FORTINET

SOLUTION BRIEF

Fortinet Load-balancing Solutions Ensure VPN and Service Availability and Security

Executive Summary

An organization’s business continuity plan must include strategies and solutions for ensuring consistent access to enterprise resources in unusual circumstances. An urgent need to transition to a mostly or wholly remote workforce will prompt a surge in inbound virtual private network (VPN) connections to the corporate network. Alternatively, unusual circumstances may render the primary data center and servers unavailable, requiring a seamless failover to backup servers in order to maintain a high customer quality of experience (QoE).

Fortinet solutions enable enterprises to address both of these situations with minimal impact on existing network infrastructure. FortiADC application delivery controllers act as high-performance load balancers for FortiGate next-generation firewalls (NGFWs), ensuring “always-on” VPN connectivity.

Alternatively, the Fortinet global server load balancing (FortiGSLB Cloud) service ensures service availability in case of outages at the primary site. The service can also optimize customer experience based upon geolocation and network traffic round-trip time (RTT). Neither solution requires modification to an organization’s existing network infrastructure, enabling an enterprise to ensure VPN and service availability without expensive architectural redesign.

Key Benefits of VPN Load Balancing:

- Increased NGFW performance (active/active)
- “Always-on” VPN connectivity
- Advanced NGFW load balancing
- Improved user QoE

Introduction

Ensuring secure, reliable connectivity to enterprise assets is an essential component of an organization’s business continuity strategy. In the event of a natural disaster, disease outbreak, or other unforeseen event, an organization may be incapable of maintaining operations on-site. In these situations, the ability to support a remote workforce and ensure the accessibility of enterprise resources is critical.

Fortinet products offer solutions to both of these business continuity challenges. FortiADC application delivery controllers can be deployed as load balancers, enabling optimized routing of inbound VPN connections to multiple FortiGate NGFWs. The Fortinet GSLB solution enables enterprises to ensure service accessibility and high customer QoE by routing traffic to backup and redundant data centers when needed.

High-performance VPN Load Balancing with FortiADC and FortiGate

Offering VPN connectivity, whether via secure sockets layer (SSL) or Internet Protocol security (IPsec), is essential to ensuring secure connectivity for a remote workforce. However, scaling VPN infrastructure to meet the needs of a business’s business continuity plan can pose a significant challenge. Encryption and decryption of inbound traffic at the VPN endpoint is extremely CPU-intensive.

Multiple FortiGate NGFWs deployed in parallel can enable even the largest enterprises to scale their VPN infrastructure to support a mostly or wholly remote workforce. This ensures that employees have access to “always-on” VPN connectivity and that all inbound connections are subjected to a full security inspection to identify malicious content before it reaches the internal network.

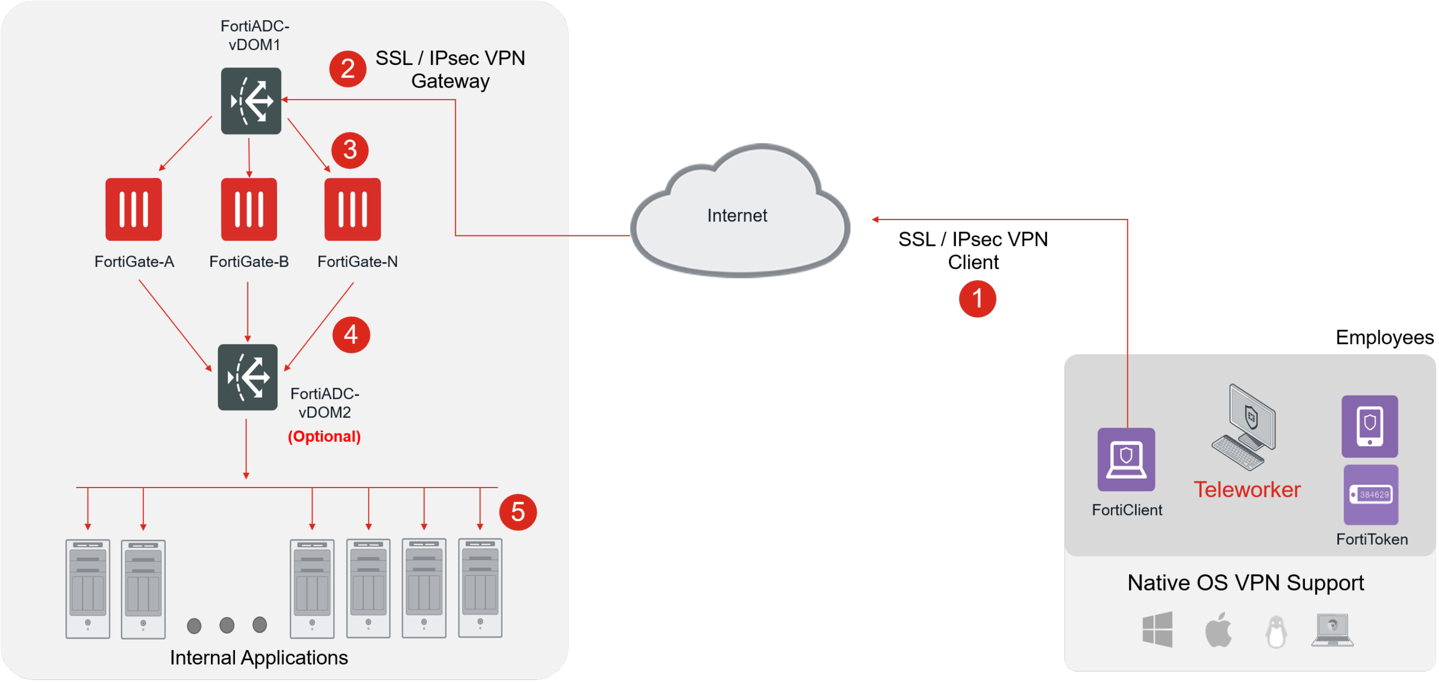

Figure 1: FortiADC enables reliable VPN connectivity for remote workers.

Deployment of a FortiADC enables an organization to load balance incoming VPN connections across multiple FortiGate NGFWs. A single FortiADC appliance can be configured to use virtual domains (VDOMs) to load balance traffic between the array of FortiGate NGFWs, and the same hardware can also be used to aggregate the output of the NGFWs into a single stream for routing to the appropriate server.

This ability to insert the FortiADC appliance in front of and behind an array of FortiGate NGFWs enables load balancing across multiple NGFWs with minimal impact on the existing network architecture. With the use of VDOMs, the view of the traffic entering the FortiGate NGFWs and the servers that they secure is identical, whether an organization has a single NGFW or several.

VPN and Service Continuity with FortiGSLB Cloud and FortiGate NGFWs

An organization's servers at the primary site can become unavailable or unusable for various reasons. The site could be experiencing a high load, due to the high CPU requirements of supporting a remote workforce or in response to an unusual event, such as a shopping holiday. Alternatively, servers at the primary site could be unavailable due to scheduled or unscheduled maintenance or in response to a business-disrupting event.

The Fortinet FortiGSLB Cloud service enables an enterprise with multiple data centers to maintain VPN and service continuity in the event that the primary site is busy or otherwise unavailable. This is essential to an organization's business continuity plan since outages could impact the productivity of a remote workforce or customer experience.

In this scenario, an organization would deploy the FortiGSLB Cloud service in front of an array of FortiGate NGFWs. The FortiGSLB Cloud service performs load balancing for incoming connections between the available FortiGate NGFWs on the same site or between multiple sites.

Key Benefits of VPN and Service Continuity with FortiGSLB Cloud:

- Improved VPN performance and user QoE
- User redirection based on geolocation and round-trip time (RTT)
- Advanced health checks for applications and NGFW
- Improved site visibility and availability

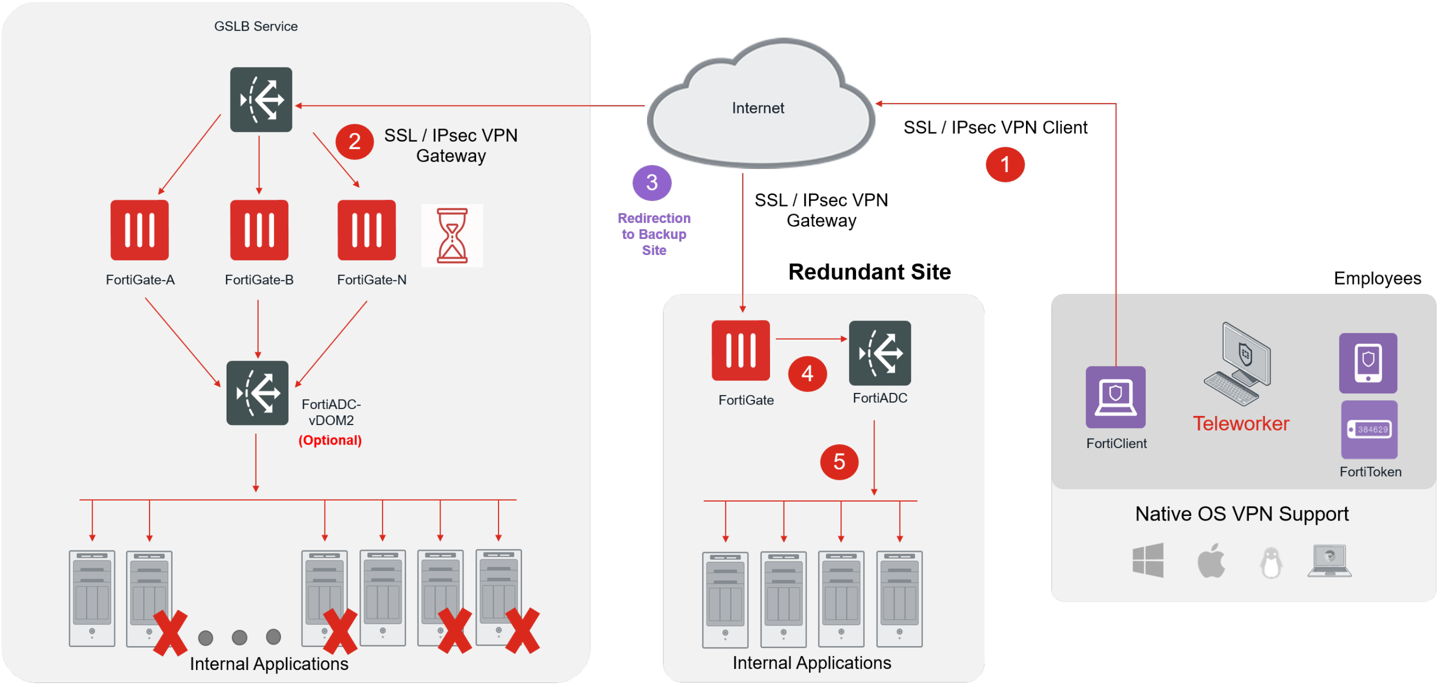

Figure 2: VPN and service continuity with FortiGSLB Cloud provides improved VPN performance and user QoE.

If the servers at the primary site, or the FortiGate NGFWs protecting them, are overwhelmed or otherwise unavailable, the FortiGSLB Cloud service invisibly reroutes inbound connections to a backup or redundant site capable of fulfilling the user's request. This ensures that increased load or outages at the main site do not result in dropped connections or loss of security.

To ensure optimal routing decisions, the FortiGSLB Cloud service frequently scans the servers and NGFWs at the primary and secondary deployment sites. It assesses each site's ability to handle inbound requests, including the average latency of responses from that site and the ability to handle additional SSL VPN connections.

The benefits of the Fortinet FortiGSLB Cloud service go beyond ensuring business continuity in the face of unusual circumstances. As enterprises deploy geographically distributed data centers, the FortiGSLB Cloud service can also route traffic based upon user geolocation and average RTT. This enables an enterprise to ensure optimal QoE for a global customer base.

Conclusion

The ability to ensure VPN and service continuity is an essential component of an organization's business plan. A massive transition to remote work or an outage at the primary site should not impact user QoE or the organization's network security.

Fortinet load-balancing solutions include both local load balancing with FortiADC and load balancing across multiple data centers with the Fortinet FortiGSLB Cloud service. These solutions require no modification to an enterprise's existing network architecture, enabling rapid deployment with no architectural redesign.