Fortinet Cloud Security Talking Points

Overview

- Enterprise data centers are rapidly transforming into agile and elastic cloud infrastructure, spanning both on-premise private clouds as well as extending into public clouds such as Amazon Web Service (AWS) and Azure.
- Infrastructure technologies such as virtualization, software-defined networking (SDN) and cloud computing are shifting the mix of data center traffic from north-south in and out of the data center, to east-west traffic moving laterally, creating challenges with traditional firewalls or network security deployed high up at the edge or core.
- Organizations need to consider how to properly *scale* protection with their elastic workloads to minimize security gaps in these dynamic environments, as well as *segment* users, applications, and data within and across these increasingly consolidated cloud environments.
- A Software-Defined Security approach brings the same agility to security infrastructure itself, using new technologies such as virtual security appliances, orchestration and automation, and single pane-of-glass management.

Did you know?

- **Cloud adoption continues to grow at a rapid rate**
  - A RightScale survey found that private cloud adoption increased from 63% to 77% in 2016, and hybrid cloud adoption from 58% to 71%.
  - The same survey found that 17% of organizations now have over 1000 VM's running in public clouds
- **Security is the top issue with running workloads in the cloud**
  - Surveys of IT leaders have repeatedly ranked privacy and security a Top 3 concern with putting applications and data in the cloud, and in many case is the #1 issue
- **75% of data center traffic is now east-west**
  - Studies by IEEE and leading networking organizations have shown that about three-quarters of data center traffic today is east-west rather than traffic to/from the data center.
  - Inspecting all traffic thus requires about 4X the security inspection throughput compared to just inspecting WAN traffic at the edge, in addition to requiring security inspection to be placed deeper in the network.
- **Traditional physical firewall and security appliances have multiple challenges with inspecting traffic in cloud environments**
  - Physical appliances often cannot see east-west inter-VM traffic since it doesn't leave virtualization hosts and vswitches.
  - Public clouds don't allow tenants to bring physical network devices into the cloud.
  - Software-defined network flows can be logical, abstracted and dynamic, and independent ofphysical network topology and chokepoints used for network inspection

The Highlights

- Comprehensive security strategy across private, public, hybrid clouds
- Support for leading private cloud (virtualization and SDN) platforms including VMware NSX, Cisco ACI, and OpenStack, and leading public cloud platforms including AWS and Azure
- Cloud-ready multitenancy and virtual domain support for network segmentation
- Integrated single-pane-of-glass management for consistent policy control and monitoring
- Extensible management- APIs for cloud automation and orchestration
- Flexible billing and licensing options deliver the best economies of scale
- Unmatched breadth of security portfolio and flexible deployment options

Target customers

- Infrastructure and network security decision-makers in enterprises, who are looking to securely *scale* and *segment* their business with Private, Hybrid, and Public Cloud transformation of their data center

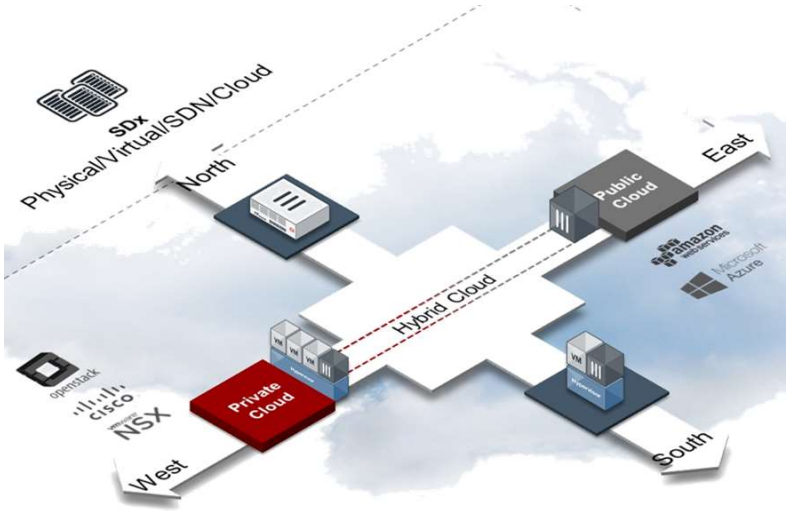
FORTINET®

Fortinet Cloud Security Talking Points

Key Resources

- Scale and Segment the Cloud - Whitepaper
- Protecting the Cloud – Solution Brief
- Securing Your Private and Hybrid Cloud – Whitepaper

Cloud Security Summary Diagram



Qualification Questions to Ask Customers and Prospects

1. Is your data center heavily virtualized or consolidated with VMware ESX/vSphere or another hypervisor? How are you ensuring visibility into all east-west inter-VM traffic? Do you face an increased concentration of data and therefore risk were a security breach to occur in heavily consolidated virntual environments?
2. Are you now augmenting virtualization with other software-defined technologies like SDN to increase your data center agility or elasticity? How do you ensure that software-defined network flows that are automatically provisioned are properly directed to a firewall or security appliance to be inspected, without slowing down your business with manual security configuration?
3. Is your organization now migrating some production workloads and applications in public clouds like AWS or Azure, and if so, how can you be assured that the application has the exact same security posture as it would running in your internal data center?
4. Do you need to ensure separation of certain sensitive data between VPN or other connection between you private or public cloud, for confidentiality or compliance reasons? How are you monitoring and inspecting hybrid cloud traffic?

Cloud Security Checklist

	Private Cloud	Public Cloud	Hybrid Cloud
Scale Protection	☒ automate service insertion and chaining of security appliances in virtual and software-defined networks ☒ auto-provision firewall and security rules to new web and app instances	☒ autoscale network security capacity with elastic workloads ☒ auto-provision firewall and security rules to new web and app instances	☒ provide site-to-site VPN connectivity to migrate workloads to provider clouds ☒ provide remote VPN access to administer workloads in the cloud
Segment End-to-End Traffic	☒ isolate applications and data in increasingly consolidated environments ☒ micro-segment increased east-west traffic in virtual and software-defined environments ☒ end-to-end segmentation between private cloud, campus and branch offices	☒ isolate applications and workloads ☒ ensure privacy and compliance in hosted provider environments	☒ segment persistent connections between private and public clouds ☒ inspect persistent traffic between clouds ☒ inspect for leakage of data between internal network and provider cloud

FORTINET®