WHITE PAPER

Fortinet's Tested and Validated Architectures for Cloud Network Security

Improve Protection and Save Design Time

Executive Summary

Cloud adoption continues to grow as organizations take advantage of cloud computing's unique ability to accelerate digital transformation. However, the rapid expansion of cloud deployments presents a new set of challenges that range from simply having a bigger attack surface to protect to ensuring network performance.

Organizations migrating to the cloud can speed deployments and improve security posture by leveraging a tested reference architecture. Fortinet offers tested and validated architectures for cloud network security that include ingress, egress, east-west traffic inspection, and SD-WAN. There are a variety of benefits to adopting these architectures including reduced risk, consistent security posture, and comprehensive protection. This white paper will explain what each of the architectures listed above achieves and how they are set up. We also cover the security services needed for each to be effective.

"The biggest cybersecurity threat is human error, accounting for over 80% of incidents. This is despite the exponential increase in organizational cyber training over the past decade, and heightened awareness and risk mitigation across businesses and industries."[1]

What Is a Tested Reference Architecture?

A tested reference architecture is essentially a blueprint that outlines best practices for designing and securing cloud environments. Developed by security experts and battle-tested against real-world threats, it provides a proven framework for organizations to build upon.

Reference architectures can increase agility and help you optimize your cloud deployments. These architectures can also reduce mistakes that may compromise security.

Key Benefits of Fortinet Reference Architectures

Use of Fortinet reference architectures will help:

Reduce risk with industry-standard security controls and configurations to mitigate the risk of misconfigurations. This predefined approach also helps organizations avoid the time-consuming process of building security from scratch, accelerating cloud adoption.

Promote consistency and repeatability by providing a standardized approach to security across all cloud deployments within your organization. This consistency simplifies security management and ensures all deployments adhere to the same baseline security controls.

Offer integration and interoperability by considering the integration of various cloud security tools and services. This ensures a well-coordinated security posture where different tools seamlessly work together to provide comprehensive protection.

Leverage expertise to implement best practices built by knowledgeable, experienced security professionals. By adopting a pre-vetted approach, you gain access to best practices that might not be readily available within your internal security team.

Fortinet Validated and Tested Architectures

The following tested architectures for securing applications and data in the cloud cover the most common cloud network security use cases. In each example, the same virtual network can also contain related tools such as the FortiWeb web application firewall (WAF) or FortiSandbox for the detection of previously unknown malware. Management and analytic tools, such as FortiManager and FortiAnalyzer, can be placed in the virtual network with the FortiGates, in another virtual network, in a separate cloud, or on-premises.

Routed ingress traffic inspection

Ingress traffic is the flow of data into a private network from an external source. A team building virtual networks in a public cloud might want an architecture specifically for ingress traffic inspection to enhance security by detecting and blocking threats without introducing latency. This can be achieved by forcing all traffic from the internet to be routed through a dedicated security virtual network with a virtual network firewall and other security tools for inspection. By implementing this architecture, the team can mitigate attacks and ensure that inbound traffic is thoroughly monitored and controlled. The goals of this architecture are:

- Inspect inbound encrypted traffic for all types of security threats
- Provide redundancy (A/A HA) and the ability to scale up or down as business needs change
- Apply SSL inspection and IPS to all inbound traffic

Ingress traffic filtering is one of the first lines of defense in a network security strategy. When configured on an edge device such as a router or firewall, ingress filtering examines all inbound packets and permits or denies entry to the network based on information in the packet header, so it is essentially a form of packet filtering. At its most basic, ingress filtering examines several attributes, most notably the source IP address. If the source address doesn't match its originating network, the filter determines the address is forged or spoofed and drops the packet. FortiGate VM also provides valuable security services including SSL inspection, IPS, AV, geolocation filtering, and traffic shaping.

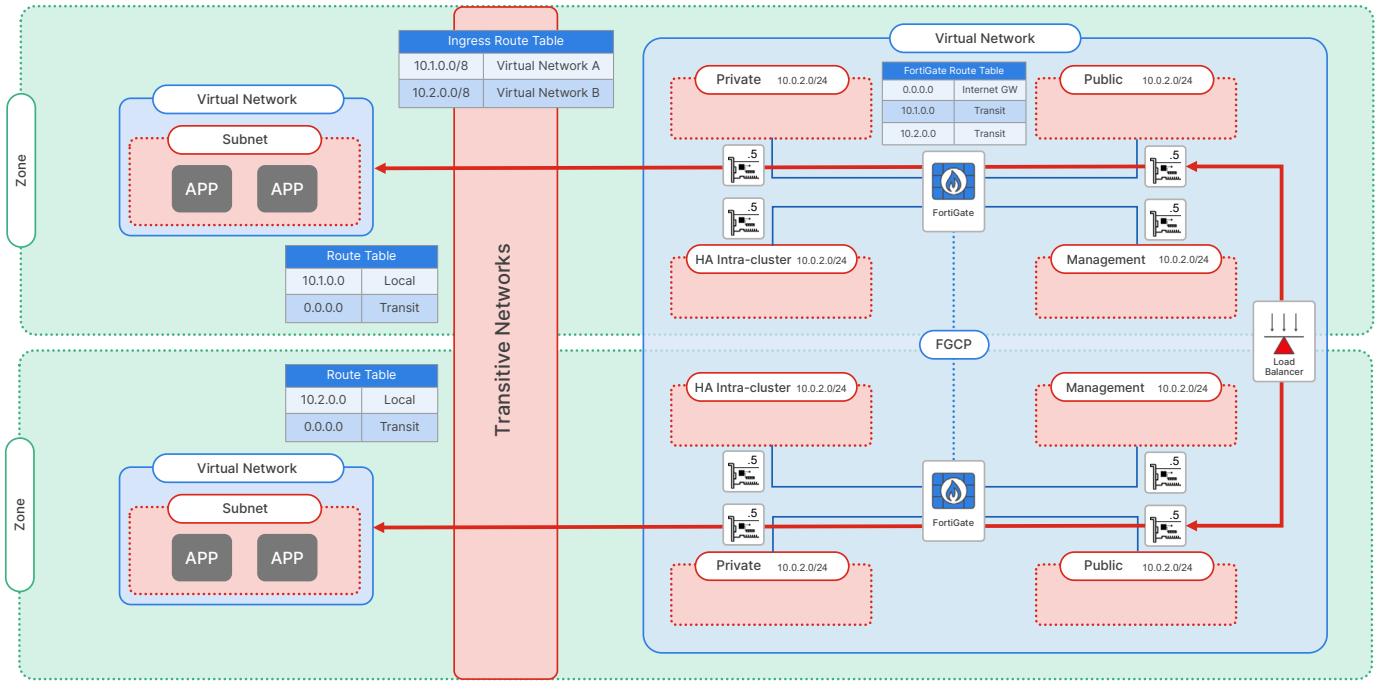

Figure 1: Ingress filtering reference architecture

The diagram above shows a public cloud network spanning two zones. Traffic will come in through a load balancer on a public IP address and destination network address translation (DNAT) traffic to the firewalls. The firewall cluster is deployed across zones for fault tolerance. The virtual network has two FortiGate NGFW VMs that are in high availability mode with a load balancer monitoring firewall availability and directing traffic. In most scenarios, return traffic is routed back through the public load balancer. The load balancer can be offered by a cloud service or be a dedicated solution such as FortiADC.

Four interfaces are most commonly used, one for the dedicated public or untrusted zone, the private or trusted zone, out-of-band management, and the dedicated channel for session and cluster syncing (as required).

Routed egress traffic inspection

Egress traffic refers to the flow of data moving out of a private network to the internet or another external network. Egress happens whenever data leaves an organization's network via email messages, as uploads to the cloud or websites, as a file transferred onto removable media like USB drives and external hard drives, or through FTP or HTTP transfers.

Egress traffic inspection is the process of examining outgoing data flowing from your network to the internet or other external destinations. It acts like a security checkpoint for outbound traffic, looking for potential threats or violations of your privacy and security policies. This process is integral to network operations, especially in cloud environments where controlled data movement is paramount for security and efficiency. Egress-only internet gateways are used to prevent internet traffic from initiating a connection with your instances by only allowing outbound communication from instances in your network to the internet.

Egress inspection is used to:

- Prevent internal users from releasing or sending sensitive or confidential data. Users may inadvertently or purposefully seek to copy customer data, product plans, financials, and other sensitive information. A good data loss prevention solution can help protect your data from insider threats.
- Prevent malware from leaking information to hackers or other nefarious entities. Malicious software or compromised systems can exfiltrate sensitive data, such as personal information or financial records, from your network. Egress traffic inspection can help identify and block such attempts by looking for patterns associated with data exfiltration.
- Prevent your systems from being used as part of a botnet for attacking other systems.
- Enforce compliance. You may need to comply with regulations that require you to monitor and control the flow of data. Egress traffic inspection can help ensure that only authorized data is leaving the network and that it complies with relevant regulations.
- Prevent accidental data loss. Egress traffic inspection can help identify and prevent the transmission of sensitive data by implementing rules that restrict the types of data that can be sent out.

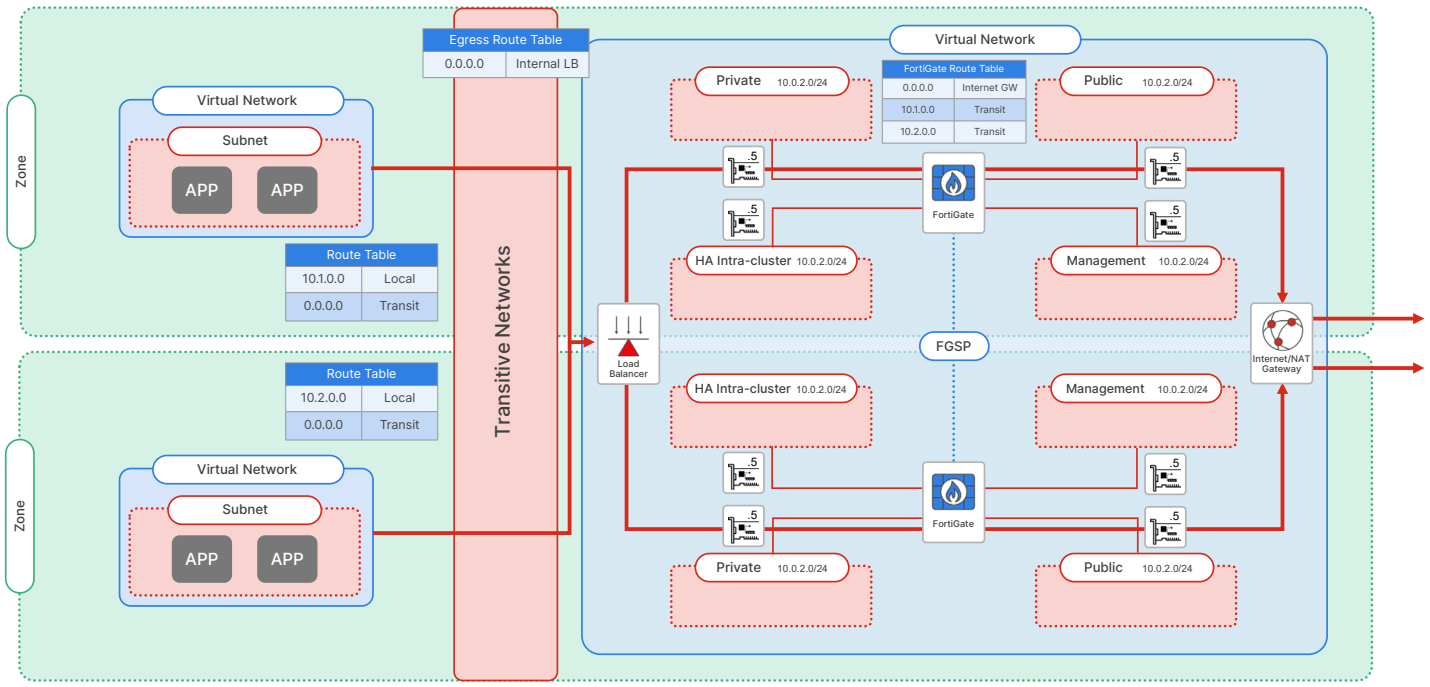

Figure 2: Egress filtering reference architecture

In the diagram above, we again have a pair of FortiGate VMs in HA mode. The FortiGate Clustering Protocol (FGCP) provides failover protection, whereby the cluster can provide FortiGate services even when one of the cluster units loses connection. FGCP is also a Layer 2 heartbeat that specifies how FortiGate units communicate in an HA cluster and keeps the cluster operating. FGCP assigns virtual MAC addresses to each primary unit interface in an HA cluster. Virtual MAC addresses are in place so that if a failover occurs, the new primary unit interfaces will have the same MAC addresses as the failed primary unit interfaces. If the MAC addresses were to change after a failover, the network would take longer to recover. Traffic is routed from other virtual networks through the FortiGates before going to the internet gateway.

"East-west traffic has grown substantially. Interestingly, the volume of this lateral traffic has surpassed the conventional North-South traffic, making its security an imperative. This shift underscores the importance of shielding East-West traffic from potential malicious actors and breaches, as threats can arise internally, moving laterally without ever touching the traditional network perimeter."[2]

East-west traffic inspection

East-west traffic inspection refers to the monitoring and analysis of network traffic that moves laterally within a data center or cloud environment. Driven by the rise of virtualization, containerization, and microservices, east-west traffic has grown dramatically in recent years. This type of traffic flows between servers, storage systems, and applications that are within the same security perimeter. While east-west segmentation deployments often focus on filtering traffic based on ports and protocols, more powerful tools are needed to prevent hackers who have penetrated part of a network from using east-west traffic flows to expand the scale of the breach.

East-west traffic inspection is crucial because it helps in detecting and preventing threats that have bypassed perimeter defenses or that arose internally. In modern cloud environments, where workloads are dynamic and distributed, the lateral movement of traffic can be exploited by attackers to spread malware or carry out data exfiltration unnoticed. Called breach traversal, it is this lateral movement attack traffic that can turn a minor issue into a catastrophe. By inspecting internal traffic, you can gain visibility into your network activity, enforce security policies, and detect anomalies that may indicate a security breach. East-west traffic inspection also aligns well with a zero-trust security model where no internal traffic is automatically trusted.

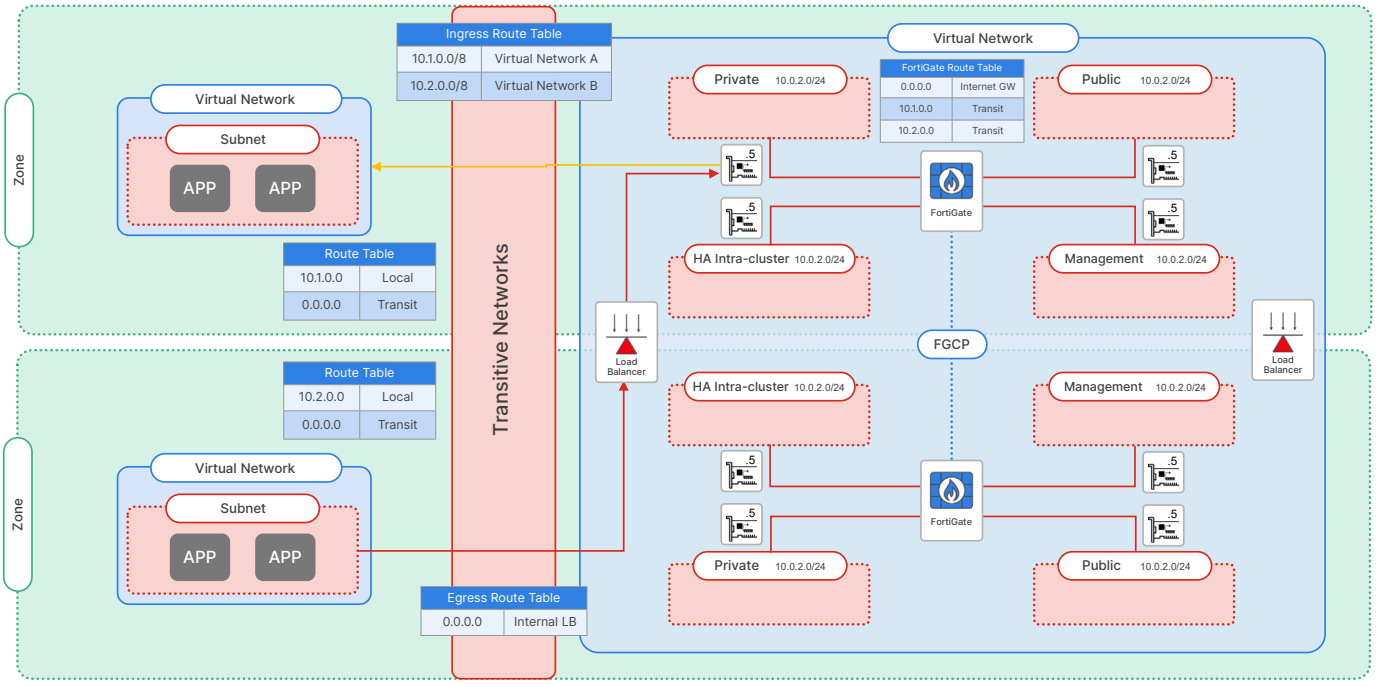

Figure 3: East-west traffic inspection reference architecture

The diagram above shows a sample architecture for east-west traffic inspection. Here we are solving the need for traffic between application tiers to be inspected and for source and destination permissions evaluated. FortiGate can both inspect and secure traffic and quarantine sources on the network to prevent the lateral spread of malware or the inappropriate movement of sensitive information.

The FortiGates are deployed in an active-active HA cluster supported by a load balancer or a full-featured application delivery controller. App control services are typically implemented to look for applications on specific ports and to identify the misuse of ports by unwanted applications.

The clusters exist across zones to help ensure availability. This approach allows for both redundancy and scaling. Route tables are configured to ensure that east-west traffic traversing the network is routed through the FortiGates. The FortiGate VM applies SNAT after inspection and performs a route lookup to forward traffic to the destination VPC, which sends traffic back to the transitive network. Response traffic is routed in the reverse path to maintain symmetry.

Four interfaces are used commonly in this design to provide multiple traffic flow-type support, where a dedicated public or untrust zone, private or trust zone, an out-of-band management interface, and a dedicated channel for session and cluster syncing are needed.

Secure SD-WAN and other cloud on-ramps

Secure access to the cloud is a critical part of your security infrastructure. Sometimes called, secure cloud on-ramp, this can be accomplished in several ways including VPNs, direct connect services, cloud exchanges, and software-defined wide area network (SD-WAN). A secure SD-WAN solution is ideal for any cloud on-ramp infrastructure.

Secure SD-WAN simplifies WAN management and reduces costs by using software to define how traffic is routed across different types of connections such as cable, DSL, and MPLS. SD-WAN is rapidly replacing traditional WAN for remote office and branch deployments. Traditional WANs can be complex, expensive, and inflexible. But while SD-WAN improves networking bandwidth, if security is not tightly integrated, it can also increase risk exposure by expanding the attack surface and allowing security breaches to spread.

This architecture is designed to provide:

- Redundancy and scale with the inline NGFWs deployed in an active-active configuration
- VPN gateways are zonal redundant so zones are not as critical in this specific use case
- Traffic flows that are dynamically optimized to improve latency and reduce costs

Fortinet Secure SD-WAN consolidates networking and security tools and eliminates the complexity of disaggregated branch infrastructures. This not only secures traffic and reduces the organization's attack surface but it also simplifies operations for networking teams.

Secure SD-WAN to the cloud speeds application access and enables the use of a cloud provider's network as an inexpensive global SD-WAN backbone. Some cloud providers, including Microsoft with Azure Virtual WAN (vWAN) and AWS with Transit Gateway, offer a central, managed hub that allows the connection of various network resources across the cloud environment. Google lacks a similar service but does offer Google Cloud VPN Interconnect to establish secure connections between a Google Cloud VPC network and on-premises networks or other cloud providers' networks. However, none of these vendors offer tools for effectively securing cloud WAN traffic.

As with the other architectures, this diagram shows a FortiGate cluster in a virtual network fronted by a load balancer. VPN traffic can be forwarded to the public cloud and offloaded on the cloud provider's VPN gateway (depicted here). Or it can be offloaded on the FortiGate VM for higher throughput and vertical scaling. Traffic from the remote location is offloaded directly into the VPN gateway, which has a dedicated subnet and virtual network, and then routed directly into the transitive network.

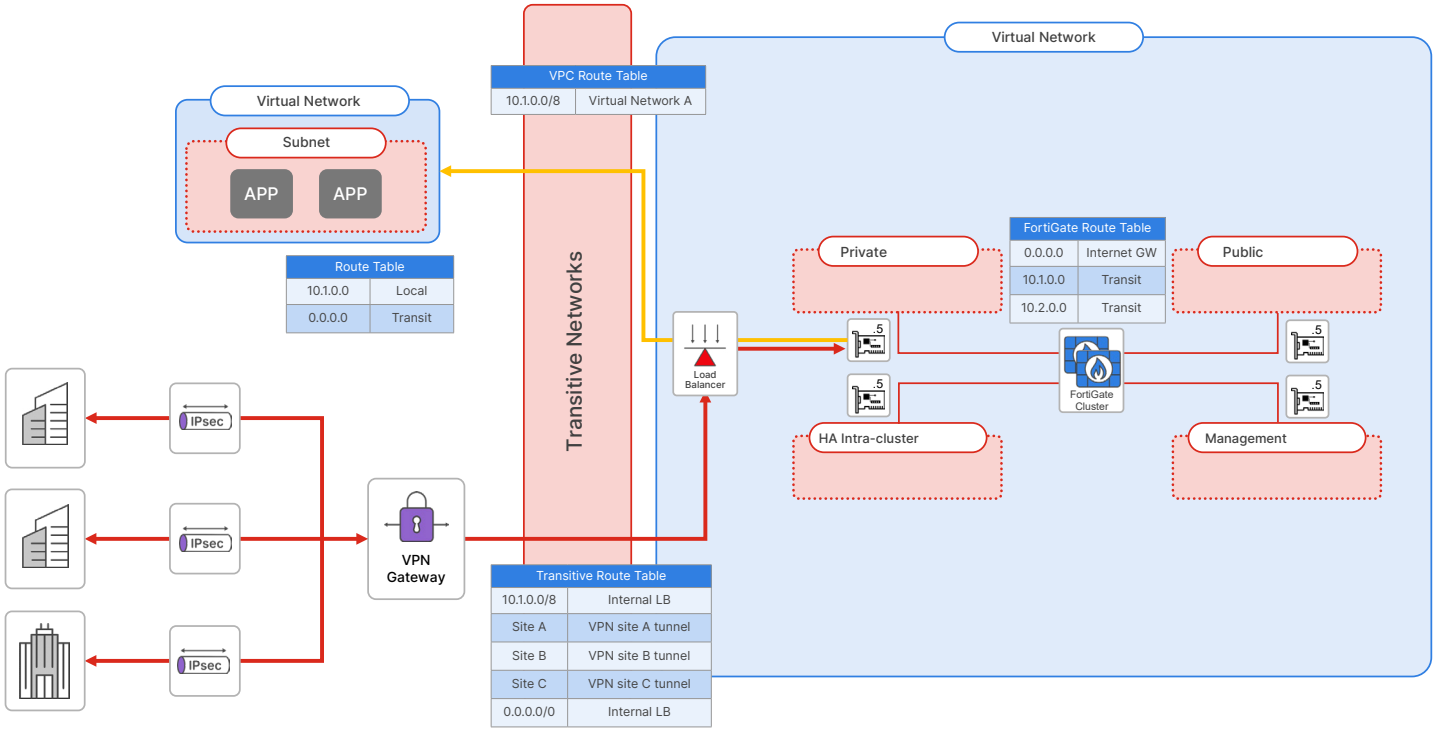

Figure 4: Cloud on-ramp reference architecture

Inbound traffic flow

- Traffic is sourced from the remote sites and routed to the VPN gateway. These provide filtering source and destination IP address ranges for security and BGP for dynamic routing propagation.
- The VPN gateways forward traffic to the transit network where the destination is referenced against the ingress route table for the target subnet whose next hop is the internal load balancer.
- The load balancer receives incoming traffic on its front-end private IP address and forwards the traffic to the target FortiGate VM based on a prescribed load-balancing method.
- FortiGate VM applies SNAT after traffic inspection and utilizes a route lookup to forward traffic to the destination VPC, which then sends the traffic back to the transitive network.
- The transit network performs a look-up on the applicable VPC route table and forwards traffic to the application VPC, where the virtual network router locally routes the traffic.

Return traffic flow

- To maintain symmetry, response traffic is routed in the reverse path in order.
- Traffic leaving the VPC uses a default route in the local subnet routing table and is forwarded via the Transitive route table to the FortiGate VM as the return path of the SNAT.

Four interfaces are used commonly in this design to provide multiple traffic flow-type support, where a dedicated public or untrust zone, private or trust zone, an out-of-band management interface, and a dedicated channel for session and cluster syncing are needed.

SDN Cloud Connectors

FortiOS, the FortiGate operating system and the backbone of the Fortinet Security Fabric, includes dedicated SDN connectors for all major public and private clouds. By using an SDN connector, you can ensure that changes to cloud environment attributes are automatically updated in the Security Fabric. You can use SDN connector address objects to create policies that provide dynamic access control based on cloud-environment attribute changes. With cloud connectors, there is no need to manually reconfigure addresses and policies whenever changes to the cloud environment occur. You will need to use the appropriate SDN connector for the architecture you are deploying.

Fortinet Services

FortiGuard AI-Powered Security Services provide industry-leading security capabilities for Fortinet products. They are offered a la carte and in bundles. Visit the FortiGuard AI-Powered Security Bundles for FortiGate page for more information.

The chart below highlights the FortiGuard AI-Powered Security Services that can be attached to the FortiGates protecting your cloud deployments. It is critical to match the service with the architecture.

SD-WAN and SASE services are available to help teams manage their SD-WAN and SASE deployments. And, FortiCare support services offer technical support and RMA services.

	Individual		Bundles		Ingress	Egress	EW	SD-WAN
FortiGuard Security Services	**A La Carte**	**Enterprise**	**UTP**	**ATP**				
Intrusion Prevention System (IPS)	✓	✓	✓	✓	✓	✓	✓	✓
Advanced Malware Protection (AMP)	✓	✓	✓	✓	✓	✓	✓	✓
Antivirus	✓	✓	✓	✓				
Anti-botnet	✓	✓	✓	✓				
Mobile Malware	✓	✓	✓	✓				
Outbreak Prevention	✓	✓	✓	✓				
Sandbox SaaS (detection only)	✓	✓	✓	✓				
AI-Based Inline Malware Prevention	✓	✓			✓	✓		
Web Security	✓	✓	✓		✓	✓		
Web and Content Filtering	✓	✓	✓					
Secure DNS Filtering	✓	✓	✓					
Video Filtering	✓	✓	✓					
Attack Surface Security Rating	✓	✓						
IoT Security	✓	✓						
Security Self-Check	✓	✓						
Inline SaaS Application Security (CASB)	✓	✓	✓	✓		✓		
Data Loss Prevention	✓	✓				✓		
OT Security*	✓				✓*	✓*		
OT Device Detection	✓							
OT Virtual Patching	✓							
OT Industrial Signature	✓							

	Individual		Bundles		Ingress	Egress	EW	SD-WAN
SD-WAN and SASE Services								
SD-WAN Underlay Bandwidth and Quality Monitoring	✓							✓
SD-WAN Overlay Orchestration Management	✓							✓
SD-WAN Connector for SASE Secure Private Access	✓							✓
SASE for FortiGate (including 10 Mbps)	✓							
FortiCare Support Services and Included Services								
Premium	✓	✓	✓	✓				
Elite	✓							

Figure 5: Mapping of services to cloud reference architectures

*The FortiGuard Operational Technology Security Service may be required depending on the nature of the systems to be protected. It provides specialized intrusion prevention system (IPS) signatures to detect and block malicious traffic targeting applications and devices in manufacturing, plant, safety, and other operational technology environments.

Conclusion

This white paper presents a few of the many ways FortiGates can be deployed in the cloud to deliver security and SD-WAN for specific use cases. These architectures, as presented, are cloud agnostic, and in theory, can be used in any public or private cloud deployment. However, there are specific integrations, including dedicated SDN connectors for all the leading clouds. They can be adapted to your particular environment and other security tools can easily be integrated. With Fortinet architectures, your teams can reduce risks and save time by leveraging proven expert-built templates. These architectures can be enhanced with the use of related Fortinet solutions such as FortiManager for central management and FortiAnalyzer for advanced analytics.

[1] Tomas Chamorro-Premuzic, "Human Error Drives Most Cyber Incidents. Could AI Help?" Harvard Business Review, May 3, 2023.

[2] Dan Daniels, "East-West Traffic: Everything You Need to Know," Gigamon, November 6, 2023.

June 26, 2024 1:51 PM / 2633718-0-0-EN