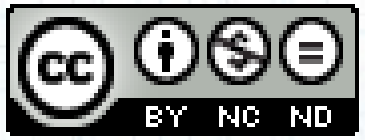
Netscaler and Networking in CloudStack

Deepak Garg
Citrix R&D, Bengaluru

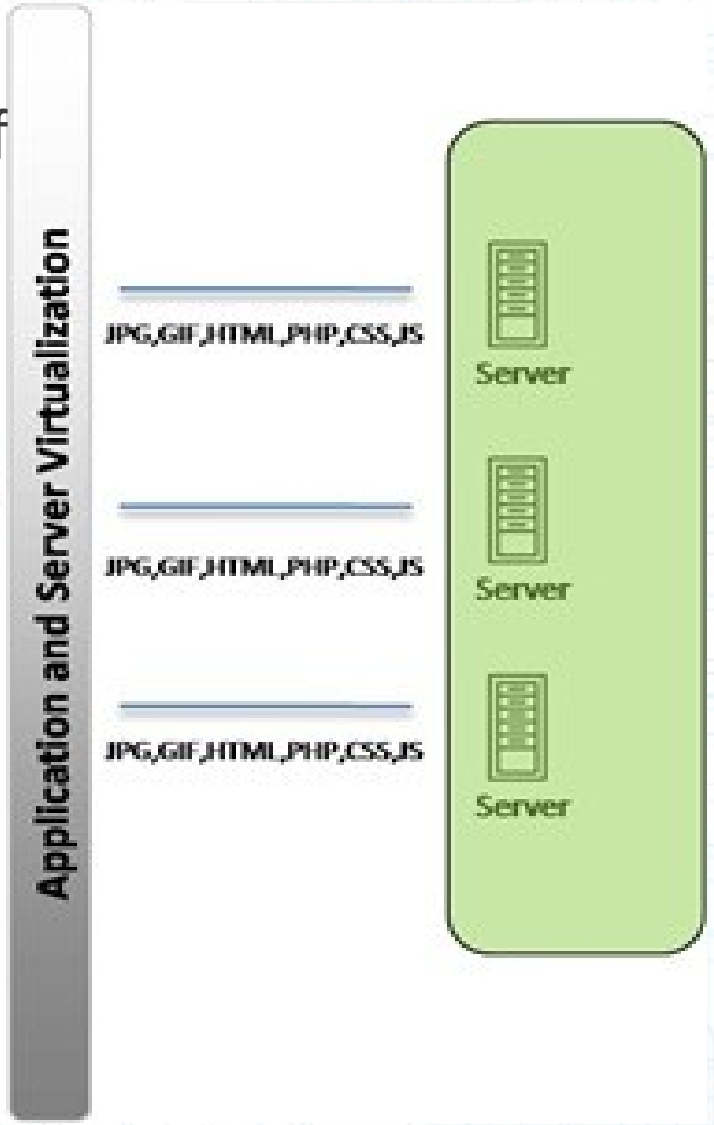


Contents

- LB
- App Delivery Controllers
- Netscaler ?
- Netscaler Features
- NS and HTTP
- NS IPs
- Operational Modes – VServer, Transparent mode
- NS Monitors
- LB Algos
- CloudStack – Networking Offering
- CloudStack – Advanced Networking
- HAProxy – LB with Virtual Router
- SSL-Offloading with Netscaler

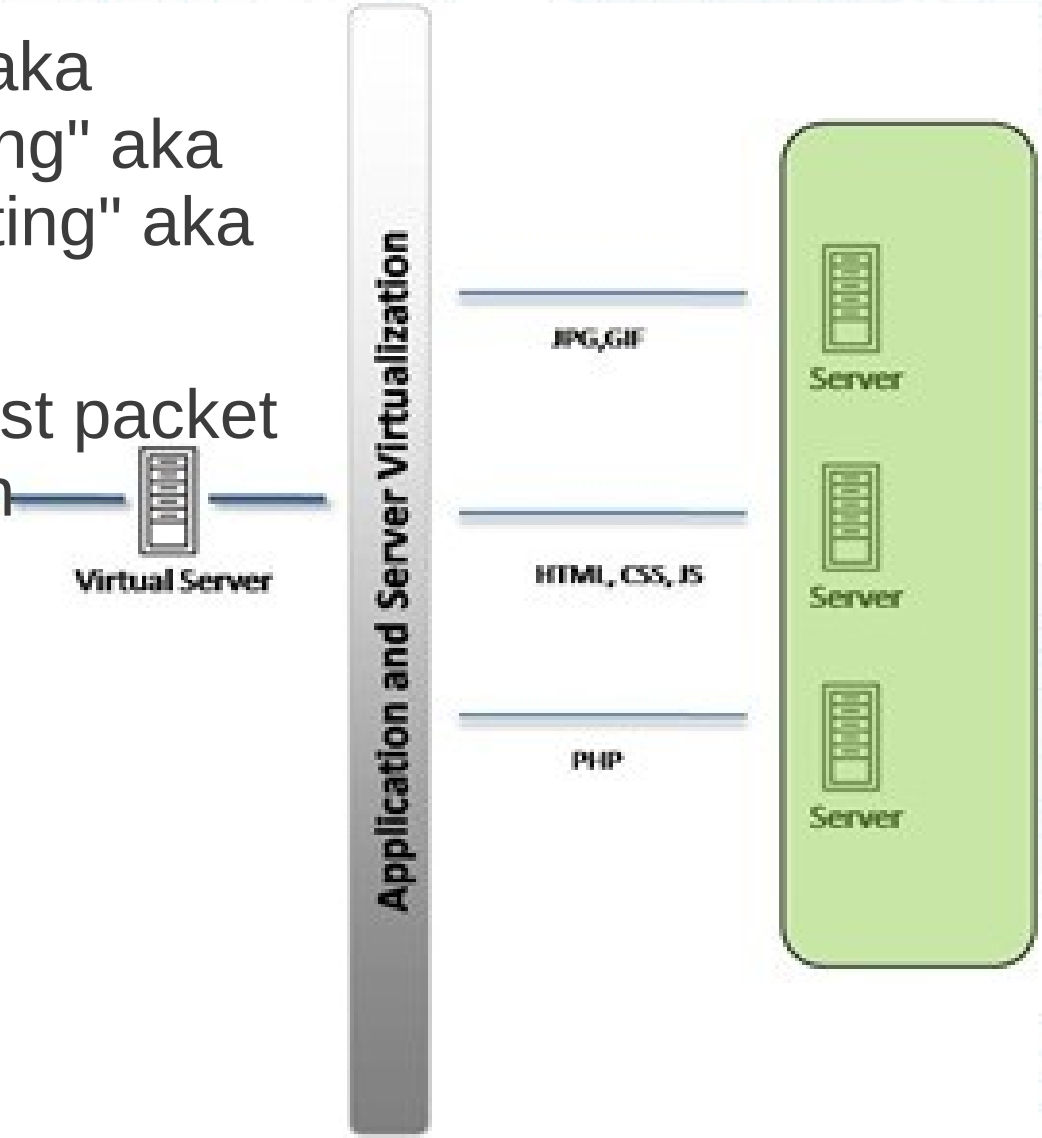
LB

- balancing load (application requests) across a number of servers based on a **load-balancing** algo
- Algos:
  - Round-robin
  - weighted round-robin
  - least connections
  - weighted least connections
- Needs **exactly** same content across all servers



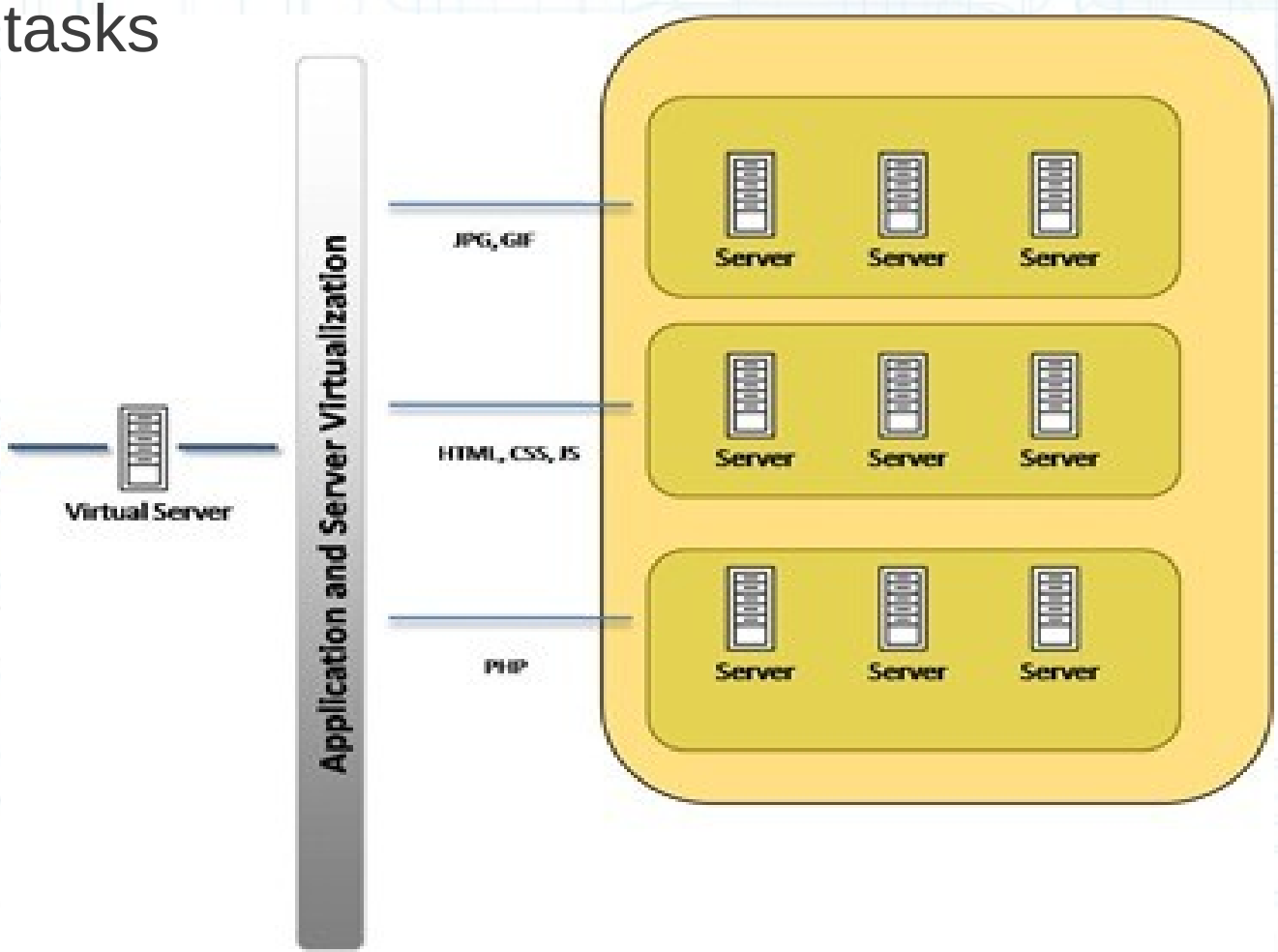
App Delivery Controllers

- Layer 7 switching aka "application switching" aka "content based routing" aka "request switching"
- Look into the request packet and takes decission



App Delivery Controllers

- The backend server content may not be the same
- Each fleet of servers may be specialized for particular tasks



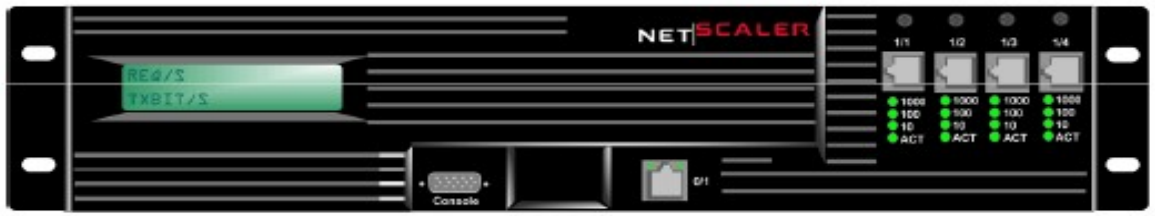
Netscaler

- L4 – L7 Switch => application aware switch
- Patented Request Switching™ technology
  - **Terminates client connections and then establishes proxy connections,** or reuses existing connections with the servers
  - Talks HTTP, SSL, FTP, TCP, UDP, RDP etc...
  - Application Switching
  - Application Acceleration / Optimization
  - Application Security / Access
  - Enhanced application security beyond perimeter defenses

NetScaler

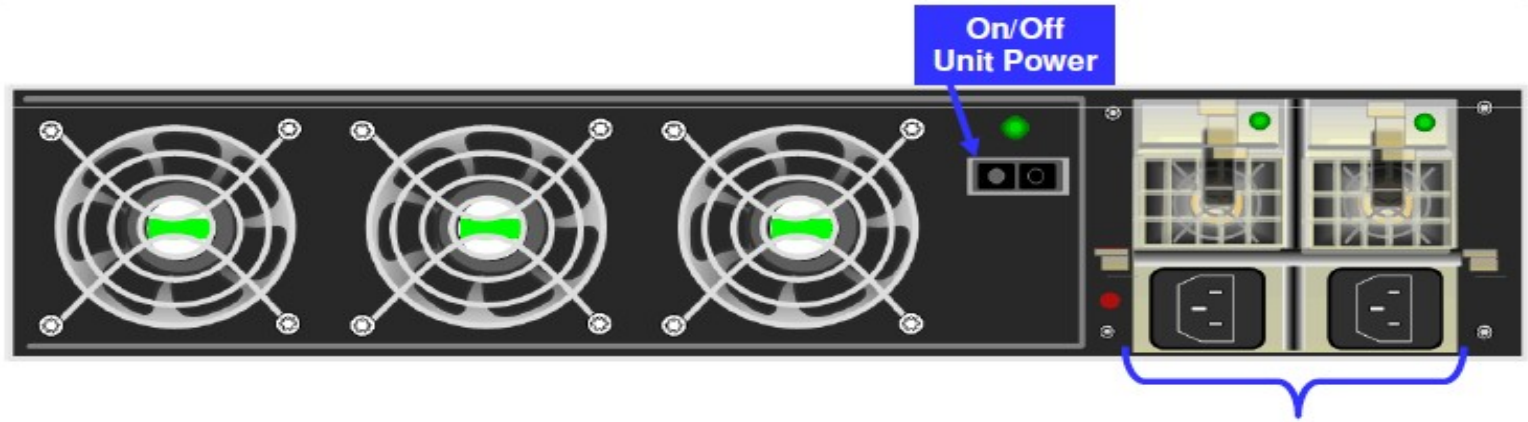
- Ships as MPX, SDX and VPX

2U RS9800-SX/ RS9800-T



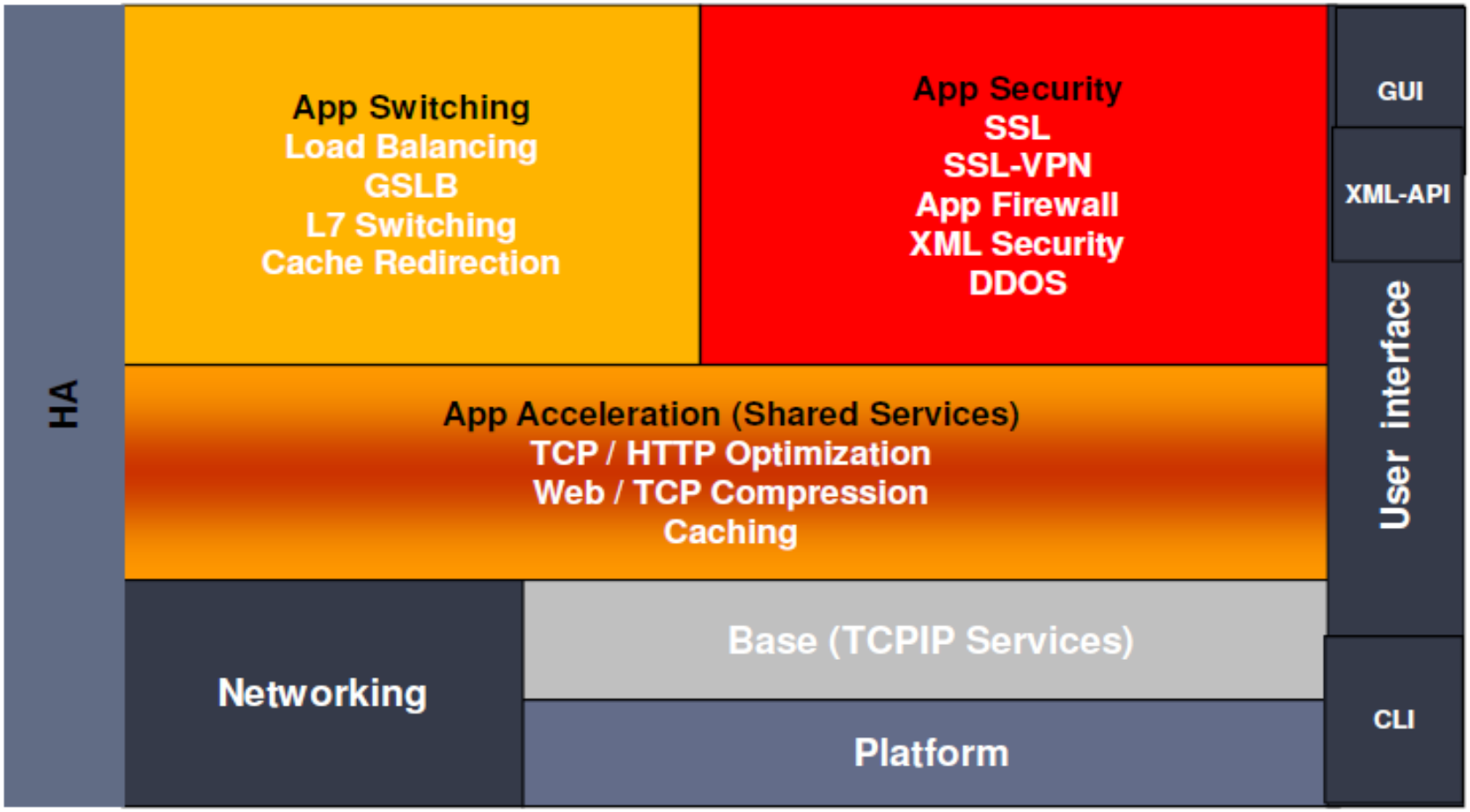
- 5 Gbps ports 1/1, 1/2, 1/3, 1/4, 0/1
  - 5 CU 10/100/1000 data ports or
  - 1 CU + 4 1000 Fiber data ports

Standard on all Citrix NetScaler RS9000 products



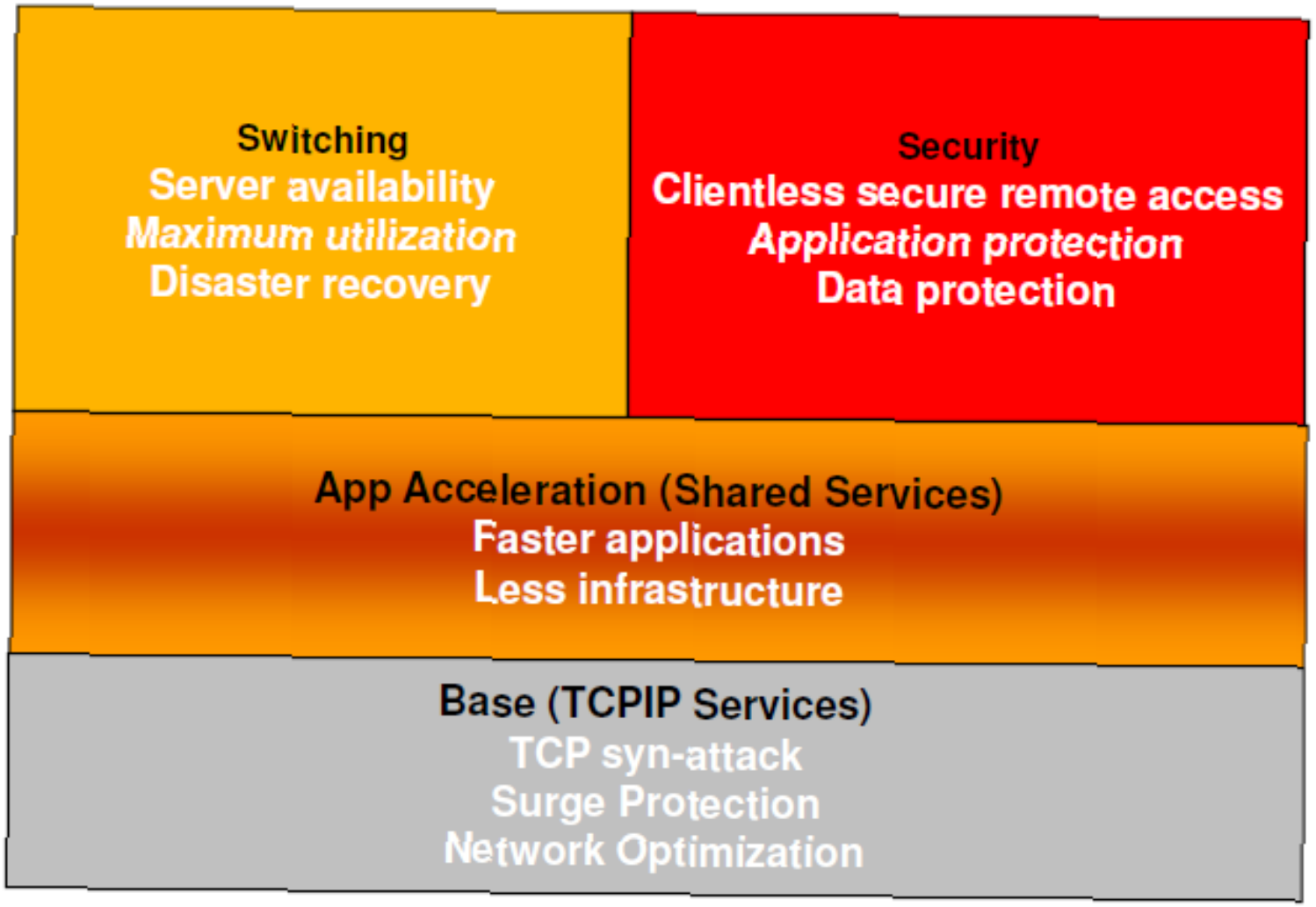
NS Features

Application Delivery Feature/Functions



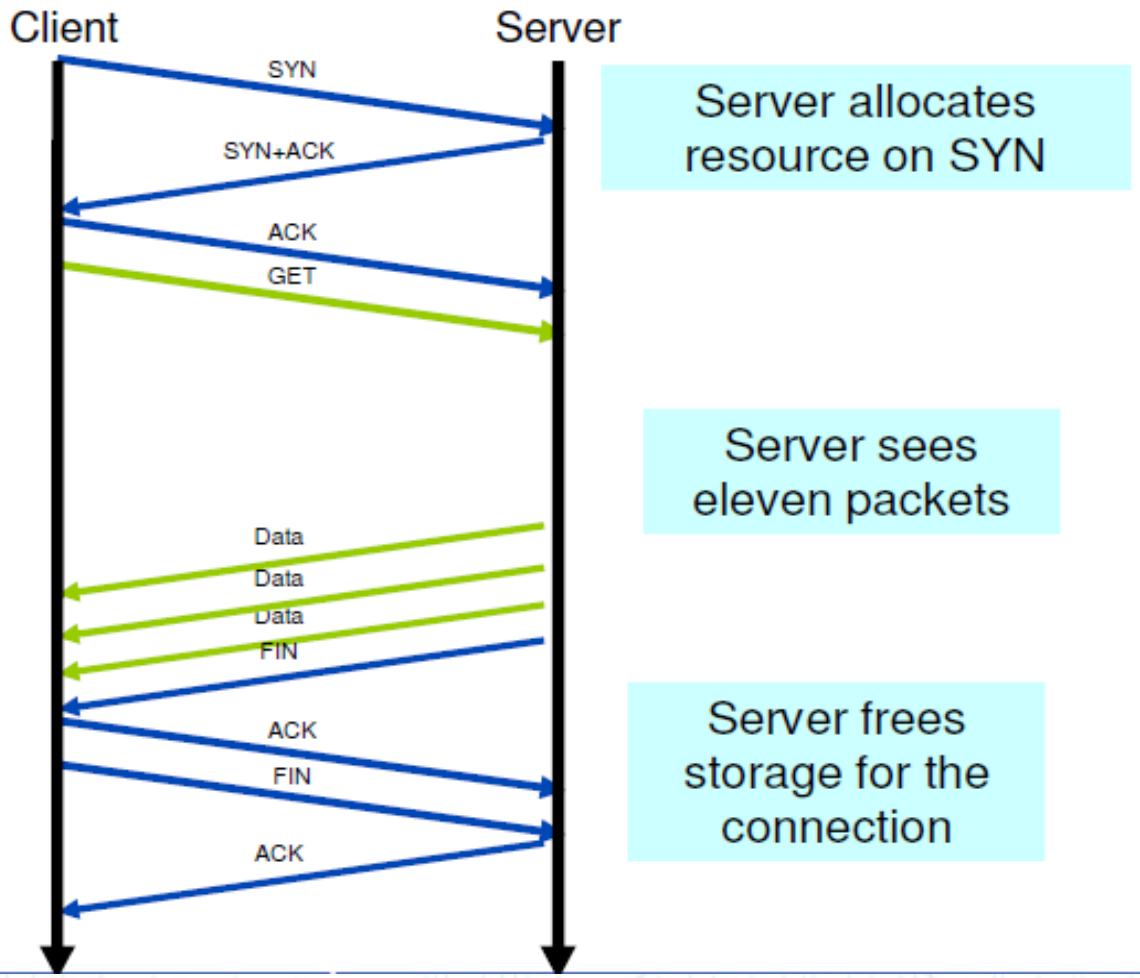
NS Features

Application Delivery Benefits



NS and HTTP

HTTP Transaction Without NetScaler



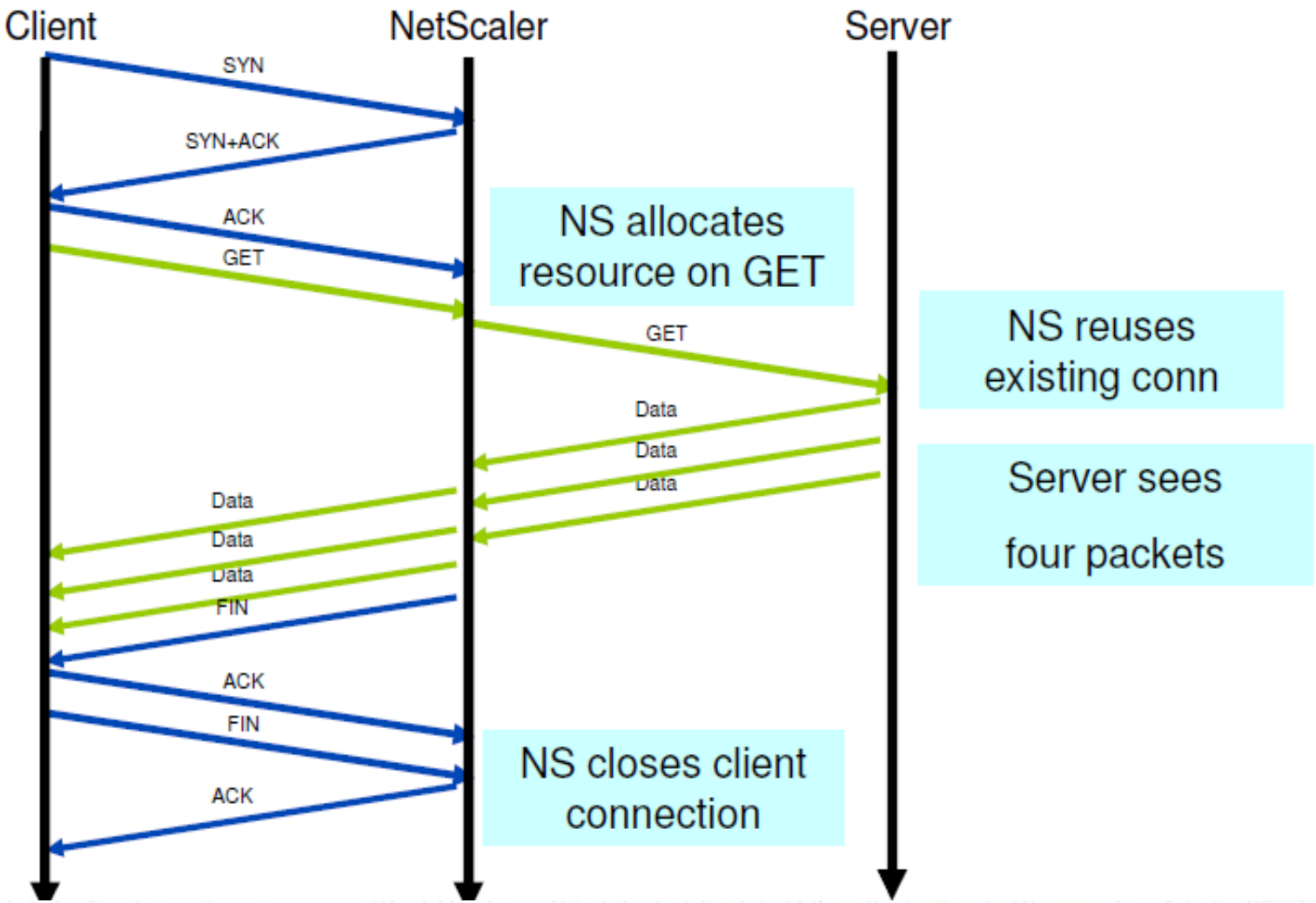
Server allocates resource on SYN

Server sees eleven packets

Server frees storage for the connection

NS and HTTP

HTTP Transaction With NetScaler



Connection Multiplexing

- Multiple clients use single connection to server - Sequentially, not simultaneously!
- Benefits:
  - Optimal reuse of each server connection
    - Slowstart vs. Fast Ramp
  - Optimal use of each client connection
    - HTTP/1.1
    - Client Keep-Alive
- Requires TCP connection manipulation
  - Connection Proxy
  - Connection Termination

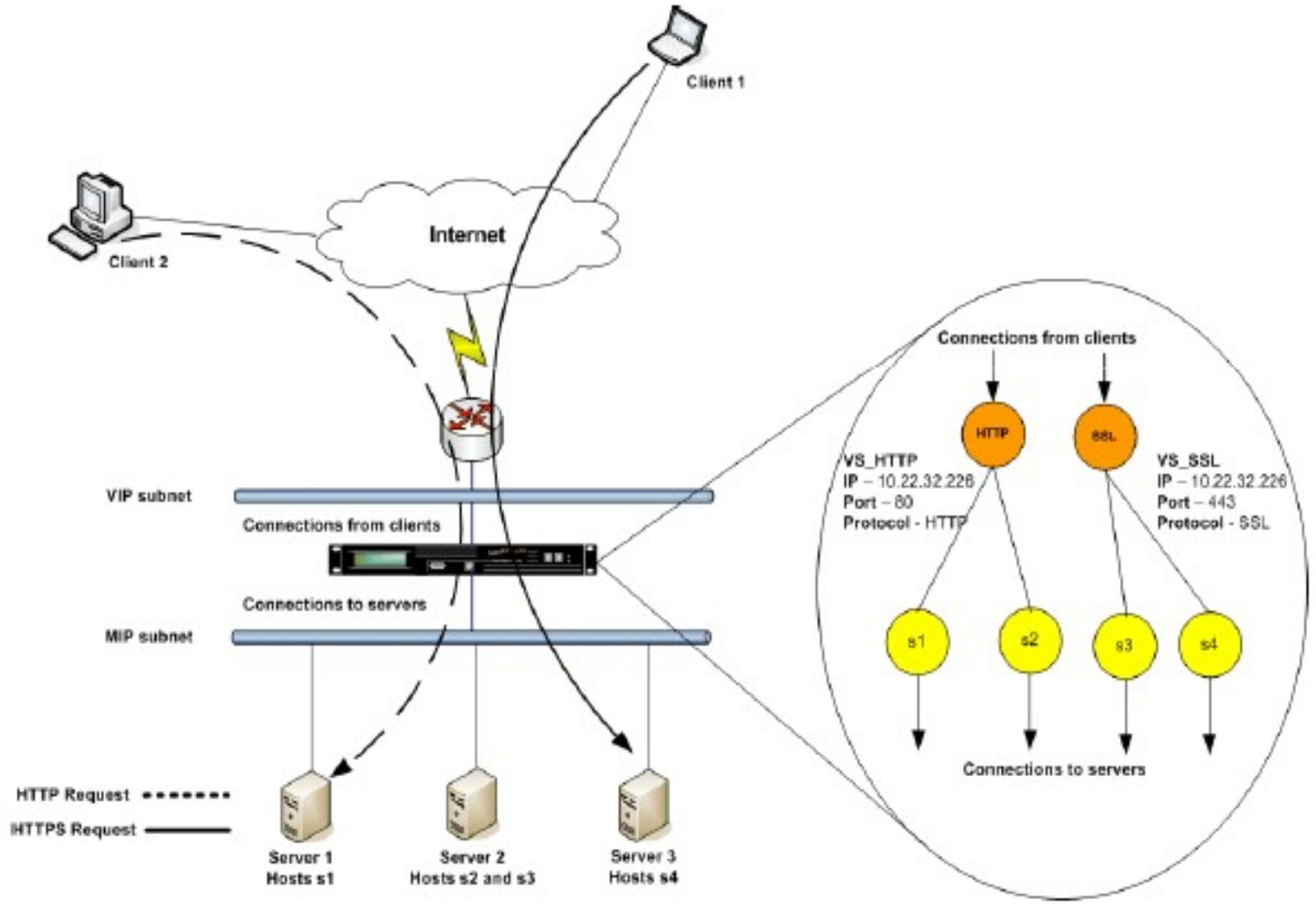
NetScaler Owned IPs

- NSIP = NetScaler IP
  - Unique management IP for the NetScaler system.
- MIP = Mapped IP(s)
  - Default set of addresses to communicate with back end servers.
- SNIP = Subnet IP
  - IP for communication to servers/clients in other subnets/vlans
- VIPs = Virtual IPs
  - Normal method for configuring explicit services

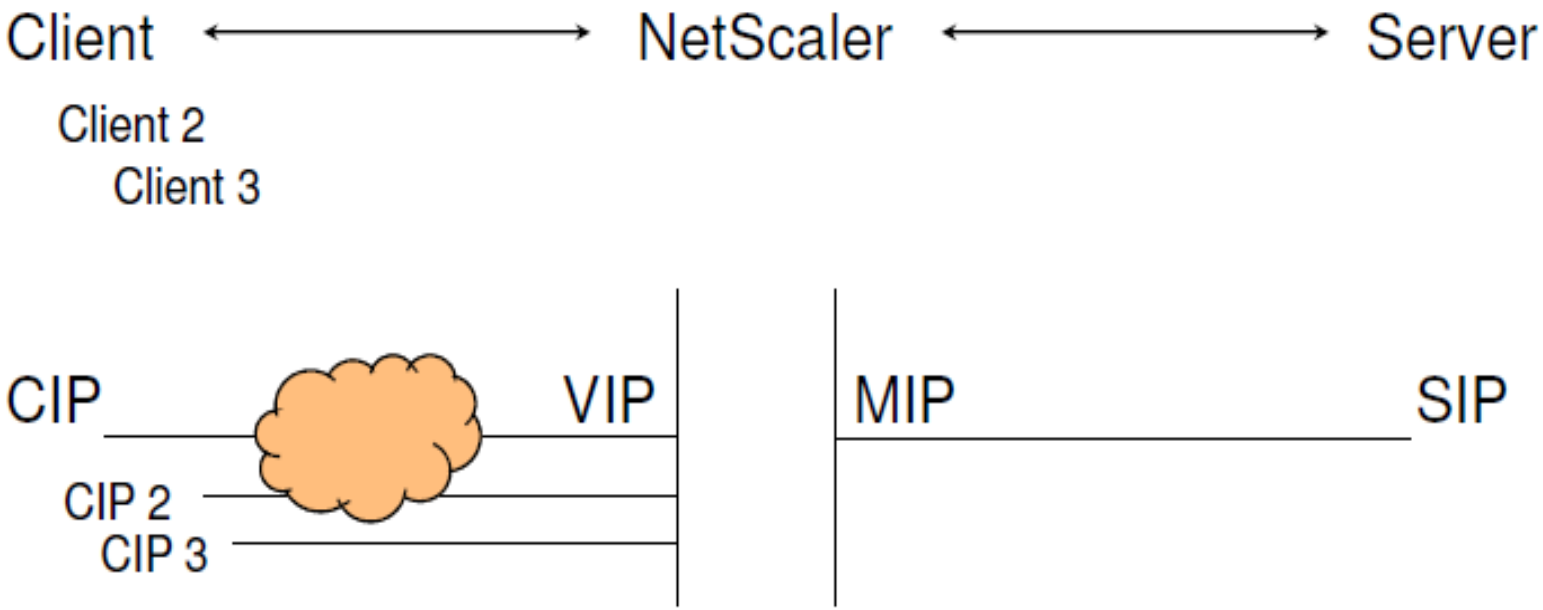
Operational Modes

- VServer proxy mode ~ Reverse Proxy
- Transparent mode ~ Forward Proxy

NS Virtual Entities



VServer (Proxy) Mode

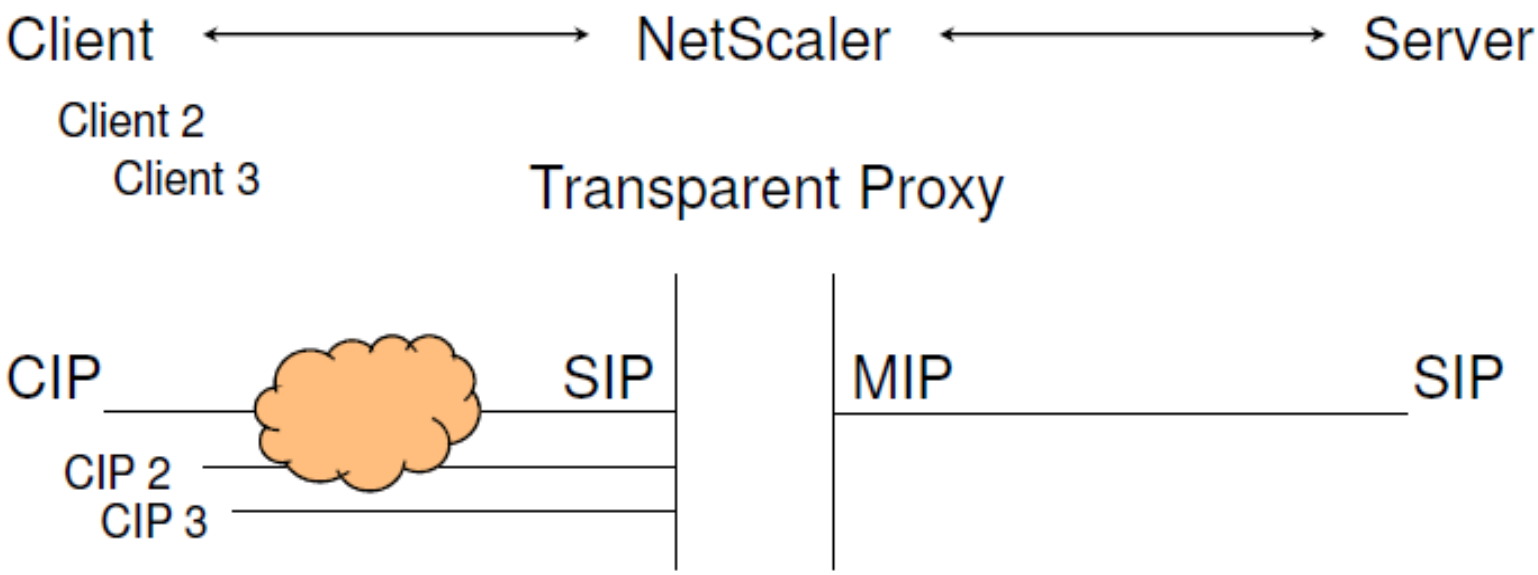


- Client and Server still maintain TCP state
- NetScaler translates IP, TCP port, sequence #

Vserver (Proxy) Mode ...

- A VIP represents a collection of servers to a client
  - For any given transaction the VIP is mapped into a single server IP
  - Usually clients don’t need to know the true server IP address
- A MIP represents a collection of clients to a server
  - For any given transaction the MIP is mapped into a single client IP
  - Usually servers don’t need to know the true client IP address
  - Options exist for those servers which do need to know
    - enable ns mode USIP

Transparent Mode



- Client and Server maintain TCP state
- NetScaler translates IP, TCP port, sequence #s

Transparent Mode ...

- Original NetScaler functionality
- Does not require extensive configuration
- Full Traffic Optimization and Traffic Security Feature Sets
  - IP address and port mapping
  - Attack prevention
  - Content Filtering
  - SSL offload
  - Compression
  - Caching
- SSL Offload and Compression require full connection termination
  - No additional configuration of TCP functionality required

NetScaler Monitors

- Monitor the backend servers
  - Simple ping
  - Tcp syn/ack
  - App aware monitor
    - If the web server delivers 404
    - If the db can execute the query
    - Take actions based on results
- Timeouts for the monitor
- If Monitor says 'No', bring down the server from the LB list
- Make a custom monitor !!

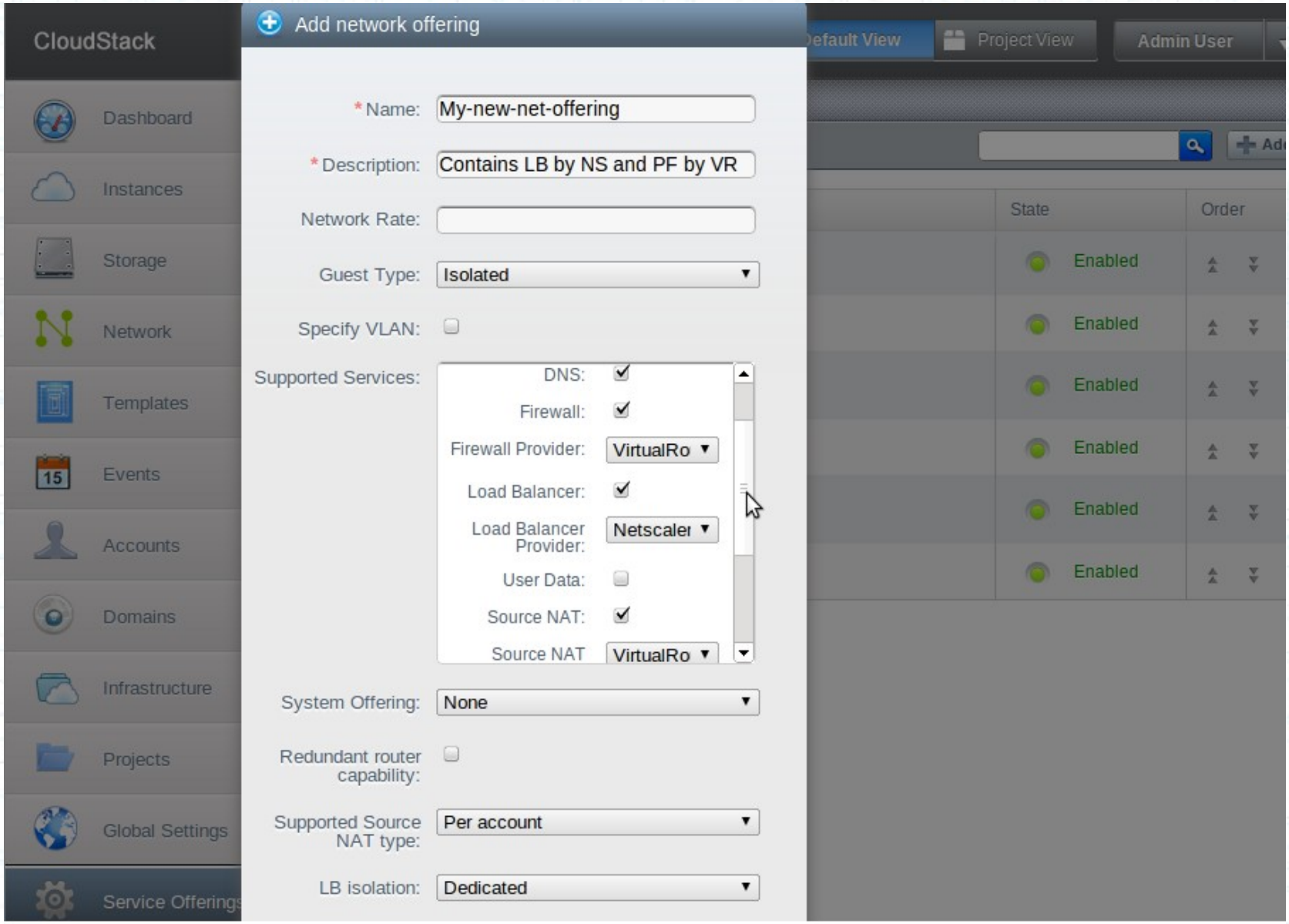
LB Algos

- Round Robin
- Least Connection (default)
  - Keeps connection pools
  - active connections opened to any backend server
- Least Response
  - Avg. Response time calculated real-time
  - Time to first byte
- Least BandWidth
- Token LB
- Etc. (source ip, URL hashing, domain hashing)

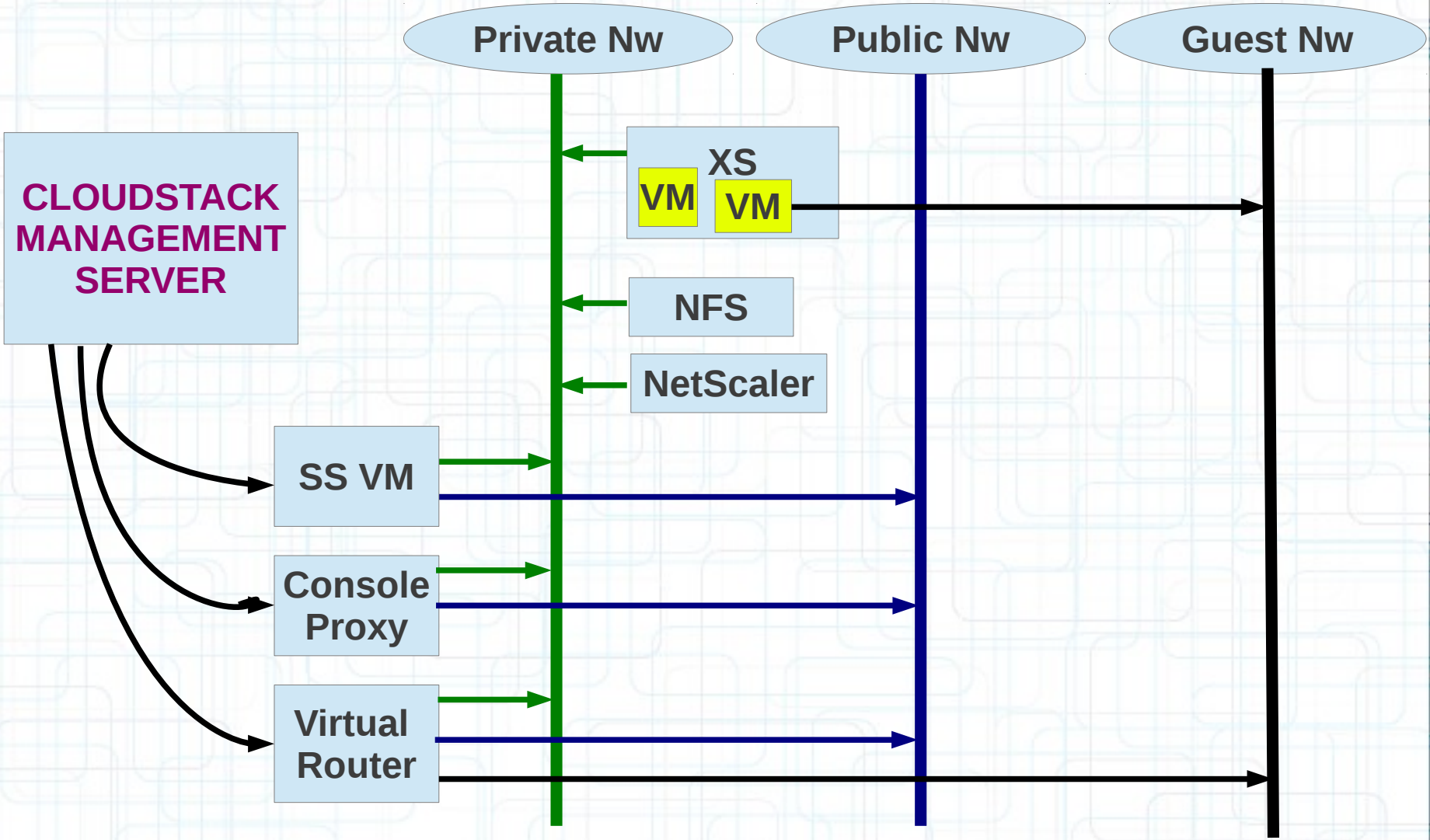
CloudStack Nw Services & Providers

Networking Mode	Network Services	Service Providers
Basic Networking	DHCP (only Virtual Router) NAT (only NetScaler) LB (only NetScaler)	Virtual Router Netscaler
Advanced Networking	DNS DHCP LB FireWall Port Forwarding NAT VPN	Virtual Router Netscaler F5 SRX

CloudStack Nw Offering

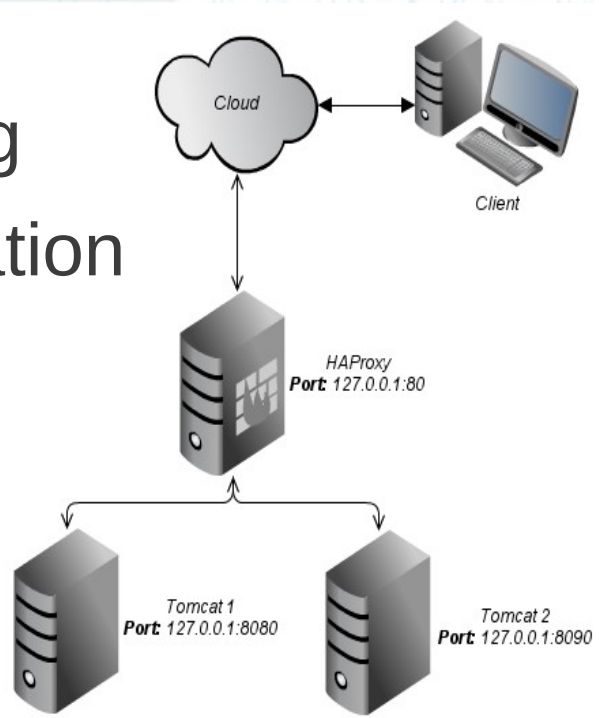


CloudStack – Advanced Nw



LB with Virtual Router

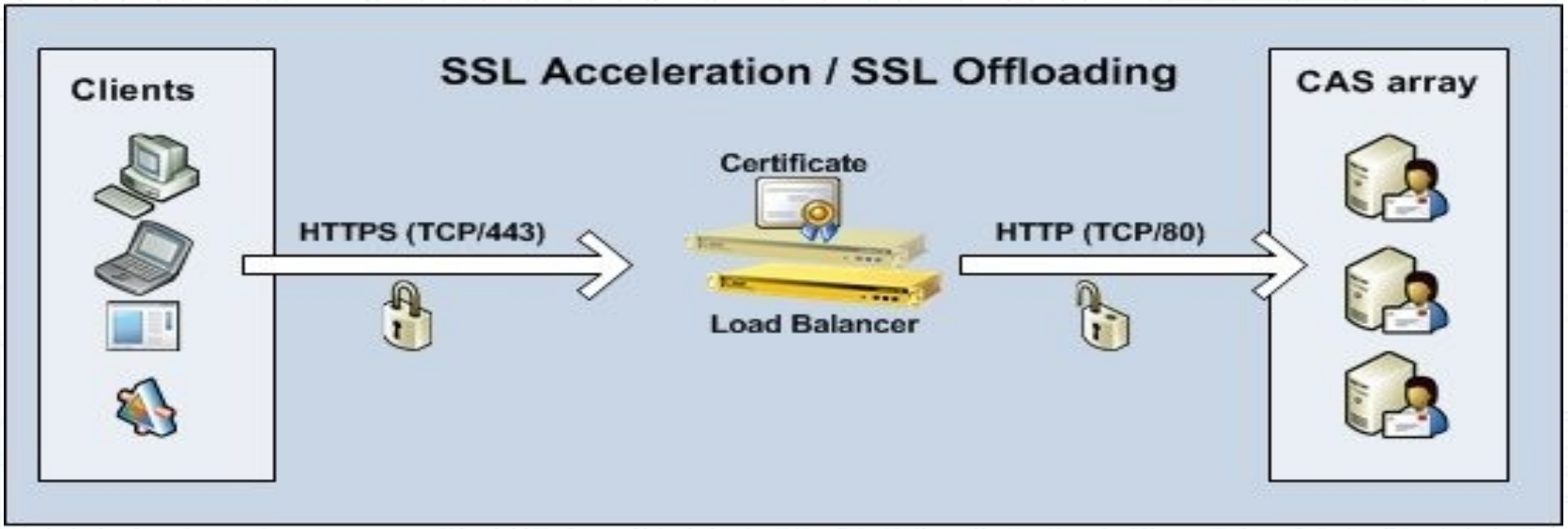
- HAProxy - High Availability Proxy
- Software LB
- Features
  - Talks TCP and HTTP
  - /etc/haproxy/haproxy.cfg
  - active/passive configuration



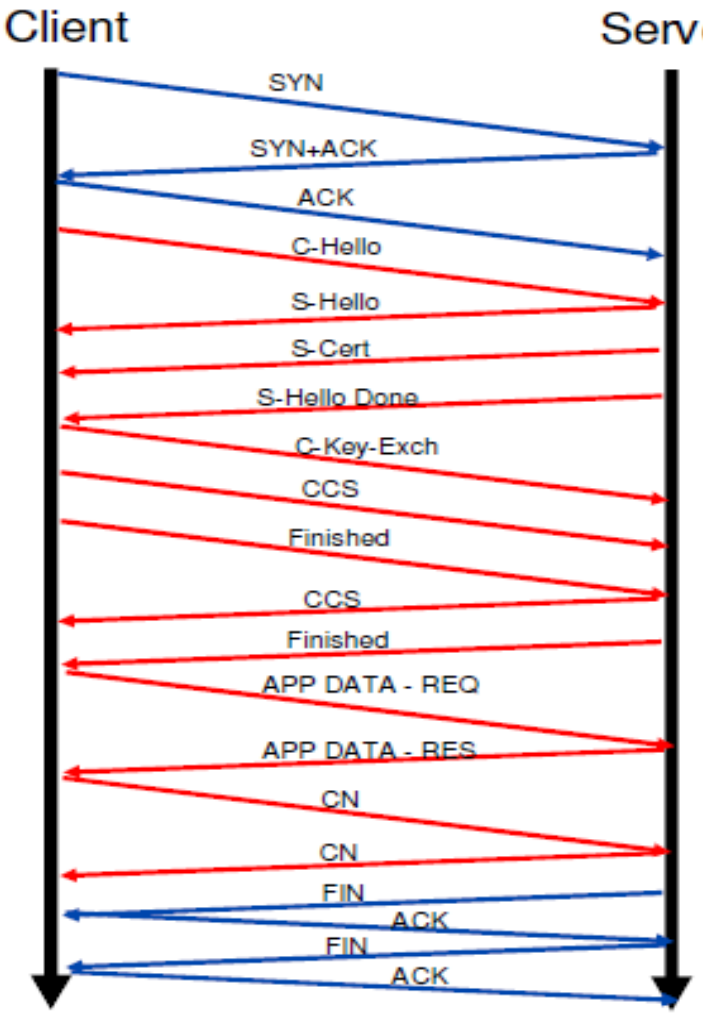
CloudStack – Netscaler Demo....

SSL-Offload with NetScaler

- Modes:
  - ssl-http
  - ssl-ssl
  - http-ssl (never used)



SSL Transaction Without NetScaler



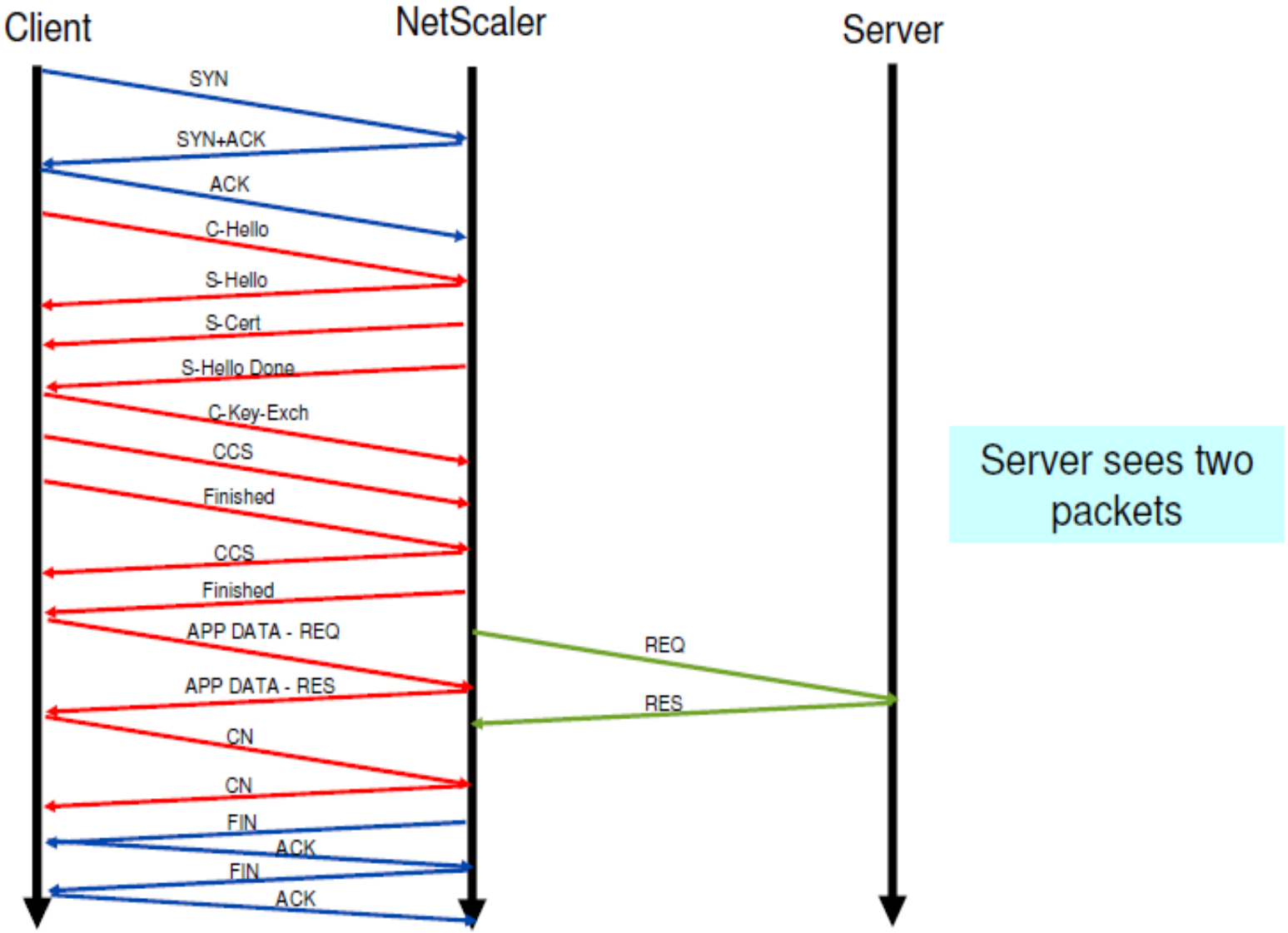
Server allocates storage for connection

Server sees twenty packets

Server does SSL handshake and enc/dec

Server frees storage for the connection

SSL Transaction With NetScaler



Server sees two packets

Thanks,

Deepak Garg

deepak.garg@citrix.com
deepakgarg.iitg@gmail.com

@donji