SOLUTION OVERVIEW

Deploy Your Preferred Security Solution across Multiple Clouds

Security service insertion from F5 Distributed Cloud Services simplifies the deployment and operation of F5 BIG-IP Advanced WAF across multi-cloud environments.

KEY BENEFITS

Simplicity and automation
Security service insertion in the F5 Distributed Cloud Platform eases complex cloud networking challenges through automated deployment and repeatable traffic-steering policies.

Enhanced security posture
Customers can leverage the powerful F5 BIG-IP Advanced WAF solution they use in their data centers for the cloud, and easily integrate them with native cloud networking constructs.

Improved productivity
SecOps, NetOps, and DevOps teams can collaborate on the same platform for enhanced situational awareness and accelerate projects with safe self-service.

Easy scale-out and load balancing
Active deployment of service instances allows effective load balancing of traffic with session awareness.

Built-in high availability
Mirror connection and persistence information to prevent interruption in service.

CI/CD Integration
The centralized controller in the Distributed Cloud Platform manages high availability for services by monitoring the health of the instances.

DEPLOYING SECURITY SOFTWARE IN THE PUBLIC CLOUD IS MORE COMPLICATED THAN DEPLOYING IT IN PRIVATE CLOUD AND ON-PREMISES ENVIRONMENTS.

Cloud Security Concerns Are Top of Mind for Many CIOs

Cybersecurity is the top priority of chief information officers in Gartner's most recent CIO survey,[1] with enterprises expected to have spent more than $150 billion on security and risk management solutions in 2021.[2] While this represented a 12% spending growth overall, cloud security was by far the leading growth segment, with a 41% spending increase over 2020.

In a separate 2021 survey of 372 IT pros in North America, 86% of respondents said they're already using multiple cloud providers. From that same survey, 93% said that cloud-native applications are being integrated into existing environments, resulting in security and compatibility challenges.[3]

Deploying security software in the public cloud—especially in multiple public clouds, which a sizable percentage of expanding companies are doing—is more complicated than deploying it in private cloud and on-premises environments. SecOps teams can vouch for this; they're the IT pros that install and configure the security solutions. NetOps teams are also impacted, as they must create policies to steer traffic through the security service.

Both deployments face the following challenges from the added complexity of public cloud:

- **Implementing security software in the public cloud is vastly different than in the private cloud.** Many enterprises want to expand their private cloud security solutions into the public cloud, but the virtualized infrastructure requires different skills and resources to accomplish this undertaking.
- **Public-cloud deployment varies by cloud provider.** Not only is public-cloud implementation different than a private cloud execution, but each public cloud—including Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, and others—has its own, unique deployment model. Learning one public cloud construct is significant, and learning multiple cloud constructs is an enormous task, especially when IT resources are limited.
- **Traffic-steering policies also vary by cloud provider.** Companies count on security solutions to inspect traffic and pinpoint or block suspicious activity. But in the cloud, it's not always straightforward to route virtual networks through security services. Traffic-steering rules can perform that rerouting, but creation and management differs from one cloud provider to another.
- **Public-cloud processes require collaboration between NetOps and SecOps teams.** They must work together to configure virtual networks, interfaces, security zones, and security policies, because security is an intrinsic aspect of public-cloud networking constructs.

KEY FEATURES

Manage Infrastructure as Code
Automate virtual network designs, configurations, and controls with intent-driven policies to manage Infrastructure as Code. Repeatable templates scale out across multiple regions in any major public or private cloud.

SaaS-based control plane and operations
Accomplish tasks faster using the SaaS-based controller and zero-touch service endpoints. Cross-functional analytics simplify maintenance and end-to-end service lifecycle management.

Granular and unified traffic-steering control
Deploy traffic-steering policies at the network or application layer, or both. Control traffic across one or more regions and cloud providers, rerouting network connections through the security service to assure coverage of cloud-hosted services.

Unified traffic observability
Achieve granular visibility and single-pane-of-glass management of security, applications, and network traffic across multiple clouds and networks, creating a consolidated source of truth.

Streamlined management of non-native security solutions
Automate the deployment and configuration of non-native services such as F5 BIG-IP Advanced WAF in public and/or private clouds, greatly simplifying the lifecycle for securing cloud-delivered services.

Enterprises seeking to ensure uniform security and visibility in the cloud should get to know security service insertion, a component of the F5 Distributed Cloud multi-cloud networking solution.

How F5 Ensures Consistent Security and Visibility in Your Public and Private Clouds

With security service insertion, companies can deploy the same F5® BIG-IP® Advanced WAF® solution in their public clouds that they do in their private cloud, with a simple and consistent deployment model and traffic-steering policy configuration.

Here's how F5® Distributed Cloud Services help to simplify and unify security solution deployments in multi-cloud and hybrid cloud environments:

1. **Ability to use Infrastructure as Code:** Implementation and policy configuration can be automated and run as Infrastructure as Code across clouds and regions, allowing policies to be repeatable in any major public or private cloud.
2. **Easy setup and management:** This simplified setup and management extends across AWS, Azure, and other clouds, as the F5 Distributed Cloud Platform automates deployment and configuration for F5 BIG-IP Advanced WAF, and supports AWS Transit Gateway, virtual network peering in Azure, and use of VPC attachments.
3. **Granular and unified traffic-steering rules:** With the Distributed Cloud Platform, traffic is rerouted from networks through the security service using the same steering rules across different public and private clouds. F5® Distributed Cloud Mesh enables users to define granular policies, both at the network layer and application layer, to control which traffic the security service inspects. Using F5® Distributed Cloud Console, IT pros get centralized granular visibility and single-pane-of-glass traffic management across clouds and networks.
4. **Self-service collaboration between NetOps, SecOps, and DevOps teams:** To increase agility, self-service can be enabled for app developers and DevOps, usually as a sub-tenant for virtual isolation from other projects. To assure compliance and control of those self-service configurations, NetOps and SecOps can create and apply intent-driven policies for networking and security. With this safe, self-service environment, project teams can make their own network and security changes at their own pace, without the risk of affecting other teams or operating without adequate security.

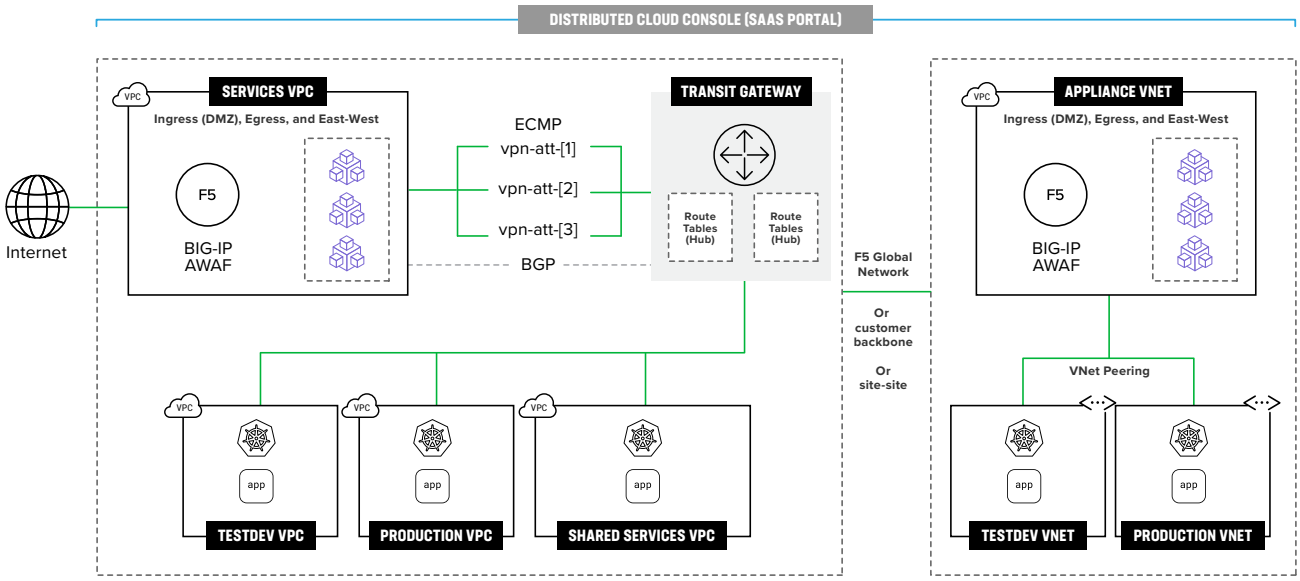

Figure 1: A schematic view of how the F5 Distributed Cloud Platform simplifies security service insertion and unifies operations.

Conclusion

Leveraging security service insertion from F5 Distributed Cloud Services can bring you several helpful outcomes:

WITH SECURITY SERVICE INSERTION, COMPANIES CAN DEPLOY SECURITY SERVICES FROM F5 BIG-IP IN THEIR PUBLIC CLOUDS AS THEY DO IN THEIR PRIVATE CLOUD.

- **Reduced operational complexity:** Simplifying the implementation of security services by automating steps and enabling repeatable policies will significantly increase the chances of a successful cloud migration.
- **Enhanced security posture:** Security professionals can leverage familiar solutions that give them better control and understanding and the confidence that they haven't left parts of the public cloud infrastructure uncovered.
- **Improved productivity:** All your IT teams—SecOps, NetOps, and DevOps—will see productivity gains from the automation and self-service technologies F5 Distributed Cloud Services provide.

F5 Distributed Cloud Services are SaaS-based security, networking, and application management services that can be deployed across multi-cloud, on-premises, and edge locations.

Sign up for a free trial or contact your local F5 representative for a demo and more details.

Appendix

[1] Gartner, "Gartner Survey of Nearly 2,000 CIOs Reveals Top Performing Enterprises are Prioritizing Digital Innovation During the Pandemic." Press Release, October 2020, found at https://www.gartner.com/en/newsroom/press-releases/2020-10-20-gartner-survey-of-nearly-2000-cios-reveals-top-performing-enterprises-are-prioritizing-digital-innovation-during-the-pandemic

[2] Gartner, "Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed $150 Billion in 2021." Press Release, May 2021, found at https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem

[3] "Distributed Cloud Series: Application Infrastructure Modernization Trends across Distributed Cloud Environments," Enterprise Strategy Group, December 2021, found at https://www.esg-global.com/research/esg-complete-survey-results-distributed-cloud-series-application-infrastructure-modernization-trends