Empty scenario is chosen as the option for Initial topology option and next
- The world is chosen as the required network scale and next
- In the maps US is selected and click next
- Click next for two times and once these steps are followed the basic workspace with the required object palette are displayed and the corresponding screenshot is as shown below Figure 5.

![Basic workspace for the network](image)

Figure 5: Basic workspace for the network

Once the basic workspace is available following objects are dragged from the object palette to the workspace and they are as listed below

- The application configuration object is used to define the applications. In this simulation database and Http applications are used and the detailed configuration is explained in the later sections
- The profile configuration object is used to define the application profiles
- Ip32_cloud object is used to act as the internet cloud
- Two ethernet4_slip8_gtwy’s are used to act as east router and west router
- 10BaseT_LAN object is used to act as the home office which supports 150 workstations and the configuration process is explained later in this section
- Two ppp_server objects are used to act as the database server and web server

Once all the objects are dragged from the object palette the basic network setup is done and the corresponding screen is as shown below Figure 6.

Figure 6: Basic network setup

4.3.1 Application configuration settings

As discussed in the previous section, two applications are created in this project to generate the required traffic over the cloud. OPNET IT guru provides a separate object known as application config and the required applications can be created at this level. The application
configuration object is dragged from the object palette and edited to add the applications and the corresponding procedure is as given below

- Right click on the Application config object and choose the edit attributes
- Add two rows to the applications definitions tab, such that two applications are created
- Rename a row as Database and choose the heavy load database against the Database application
- Rename another row as web and choose heavy browsing against HTTP application and the corresponding screenshot is as shown below Figure 7.

Figure 7: Application configuration settings
Once the application definitions are chosen click on the Ok button and save the project.

Next step is to define the corresponding profiles and the procedure is as explained below

4.3.2 Profile configuration settings

Each and every application has a profile such that to generate the required application traffic over the network. OPNET IT guru provides a profile configuration object and it can be dragged from the object palette. The following steps are followed to set the profile definitions

- Right click on the profile configuration object and edit the attributes
- Add two rows for profile configuration
- Name a row as Database_User and choose database as the desired application
- Name another row as Web_User and choose web as the desired application and the corresponding screen is as shown below Figure 8 and 9.

Figure 8: Database Profile Configuration
When both the profiles are created, it indicates that the applications are ready to generate the traffic and the next step is to configure the cloud and it is discussed in the next section.

### 4.3.3 Cloud configuration

OPNET IT guru provides an IP32 cloud which acts a simple public internet based cloud. In this project this cloud is used to support the database and web applications and the configuration aspects are discussed in this section. Drag the ip32_cloud from the object palette to the workspace and edit its attributes accordingly as given below:

- Right click on the cloud and choose edit attributes
• Edit the packet latency attribute and set the value as constant 0.05 seconds and the corresponding screenshot is as given below Figure 10.

![Image of IP32 cloud configuration](image)

**Figure 10: IP32 cloud configuration**

When the packet latency is set to 0.05 seconds it indicates that, the maximum packet delay across the cloud due to the web and database applications is 50ms. Each and every packet is processed across the cloud with this limited delay. Once the cloud configuration is done now the west router attributes are edited and the corresponding procedure is as shown below.

**4.3.4 West router and East router configuration**

As discussed in the previous section, two routers are added in this simulation and this section deal with west router configuration. Ethernet4_slip8_gtwy object is dragged from the object palette and renamed as Router_West. Similarly another object is dragged and renamed as Router_East and they are connected to the IP32 cloud using the PPP_DS1 links available across the object palette. The corresponding is shown in below Figure 11.
4.3.5 Home office configuration

As mentioned in the previous sections a home office is created and the configuration is explained in this section. Select 10BaseT_LAN object from the object palette and follow the below steps to configure the same

- Right click on the object and edit the attributes
- Number of workstations are set to 150
- An application supported profiles section is expanded and two rows are added
- Database profile is added the number of users are set to 50
- Another profile is set to web profile and the number of users are set to 100 and the corresponding Figure 12 is as given below
Figure 12: Home office configurations

Now the home office is connected to Router_West using the 10BaseT links and the corresponding Figure 13 is as given below

Figure 13: Home office connection to Router west
4.3.6 Server configurations

Two PPS servers are dragged from the object palette and they are set as database server and web server. Each of the servers is edited to support the corresponding applications and the following steps are used in this context:

- Right click on the database server and choose edit attributes
- Edit the application supported profiles and set Database application as supported
- A similar procedure is followed for web server, where the web application is supported at this level and the corresponding Figure 14 and 15 is as shown below.

![Database server configuration](image)

Figure 14: Database server configuration
Once the servers are configured they are connected to the Router east and using the PPP_DS1 links and the corresponding Figure 16 is as given below.

Figure 15: Web server configuration

Figure 16: Server connections to Router East
4.3.7 Performance metrics

All the required configuration steps are explained in the previous sections and with this the setup of complete network along with the configuration is done. To evaluate the performance of cloud against the database and web applications few parameters are required and they are given in this section. As discussed in the previous sections, OPNET IT guru provides three levels of performance evaluation like at the global level, node level and link level all of them are used in this simulation. The following steps are followed to set the performance metrics:

- Right click on the workspace and choose the option Choose Individual statistics
- Now a separate window is opened where the option to choose the global, node and link level metrics is available and the corresponding Figure 17 is as given below

![Choose Results](image)

Figure 17: Three levels of performance metrics
Following metrics are chosen for performance evaluation

- From the Global level statistics, expand the DB query option and choose response time
- From the global level statistics, expand the Http option and choose the page response time and the corresponding Figure 18 is as given below

![Image of Global Statistics]

Figure 18: Global statistics

From the node level statistics following are selected

- Expand the server DB query and choose load
- Expand server HTTP and choose load and the corresponding Figure 19 is as given below
Figure 19: Node level statistics

From the link level statistics following are chosen

- Expand point to point option and check both the utilization metrics and the corresponding

  Figure 20 is as shown below

Figure 20: Link level statistics
Once all the required performance metrics are chosen, simulation of the first scenario is done. Similar performance metrics are used for the other scenarios as well and the corresponding procedure is as given below

### 4.4 Firewall scenario

The first scenario is duplicated to create this scenario. The main aim of this scenario is to impose the firewall policies over the cloud. The firewall created in this scenario allows the required traffic across the network, and a perfect packet filtering is done. Duplicate scenario option is chosen from the scenarios menu to create this scenario and the corresponding Figure 21 is as given below

![Figure 21: Procedure to duplicate the scenario](image)

Once the scenario is duplicated similar network is created and the following steps are followed to make the required firewall scenario

- Right click on the Router West and edit the attributes
• From the option model choose, ethernet2_slip8_firewall such that now the router acts as a firewall

• Proxy server information option is expanded and the row 1 option is edited such that the latency is set a constant value of 0.05

• Now expand the row 4 and set the latency to a constant value of 0.05 and the corresponding Figure 22 is as shown below

![Figure 22: Firewall configuration](image)

The latency for database and web application is set to a constant value of 0.05 and this indicates that, the packet filtering is done at the firewall and thus a delay of 50ms is incurred over the router. Once the required firewall configuration steps are followed the corresponding network is as shown in the below Figure 23
Figure 23: Firewall scenario setup

With this the simulation of firewall scenario is done and the similar performance metrics are used across this scenario as well.

4.5 Firewall blocking scenario

The main aim of this scenario is to block the web traffic over the network and this scenario is created by duplicating the second scenario. Following are the changes done to the network in this scenario and they are as given below

- Right click on the Router west and edit the attributes
- Expand the Proxy server information and choose the row 4 i.e. HTTP
- Set the proxy server deployed option to no and the corresponding Figure 24 is as given below
With this all the web traffic across the cloud is blocked and thus the simulation of firewall blocking scenario is done.

4.6 Running the simulation

Once all the three scenarios are done the simulation is run for one hour. It can be done from the scenarios menu by choosing the manage scenarios option as shown in the Figure 25.
When this option is selected a new window is opened and from the simulation is run for one hour and the corresponding Figure 26 is as shown below

![Simulation GUI](image)

**Figure 26**: Simulation runs for one hour

Once the simulation is done the next step is to evaluate the results and a detailed evaluation of results is given in the next chapter. All the three scenarios are compared against the performance metrics chosen.
5. Results and Evaluation

A detailed explanation for the simulation steps followed and the process implemented to create the required scenarios is given in the previous section. This chapter deals with the results evaluation once the simulation runs for one hour as explained in the previous chapter. As mentioned three scenarios are created in this simulation like the no firewall scenario, where there is no firewall, firewall scenario where the firewall is created to filter the database and web application packets and the third scenario is created to block the web traffic across the cloud. The performance of the database application and web application are evaluated in this chapter based on the performance metrics chosen at all the three levels like global level, node level and link level. All the obtained graphs are compared against the performance metrics and a detailed evaluation is as given below

5.1 Results for Database application

As discussed two applications are created in this simulation and they are database and web application. This section deals with the performance evaluation of database application under the three scenarios. First scenario has no firewall, where the second scenario has a firewall which filters the database application packets and the third scenario blocks the web access completely. The overall database performance against these three scenarios is estimated as per the performance metrics chosen and the corresponding graphs are as given below
5.2.1 Database query response time

Query response time for a database operation indicates the overall performance of the database application. In general if there are no security policies or barriers to the application traffic across the network, the query response time would be very less and the actual comparison graph is as shown below Figure 27.

![Figure 27: Response time](image)

From the above graph it can be understood that the average query response time is more when there is a firewall. This is due to the fact that, the packet latency across the firewall router is set to a constant value 0.05 seconds and thus the delay is incurred due to the packet filtering.
Even the delay is more due to the packet filtering initially, later the response time is reduced after 10 minutes of simulation. When the case with no firewall scenario is considered the response time is very less when compared to firewalls scenario. As there is no packet delay across the west router, the response time is very quick and the application performance is enhanced.

When the case with the web application blocking scenario, the response time is reduced even there is a firewall which filters the packets. As the firewall completely blocks the web traffic, the load on the firewalls is reduced and thus the performance of the database application is enhanced. From the overall analysis it can be concluded that when the unwanted web traffic is blocked, the overall performance of the database application is enhanced and also the security across the cloud is enhanced.

5.2.2 Server DB query load

The overall load on the database server is estimated in this section. As there are three scenarios, the load under each scenario is estimated and the corresponding comparison graph is as given below in Figure 28
Figure 28: Load on database server

It can be analyzed from the above comparison graph that, when there is no firewall the load is less when compared to the other scenarios. The load on the database server is almost equal across all the three scenarios, apart from the firewall implementation. This situation indicates that, due to the extra firewall policies there could be some packet delay as they are filtered, but the overall burden on the server is not affected. When the case with the firewall blocking scenario is considered the load is almost equal where no firewall is even the web application traffic is blocked. When there is firewall over the network the overall load on the database server is increased as due to the additional security firewall policies.
5.2.3 Database Server point to point utilization

The overall utilization of the database server across the router indicates the application performance against the key security issues. The actual comparison graph of all the three scenarios is as given below Figure 29

![Database server across router](image)

Figure 29: Database server across router

The average database server point to point utilization across the three scenarios is as shown above. From the graph it is clear that the overall utilization of the database server is more when there is firewall across the cloud. It can be observed that, the point to point utilization is less when there is no firewall and this indicates that, when there are no packet filtering or
external firewall policies the overall utilization of the server is reduced. When the web traffic is blocked across the third scenario the utilization of the server is increased. From the overall analysis it is clear that, the point to point utilization of the database server is increased when there is firewall across the cloud.

5.3 Results for web application

The web application is also created in this simulation and the performance of the web application is estimated against the page response time. As the web application is blocked across the third scenario only two scenario results are evaluated for the first two scenarios individually and they are as given below

5.3.1 Page response time for no firewall scenario

The overall page response time across the web application when there is no firewall is given as below in Figure 30
From the above graph it is clear that, the average response time is constant across the simulation and the maximum time consumed in this context is one minute. It can be analyzed that when there is no firewall the overall page response time is constant and this indicates that the flow of the web application is constant across the cloud without any limitations.

**5.3.2 Page response time across firewall scenarios**

When there is a firewall the page response time across the web application is given in the below graph as Figure 31
From the above graph it is clear that, the average maximum page response time across the web application is 6 seconds and this value is very high when compared to the previous scenario. Even the page response time is not constant as the firewall policies impose some packet latency against the packet filtering process. As the web traffic is filtered the overall page response time is increased.

When both the scenarios are compared it can be understood the overall page response time is very high when there is a firewall implementation over the cloud. Due to the security policies and the packet latency time imposed over the firewall the overall response time is increased. From the overall analysis it can be understood that blocking the web traffic will increase the page response time.
5.4 Cloud performance

The performance of web application and database application is evaluated against the three scenarios in the previous section. The actual performance of cloud across the three scenarios is discussed in this section and the corresponding comparison graphs are as shown below.

5.4.1 Point to point cloud utilization across west router

The overall point to point cloud utilization across the west router is given in the below graph as Figure 32.
It can be observed from the above graph that the overall point to point utilization of cloud is more when there is firewall across the network. As the firewalls imposes some security policies and also delays the packets due to filtering the cloud utilization is increased. When the third scenario where the web traffic is blocked the overall utilization of the cloud is reduced as shown in the above graph. As the complete web traffic is blocked the cloud has ample space to process the database packets and the overall utilization is reduced. When there is no firewall also the utilization is more as the cloud needs to process the database and Http packets continuously. Thus from the overall analysis it can be estimated that the overall utilization of the cloud can be optimized when the web traffic is blocked using the firewalls.
From the overall analysis of the results the proposed firewall model is well used for enhancing the database application. In this simulation two applications are used like the database application and web application and it is proved the overall performance of database application is enhanced when the web traffic is blocked. When the web traffic is blocked across the third scenario, even the cloud utilization is improved against processing the database application towards the home office. As mentioned 150 workstations are used and out of that 50 users support the database application. The overall database point to point utilization for all the users is enhanced as well even against the security policies and packet latency of firewalls. Thus the main aim of the project to improve the overall performance of cloud under the firewalls and also improve the security by blocking the web traffic is proved from the result analysis. When there is heavy browsing across the clouds the overall cloud utilization is increased and thus the performance is reduced. As the proposed design blocks the web traffic the database users are provided with quick query response time and also the overall performance of the cloud is also increased in terms of reducing the point to point utilization.
6: Testing

In order to prove the above results, to the proposed model the number of workstations and the packet latency is changed to test. Two cases are used to prove the results, in the first case the number of workstations is changed to 300 and in the second case packet latency is changed to 0.10.

6.1 First case:

In this case, the number of workstations is changed to 300. By increasing the number of workstations, the numbers of users in the cloud are also increased. By right clicking on the HomeOffice, the attributes of workstations is changed from 150 to 300. After changing the number of workstations in each scenario, the simulation runs for an hour. The following results are observed:

6.1.1 Database query response time:

Response time indicates the overall performance of the database application. When there are no firewalls the page response time would be very less when compared with the firewall scenario.
Figure 33: Response time

The above graph indicates that when web access is blocked the average response time is very less when compared with other scenarios. As the response time is indirectly proportional to performance, thus it can be stated that the performance of cloud is enhanced.

6.1.2 Server DB Query load:

The overall load of the database server can be estimated here. Load on database server at each scenario, when there are 300 workstations can be known from below graph.
When there is no firewall the load is less when compared to the other scenarios. The load on the database server is almost equal across all the three scenarios, apart from the firewall implementation. This situation indicates that, due to the extra firewall policies there could be some packet delay as they are filtered, but the overall burden on the server is not affected.

Even if the number of workstations is increased, the same result is observed i.e. there will be no extra load on database server when a firewall is placed across the cloud.
6.1.3 Database server point to point utilization:

The overall utilization of the database server across the router indicates the application performance against the key security issues.

When the numbers of workstations are increased, the utilization of database server is same in all three scenarios. From the graph it is clear that, the point to point utilization of the database server is increased when there is firewall across the cloud.

Figure 35: Database server across router
6.1.4 Point to point cloud utilization across west router

The overall point to point cloud utilization across the west router is given in the below graph.

Figure 36: point to point cloud utilization

It can be observed from the above graph that the overall point to point utilization of cloud is more when there is firewall across the network. In the third scenario where the web traffic is blocked the overall utilization of the cloud is reduced as shown in the above graph. As the complete web traffic is blocked the cloud has ample space to process the database packets and the overall utilization is reduced. From the overall analysis it can be estimated that, irrespective
of the number of workstations the overall utilization of the cloud can be optimized when the web traffic is blocked using the firewalls.

6.2 Second case:

Here the packet latency of IP cloud is changed from 0.05 to 0.10, there by generating the result. The simulation will be results will be generated after an hour.

6.2.1 Database query response time:

The response time is almost similar to above cases if there are no security policies or barriers to the application traffic across the network, the query response time would be very less and the actual comparison graph is as shown below
Figure 37: Response time

In the case with the web application blocking scenario, the response time is reduced even there is a firewall which filters the packets. As the firewall completely blocks the web traffic, the load on the firewalls is reduced and thus the performance of the database application is enhanced. Though the packet latency is changed, the behavior of the database server is not changed.

6.2.2 Server DB query load

The load of the database server is estimated here, where the load under three scenarios are shown in the graph.
From the above graph it can be observed that due to the extra firewall policies there could be some packet delay as they are filtered, but the overall burden on the server is not affected. The load is almost equal in the three scenarios.

6.2.3 Database Server point to point utilization

The overall utilization of the database server across the router indicates the application performance against the key security issues.
It can be observed that, the point to point utilization is less when there is no firewall and this indicates that, when there are no packet filtering or external firewall policies the overall utilization of the server is reduced. The overall performance of the cloud is same as in the above cases even if the packet latency is changed.

Figure 39: Database server across router
6.2.4 Point to point cloud utilization across east router

The overall point to point cloud utilization across the east router is given in the below graph.

Figure 40: Point to point cloud utilization

Even if the packet latency is changed the overall point to point utilization of cloud is more when there is firewall across the network. When there is no firewall also the utilization is more as the cloud needs to process the database and Http packets continuously.
By observing the above two test cases, the overall performance is enhanced when unauthorized web access is blocked. Apart from the above cases, this network is been tested by changing the number of workstations and the packet latency.
7: Conclusion and future work

7.1 Conclusion

With the increase in the usage of the internet the demand for cloud computing has increased drastically. A lot of cloud service providers have emerged in the market and they are successful in attracting many clients. In general cloud service providers offers wide range of services to their clients and the key among them are database and other software services. The main advantage with cloud computing is that, the risk of infrastructure maintenance is reduced to the direct parties. Third parties are involved across the cloud maintenance and thus the overall cost to the organization is also reduced a lot. Apart from the advantages with cloud computing the key limitation is security. As the database and the key resources of the organization are maintained across a remote location, the level of user control over the resources would be very less. Providing security to the database resources and web resources is a tedious task and in this context there were lots of security models proposed. Based on the literature survey reports it is clear that there was no clear model that defines the performance of the database applications due to the security models imposed over the cloud.

The main aim of this project is to evaluate the performance of the database applications that were accessed from an internet cloud under the guidance of a firewall. In general when a firewall is attached to the network, the overall performance of any application against the traffic sent or received is degraded. In this context an alternative security model is required to make sure that the performance of the applications is not affected due to the unnecessary web traffic or packet filtering done by firewalls. In this project a new security model is proposed and the proposed design is explained in the previous chapters. OPNET IT guru is used as the simulation
tool in this project and three scenarios are created based on an IP based cloud. First scenario has no firewall across the cloud, second scenario has a firewall router and the third scenario completely blocks the web traffic over the cloud. Database and web application are used across the cloud and a home network with 150 users is created such that to support the corresponding applications. Few performance metrics like database query response and web page load response are used for the performance evaluation.

From the overall analysis of the results the proposed firewall model is well used for enhancing the database application. In this simulation two applications are used like the database application and web application and it is proved the overall performance of database application is enhanced when the web traffic is blocked. When the web traffic is blocked across the third scenario, even the cloud utilization is improved against processing the database application towards the home office. As mentioned 150 workstations are used and out of that 50 users support the database application. The overall database point to point utilization for all the users is enhanced as well even against the security policies and packet latency of firewalls. Thus the main aim of the project to improve the overall performance of cloud under the firewalls and also improve the security by blocking the web traffic is proved from the result analysis. When there is heavy browsing across the clouds the overall cloud utilization is increased and thus the performance is reduced. As the proposed design blocks the web traffic the database users are provided with quick query response time and also the overall performance of the cloud is also increased in terms of reducing the point to point utilization.
7.2 Future work

Apart from the work done towards the proposed design, there is some future scope and it is as given below

- More number of applications can be used to evaluate the performance of the security model proposed
- Combined clouds and hybrid clouds can be used in the future to evaluate the security requirements

Bibliography and References


