Application Delivery in Data Centers: Middleboxes

ABSTRACT

Application delivery controller is a computer network device in a data center which is a part of an application delivery network which perform some common tasks. Basically what it does is managing and optimizing how client machines connect to web and enterprise application servers. It does the load balancing between servers so it accelerate the applications.

Contents

CHAPTER I

1) INTRODUCTION

1.1) What is a data center?

Data centers are the facilities which provides the data storing and distributing mechanisms, on the internet. In another way it's a huge group of networked computer servers which are used by organizations (i.e. Google, Microsoft, and NSA) for the remote storage, processing, or distribution of large amounts of data. Inside data centers a huge amount of traffic can be generated. In fact the highst amount of traffic is generated inside the data centers.

1.2) What is application Delivery?

Application delivery is the process of using the suitable technologies to ensure that application content and functionality are efficiently and reliably accessible by a large number of clients or users. An application can be anything like shopping cart in a web site like EBay, a banking application etc. These application must provide the service to millions of people. So it should me fast, safe and reliable in order to satisfy the customer requirements.

1.3) Application Delivery Controller (ADC) in Data Centers

Whether you need to expand an application from one server to more servers or to deliver an applications to millions of people in the world you'll need an Application Delivery Controller. It provides the services like scalability, availability and reliability and it has some more advanced features for present day dynamic, content-rich applications such as hardware based secure traffic acceleration, virtual environment integration and HTTP compression.

Application Delivery Controller is a device in a data center which placed between the firewall and one or more application servers. It's an area known as the DMZ (demilitarized zone). The task of the first generation application delivery controller is basically the application acceleration and load balancing between servers. As the technology develops the new ADC has some newer functions like secure Sockets Layer offloading, rate shaping or firewalls for web applications.

Instead of the features mentioned above application delivery controllers can provide services like maintain the availability, speed, and security of Internet based applications. Also some advanced application delivery controllers have the services need for critical data centers such as application acceleration, application health-checks, SSL offload, DNS application firewalls, DDoS protection and layer 4-7 load balancing.

CHAPTER II

2) TECHNIQUES USED IN DATA CENTERS

2.1) Firewall Load Balancing

Firewall load balancing distributes the traffic across multiple firewalls which provides fault tolerance. Also it increases the throughput. This mechanism can protect the network by

- Dividing the load between the firewalls, which eliminates a single point of failure and allows the network to scale.
- Increasing high availability

A hash value of each new traffic flow will be calculated to perform Firewall load balancing which is called "route lookup". Firewall load balancing can identify a firewall failure by monitoring probe activity.

Firewall Load Balancing Methods

- Least Connections
- Round Robin
- Least Packets
- Least Bandwidth
- Source IP Hash
- Destination IP Hash
- Source IP Destination IP Hash
- Source IP Source Port hash
- Least Response Time Method (LRTM)
- Custom Load

2.2) Reverse Proxy Load Balancing

A reverse proxy accepts a request from a client and forwards it to s server to get the work done and sends the result back to the client.

A load balancer distributes incoming client requests among a group of servers, in each case returning the response from the selected server to the appropriate client. There are two main benefits of reverse proxy.

1) Increased scalability and flexibility – Here only the reverse proxy IP address is visible to the clients, so the administrators are free to change their backend as they need.
2) Increased security - Backend server will not be exposed to outside world. So no one can access tem directly. Many of the reverser proxy servers protect the backend servers from Distributed Denial of Service attacks.

In Reverse Proxy Load Balancing

- Proxies used for security, caching, application acceleration
- Proxies are usually used for outgoing requests

- Reverse proxies are used for incoming requests
- Usually transparent mode is used
- Load balancing using predictors such as hashing or round robin

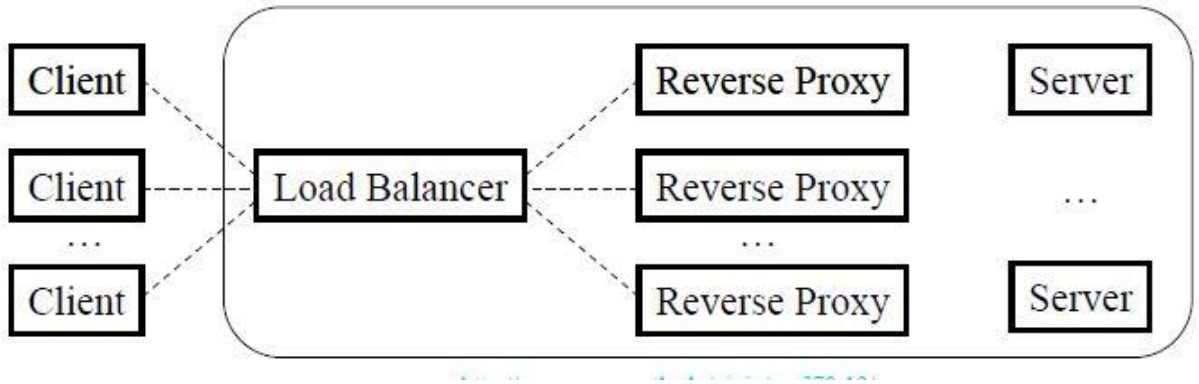

Figure 1.1

2.3) Different Types of NAT

2.3.1) NAT64 and NAT46

There are two different forms of NAT64,

- Stateless
- Statefull.

The stateless version maps the IPv4 address into an IPv6 prefix. This doesn't keep the state.

Stateless	State full
1:1 Translation	1:N Translation
No conservation of V4 address	Conservation of V4 address
No state or bindings is kept	No state or bindings is kept on every single unique translation
End to end transparent	Due to overloading. No end to end transparent
Needs IPv4 translatable IPv6 address	Not needed any special requirements

Table 1.1

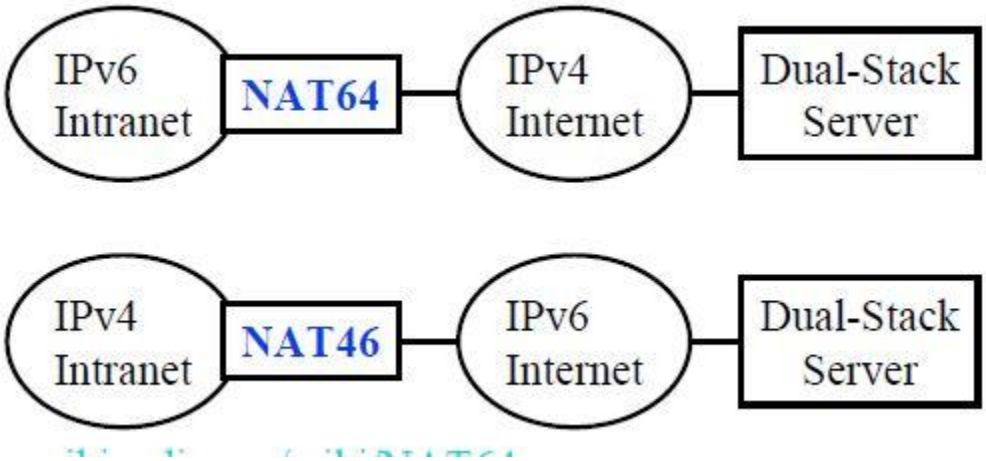

Figure 1.2

2.3.2) Carrier Grade NAT (CGN)

It's a large-scale NAT that translates private IPv4 addresses into public IPv4 addresses. It uses Network Address and Port Translation methods to combine multiple private IPv4 addresses into lesser public IPv4 addresses. This method can be used to reduce the IPv4 address exhaustion.

Earlier it was used some simple round robin and least connections algorithms as load balancing algorithms. But present it uses far more complicated and advanced algorithms in ADC.

2.3.3) Dual NAT

It's also knows as One Arm Mode.

Like in regular NAT load balancer changes the source address and destination address and destination port numbers according to the client request. Server sends the response to the load balancer, so the load balancer uses the port number to clarify the address of the client to forward it to the clients.

Both the Server and Client can be on the same subnet and Serves will not see the real client addresses

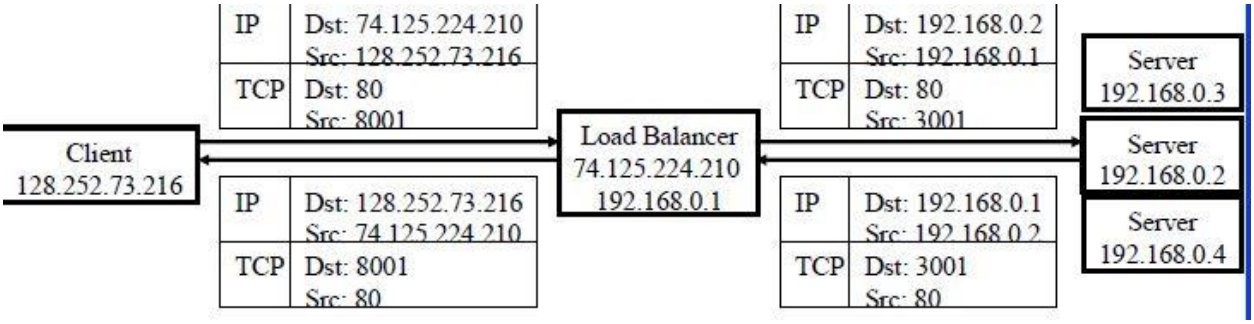

Figure 1.3

2.3.4) Server NAT

It's also known as the "Routed Mode".

Without a change in the port numbers, on client requests, Load balancer will change the destination IP addresses. Server will send the response directly to the client. Load balancer will change the IP addresses on the responses and all the server responses will have to go through the Load Balancer. This can be applied if only the both client and server are on different subnets. His is good for security because the servers can see the real addresses of the clients.

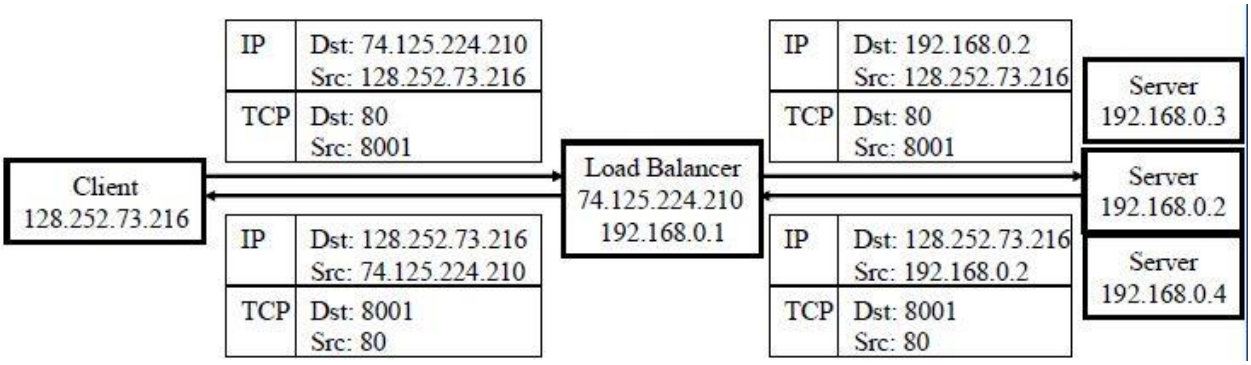

Figure 1.4

2.4) SSL Offloading

Secure socket layer (SSL) certificates provide authentication between a server and a client computer in a Web application. Secure Socket Layer (SSL) and Transport Layer Security (TLS) are used for secure connections.

Example: https

2.5) TCP multiplexing ADC

3-way handshake is used by TCP, “ack” for segments, “sliding window mechanism” flow control, congestion control, and termination for each connection.

An ADC can be used to reduce the number of TCP connections and also it can reduce the total latency because LB to server connection runs at high window levels.

This improves performance, improves capacity of servers, and makes consolidation easier.

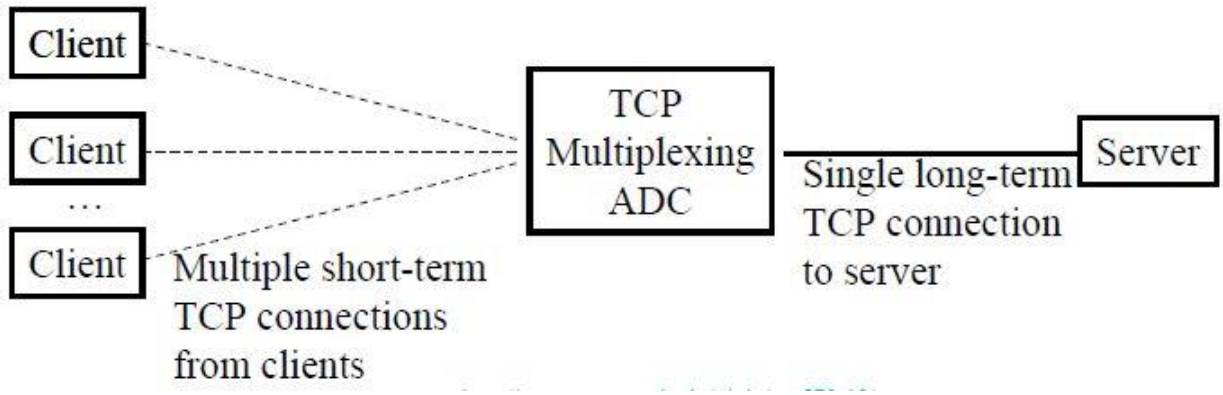

Figure 1.5

2.6) HTTP Compression

Before the content is transferred to the client that content is compressed. For some kind of resources like text, applying this method can significantly reduce the size of the response message which results in less bandwidth requirements and download times.

But some content type like zip files which are already compressed and may not respond to compression again. So trying to compress those kind of content may result in increasing the size of the response message and waste of time.

Compression is useful when secure SSL connections are used as it decreases the amount of content that has to be encrypted on the server and decrypted by the client.

- Most http responses are compressed to reduce the usage of the bandwidth.
- A load balancer can provide this feature

2.7) Virtual ADCs

ADC is typically located in a data center. As the technology develops it's all becoming virtual, also companies trying to virtualize the physical stuff to reduce the cost. It's been considered to replace physical ADC's to virtual ADC's but it hasn't worked well because it hasn't provided any new solution or real benefits except getting rid of hardware. But virtual ADCs can help reduce costs, the savings may not be worth the sacrifice in functionality.

There can be two type of virtual ADC's

- Hardware based- A single physical ADC have multiple virtual context with it, where each of the separate virtual device can be used by different applications.
- Software based – It runs of standard processors

3) CHAPTER 3

3.1) MIDDLEBOX

A 'Middlebox' also known as network appliance is a computer networking device which manipulates traffic for purposes other than packet forwarding. An example for middlebox is firewall which filter the unwanted or malicious traffic. Dedicated middlebox hardware is very frequently used in enterprise networks to ensure security and increase performance.

Security benefits:

- Firewalls
- Application Firewalls
- Intrusion Detections System (IDS)
- Intrusion Prevention System (IDS)

Performance Benefits:

- Proxy/Caches
- WAN Optimizers
- Protocol Accelerators

Key differences between middleboxes and routers:

Middleboxes are often statefull. It can remember great amount of data that is updated as frequently as every packet or every connection. Middleboxes perform very complex and varied operation on the packets.

CHAPTER IV

1) REFERENCE

2) https://en.wikipedia.org/wiki/Application_delivery_network
3) http://searchnetworking.techtarget.com/definition/Application-delivery-controller
4) A Ten Minute Introduction to Middleboxes | Justine Sherry, UC Berkeley