CHAPTER 6

ARCHITECTURE TO MITIGATE DDoS ATTACKS ON HYBRID CLOUDS

6.1 ABSTRACT

This chapter presents an approach for selecting the correct mitigation solution, performance parameters to measure and then illustrates the design and implementation of single tier data center and the proposed three tier secure Hybrid Cloud architecture to mitigate DDoS attacks.

6.2 SELECTING DDoS MITIGATION SOLUTION

There are few approaches to DDoS attack mitigation solutions from design perspective that are discussed here: on premise, Cloud and Hybrid based designs with regards to their ability to defend volumetric attacks so the need of Cloud component, ability to block application attacks without requiring any SSL key surrender and Deploy network infrastructure is acceptable to the IT operations team. A workable solution is required with recommendations for defending and mitigating DDoS Attacks as described in the below section.

- **On-premise Based DDoS Solutions**

Before 2010 DDoS attacks simply 'flooded the pipes', now the attack trend has shifted in terms of tools, capability, capacity and techniques. Instead of targeting and flooding, attackers use slow, legitimate traffic to target application layer web services. Having a dedicated On Premise DDoS attack mitigation solution are best suited for government entities, financial institutions and healthcare but not useful for all. When the highest level of security is mandatory and organizations prefer to give as little visibility into their customer data or about their encryption certificates to as few third party providers, this can be looked as a limited scope option. On premise DDoS devices would store encryption certificates and inspect traffic locally without any scrubbing, redirection or inspection. The mitigation system would be required to protect against various DDoS vectors as described by François, et al. (2012) like Flooding (UDP, ICMP, SYN), SSL based, Application layer (HTTP GET / POST) or Low & Slow attacks. With mitigation systems in house the proximity to data center resources is useful and the systems can be fine-tuned immediately by the in house IT teams. They tend to have a far greater awareness to their setup for any changes in traffic flows or from the application servers. Thus would tend to have a higher probability of detecting any suspicious trends or traffic requests. While the organizations benefits from an immediate response, in case of network floods, an on premise DDoS solution cannot be expected to handle volumetric network floods and must be mitigated from the Cloud away from on premise infrastructure.

- **Cloud Based DDoS Services**

Providing anti-DDoS and advanced mitigation protection in form of managed security services, Cloud service providers offer protection from network floods by deploying mitigation equipment at the ISP network edge level or with scrubbing centers as described by Hussain, et al. (2013). This involves traffic diversion from the enterprise network to detection or scrubbing center. When a DDoS attack starts, human intervention is required and takes at least 15-30 minutes during which the online services are left unprotected and exposed. Although the Cloud based DDoS mitigation service guarantees to an extent blocking of network flood attacks from reaching the enterprise edge devices or flooding the WAN circuit which is free of volumetric network flood attack. However, there exist glaring issues with a Cloud based DDoS mitigation services as this cannot detect and block Application layer attacks and slow attacks, it is unable to protect Statefull infrastructure systems like firewalls or IPS and is unable to deal with attacks like application layer attack, state exhaustion and multi vector attacks.

- **Hybrid Cloud Based DDoS Solutions**

Using Hybrid Cloud features offers the best-of-breed mitigation options as shown by Girma, et al. (2015). The design combines the on premise, in house setup along with public clouds and cloud service mitigation providers working as an integrated system. For enterprises working with critical financial domains or with government organizations, use of multi layered architecture (Seethalakshmi, et al, 2016) design is the ideal design to implement. In a Hybrid Cloud solution, by using a dedicated DDoS mitigation provider's ability to detect and block multiple DDoS vectors or even have a Public Cloud provider dynamically increase the network pipe bandwidth during a DDoS attack, can take off critical time after the attack has been detected. This provides a breather till the time mitigation actually starts. This saves the on premise infrastructure from the attack impact and minimizes the downtime of the online services. During the DDoS attack, the entire traffic is diverted to a DDoS mitigation provider's Cloud. Here the traffic is scanned and the attack traffic is identified and removed. Then the traffic is re-routed back to the enterprise in house data center. This contains only the intended user requests.

Hybrid Cloud design also offer inherent benefits as described below.

- Achieve wide security coverage by combining on premise and Cloud data centers.
- Have the shortest response time achieved when employing an on premise solution as a fallback, which initiates immediately to mitigate DDoS attacks.
- Single point of contact (SPOC) during an attack for on premise and Cloud setup
- Each tier is independent of the other and can scale horizontally - in case of a web application attack spike, WAF devices can be added to the application defense tier without affecting the network tier.
- Performance levels improve since user requests come in tiers basis, so the network utilization is minimized and the overall traffic load gets reduced
- If a device in any tier is down, another option can be initiated to process the requests
- Vendor independence is achieved as network and application defense infrastructure is implemented using hardware platforms of different software versions and brands.
- Policy independence is realized since new or custom policies can be applied at the application defense tier, independent of the network defense tier. The other tiers directs only that specific traffic towards the policies after validation and production testing is successful.

6.3 REAL USER MONITORING PARAMETERS

In this section, the system and device logs are collected from network devices and servers to illustrate the success or failure of the designed infrastructures against the DDoS attacks. From the logs key performance indicators are considered in form of Real User Monitoring parameters as the criteria for measuring the infrastructure resilience and to determine the end user visibility. This gives a real time indication on how the application behaves when loading on the user systems during the DDoS attacks. These parameters present the real user performance experience as opposed to synthetic monitoring which only provides availability, uptime or the web application performance using average or percentiles. These key performance indicators offer deeper visibility into the web application user experience as described below.

- Browser Throughput is defined as the page requests received per minute by the user browsers
- Application Server Response – determining the % of time for page load process
- SaaS Application status code – HTTP status codes when sessions between the Web browser or User agent and the Web application server is in process.
- ICMP latency (milliseconds) – before and during DDoS attack on Cloud application
- Portal Page Load Response time – after portal opens and the user logs and authenticates to get inside the Cloud application. This involves responses sent back and forth over the network and are rendered in the user browser

6.4 ALGORITHAMIC REPRESENTATION OF DDoS ATTACK MITIGATION

The DDoS attack mitigation methodology followed in this for executing the DDoS on designed architectures is presented in form of an algorithm as illustrated below.

```
Start DDoS Attack
Identify Attack Target
Scan for open ports and IP address
Initiate Botnet Army using Command & Control server
Load DDoS Tools with attack parameter value
Start DDoS Attack on Three tier infrastructure
  High Rate Attack (ICMP Flood or Malformed UDP Packets)
    If (Inbound Rate > Average Rate)
      Review Network Firewall logs                    /*** Confirmed Flood Attack
      If (ICMP count < Minimum Threshold Size)
            Firewall Logs → Data (Flow = Malicious)  /*** Drop Packets @ Tier 1
        If (UPD Packet > UDP Packet (Threshold Rate)
          Review Wireshark Logs                       /*** Confirmed UDP Attack
        Low Rate Flood Attack (HTTP Get)
          If (Average Packet Size < Minimum Threshold Size)
            WAF Logs → Data (Flow = Malicious)       /*** Drop Packets @ Tier 2
          Else
```

```
            Indicates authentic user                 /*** Admit Packets
             Else continue filtering                 /*** Throughput analysis
              Select Random UDP Packets from queue
             If (Both Packets = similar IP source)
               Calculate Threat level for multiple occurrences
              If (Threat determined > Threshold)
                Network Firewall                     /*** Blocks the data flow
              Else
                Drop packet → Attacker
                  Else continue filtering  → throughput analysis
                If (Inbound (burst traffic) > Received (Threshold traffic))
                  Drop packet
                Else indicates clean traffic
                  Admit data packet → Authenticated User    /*** Allowed access
Initiate DDoS Attack Alert
Notify for DDoS Flood and HTTP Attack mitigation process
Execute DDoS on Single Tier and Three Tier infrastructures
Collect logs from the devices and servers for attack sequences
Compare and illustrate results from key performance indicators
Close
```

Table 6.1: Algorithmic representation of DDoS attack mitigation

6.5 DESIGNING SINGLE TIER ARCHITECTURE

The author designed and implemented the Single Tier architecture as a flat single tier architecture with standard network services and web application portal simulating a Cloud hosted application in a data center. The Web Portal comprises of web pages running scripts gathering real time data like Temperatures, NSE Stock values and saving them on a database. This simulated the web portal application. This architecture is designed with the standard routing and switching network devices running in an on premise private data center, connecting the web portal to the Internet (Joshi, et al., 2012) as illustrated in Figure 6.1 below. The red arrows denote the attack traffic, blue arrows designates the user traffic while the green arrows illustrate the outbound traffic.

This design has the same single inbound and exit default gateway (11.252.15.1) for the web traffic. The legitimate users as well as attackers enter and exit following the same data flow route. The Web application running .NET and IIS services comprises of VMware virtual machines hosting the front end web portal (11.252.15.200) and backend SQL Server Database (11.252.15.25) which simulates the Cloud application environment. Hardware Devices and servers implemented for the Single Tier Data Center infrastructure are presented in Table 6.2 below.

Hardware for Single Tier Infrastructure	Router → Cisco 3600: *11.252.15.1* Network Firewall → Cisco ASA 5506-X: *11.252.15.2* Web Application Firewall → Imperva WAF: *11.252.15.3* Load Balancer → F5 Big IP 4200v LTM: *11.252.15.5* Switch → Cisco 3550: *11.252.15.100* Servers → Dell Server 64-bit i5 quad core, 16 GB RAM, 2 x 500GB SCSI
Software	Bare Metal Servers → VMware Workstation version 10: *11.252.15.200* Windows OS → Server 2008: *11.252.15.251* Web Application → SaaS Portal, .NET over IIS: *11.252.15.252* Database → SQL 2008 Database: *11.252.15.250*
DDoS Attacks	Performed from multiple Windows 7 systems acting as bots

Table 6.2: Requirements for Single Tier Infrastructure

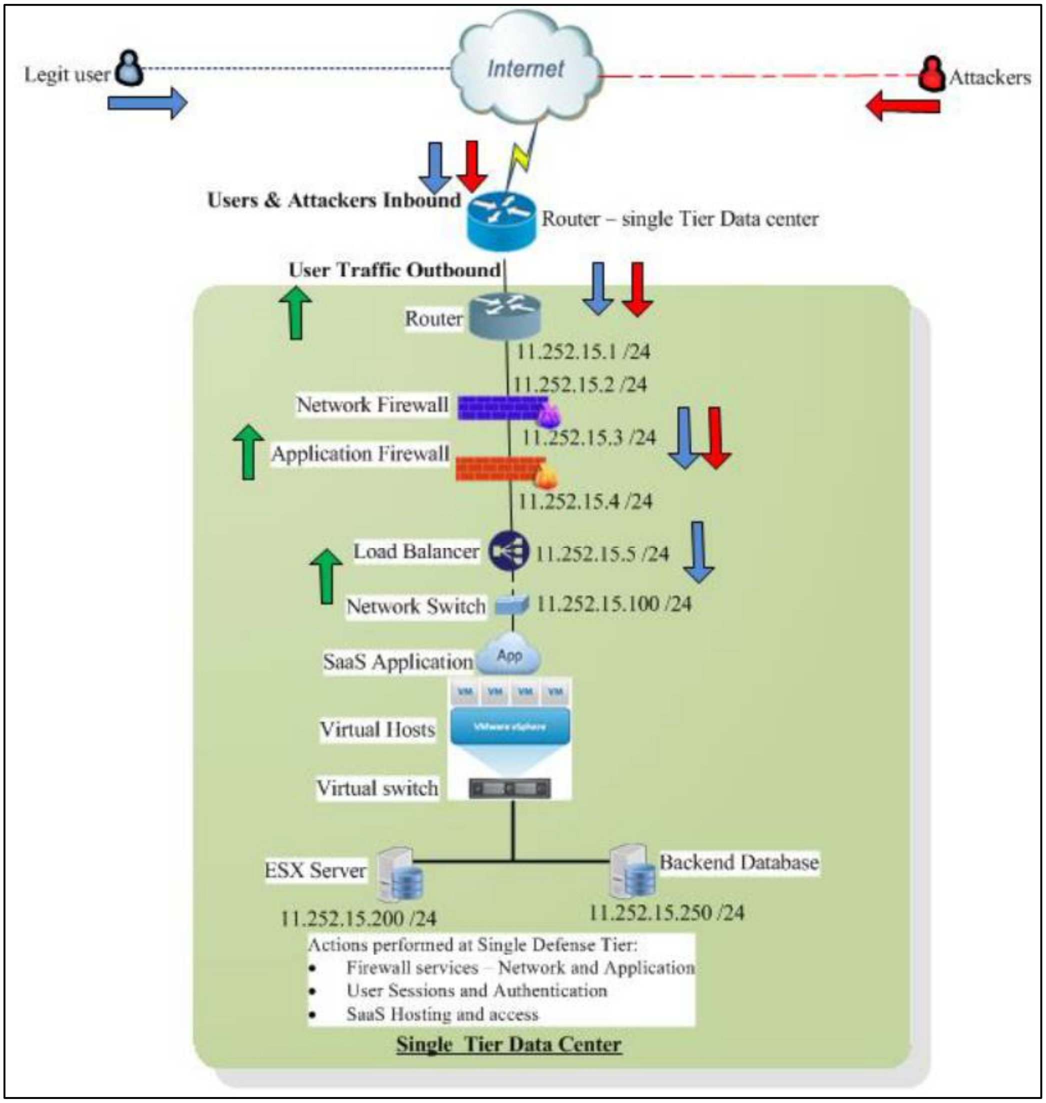


Figure 6.1: Single Tier Architecture Design

DDoS attacks are executed on the single tier infrastructure as ICMP flooding with 1000 echo requests with increasing buffer size (from 3700 to 3805 bytes) as

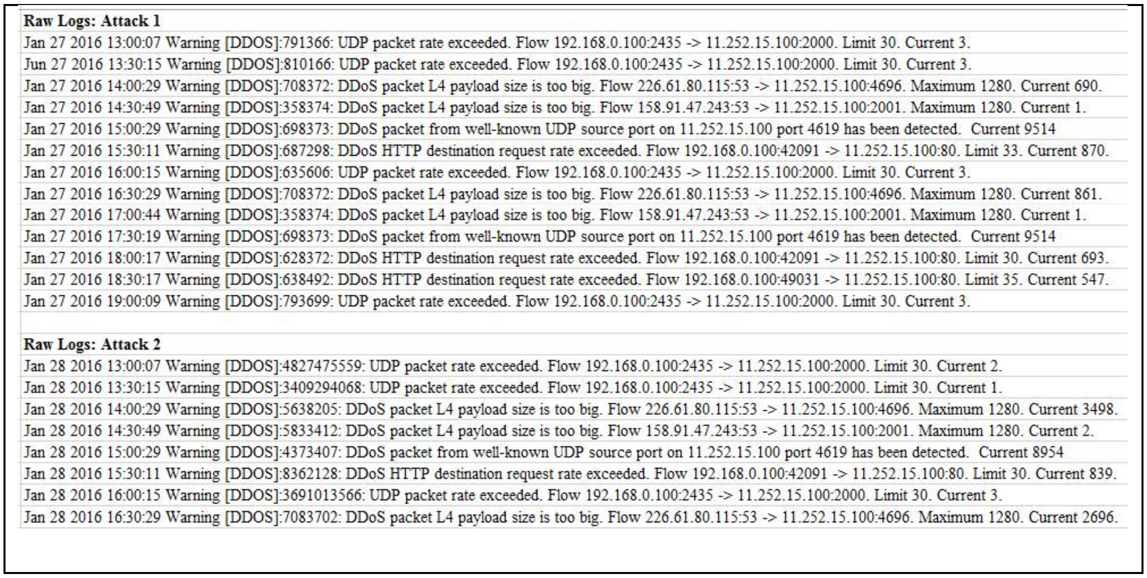
```
C:\> Ping –t –l 202.122.134.1
```

Application level attacks are executed using tools such as LOIC, R.U.D.Y and Slowloris. Slow socket buildup is performed for slow web attacks and HTTP Floods by increasing the thread count as

GET /app/?id=437793msg=BOOM%2520HEADSHOT!HTTP/1.1Host: 11.152.15.200.

These attacks simulated DDoS network and application level attacks that deny legitimate users the access to the web application portal running on the single tier infrastructure. Logs are collected from the network devices and servers during the DDoS attacks are performed for detailed analysis.

Figure 6.2 presents the raw logs obtained after the DDoS attack. This shows the excess DDoS HTTP rate and large sized data packets depicting the DDoS attack.

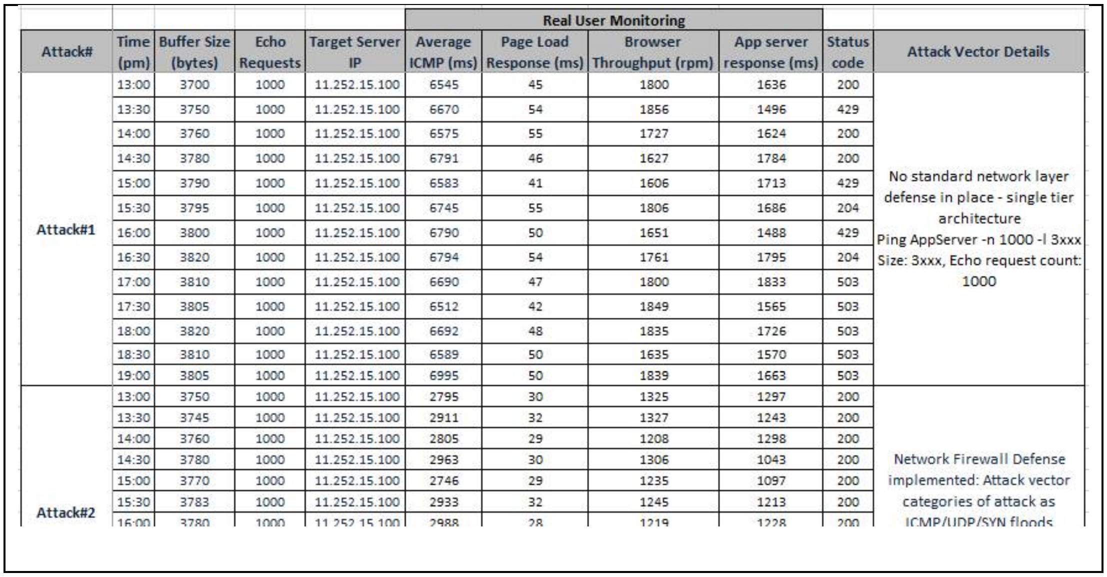


```
Raw Logs: Attack 1
Jan 27 2016 13:00:07 Warning [DDOS]:791366: UDP packet rate exceeded. Flow 192.168.0.100:2435 -> 11.252.15.100:2000. Limit 30. Current 3.
Jun 27 2016 13:30:15 Warning [DDOS]:810166: UDP packet rate exceeded. Flow 192.168.0.100:2435 -> 11.252.15.100:2000. Limit 30. Current 3.
Jan 27 2016 14:00:29 Warning [DDOS]:708372: DDoS packet L4 payload size is too big. Flow 226.61.80.115:53 -> 11.252.15.100:4696. Maximum 1280. Current 690.
Jan 27 2016 14:30:49 Warning [DDOS]:358374: DDoS packet L4 payload size is too big. Flow 158.91.47.243:53 -> 11.252.15.100:2001. Maximum 1280. Current 1.
Jan 27 2016 15:00:29 Warning [DDOS]:698373: DDoS packet from well-known UDP source port on 11.252.15.100 port 4619 has been detected.  Current 9514
Jan 27 2016 15:30:11 Warning [DDOS]:687298: DDoS HTTP destination request rate exceeded. Flow 192.168.0.100:42091 -> 11.252.15.100:80. Limit 33. Current 870.
Jan 27 2016 16:00:15 Warning [DDOS]:635606: UDP packet rate exceeded. Flow 192.168.0.100:2435 -> 11.252.15.100:2000. Limit 30. Current 3.
Jan 27 2016 16:30:29 Warning [DDOS]:708372: DDoS packet L4 payload size is too big. Flow 226.61.80.115:53 -> 11.252.15.100:4696. Maximum 1280. Current 861.
Jan 27 2016 17:00:44 Warning [DDOS]:358374: DDoS packet L4 payload size is too big. Flow 158.91.47.243:53 -> 11.252.15.100:2001. Maximum 1280. Current 1.
Jan 27 2016 17:30:19 Warning [DDOS]:698373: DDoS packet from well-known UDP source port on 11.252.15.100 port 4619 has been detected.  Current 9514
Jan 27 2016 18:00:17 Warning [DDOS]:628372: DDoS HTTP destination request rate exceeded. Flow 192.168.0.100:42091 -> 11.252.15.100:80. Limit 30. Current 693.
Jan 27 2016 18:30:17 Warning [DDOS]:638492: DDoS HTTP destination request rate exceeded. Flow 192.168.0.100:49031 -> 11.252.15.100:80. Limit 35. Current 547.
Jan 27 2016 19:00:09 Warning [DDOS]:793699: UDP packet rate exceeded. Flow 192.168.0.100:2435 -> 11.252.15.100:2000. Limit 30. Current 3.

Raw Logs: Attack 2
Jan 28 2016 13:00:07 Warning [DDOS]:4827475559: UDP packet rate exceeded. Flow 192.168.0.100:2435 -> 11.252.15.100:2000. Limit 30. Current 2.
Jan 28 2016 13:30:15 Warning [DDOS]:3409294068: UDP packet rate exceeded. Flow 192.168.0.100:2435 -> 11.252.15.100:2000. Limit 30. Current 1.
Jan 28 2016 14:00:29 Warning [DDOS]:5638205: DDoS packet L4 payload size is too big. Flow 226.61.80.115:53 -> 11.252.15.100:4696. Maximum 1280. Current 3498.
Jan 28 2016 14:30:49 Warning [DDOS]:5833412: DDoS packet L4 payload size is too big. Flow 158.91.47.243:53 -> 11.252.15.100:2001. Maximum 1280. Current 2.
Jan 28 2016 15:00:29 Warning [DDOS]:4373407: DDoS packet from well-known UDP source port on 11.252.15.100 port 4619 has been detected.  Current 8954
Jan 28 2016 15:30:11 Warning [DDOS]:8362128: DDoS HTTP destination request rate exceeded. Flow 192.168.0.100:42091 -> 11.252.15.100:80. Limit 30. Current 839.
Jan 28 2016 16:00:15 Warning [DDOS]:3691013566: UDP packet rate exceeded. Flow 192.168.0.100:2435 -> 11.252.15.100:2000. Limit 30. Current 3.
Jan 28 2016 16:30:29 Warning [DDOS]:7083702: DDoS packet L4 payload size is too big. Flow 226.61.80.115:53 -> 11.252.15.100:4696. Maximum 1280. Current 2696.
```

Figure 6.2: Raw DDoS Attack Logs

After detecting the DDoS attack, Network firewall defense is initiated during attack#2 and the logs are collected as illustrated in Figure 6.3 below.



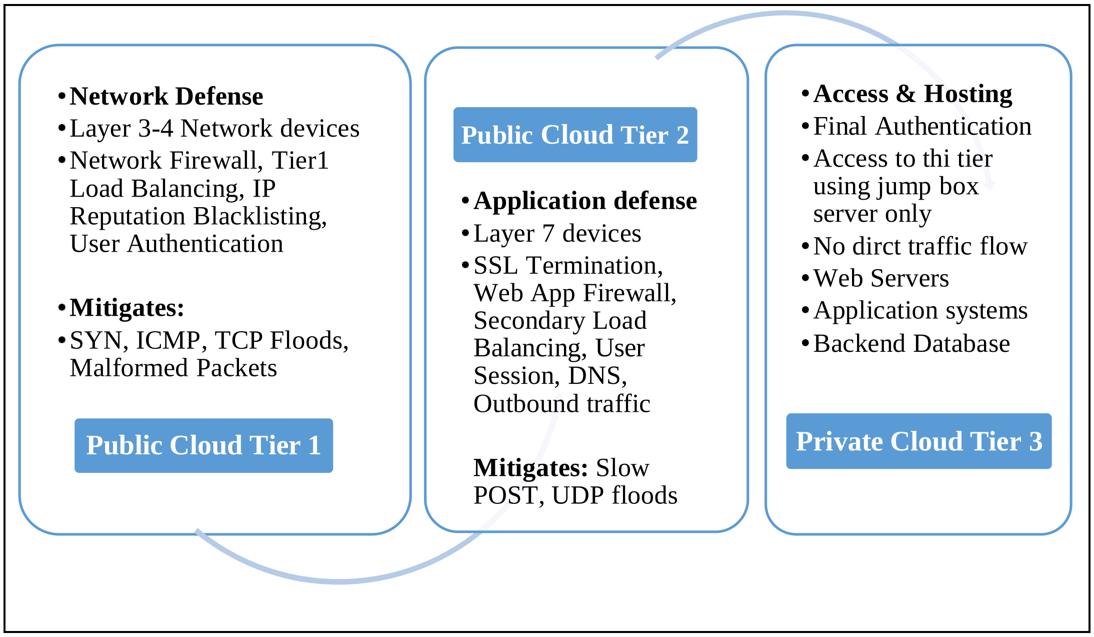
					Real User Monitoring					
Attack#	Time (pm)	Buffer Size (bytes)	Echo Requests	Target Server IP	Average ICMP (ms)	Page Load Response (ms)	Browser Throughput (rpm)	App server response (ms)	Status code	Attack Vector Details
Attack#1	13:00	3700	1000	11.252.15.100	6545	45	1800	1636	200	No standard network layer defense in place - single tier architecture Ping AppServer -n 1000 -l 3xxx Size: 3xxx, Echo request count: 1000
	13:30	3750	1000	11.252.15.100	6670	54	1856	1496	429	
	14:00	3760	1000	11.252.15.100	6575	55	1727	1624	200	
	14:30	3780	1000	11.252.15.100	6791	46	1627	1784	200	
	15:00	3790	1000	11.252.15.100	6583	41	1606	1713	429	
	15:30	3795	1000	11.252.15.100	6745	55	1806	1686	204	
	16:00	3800	1000	11.252.15.100	6790	50	1651	1488	429	
	16:30	3820	1000	11.252.15.100	6794	54	1761	1795	204	
	17:00	3810	1000	11.252.15.100	6690	47	1800	1833	503	
	17:30	3805	1000	11.252.15.100	6512	42	1849	1565	503	
	18:00	3820	1000	11.252.15.100	6692	48	1835	1726	503	
	18:30	3810	1000	11.252.15.100	6589	50	1635	1570	503	
	19:00	3805	1000	11.252.15.100	6995	50	1839	1663	503	
Attack#2	13:00	3750	1000	11.252.15.100	2795	30	1325	1297	200	Network Firewall Defense implemented: Attack vector categories of attack as ICMP/UDP/SYN floods
	13:30	3745	1000	11.252.15.100	2911	32	1327	1243	200	
	14:00	3760	1000	11.252.15.100	2805	29	1208	1298	200	
	14:30	3780	1000	11.252.15.100	2963	30	1306	1043	200	
	15:00	3770	1000	11.252.15.100	2746	29	1235	1097	200	
	15:30	3783	1000	11.252.15.100	2933	32	1245	1213	200	
	16:00	3780	1000	11.252.15.100	2988	28	1219	1228	200	

Figure 6.3 Single Tier – Real User Monitoring Parameters

From initial analysis of these system and device logs, the single tier displays a steadily degraded performance and response towards the end user accessing the web portal. To further validate this theory, the single tier logs are analyzed for Real User Monitoring parameters and is investigated further and presented in detail in the subsequent chapter.

6.6 DESIGNING THREE TIER ARCHITECTURE

The author designed the three tier architecture to mitigate DDoS attacks on Hybrid Clouds which is further illustrated in detail in the Figure 6.4 below.



•Network Defense
•Layer 3-4 Network devices
•Network Firewall, Tier1 Load Balancing, IP Reputation Blacklisting, User Authentication
•Mitigates:
•SYN, ICMP, TCP Floods, Malformed Packets
Public Cloud Tier 1
Public Cloud Tier 2
•Application defense
•Layer 7 devices
•SSL Termination, Web App Firewall, Secondary Load Balancing, User Session, DNS, Outbound traffic
Mitigates: Slow POST, UDP floods
•Access & Hosting
•Final Authentication
•Access to thi tier using jump box server only
•No dirct traffic flow
•Web Servers
•Application systems
•Backend Database
Private Cloud Tier 3

Figure 6.4: Three Tier Architcture Design Model

The first and second tiers are implemented as defense tiers while the third tier is the actual Cloud access tier hosting the portal. The three tiers are interconnected with each other via a secure virtual private network. Figure 6.5 below illustrates the detailed network diagram with IP Address scheme and device details. This infrastructure tiers are discussed in detail in the section below.

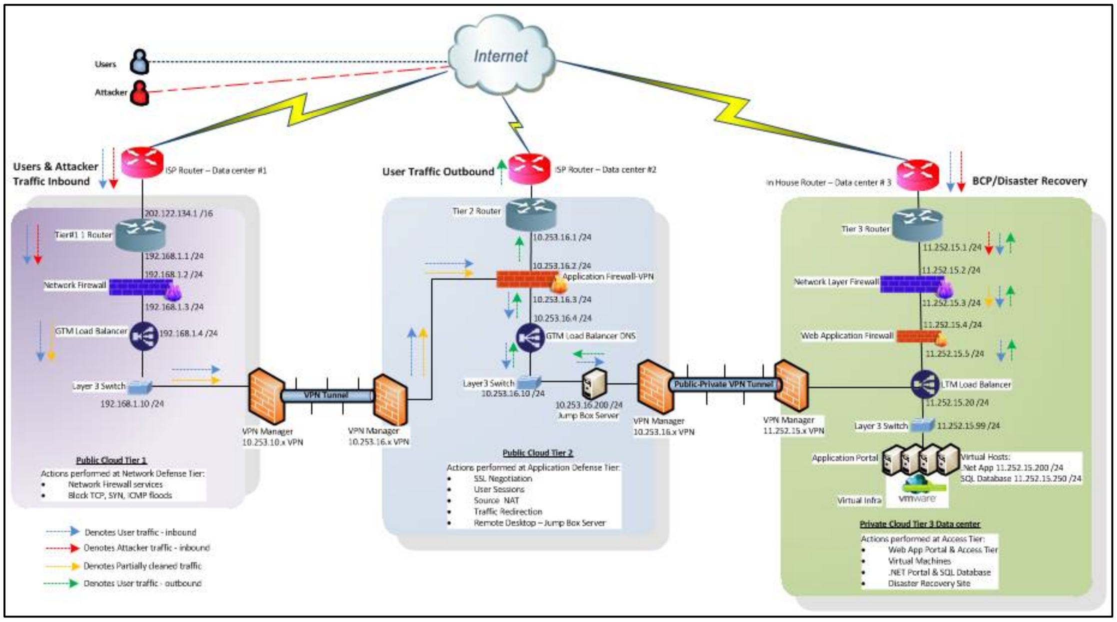

Internet
Users
Attacker
Users & Attacker Traffic Inbound
ISP Router – Data center #1
202.122.134.1 /16
Tier#1 1 Router
192.168.1.1 /24
192.168.1.2 /24
Network Firewall
192.168.1.3 /24
GTM Load Balancer
192.168.1.4 /24
Layer 3 Switch
192.168.1.10 /24
VPN Tunnel
VPN Manager 10.253.10.x VPN
VPN Manager 10.253.16.x VPN
Public Cloud Tier 1
Actions performed at Network Defense Tier:
Network Firewall services
Block TCP, SYN, ICMP floods
Denotes User traffic - inbound
Denotes Attacker traffic - inbound
Denotes Partially cleaned traffic
Denotes User traffic - outbound
User Traffic Outbound
ISP Router – Data center #2
Tier 2 Router
10.253.16.1 /24
10.253.16.2 /24
Application Firewall-VPN
10.253.16.3 /24
10.253.16.4 /24
GTM Load Balancer DNS
Layer3 Switch 10.253.16.10 /24
10.253.16.200 /24 Jump Box Server
VPN Manager 10.253.16.x VPN
Public-Private VPN Tunnel
Public Cloud Tier 2
Actions performed at Application Defense Tier:
SSL Negotiation
User Sessions
Source NAT
Traffic Redirection
Remote Desktop – Jump Box Server
In House Router – Data center # 3
BCP/Disaster Recovery
Tier 3 Router
11.252.15.1 /24
11.252.15.2 /24
Network Layer Firewall
11.252.15.3 /24
11.252.15.4 /24
Web Application Firewall
11.252.15.5 /24
VPN Manager 11.252.15.x VPN
LTM Load Balancer
11.252.15.20 /24
Layer 3 Switch
11.252.15.99 /24
Application Portal
Virtual Hosts:
.Net App 11.252.15.200 /24
SQL Database 11.252.15.250 /24
Virtual Infra
vmware
Private Cloud Tier 3 Data center
Actions performed at Access Tier:
Web App Portal & Access Tier
Virtual Machines
.NET Portal & SQL Database
Disaster Recovery Site

Figure 6.5: Three Tier Architecture Design

The below section illustrates each tier in detail regarding the implementation and setup.

6.6.1 NETWORK DEFENSE TIER

The first tier is implemented using Public Cloud for network layer defense services running only Layer 3 and 4. This tier receives inbound traffic comprising of cyber attackers as well as legitimate users. This tier provides Network level mitigation services for volumetric network attacks as ICMP, UDP, SYN floods and malformed packets along with basic Load Balancer features. Inbound HTTP TCP traffic enters from this tier as illustrated in Figure 6.6. In the first tier, the inbound traffic is checked for Network firewall defense while the remaining traffic is routed to the second tier via a secure virtual private network circuit connecting tier 1 and tier 2 data centers.

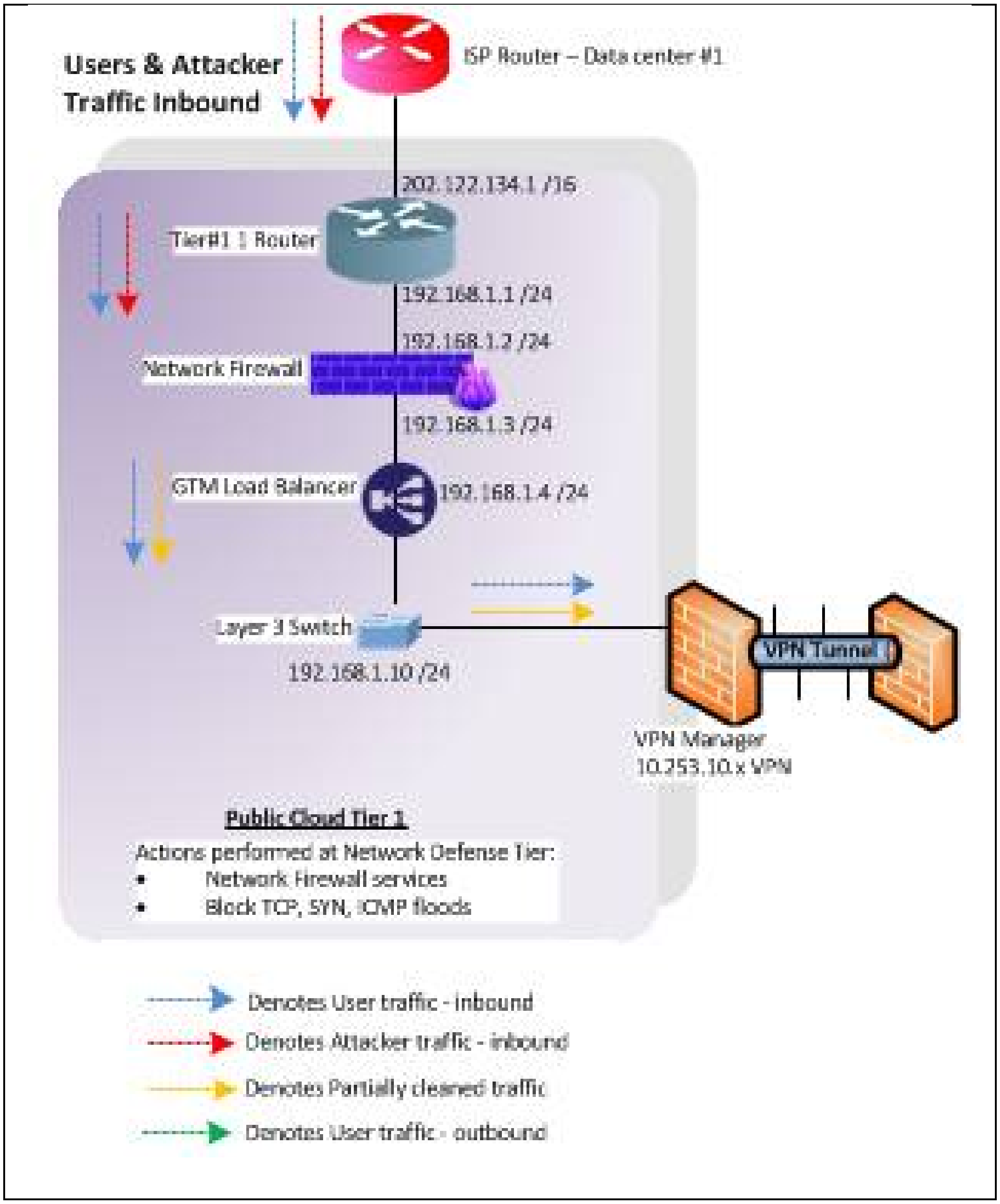

Users & Attacker
Traffic Inbound
ISP Router – Data center #1
202.122.134.1 /16
Tier#1 1 Router
192.168.1.1 /24
192.168.1.2 /24
Network Firewall
192.168.1.3 /24
GTM Load Balancer
192.168.1.4 /24
Layer 3 Switch
192.168.1.10 /24
VPN Tunnel
VPN Manager
10.253.10.x VPN
Public Cloud Tier 1
Actions performed at Network Defense Tier:
• Network Firewall services
• Block TCP, SYN, ICMP floods
Denotes User traffic - inbound
Denotes Attacker traffic - inbound
Denotes Partially cleaned traffic
Denotes User traffic - outbound

Figure 6.6: Three Tier Architecture – Network Defense Tier

Hardware devices implemented in the Network Defense Tier are presented in Table 6.3.

Hardware for Network Defense Infrastructure	Router → Cisco 3600: *192.168.1.1* Network Firewall → Cisco ASA 5506-X: *192.168.1.2* Web Application Firewall → Imperva WAF: *192.168.1.3* Load Balancer → F5 Big IP 4200v LTM: *192.168.1.4* Switch → Cisco 3550: *192.168.1.10* IPSec VPN → Cisco ASA: *192.168.1.110*
DDoS Attacks	Performed from multiple Windows 7 systems acting as bots

Table 6.3: Requirements for Network Defense Infrastructure

This functionally is made available by customizing Cisco ASA (192.168.1.2) for network flood attack checks and Big-IP Load Balancer (192.168.1.4) to deliver Basic

Load Balancing features as the Global Traffic Manager. This configuration provides network level detection for SYN floods, Post Scans, HPing, UDP floods along with PUSH and ACK flood attacks with full proxy traffic visibility and rate limiting.

On running the command '*HPING3 -1 -C -K 3 --flood 202.122.134.1*' from a single system, 180Mbps DoS attack is generated. Combining several Windows 7 systems, the output well be magnified. In order to detect and block ICMP HPING, the Network Firewall (192.168.1.2) is re-configured as:

```
Tier1NwFw(config-cmap)# icmp unreachable rate-limit 1 burst-size 1
                        icmp deny any time-exceeded WAN
                        icmp deny any unreachable WAN
```

In order to view the traffic inspection map, the Network Firewall is re-configured as:

```
Tier1NwFw(config-cmap)# show running-config class-map inspection_default
                        class-map inspection_default
                        match default-inspection-traffic
                        match access-list inspect
```

After network defense is completed, the traffic is route to the second tier using IPSec VPN configured for the following.

```
Tier1-VPN(config-ikev1-policy)# encryption 3des SHA-1       ** 3DES for encryption algorithm
Tier1-VPN(config-ikev1-policy)# hash md5                    ** MD5 for hash
Tier1-VPN(config-ikev1-policy)# authentication rsa-sig      ** RSA for authentication
Tier1-VPN(config-ikev1-policy)# group 2                     ** Diffe-Hellman Identifier
Tier1-VPN(config-ikev1-policy)# lifetime 86400              ** 24 hours for SA Lifetime
Tier1-VPN(config-ikev1-policy)# crypto ike1 enable outport ** Terminate VPN
```

6.6.2 APPLICATION DEFENSE LAYER

The second tier is also implemented using Public Cloud and designed for providing application layer defense against the layer 7 attack mitigations Slow POST, UDP Floods using Web Application Firewall with advanced Load Balancing rules. Here application layer defense is performed using the web application firewall (10.253.16.2) against application level vulnerabilities like SQL Injection or Cross Site Scripting request forgery. The WAF is configured to detect slow read or slow write sent from Slowloris DDoS attacks and restricts such user requests by dropping the sessions.

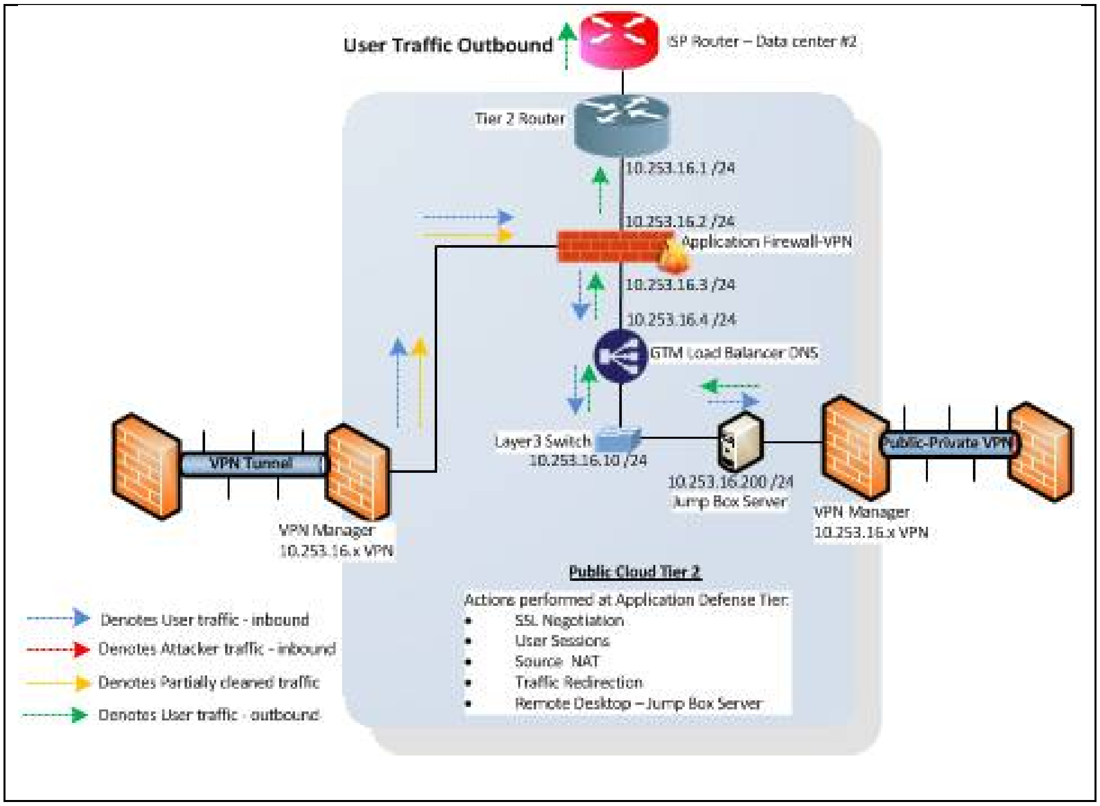


Figure 6.7: Three Tier Architecture – Application Defense Tier

Devices and Servers implemented at Tier 2 data center are presented in Table 6.4 below.

Hardware for Application Defense Infrastructure	Router → Cisco 3600: *10.253.16.1* Web Application Firewall → Imperva WAF: *10.253.16.2* Load Balancer → F5 Big IP 4200v LTM: *10.253.16.4* Switch → Cisco 3550: *10.253.16.10* IPSec VPN → Cisco ASA: *10.253.16.110* Servers → Dell Server 64-bit i5 quad core, 16 GB RAM, 2 x 500GB SCSI
Software	Remote Access Server → Windows 2008 Jump Box: *10.253.16.200*
DDoS Attacks	Performed from multiple Windows 7 systems acting as bots

Table 6.4: Requirements for Application Defense Infrastructure

Application level attacks like HTTP Floods or Ping backs are detected and mitigated at this level as well along with SSL termination. Using the Load Balancer as Global Traffic Manager (10.253.16.4), elastic load balancing is implemented to detecting the well-formed TCP connections. This reduces the risk of malicious overloading requests on applications. Synching user sessions between the Load Balancers in first and second tiers is also performed here.

The author cached static content from the application portals and allowed accessing of the portal contents at the edge level instead of the access layer. Since both these defense tiers are Public Clouds, scalability and provisioning is never an issue.

6.6.3 ACCESS LAYER

After the traffic is scanned for the DDoS attacks, the remaining traffic of authenticated, legitimate Cloud service users is allowed to access the third tier for accessing the application by using the hardened access server as illustrated in Figure 6.8 below.

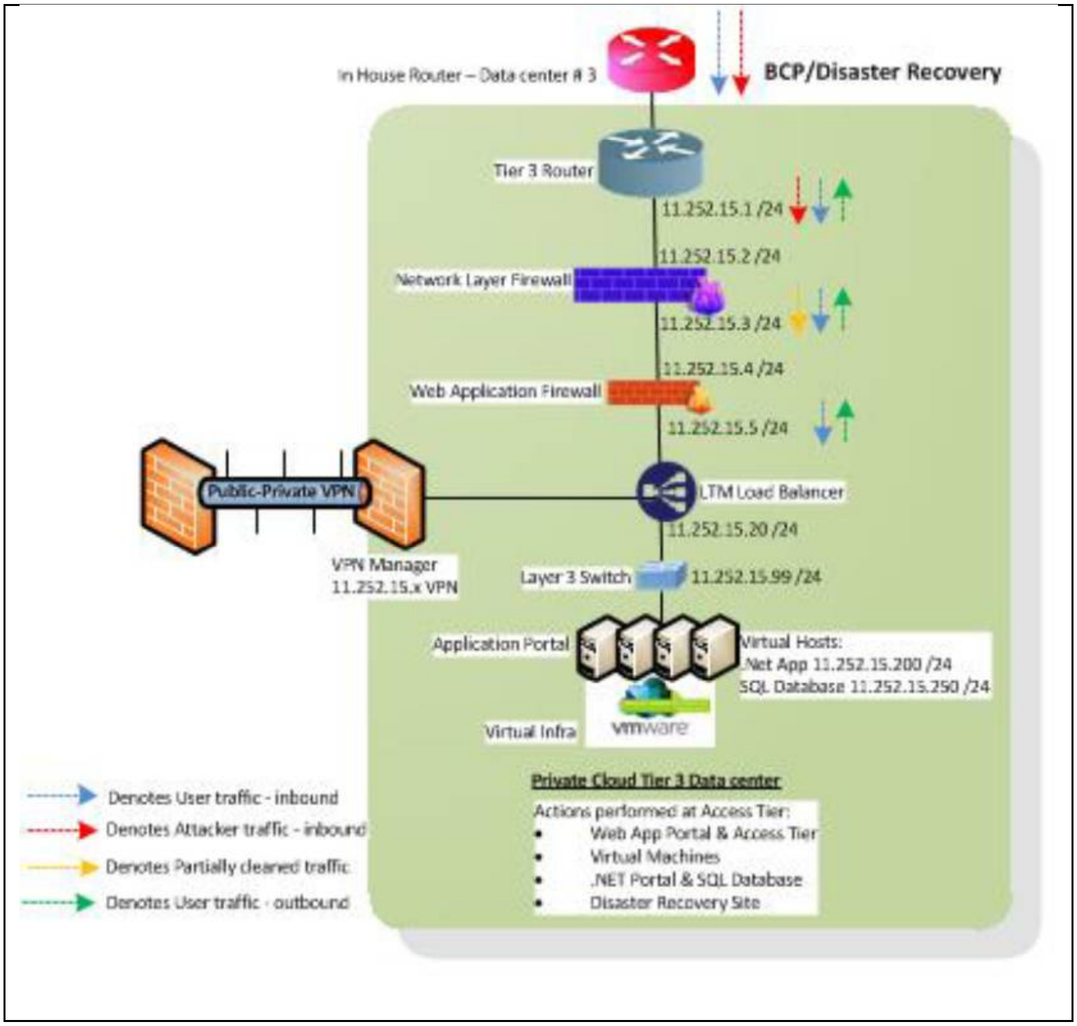


Figure 6.8: Three Tier Architecture – Access Tier

After dropping DDoS attack sessions and cleaning the traffic from network and application attackers, the remaining traffic is allowed to access the Cloud application (11.252.15.251). This is hosted in the access tier and has the Web portal application (11.252.15.252) and Database (11.252.15.250).

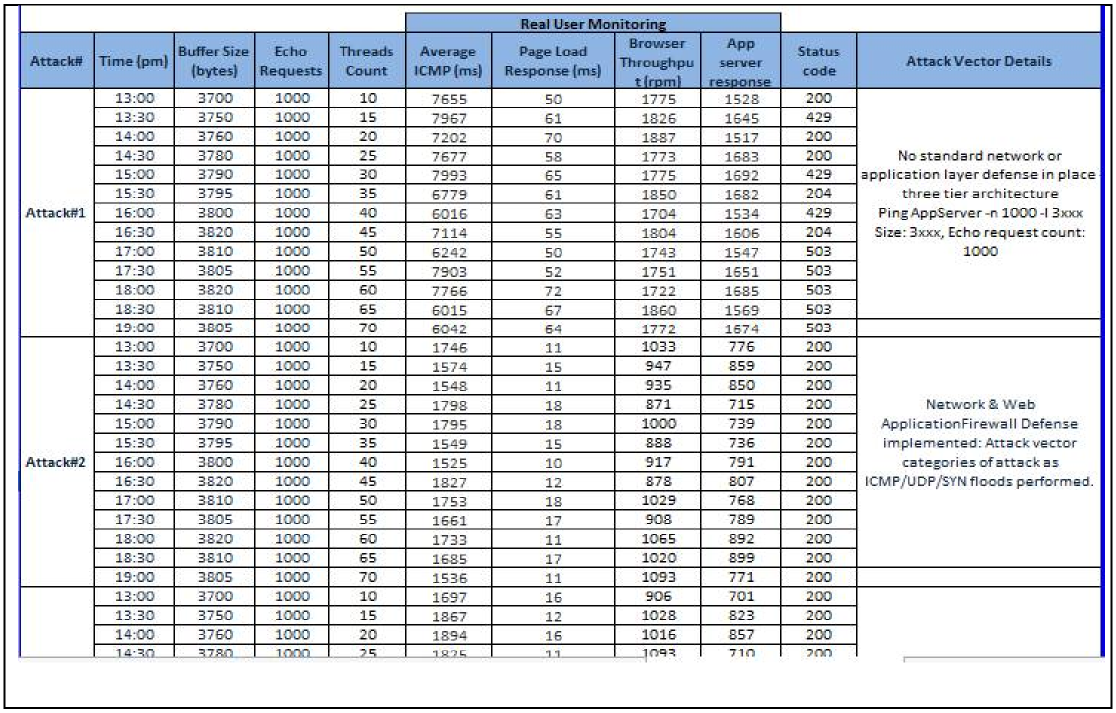
Devices and Servers implemented at Access layer tier are presented in Table 6.5 below.

Hardware for Access Tier Infrastructure	Router → Cisco 3600: *11.252.15.1* Network Firewall → Cisco ASA: *11.252.15.2* Web Application Firewall → Imperva WAF: *11.252.15.4* Load Balancer → F5 Big IP 4200v LTM: *11.252.15.20*

	Switch → Cisco 3550: *11.252.15.99* IPSec VPN → Cisco ASA: *11.252.15.110* Servers → Dell Server 64-bit i5 quad core, 16 GB RAM, 2 x 500GB SCSI
Software Infrastructure	Remote Access Server → Windows 2008 Jump Box: *10.253.16.200* Bare Metal Servers → VMware Workstation version 10: *11.252.15.200* Windows OS → Server 2008: *11.252.15.251* Web Application → SaaS Portal, .NET over IIS: *11.252.15.252* Database → SQL 2008 Database: *11.252.15.250*

Table 6.5: Requirements for Access Tier Infrastructure

DDoS attacks are performed on the designed three tier architectures for Network and Application layers and the results are collected for before and after attack, these are displayed in Figure 6.9 below.



					Real User Monitoring					
Attack#	Time (pm)	Buffer Size (bytes)	Echo Requests	Threads Count	Average ICMP (ms)	Page Load Response (ms)	Browser Throughput (rpm)	App server response	Status code	Attack Vector Details
Attack#1	13:00	3700	1000	10	7655	50	1775	1528	200	No standard network or application layer defense in place three tier architecture Ping AppServer -n 1000 -l 3xxx Size: 3xxx, Echo request count: 1000
	13:30	3750	1000	15	7967	61	1826	1645	429	
	14:00	3760	1000	20	7202	70	1887	1517	200	
	14:30	3780	1000	25	7677	58	1773	1683	200	
	15:00	3790	1000	30	7993	65	1775	1692	429	
	15:30	3795	1000	35	6779	61	1850	1682	204	
	16:00	3800	1000	40	6016	63	1704	1534	429	
	16:30	3820	1000	45	7114	55	1804	1606	204	
	17:00	3810	1000	50	6242	50	1743	1547	503	
	17:30	3805	1000	55	7903	52	1751	1651	503	
	18:00	3820	1000	60	7766	72	1722	1685	503	
	18:30	3810	1000	65	6015	67	1860	1569	503	
	19:00	3805	1000	70	6042	64	1772	1674	503	
Attack#2	13:00	3700	1000	10	1746	11	1033	776	200	Network & Web ApplicationFirewall Defense implemented: Attack vector categories of attack as ICMP/UDP/SYN floods performed.
	13:30	3750	1000	15	1574	15	947	859	200	
	14:00	3760	1000	20	1548	11	935	850	200	
	14:30	3780	1000	25	1798	18	871	715	200	
	15:00	3790	1000	30	1795	18	1000	739	200	
	15:30	3795	1000	35	1549	15	888	736	200	
	16:00	3800	1000	40	1525	10	917	791	200	
	16:30	3820	1000	45	1827	12	878	807	200	
	17:00	3810	1000	50	1753	18	1029	768	200	
	17:30	3805	1000	55	1661	17	908	789	200	
	18:00	3820	1000	60	1733	11	1065	892	200	
	18:30	3810	1000	65	1685	17	1020	899	200	
	19:00	3805	1000	70	1536	11	1093	771	200	
	13:00	3700	1000	10	1697	16	906	701	200	
	13:30	3750	1000	15	1867	12	1028	823	200	
	14:00	3760	1000	20	1894	16	1016	857	200	
	14:30	3780	1000	25	1825	11	1093	710	200	

Figure 6.9: Three Tier Network Architecture Attack Logs

Access to the Cloud application is allowed using a hardened Windows 2008 Server (10.253.16.200), running only remote access services with a web browser application for the user profile. The end user authenticates on this jump box with a two factor authentication (User Id/Password plus an OTP sent on user mobile) and then allowed to access the Cloud application connected to the backend database. Once the user finishes accessing the application, the user traffic is routed from the second tier back to the user form the second tier router which is not the default route back to the user, but in form of asynchronous routing. This asynchronous routing helps break any remaining attack sequence seeking to return back from the first tier gateway.

From initial analysis of the logs, by splitting the defense tiers and segregating the traffic, the network and application layer attacks face limited exposure to the attack surface area and lesser opportunities to attack the targets. Hence, the number of HTTP(s) requests, Bytes received by network devices, Requests queued on Load Balancers, unhealthy instances all show reduced trend. This is due to the segregation of the defense layers.

CHAPTER SUMMARY

Corporate enterprises today are recognizing the advantages of the recommended multi-tiered Hybrid architecture. Enterprises valuing cyber security are re-architecting their security controls and the Hybrid DDoS Protection architecture could prove to provide flexibility and manageability required to combat the modern DDoS multi vector threats. By providing increased layers of network and web application security in form of separate tiers, it is possible to protect the integrity, availability and performance of critical web applications, resulting in improved brand and customer confidence and reduced business risk from under-provisioning security devices.

For further research the author proposes Rate controls, built-in intelligent WAFs, client reputational monitoring and advanced Cloud security approaches should be used in combination as part of a comprehensive defense against the various types and sizes of cyber threats.