Solution Overview

Elastic Application Secure Edge from VMware

Enable seamless multi-cloud connectivity, end-to-end security, and observability

At a glance

Multi-cloud environments that span on-premises data centers and multiple cloud service providers are inherently elastic, highly scalable and complex. VMware's elastic application secure edge (EASE) provides a common policy model across multi-cloud environments to connect, secure, observe and make workloads highly available across different cloud environments. Coupled with VMware SASE™ and VMware Tanzu® Service Mesh™ Advanced edition, EASE provides the final piece for measuring, orchestrating and securing application experience across private and public cloud environments.

Key highlights

- Seamless connectivity – Enable true automated self-service connectivity across cloud environments.
- CapEx/OpEx savings – Consolidate expensive hardware and reduce operational costs for enterprises via network simplicity and automation across multi-cloud environments.
- Business agility – Enable enterprises to react to dynamic market and customer demands in near real time with networking at the speed of development.

As multi-cloud environments become the norm for today's distributed applications, it's become increasingly difficult to connect cloud-based services through a more efficient, software-defined approach to networking. Traditional networking solutions such as physical/virtual firewalls, routers and VPNs require manual stitching together of services, provide little visibility into cloud service provider environments, create security gaps, and are cobbled together with multiple proprietary tools. It's clear that modern enterprises need a new way to ensure seamless connectivity, end-to-end security, and observability between services in a multi-cloud environment.

The solution: Elastic application secure edge

VMware's elastic application secure edge provides a common set of services that span multi-cloud environments to connect, secure, observe and make workloads highly available across different cloud environments, providing the operational consistency across cloud environments that makes it simple to deploy services modularly with choice and flexibility. Elastic application secure edge intelligently creates, connects, updates and deletes networking, security and observability services across edge devices placed in pubic cloud and private cloud environments as well as close to users, ensuring services are spun up on the appropriate infrastructure based on traffic characteristics and predetermined service-level agreements (SLAs).

EASE spans three components:

- Networking:
  - Site-to-site VPN
  - Routing
  - Global server load balancing
  - Local load balancing
  - Direct cloud-to-cloud interconnect

- Security:
  - Edge firewall
  - Intrusion detection system and intrusion prevention system (IDS/IPS)
  - Web application firewall
  - Network traffic analysis (NTA) and network detection and response (NDR)
  - Distributed denial-of-service (DDoS) attack mitigation
  - API protection
- Observability:
  - Network and application performance monitoring
  - Anomaly detection
  - Security violation

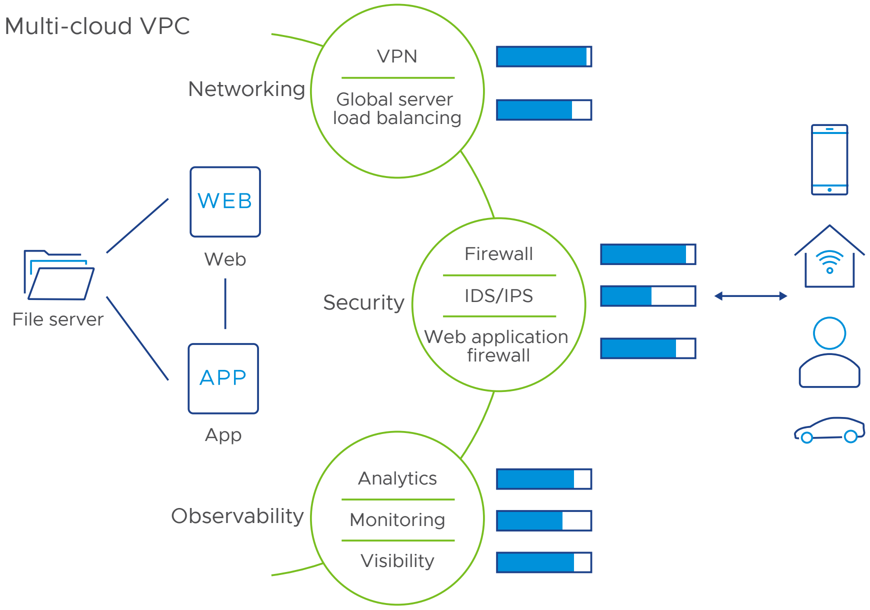

Figure 1: The elastic application secure edge.

Key capabilities

Elastic

As traffic patterns change, edge services are dynamically scaled on demand based on traffic characteristics and SLAs.

Consistent policy management

Consistent policies ensure workloads can connect and are secure, regardless of the underlying cloud infrastructure.

Learn more

Check out these resources to learn more about how to deliver seamless connectivity, end-to-end security, and observability across multi-cloud environments:

- Cloud networking by VMware
- Network security solutions
- VMware NSX® Advanced Load Balancer™
- Multi-cloud networking solution

Reach out to your VMware sales representative for further details.

Multi-cloud

Edges are infrastructure agnostic and function uniformly in the private cloud as well as on public clouds, such as Google Cloud Platform, AWS and Azure.

End-to-end security

Elastic application secure edge extends secure connectivity to the virtual private cloud (VPC)[1] edge rather than the data center edge—a key requirement for multi-cloud connectivity. This provides full, complete visibility into threat detection, NTA/NDR, distributed firewalls, and other security services.

Highly automated

EASE uses AI and machine learning techniques to learn how traffic patterns vary over time and scale automatically to meet these dynamic demands.

Operationally simple

Elastic application secure edge provides central control with a distributed data plane of services delivered at the enterprise edge. This means that policies, lifecycle management, observability and automation decisions are consolidated in a central management and control plane while functions are delivered close to the applications.

Delivered as SaaS

Delivering this intent, policy management and orchestration layer via software as a service (SaaS) eliminates on-premises and cloud tools, making it much more flexible and easier to measure and ensure application experiences.

Modern networks need modern connectivity solutions

Legacy networking is not agile or secure enough to deliver the expected user experience across today's multi-cloud environments. Based on its breadth and depth of networking solutions across private and public cloud environments, VMware is uniquely positioned to help organizations orchestrate and ensure expected application experience, regardless of the underlying infrastructure.

[1] A virtual private cloud is an on-demand configurable pool of shared resources allocated within a public or private cloud environment, providing isolation between the different organizations using the resources.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001