SOLUTION BRIEF

FortiGSLB Quickly and Securely Delivers Applications Anywhere

Executive Summary

Horizontal scalability is a key factor when it comes to designing and deploying internet-based services and solutions for enterprise and carrier networks. These organizations must be able to quickly and easily add new network resources and deploy cloud-based applications to ensure business continuity as well as smooth disaster recovery in the event of data center or server failure. Yet, if internet connectivity or security is unreliable, these efforts are often stalled.

Without this flexibility, business demands often force enterprises to upgrade to bigger and more powerful hardware devices to manage these capacity challenges. These upgrades can be costly and add significantly to the total cost of ownership (TCO) without addressing the issues of failover and service availability.

Fortinet Global Server Load Balancing (GSLB) Cloud is a DNS service that enables organizations to move beyond the data center to create new types of multitenant architectures that rapidly and securely deliver network and internet-based applications and services.

Easily Scale Infrastructure with FortiGSLB

Regardless of the size of an application environment, organizations can easily expand applications without deploying additional hardware.

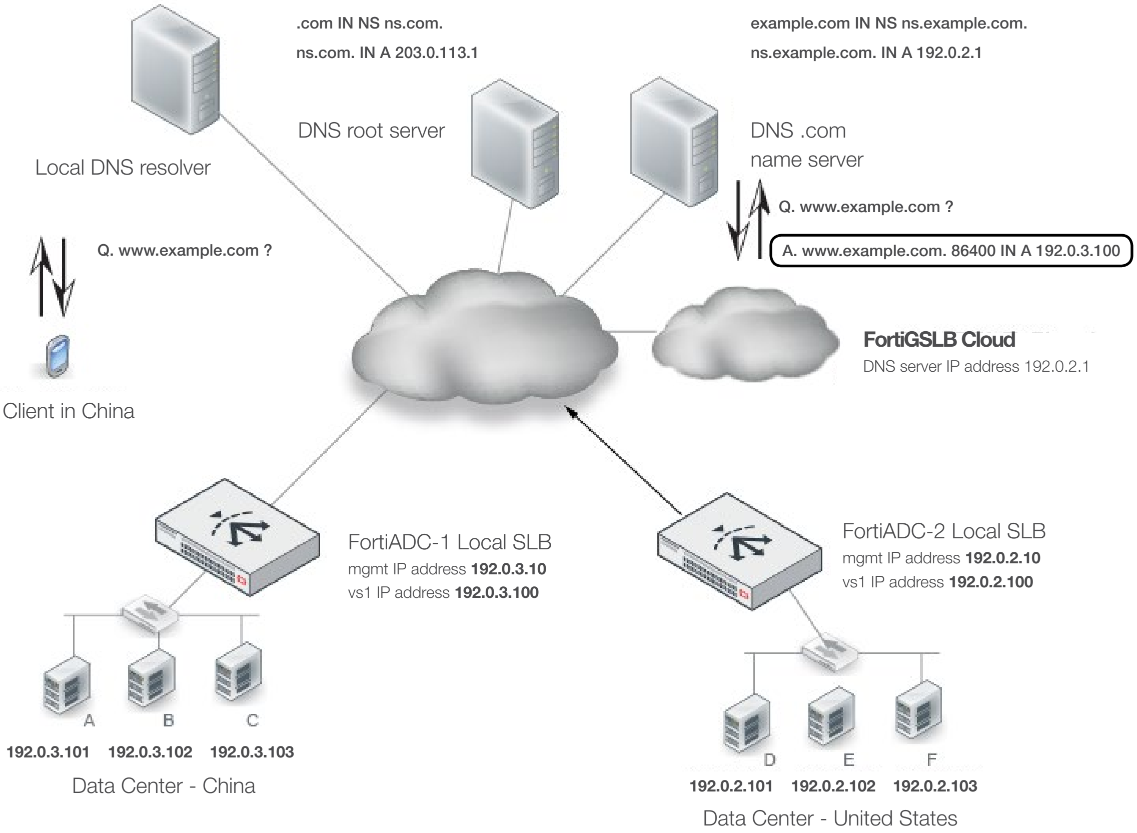

Figure 1: FortiGSLB Cloud deployment model.

Introduction

FortiGSLB is a cloud-based approach that simplifies the complexities of increasingly expanding resources and applications across multiple data centers. It streamlines disaster recovery, improves performance, and reduces application delivery costs. Unlike traditional application delivery solutions, FortiGSLB provides an always-on, always-available, and hosted GSLB solution that does not require a device at every data-center location.

With an easy-to-use FortiGSLB interface, organizations can configure rules based on network elements, geography, server performance, and custom policies to meet a range of business requirements. FortiGSLB also delivers advanced health checking mechanisms to accommodate almost any load-balancing requirement or failover scenario, providing 100% uptime for mission-critical applications.

FortiGSLB provides load-sharing and failover functionality with a reach and level of resiliency that exceeds that of traditional, device-based solutions.

FortiGSLB Benefits

The rule-based redirection and health checking mechanism features within FortiGSLB enable organizations to:

- **Scale client infrastructure horizontally** using applications and services located in multiple colocation or other types of data centers, without the limitations of vertical-scale solutions that are restricted to a single location.
- **Leverage all Fortinet appliances and services** to add service resiliency and deploy best practices such as multitenant business continuity planning (BCP) and disaster recovery (DR) models.
- **Extend the capacity of legacy devices** using the FortiGSLB “weighted round-robin” approach to load balancing, which maximizes the utilization of higher-performing devices.
- **Ensure the best performance** for employees and clients by directing them to the source that is closest to them geographically.
- **Build or develop** new and improved features and functionality.

The following three scenario descriptions and solutions pair FortiGSLB with other Fortinet products and content delivery networks to illustrate how organizations can scale applications and services across multiple data centers.

Use Case 1: FortiGSLB with FortiGate SSL/IPsec VPN for Reliable and Improved VPN Performance

Many organizations have installed VPN endpoints in each region to improve network performance for telecommuters and to establish secure communications on mobile devices. The ability to securely connect to corporate networks is increasingly important to support employees who work from home, while travelling, from coffee shops, or other nontraditional environments.

While it may be acceptable for a small-scale business to configure a VPN client with a single endpoint, large-scale enterprises require more robust solutions for workers that travel often. This is especially true for organizations that have grown internationally or are planning to do so, where the work of high-level employees is often hampered by inadequate network access.

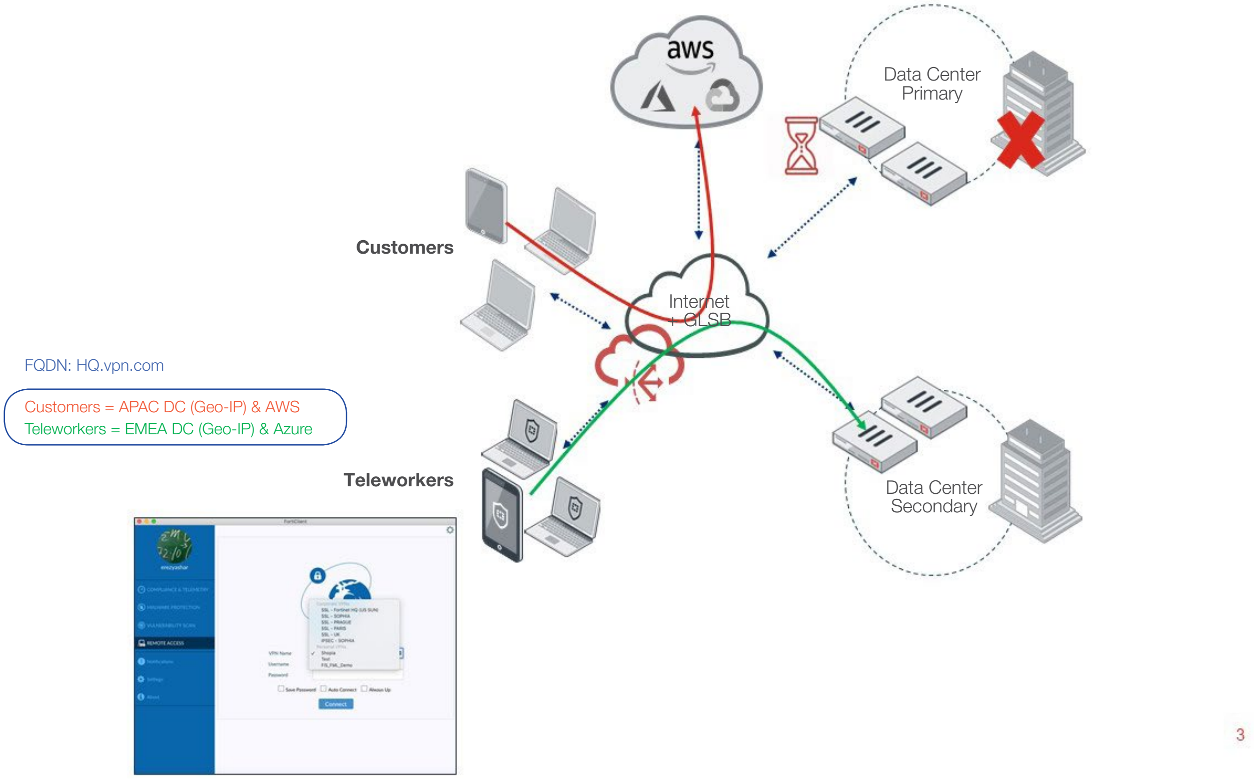

Figure 2: FortiGSLB detects the failed server and redirects traffic.

Solution

To improve VPN performance and scalability, FortiGSLB can be configured to automatically connect mobile clients with the FortiGate VPN server that is geographically nearest to an employee's current location.

Geographic distance correlates to performance. Connecting directly to the closest VPN server allows client communications, such as email or instant message, to travel between corporate locations over the customer's own private network. In addition, the FortiGSLB health check mechanism automatically removes any unresponsive VPN endpoints, delivering a seamless user experience during maintenance periods. This VPN connection is more reliable and communication is more responsive than relying on it to travel across the public internet.

Use Case 2: FortiGSLB with FortiWeb for Secure Web Applications Anywhere

An organization with a single FortiWeb device in a data center on the west coast of the United States is over capacity, while clients across the east coast, Asia, and Europe are experiencing severe lag. While upgrading FortiWeb is an option, this solution does not address the issue of latency for international customers. A better solution is to use FortiGSLB with multiple deployments of FortiWeb in the appropriate regions.

FortiGSLB with FortiWeb routes web traffic to the closest data center or provides disaster recovery should a data center or server fail.

Solution

The FortiWeb web application firewall protects web-based applications and internet-facing data. FortiGSLB provides customers with greater flexibility as they grow their FortiWeb presence. For example, FortiGSLB can add automatic failover between FortiWeb devices in the event of data center or server failure, or route clients to data centers based on geographic distance or server performance.

With three additional FortiWeb devices installed in data centers across central locations on the east coast, Asia, and Europe, the load is now distributed evenly among all four locations, allowing the original FortiWeb device to provide a better customer experience. If any of the FortiWeb appliances fail the health check, FortiGSLB automatically redirects traffic to another route. This automatic redirection increases the organization's BCP and DR capabilities while reducing the complexity of those processes.

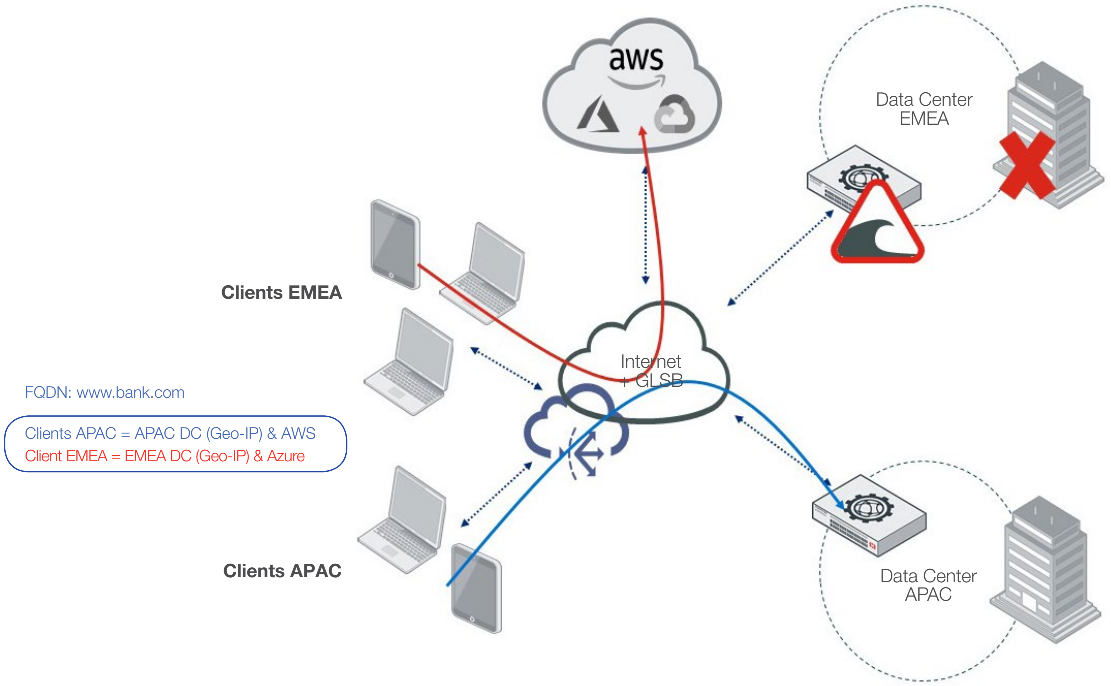

Figure 3: FortiGSLB directs traffic to the geographically closest VPN node.

Use Case 3: FortiGSLB with FortiMail for Multitenant Mail Server Failover Configuration

Use FortiGSLB with FortiMail to provide seamless routing of internal and external traffic, should a primary FortiMail server go offline.

The FortiMail high-availability feature allows two appliances—a primary appliance and a secondary backup appliance—to work as a pair. The primary appliance accepts connections and traffic for SMTP, POP, and IMAP, while the backup does not accept connections or traffic as long as the primary appliance is up and running.

This scenario is effective for handling incoming email from servers outside of the organization. However, it can create problems when employees' individual mail clients use a single hostname for sending and receiving mail, and the primary server goes offline or is unreachable. As a result, employees cannot access or send email, grinding business to a halt.

Existing solutions require organizations to change or update DNS entries for mail.company.com and are subject to expiration TTLs on DNS records and recursive DNS caches. Alternatively, an organization can redirect email to insecure cloud services such as Google applications. However, both of these methods delay the transfer of email clients to the backup server, slow productivity, and hinder cybersecurity. In addition, it is becoming increasingly popular for organizations to install their secondary email servers in a separate location to provide further security against infrastructure failure. In this scenario, the high-availability feature may not be a viable option.

Solution

FortiGSLB performs health checks to verify server availability. If a server is down, FortiGSLB automatically redirects the user to a different server to receive emails.

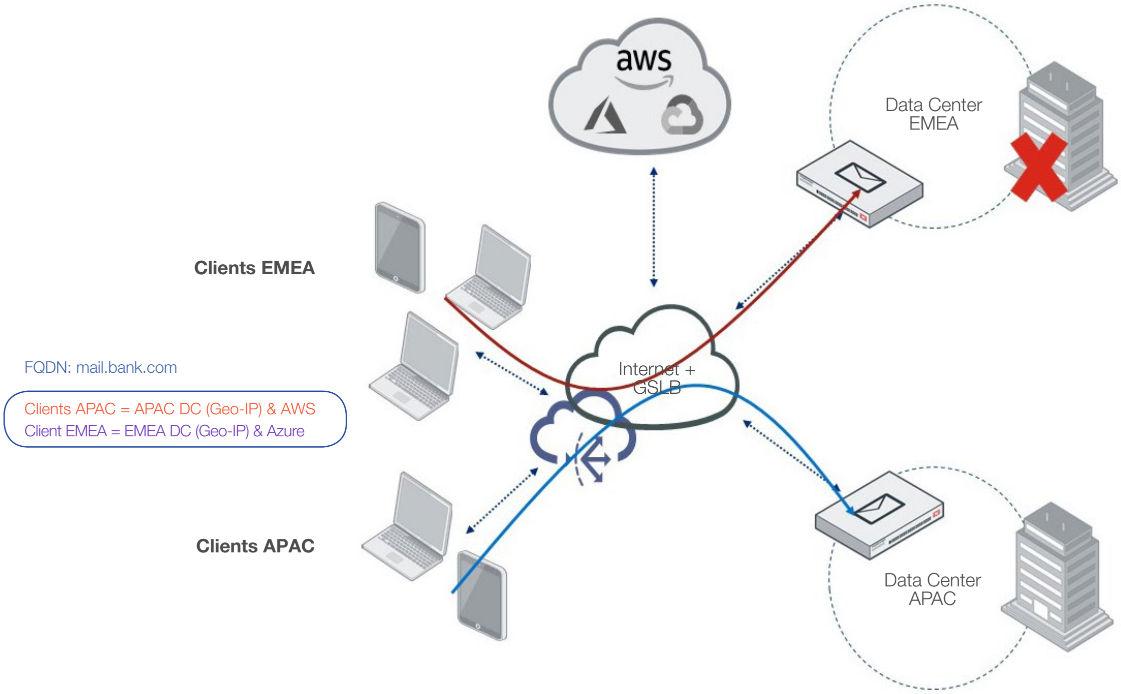

Figure 4: FortiGSLB directs traffic to multiple FortiWeb devices behind FortiGate firewalls.

Conclusion

FortiGSLB provides a complete, easy-to-manage, and reliable approach to extending web-based applications across the globe to any number of data centers without the addition of a single piece of hardware. Organizations can use FortiGSLB to scale other Fortinet products, such as FortiMail, VPN, and FortiWeb. These scenarios and examples are just the beginning of the many ways FortiGSLB can provide scalability and redundancy to an organization's application delivery challenges. For more information on FortiGSLB or to request a free demo, please contact your Fortinet sales representative or Fortinet authorized resale partner.