IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Volume 10, PP 87-90

Emplacing Security Devices in a Cloud Network: Survey & Implementation

Rashika Abbi, Priyanka Paygude, Snehal Chaudhary, Sonali Idate
*(Dept. Of Information Technology, Bharati Vidyapeeth (Deemed To Be University), India,
College Of Engineering, Pune)*

Abstract :*Cloud Networking Is Extensively Used And Cloud Service Providers (Csps) Deploy Various Security Devices. In Our Work We Consider Only The Placement Of Security Devices Between Servers Is Defined Using Four Partition Patterns - Firewall, Ipsec, IDS And NAT – To Meet The Security Needs In A Cost Effective Manner. This Paper, Presents An Automated Framework For Analyzing Data Centre Security Configurations. We Have Considered A Dummy Data Centre Topology, Requirements By CSP (Basically Connectivity And Isolation), Business Constraints As Inputs (Basically Usability And Cost Optimization) And Then Analyzes The Optimal Data Centre Security. Henceforth, Determining The Emplacement Of Different Security Devices In The Data Centre.*

Keywords *-Cloud Data Centre, Security Devices, Security Configuration, Cloud Service Provider*

I. INTRODUCTION

1.1 Introduction

Cloud Data Centre Security Have The Provisions And Policies Adopted By An Administrator To Continuously Prevent And Monitor Unauthorized Access, Misuse, Modification, Or Denial Of A Computer Network And Network Accessible Resources. Usually, The Cloud Service Provider Security Requirements Cover The Connectivity Requirements That Define The Service Flows Between Various Data Centre Devicesand Partition Requirements That Define Various Partition Patterns As Combination Of Different Security Devices (Firewall, Ipsec, IDS, And NAT Etc.) And Their Relative Arrangements Based On The Security Enabling Device Capability.

1.2 Introduction To Security Issues In A Cloud Network

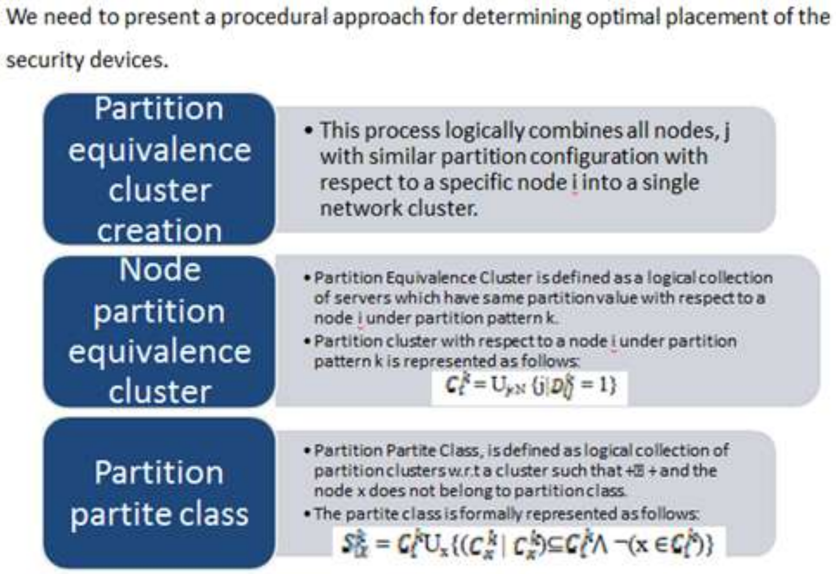
Cloud Computing And Storage Lets Their Users With Capabilities To Store & Process Data In Third-Party Data Centres. Organizations Use The Cloud In A Variety Of Different Service Models (With Acronyms Such As Saas, Paas, And Iaas) And Deployment Models (Private, Public, Hybrid, And Community).Security Issues With Cloud Computing May Fall Into Two Categories: First Issues Faced By Cloud Providers (Organizations Providing Software-, Platform-, Or Infrastructure-As-A-Service Via The Cloud) And Second,Issues Faced By Their Customers (Companies Or Organizations Who Host Applications Or Store Data On The Cloud). The Responsibility Is Shared Mutually. The Provider Must Ensure That The Infrastructure Is Secure & That The Clients' Data & Applications Are Well Protected, While The User Must Take Measures To Fortify The Application And Use Stronger And Better Passwords & Authentication Means. When An Organization Elects Data Repository Or Hosts Applications On The Public Cloud, It Loses Its Ability To Have Physical Access To The Servers Having Its Information. As A Result, Potentially Sensitive Data Is At Risk From Insider Attacks.Cloud Service Providers Often Store Multiple Customers Data On The Same Server To Conserve Resources, Optimize Costs And Efficiency. As An Outcome, There Is A Chance That A User's Private Data Can Be Accessed By Other Users (Possibly Competitors). To Handle Such Sensitive Conditions, Cloud Service Providers Must Ensure Proper Data Isolation And Logical Storage Segregation. Virtualization Is Widely Used In Implementing Cloud Infrastructure Enhances Unique Security Concerns For Customers Or Tenants Of A Public Cloud Service.It Alters The Relationship Between The OS And Underlying Hardware – For That Matter Be It Computing, Storage Or Even Networking. This Introduces An Additional Layer - Virtualization - That Itself Must Be Properly Configured, Managed And Secured. Specific Concerns Include The Potential To Compromise The Virtualization Software, Or "Hypervisor". While These Concerns Are Largely Theoretical, They Do Exist.For Example, A Breach In The Administrator Workstation With The Management Software Of The Virtualization Software Can Cause The Whole Data Centre To Go Down Or Be Reconfigured To An Attacker's Liking.

1.3Cloud Security Controls

Preventive Controls, Detective Controls, Corrective Controls, Deterrent Controls.

1.4 Partition Characteristicsin Our Work We Consider Only The Placement Of Security Devices Between Servers Is Defined Using Four Partition Patterns – To Meet The Security Needs In Cost Effective Manner, Namely Firewall, Internet Protocol, Securityintrusion, Detection System, And Network Address Translation.

1.5 Emplacement Of Security Devices



We need to present a procedural approach for determining optimal placement of the security devices.

Partition equivalence cluster creation

- This process logically combines all nodes, j with similar partition configuration with respect to a specific node i into a single network cluster.

Node partition equivalence cluster

- Partition Equivalence Cluster is defined as a logical collection of servers which have same partition value with respect to a node i under partition pattern k.
- Partition cluster with respect to a node i under partition pattern k is represented as follows:

$$C_i^k = \cup_{j \in N} \{j | D_{ij}^k = 1\}$$

Partition partite class

- Partition Partite Class, is defined as logical collection of partition clusters w.r.t a cluster such that +□+ and the node x does not belong to partition class.
- The partite class is formally represented as follows:

$$S_{ix}^k = C_i^k \cup_x \{(C_x^k | C_x^k) \subseteq C_i^k \wedge \neg(x \in C_i^k)\}$$

II. Objectives

No Matter How Cheap, Fast Or Efficient Using Cloud Computing Is, Users Will Be Hesitant To Use It Unless They Are Guaranteed Complete Security Of Their Data. The Main Objective Is To Tackle This Issue.Determining The Emplacement Of Different Security Devices In The Cloud Data Centre And Addressing Security Issues In A Cloud Network To Meet The Security Needs In A Cost Effective Manner.

III. Algorithms

3.1 Algorithm 1: Class Creation

1. The Initial Cluster Is To Be Selected And The Number Of Nodes In It Are To Be Counted.
2. Check Left Over Clusters, Except The Initial One, With Less Than Or An Equal Number Of Nodes As In The Initial One.
3. When Step 2 Is Satisfied, Check For The Nodes In The Initial One If Matches Exactly With The Next Corresponding Cluster.
4. If Step 3 Is Satisfied, Go Checking For Similar Partition Patterns, That Can Be Overlapped Or Discarded And Then Combine The Clusters Together In The Same Class.
5. Continue Repeating This Until All Clusters Are Taken Into Consideration.
6. Then Create The Next Class And Go To Step 1.

3.2 Algorithm 2: Deriving Security Device Placement

7. Start.
8. Make A Sorted List S (S_1 , S_2 ,S_3 ….S□) Based On The Descending Order Of Ꞵ$^k_{ix}$|Such That S_1 =$S_{x1\ x2}$ & Select The First Element, S_1 , From S.
9. Place A Kth Level Security Device Between The Left Partite Cluster {X1x2…} And The Right Cluster In $S_{x1\ x2}$. The Kth Level Security Can Be Anything Ranging From A Single Partition Pattern To Multiple Partition Pattern. To Simplify K^{x}x Can Be Anything 1,2,3,4 Or 1234 Or Combinations Of These Four Partition Patterns, That Is Described In Detail In The Coming Example.
10. Remove All Of The Clusters {C_{x1} , Z_{x2} ….} From (S_1 , S_2 , S_3 ….S□).
11. Remove All Empty Sets From S'.
12. Go To Step 2 If S' Is Non-Empty.
13. End.

We First Create A Sorted List, S′, Of Partite Classes Based On The Decreasing Order Of Class Size, |S_{ix}^k|, The Total Number Of Distinct Nodes In All Participating Clusters In A Class. Then, We Gradually Select

Each Element Class (Each Element Represents A Partite Class, Sx1x2…) Insequence From S′ And Place A Security Device Between The Two Partition Of That Class. After The Placement Of The Corresponding Device, We Remove The Clusters That Have Already Been Considered From All Classes. This Process Runs Continually Until The List S′ Becomes An Empty Set. Like This, For Each Partition Pattern K, Our Framework Derives The Optimal Device Placement In The Network.

IV. IMPLEMENTATION AND EVALUATION

4.1 SETUP

Bothwindows And Linux May Be Used For Our Algorithm, But We Have Used A Windows Environment. The Max Number Of Nodes That Algorithm May Evaluate Efficiently Is 100.

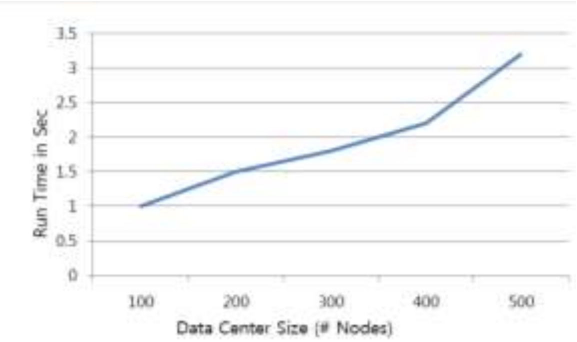
4.2 SOFTWARE USED

We Need A C Compiler, Gcc 4.3.8 Version. Code::Blocks Is A Free C, C++ And Fortran IDE Built To Meet The Most Demanding Needs Of Its Users. A Gvedit Graph File Editor For Graphvizversion1.02 To Version 2.38.0 Is Used.

4.3 TIME COMPLEXITY

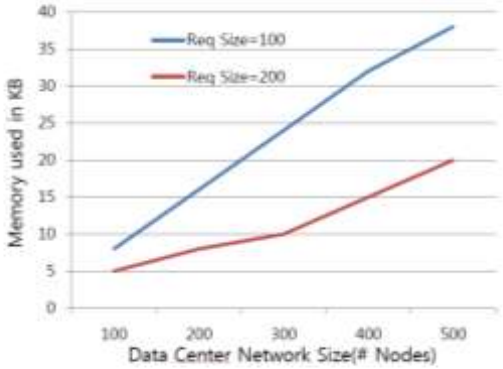
We Evaluate The Device Placement With Respect To Test Cases And Time Complexity. We Evaluate The Time Required For Device Placement Based On Separation Results. It Has Three Major Components: 1) Creation Of Separation Zone Based On Similar Service. 2) Separation Of Class Creation. 3) Time Required For Device Placement.

The Time Complexity Of Both Algorithms Are O (N^2), Where N Is The Number Of Computing And Security Nodes Present In The Cloud Data Centre Network.



4.4 SPACE COMPLEXITY

The Space Requirements Represent The Memory Used For Solving Problems Related To Device Placement. Figure Here Shows That The Memory Used Linearly Varies With The Network Size Under Different Requirements.

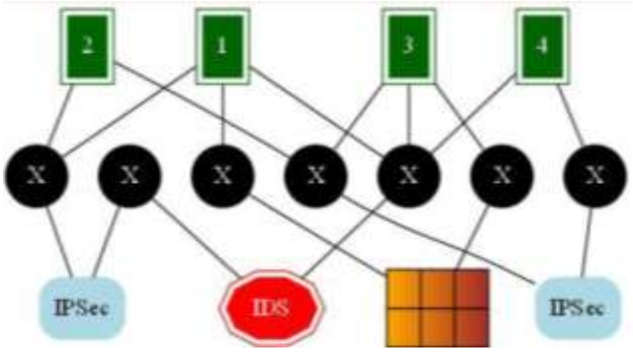


4.6EXAMPLE

Let Us Implement The Above Evaluation Into An Example Of Multiple Patterns Where K=1,2,3 Or Their Combinations, I.E, Firewall, IDS And Ipsec. Considering The Following Partition Equivalent Clusters Under The Given Partition Pattern (Based On Partition Variables) For A Network Of Say 4 Nodes (1,2,3 And 4): $C_1{}^{123}$= {3,4}, I.E., Firewall, Ipsec. And IDS Are Placed Between The Nodes Node1 And Node 3 And Node 4.

$C^{23}{}_2$ = {4} Ipsec And IDS Must Be Placed Between Node 2 And Node 4.

C^1_3 = {1} Only Firewall Must Be Placed Between Node 1 And Node 3.
C^{12}_4 = {2,3} Firewall As Well Ipsec Should Be Placed Between Node 4 And Node 2 And Node 3.
Now Here The Clusters Which Need To Place Firewall As Well As Ipsec Between The Nodes Are Only Allowed To Have Ipsec Between Them Since Ipsec Acts As Firewal So There Is No Such Need To Put Both The Security Devices. The Associated Partition Classes For These Clusters After The Modicfication Of The Partition Patterns Of Clusters Are As Follows : $S^{23}_{1\ 2}$ = {C_1 , C_2 } : S^3_2 = {C_2 } : S^2_4 = {C_4 }
Different Iterations Of Device Placement Are Possible As Follows :
Iteration 1: S' ($S_{1\ 2}$, S_4 , S_3 , S_2); (1,2)Δ {C_1 , C_2 }~ (3,4)
Iteration 2 : S'(S_4 , S_3); (4) Δ {C_4 }~ (2,3)
Iteration 3: S' (S_3); (3)Δ{C_3 }~ (3,4) Now Here XΔY Are In The Usual Form.



V. Conclusion

5.1 OVERALL OUTCOME

Security Issues In The Area Of Cloud Computing Are Active Area Of Research And Experimentation..Therefore, Generating A Usable And Optimal Security Configuration That Resolves The Contention Between The Security Requirements And Business Constraints Is An Important But Challenging Problem.

5.2 FUTURE SCOPE

Security Abstraction: There Has Always Been A Room In The IT World For New Traditionally Unified Threat Management Devices Or Security Management Tools. So However, Hardening Physical Appliances Aside, More Organizations Have Developed &Deployed Security Platforms On Top Of A VM. The Reachability To Clone The Security Devices, Place Them At Different Points Within Organization And Assigning Particular Functions To Them Makes The Security Virtualization Very Attractive. Imagine Having A Security Device VM Only Doing DLP, IPS/IDS. This Type Of Development &Deployment Can Be Very Strategic And Profitable. Furthermore, Virtual Services Specifically Designed To Protect Your Cloud Will Be Generated Sooner. Inter-Cloud Connectivity Needs A Good Security Practice Before Coming Into Action. This Is Where More Virtual Appliances That Are Helping Bind Security Services Offering Multiple Cloud Services Are Really Going To Help.

References

[1] International Conference On Information Security & Privacy (ICISP2015), 11-12 December 2015,Nagpur, INDIA"Placement Of Security Devices In Cloud Data Centre Network:Analysis And Implementation" Santosh Kumar Majhi, Sunil Kumar Dhal,Veer Surendrasai University Of Technology, Odisha-768018, India, Sri Sri University, Odisha, India

[2] S. Majhi, S. Kumar, P.Bera, E. Al. Shaer, M. Satapathy. "Synthesizing Optimal Security Configuration For Enterprise Network" In IET System Safety And Cyber Security Conference, Manchester, UK, Oct. 2014.

[3] Cloud Security And Management – Book

[4] Www.Dl.Acm.Org, Www.Wikipedia.Com, Www.Google.Com, Www.Skyboxsecurity.Com, Www.Researchgate.Net, Http://Www.Graphviz.Org/