Cloud Load Balancing 72 Computers use protocols to communicat e Multiple layers and multiple protocols Network Layer - T ransfer bits and bytes T ransport Layer - Are the bits and bytes transferred properly? Application Layer - Ma ke REST API calls and Send Emails (Remember) Each layer makes use of the layers beneath it (Remember) Most applications talk at application layer. BUT some applications talk at transport layer directly(high performance). H T T P v s H T T P S v s T C P v s T L S v s UDP 73 Network Layer: IP (Internet Protocol): Transfer bytes. Unreliable. Transport Layer: TCP (Transmission Control): Reliability > Performance TLS (Transport Layer Security): Secure TCP UDP (User Datagram Protocol): Performance > Reliability Application Layer: HTTP(Hypertext Transfer Protocol): Stateless Request Response Cycle HTTPS: Secure HTTP SMTP: Email Transfer Protocol and a lot of others... HTTP vs HTTPS vs TCP vs TLS vs UDP 74 Most applications typically communicate at application layer Web apps/REST API(HTTP/HTTPS), Email Servers(SMTP), File Transfers(FTP) All these applications use TCP/TLS at network layer(for reliability) HOWEVER applications needing high performance directly communicate at transport layer: Gaming applications and live video streaming use UDP (sacrifice reliability for performance) Objective: Understand Big Picture. Its OK if you do not understand all details. HTTP vs HTTPS vs TCP vs TLS vs UDP 75 Cloud Load Balancing - Terminology Backend - Group of endpoints that receive traffic from a Google Cloud load balancer (example: instance groups) Frontend - Specify an IP address, port and protocol. This IP address is the frontend IP for your clients requests. For SSL, a certificate must also be assigned. Host and path rules (For HTTP(S) Load Balancing) - Define rules redirecting the traffic to different backends: Based on path - in28minutes.com/a vs in28minutes.com/b Based on Host - a.in28minutes.com vs b.in28minutes.com Based on HTTP headers (Authorization header) and methods (POST, GET, etc) etc.. 76 Load Balancing - SSL/TLS Termination/Offffloading Client to Load Balancer: Over internet HTTPS recommended Load Balancer to VM instance: Through Google internal network HTTP is ok. HTTPS is preferred. SSL/TLS Termination/Offloading Client to Load Balancer: HTTPS/TLS Load Balancer to VM instance: HTTP/TCP 77 Cloud Load Balancing - Choosing Load Balancer https://cloud.google.com/load-balancing/images/choose-lb.svg 78 Cloud Load Balancing - Features Load Balancer Type of Traffic Proxy or passthrough Destination Ports External HTTP(S) Global, External, HTTP or HTTPS Proxy HTTP on 80 or 8080 HTTPS on 443 Internal HTTP(S) Regional, Internal, HTTP or HTTPS Proxy HTTP on 80 or 8080 HTTPS on 443 SSL Proxy Global, External, TCP with SSL offload Proxy A big list TCP Proxy Global, External, TCP without SSL offload Proxy A big list External Network TCP/UDP Regional, External, TCP or UDP Pass-through any Internal TCP/UDP Regional, Internal, TCP or UDP Pass-through any 79 Load Balancer Scenarios Scenario Solution You want only healthy instances to receive traffic Configure health check You want high availability for your VM instances Create Multiple MIGs for your VM instances in multiple regions. Load balance using a Load Balancer. You want to route requests to multiple microservices using the same load balancer Create individual MIGs and backends for each microservice. Create Host and path rules to redirect to specific microservice backend based on the path (/microservice-a, /microservice-b etc). You can route to a backend Cloud Storage bucket as well. You want to load balance Global external HTTPS traffic across backend instances, across multiple regions Choose External HTTP(S) Load Balancer You want SSL termination for Global non-HTTPS traffic with load balancing Choose SSL Proxy Load Balancer