



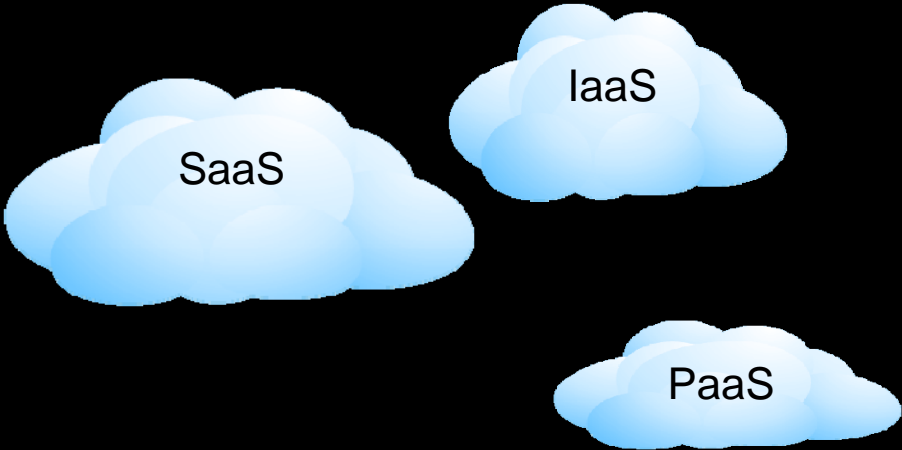
## Cloud Computing for the Government



**Daniel Kent**  
**Federal Solutions**  
**Cisco Systems Inc.**  
**dakent@cisco.com**

1

# Not all Clouds are the same



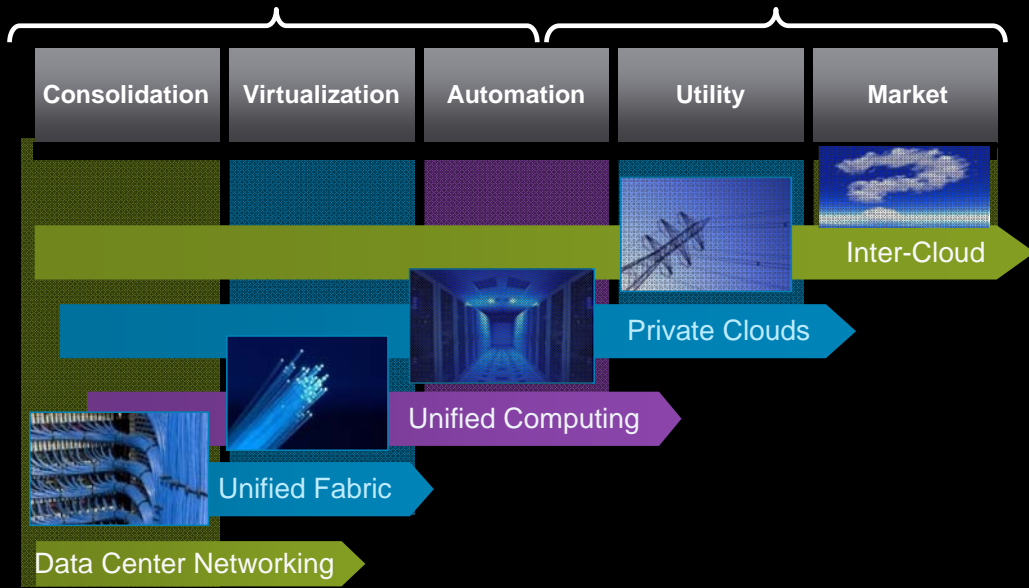
# Not all Clouds are the same:



# Data Center 3.0 → Cloud Computing

Virtualization

Cloud Computing



# Challenges in Virtualization & Building Clouds



## New Paradigm

- Virtual Machine is the New “Atomic Unit”
- Dynamic Movement of VMs / Applications
- New Options: VDI, Clouds, Workload Portability

## Infrastructure

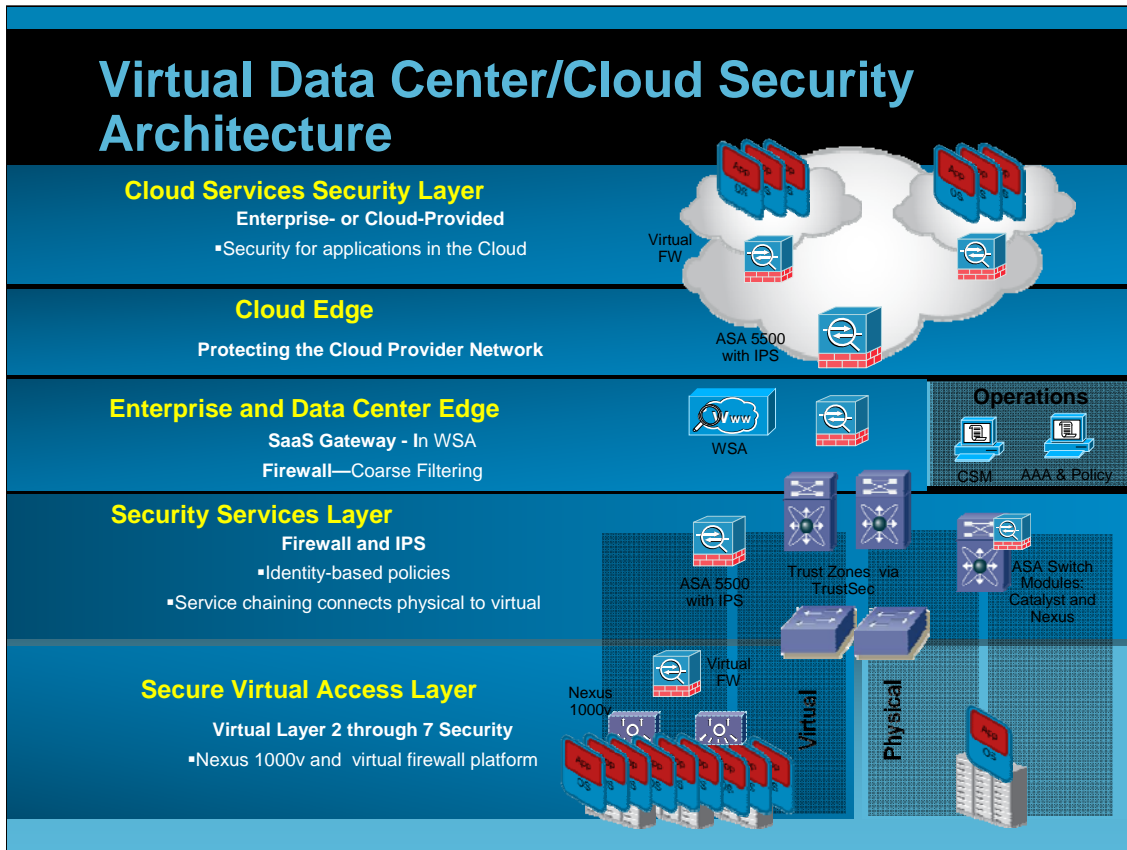
- Per-Virtual Machine services required
- Multi-Core CPU's, More I/O Bandwidth
- New emphasis on Security, Trust, QoS

## Organization

- Challenges Current Organizational Model
- Reduces Visibility into ‘Hidden’ Resources
- Requires Continuous Availability/Provisioning

5

- VM is the new “**atomic unit**” – applications no longer tied to a **single physical server**
- The infrastructure must provide **per-VM services** now – virtualization allows us to **fill the pipes** and therefore the network must support **more BW** per physical machine and **individual services per VM** (security, VLAN, VSAN, QoS)
- We are also challenged with our operational model, in that virtualization provides a new discipline that is integrated with OS, app, storage and network . It's no longer a matter of provisioning one aspect of the system and throwing a project over the fence to the next group, we have to work closer together to effectively provision the system.



We find the Secure Borderless Data Center Architecture of tomorrow.

This will include some additional items above and beyond today's requirements in the Enterprise.

First, you will see the emergence of the cloud itself as an important security layer to the Enterprise. The cloud is secured for the Enterprise by Cisco in two ways. (1) at the cloud edge itself with Firewall and IPS services being delivered to protect the cloud infrastructure itself. (2) in the Cloud Services Security Layer, in which cloud providers can provide both a virtual and physical footprint to customers of IaaS and PaaS services to protect the applications running in the cloud. This would be delivered in a virtual firewall and virtual context form in the ASA.

Secondly, we see the emergence of the Secure Virtual Access Layer. This layer in the data center grows out of the massive move from traditional deployments to virtualization in the DC. As the requirement for virtual security zones increases, the need for layer 2 through 7 security also emerges. This is where the virtual firewall becomes important, as the scale of the VMs grows larger and segmentation and security service needs grow with it.

Concurrently, the physical firewall will always play a role in the DC as there are many applications that will not be virtualized and continue to require an external, performance guaranteed solutions.