Securing Government Private and Community Clouds

At-A-Glance

Security Challenges for Private Clouds and Community Clouds

To confidently adopt private clouds and community clouds, government and other public sector customers need assurance that their data will remain confidential and isolated on shared compute, networking, and storage resources. Keeping each department's data secure in a multitenant environment requires technology and processes for:

- Identity management
- Data protection and integrity
- Data governance, including policy management and adherence to government restrictions on geographical reach of data

Identity Management

Whether the cloud is private, public, or shared by a community, service providers need to manage who and what can access the network, as well as when, where, and how access is permitted. Identity management requires enforcement, provisioning, and monitoring. Enforcement involves authenticating users and devices and then determining access privileges based on policy. Provisioning involves authorizing and controlling network access by pushing access policy to network devices and using VLANs, access control lists (ACLs), and other technologies. Monitoring requires tools for accounting, auditing, and forensics.

Cisco's Trust and Identity Management solutions meet these requirements by recruiting existing network devices into the overall security strategy. This approach enables cloud providers to secure network access and admission at any point in the network. Solution elements include:

- **Identity management services:** These services evaluate the integrity of every entity on the network and apply the appropriate access policy. They give the cloud provider visibility into network activity and enable secure centralized management of remote devices. The services also include Authentication, Authorization, and Accounting (AAA) for all network devices.
- **Identity-Based Networking Services (IBNS):** IBNS uses the IEEE 802.1X standard to identify users and route them to the VLAN with the appropriate access privileges, such as a guest VLAN. In addition, IBNS prevents users from accessing the cloud using unauthorized wireless access points.
- **Cisco® Network Admission Control (NAC):** Cisco NAC ensures that people can access the cloud service only if they are using a trusted endpoint. To accomplish this, Cisco NAC verifies the endpoint's compliance with network security policies, including current antivirus software, operating system patches, and application configuration. Cisco NAC can permit, deny, or restrict network access, and quarantine and remediate noncompliant devices.

Data Protection

Government cloud platforms need a robust mechanism to protect each tenant's data as it moves through the system. The need for data protection is especially important when the goals of cloud computing include higher utilization and greater density. Hardware eventually fails, and cloud providers need sophisticated software to prevent hardware failures from affecting data integrity. Virtualization for both network and security resources are extremely critical and it is important to leverage these technologies to provide isolated access and management across for each governmental agency.

Each cloud tenant's data must be kept separate on servers, on the network, and in storage:

- **Servers:** Server virtualization introduces new security challenges for secure access, firewall access, ACLs, and visibility. The Cisco Nexus® 1000V Switch addresses these challenges by providing policy-based security services to individual virtual machines. It also allows for control and visibility with virtual switching, virtual security, policy mobility (port profiles), and workflows that are maintained between network, security, server teams to drive policy into this environment. Network and security policies accompany a virtual machine as the administrator moves it to other servers in the data center using VMware VMotion. Administrators can also access security services and distribute them across virtual machines in the same or other servers using VPATH technology.
- **Storage:** Storage technologies from Cisco ecosystem partners allow the creation of separate and completely private logical partitions on a single storage system. Cloud providers have the option to delegate administrative control of the logical partition directly to the customer.
- **Network:** Cloud providers commonly use VLANs to logically segment and secure networks based on the department, workgroup, or application. To maintain the privacy of traffic traveling over the core network, the cloud provider can partition a single Cisco Nexus 7000 Series Switch into multiple virtual switches called virtual device contexts (VDCs). Each VDC has separate instances of Layer 2 and Layer 3 services. Other Cisco technologies that isolate each tenant's data on the network include:

- Virtual routing and forwarding (VRF)
- IP and MAC address–based ACLs
- Virtual firewalls
- Control Plane Policing (CoPP), which helps prevent unnecessary traffic from overwhelming the route processor

Data Governance

Data governance refers to the processes that cloud providers follow to be responsible stewards of data in a multitenant environment and to comply with regulations and certification mandates. Cloud providers need to set up systems and platforms to support regulations related to governance. They also need to establish governance policies throughout the data lifecycle, including creation and receipt, distribution (including geographical restrictions), use, maintenance, and disposition. Technologies that support governance are built into Cisco platforms and include:

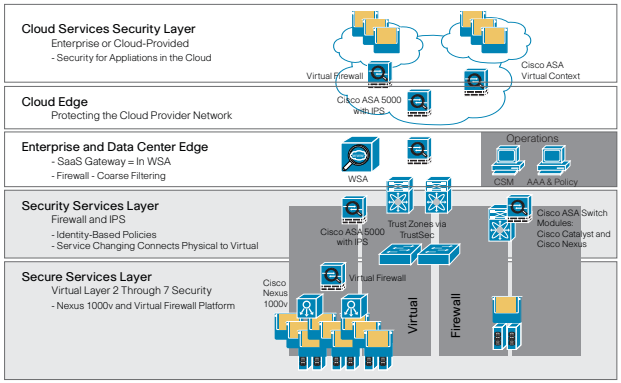
- Cisco NetFlow technology is integrated into all Cisco network devices, enabling monitoring and forensics.
- IEEE 802.1X and the Cisco TrustSec™ solution enable policy-based network access control, identity-aware networking, and data confidentiality and integrity.
- Cisco IronPort™ security management technologies provide centralized reporting, message tracking, and spam quarantine services.
- CiscoWorks Network Compliance Manager identifies and corrects trends that could lead to network instability or service interruption.

Cisco Advanced Services can work with government IT groups to collaboratively develop data governance processes and implement monitoring software.

Implementing Cloud Security

A secure cloud architecture requires certain security protections not required in traditional enterprise architectures (Figure 1).

Figure 1. A Secure Cloud Layered Architecture



Five layers of security are needed to secure private and community clouds:

- **Cloud services security layer:** To protect applications and services residing in the cloud, each tenant needs a virtual firewall. A single Cisco ASA Adaptive Security Appliance acts as a services node and can be partitioned into multiple virtual firewalls called security contexts. The services node, inserted between the physical network and the virtual networks in the cloud, gives each tenant one or more separate security contexts for VLANs, VRF, and firewall services.
- **Cloud edge:** To protect and secure the cloud service provider network and the cloud infrastructure, providers need firewall technologies, intrusion detection systems (IDSs), and intrusion prevention systems (IPSs) at the cloud edge.
- **Enterprise and data center edge:** This layer protects the cloud from threats originating from applications or the web. The Cisco IronPort S-Series Web Security Appliance (WSA) acts as a secure web gateway or software-as-a-service (SaaS) gateway, combining acceptable-use-policy (AUP) controls, reputation filtering, malware filtering, data security, and application visibility and control.
- **Security services layer:** Like traditional IT infrastructures, cloud architectures need physical firewalls, IDSs, and IPSs. Cloud architectures still need physical firewalls because certain applications cannot be virtualized.
- **Secure virtual access layer:** Securing the virtual access layer requires Layer 2 through 7 security, especially as agencies virtualize more applications. Technologies to secure the virtual machine environment include a hardened OS layer, hypervisor layer security, VMware VMsafe, and the Cisco Nexus 1000V Switch. In addition, Cisco Nexus 7000 Series Switches use VDCs and VRF to isolate each tenant's data as it travels through the cloud.

For more information about Cisco cloud security, visit http://www.cisco.com/go/cloud.

C45-617006 08/10