Chapter 4: Cloud Security

Topics covered:

4.1 Security element in the cloud
4.2 Authentication, Authorization and Accounting
4.3 Security risk for the virtualised environment
4.4 Identity management
4.5 Privacy, compliance and safeguard
4.6 Private cloud components
4.7 Risk to connect to a public cloud
4.8 VMware vCloud Networking and Security
1. Security element in the cloud

Threat in the Cloud: Cloud computing can be unsecure which makes it a scapegoat for any failed security measure. But cloud computing can become very secure no matter the architecture or the type used. It requires a strong governance framework.

The Solution: Security Governance Framework

A governance framework is essential for any concept of technology to succeed. The cloud computing security governance framework must do the following things.

- **Educate your workforce.** Educate internal users. Let them know where is the danger and what can or cannot be done when they use the network. Make them comply with the rules and regulation.

- **Audit compliance.** Use an audit tool which can view the organization’s vulnerabilities across the board giving security administrators a single overview.

- **Employ Identity and Access Management (IAM).**
  
  Ability to keep track of people who have access to sensitive data

  Prevents breaches and attacks from internal sources

  Paired with a data logging solution. Logging allows administrators to know who does what, when and where; All changes are logged and audited properly.

- **Employ Security Information and Event Management (SIEM).**

  Organization must integrate its access management so as to have a complete view of where the organization stands in terms of security.

- **Look for guidance but ensure your own security.**

  European Network and Information Security Agency (ENISA) and the Cloud Security Alliance (CSA) can be a reference for security guidance. But Organizations must form their own way of securing their cloud depending on their needs.

A governance framework is essential for cloud computing. All organizations need a security governance framework for any cloud infrastructure

Cloud security will have to be based on ‘Internet-routable’ protocols. But standardization between the different Cloud component infrastructure and service providers does not yet exist.

The 3 security cornerstones of IP based network management and policy administration are:

- **Authentication** - the process where someone’s or something’s *identity is authenticated* (verified to be true); examples are a digital certificate, a password and user-id or a security token.

- **Authorization** - determines whether a particular entity is authorized for the requested action; eg, is Tom authorized to access restricted data?
  - time restrictions prevent people from logging into the system outside office hours; Is Tom allowed to go into the office between 12am and 6am?

- **Accounting** - *tracking of resource usage by users*, Who uses what are monitored and tracked. Eg, who used the printer, scanner, photocopy machines, etc.
  These information can be used as part of an audit trail, costing or billing, or capacity monitoring.
**RADIUS**

RADIUS stands for ‘Remote Authentication Dial In User Service’.  

a. It is a networking protocol.  
b. It provides centralized access, authorization and accounting management for people or computers to connect and use a network service.  
c. It determines what rights or privileges the person or computer is "Authorized" to perform.  
d. It makes a record of this access in the "Accounting" feature of the server.

### The process:

a. The user or machine sends a request to a Network Access Server (NAS) to gain access to a network resource using access credentials.  

b. The credentials are passed to the NAS device via the link-layer protocol.  

c. The NAS sends a RADIUS Access Request message to the RADIUS server, requesting authorization to grant access via the RADIUS protocol. This request includes access credentials, in the form of **username** and **password**. The RADIUS server checks that the information is correct using authentication schemes.  

In the past, RADIUS servers checked the user's information against a locally stored flat file database. Today, RADIUS servers can do this, or can refer to external sources - commonly SQL, Kerberos, LDAP, or Active Directory servers - to verify the user's credentials.
d. The RADIUS server returns one of three responses to the NAS:
- "Nay" (Access Reject)
- "Challenge" (Access Challenge) or
- "Yea" (Access Accept).

3: Security risks for the virtualized environment
The top threats to Cloud computing according to the CSA are,

a. Data loss/leakage:
   • Data in the Cloud has many advantages, but can be compromised in many
     ways. It can be altered or deleted without a backup; it may be unlinked from
     its context or accessed by unauthorized people.

b. Shared technology vulnerabilities:
   • A multi-tenant architecture has its own challenges. Some components may
     not have been developed for this type of use and may cause security issues.

c. Insecure application interfaces:
   • Application interfaces, or APIs, if not properly designed for security can
     become a risk 'waiting to happen'.

d. Malicious insiders:
   • Cloud providers, some of their staff or sub-contractor staff may be
     untrustworthy.

e. Abuse and improper use of Cloud computing:
   • Many Cloud providers give anonymous free trial period access to their
     services. It will attract 'darker customers' like spammers and hackers. Your
     Cloud provider may not only host your data and applications, but also
     malicious software.

f. Account, Service and traffic hijacking:
   • Most private users of E-mail and the Internet will be aware of fraudulent
     tactics like phishing, password hacking and identity theft. Passwords giving
     access to Cloud services go outside your own company IT domain, and
     therefore can be compromised. For businesses this can mean they are
     vulnerable to industrial espionage or can lose important business data or
     processes.

Measures mitigating security risks
An objective way to ensure a provider’s compliance with security best practices is to
demand ISO certification like:

ISO/IEC 20000:2011, Information Technology-Service management part 1
Service management system requirement

Information Security management system requirement

Code of practice for Information Security management

Mitigating Measures

1. Data loss/leakage > *Engage authentication, audit* (i.e. ISO/IEC 27001, Data Security) and *authorization*, as well as the use of *encryption and a proper backup strategy*.

2. Shared technology vulnerabilities > *enhanced operations procedures for monitoring and escalations* upon security breaches and *adoption of good security practice during installation, configuration and application of patches*.

3. Insecure application interfaces > *designing for security, proper testing methods*, understanding how they interact with other interfaces and software and strong authentication and access control.

4. Malicious insiders > *good HR vetting procedures*, strong information security policies and procedures.

5. Abuse and improper use of Cloud computing > *validation of credentials, increased monitoring of traffic* between customers and known suspicious sites.

6. Account, service and traffic hijacking> *strong authentication techniques and monitoring of user behaviour*. 
4 Identity management

Organizations need proper identity control and access governance on file, Database and applications. There are several identity management solutions available like Microsoft’s Forefront platform and IBM’s Tivoli platform.

Typical characteristics of an Identity management system are:
- Role management; IT implementation of a business role.
- Role hierarchy; a representation of an organization chart.
- Separation of duties.
- Group management; permissions are not given to people but to roles.
- Self-service functions.
- Password synchronization
- Digital Identity; presence and location determine available services and capabilities.
- Federation Identity Management; enables single sign-on

Two examples of identity management solutions are:
- a. single sign-on (SSO) and
- b. a special type of SSO called Federation Identity Management.

a. SSO Single Sign-on

As Cloud infrastructure is distributed, security features and algorithms are spread all over a certain domain. Single Sign On (SSO) principle is the solution. All distributed security elements are consolidated on one SSO-server.

Users only need to sign on once, using a security measure like a smart-card, a security token or an active directory (AD) account. The SSO architecture uses the SOAP protocol, a protocol for the exchange of information in the implementation of Web Services in the Cloud or any other network.

SSO System Components are:
- a Credential database
- a master secret server, and
- one or more Single Sign-On servers.

The SSO system contains a system or sub-system such as a host, back-end system, or line-of-business application to which you are connecting using Enterprise Single Sign-On.

Each affiliate application has multiple user mappings; for example, it has the mappings between the credentials for a user in Active Directory and their corresponding RACF credentials.

The Credential database is the SQL Server database that stores the information about the affiliate applications, as well as all the encrypted user credentials to all the affiliate applications.
The master secret server is the Enterprise Single Sign-On server that stores the master secret. All other Single Sign-On servers in the system obtain the master secret from the master secret server.

The SSO system also contains one or more SSO servers. These servers do the mapping between the Windows and back-end credentials and look up the credentials in the Credential database. Administrators use them to maintain the SSO system.

**Federation Identity Management**

The goal of identity federation is to enable users of one domain to securely access data or systems of another domain seamlessly, without the need for redundant user administration.

It can be based on "user-controlled" or "user-centric" scenarios, as well as enterprise controlled or Business to Business (B2B) scenarios.

Federation is enabled through the use of open industry standards and/or openly published specifications, such that multiple parties can achieve interoperability for common use cases. Typical use-cases involve things such as cross-domain, web-based single sign-on, cross-domain user account provisioning, cross-domain entitlement management and cross-domain user attribute exchange.

**5: Privacy, compliance and safeguards**

Personally Identifiable Information (PII), is information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

Examples:

- Types of identification: SSN, passport, fingerprints, iris-scans
- Occupational: job title, company name
- Financial: bank numbers, credit records, PIN-number
- Health care: insurance, genetic
- Online activity: log-ins
- Demographic: ethnicity
- Contact: phone, email, social media accounts, address

**Good** safeguards need to be put in place in a Cloud environment, including,

- Access Control and Audit (e.g. Single Sign On (SSO)),
- strong authentication: password & biometric measure and review of audit logs.

Secure Cloud Storage requires encryption and Integrity control by mechanisms as hashing. A secure Network Infrastructure uses encryption protocols against leakage and Integrity protocols (digital signatures) against modification.
Lesson 6: Private Cloud components

The private cloud features a layered architecture. This is where virtualization abstracts operating systems, data, applications, and user state from the underlying hardware. This layer enables a wide range of automation and management capabilities that differentiate a cloud infrastructure from a highly virtualized LAN.

Virtualization de-couples operating systems, data, and applications from the underlying hardware. This abstraction powers elements that define an elastic cloud infrastructure, and also the 5 layers:

- Automation
- Management
- Orchestration
- Services Management
- Self Service
The Automation Layer

The automation layer is made up of the foundational automation technology plus a series of single-purpose commands and scripts. Operations performed are

- starting or stopping a virtual machine (VM),
- rebooting a server, or
- applying a software update.

These atomic units of automation are combined and executed by higher-level management systems. The modularity of this layered approach dramatically simplifies development, debugging, and maintenance.

The Management Layer

The management layer consists of tool sets for managing hardware, software, and applications. It is used to perform activities such as

- provisioning the storage area network (SAN),
- deploying an operating system, or
- monitoring an application.

A key attribute is its abilities to manage and monitor every single component of the infrastructure remotely, and to capture the dependencies among all of the infrastructure components.

The Orchestration Layer

- The orchestration layer takes advantage of the management and automation layers.
- It provides an engine for IT-process automation and workflow. This is where events and activities are transformed into workflow and automation.
- It provides a graphical interface in which complex workflows can be combined to form an end-to-end IT business process. Some processes are automated patch management or automatic power management.
- It must provide the ability to design, test, implement, and monitor these IT workflows.

The Services Management Layer

- The Service Management layer provides the means for automating and adapting IT service management best practices.
- It provides built-in processes for incident resolution, problem resolution, and change control.
- It provides an integrated service management platform IT to reduce costly downtime and improve the quality of the services in the data centre.
The Self-Service Layer

The Self-Service layer provides an interface for private cloud tenants or authorized users to request, manage, and access the services, such as virtual machines.

Role-based access control and authorization provides the ability to delegate certain aspects of the administration (such as starting/stoping VMs) to designated “tenant administrators.”

7: Risk of connecting a private cloud to a public cloud

When a private cloud joins a public cloud, it forms the hybrid cloud. A hybrid cloud,
- offers better economics and business agility
- Organizations can take advantage of public clouds to reduce capital expenditure (capex) while still keeping their mission-critical workloads inside the organization.

But hybrid clouds have the largest attack surface. Businesses must deploy security across both the private and public cloud elements.

Five Security Best Practices for hybrid clouds are:

1. **VM-level security:** Self-defending security at the virtual machine level that travels through the on-premise data centre, in the cloud and between multiple cloud providers.

2. **Multi-layered defence:** Defence of virtual machines with tools like firewall, IDS/IPS, log inspection, etc. The traffic between the virtual machines should be continuously monitored by setting policies.

3. **Traffic control:** An on-premise gateway should be used to control incoming traffic to the public cloud rather than provide direct access.

4. **Data and encryption:** Data in the cloud should be encrypted. An encryption solution should have well-designed encryption key management policies to ensure data integrity.

5. **Security control:** Cloud security should be controlled by the business and not the cloud vendor. It can be done using a single sign-on or by using a third-party tool to securely extend the perimeter to the public cloud. The control over security should be with the business organization deploying the hybrid environment.
8: VMware vCloud Networking and Security Software

VMware vCloud® Networking and Security is the leading networking and security solution that enhances operational efficiency.

It provides a broad range of services in a single solution, including virtual firewall, VPN load balancing and VXLAN extended networks.

Management integration with VMware vCenter™ and vCloud Director™,
- reduces the cost and complexity of datacenter operations and
- unlocks the operational efficiency and agility of virtual datacenters and private cloud deployments.

VMware vCloud Networking and Security solves these datacenter challenges by virtualizing networks and security to create efficient, agile, extensible logical constructs that meet the performance and scale requirements of virtualized datacenters.
Key Features of vCloud Networking and Security

• **Edge**
This virtual appliance includes services such as firewall, network address translation (NAT), load balancing and VPN. Edge High Availability protects against network, host and software failures.

• **App Firewall**
Protects and isolates critical applications with security applied immediately to surround a virtual machine. vCenter integration enables robust isolation while enhancing operational efficiency.

• **VXLAN**
This software enables technology for network virtualization, providing network abstraction, elasticity and scale across the datacenter. VXLAN provides an architecture for scaling your applications across clusters and pods without any physical network reconfiguration.

• **Management and Reporting**
VMware vCenter Server™ and vCloud Director, provides a central point of control for deploying, managing, reporting, logging, and integrating security and gateway services. This is done seamlessly. Role-based access control enables separation of duties and compliance.

• **vCloud Ecosystem Framework**
Integrates partner services at either the virtual network interface card (vNIC) or virtual edge through REST APIs. vCloud Networking and Security improves operational efficiency and optimizes resource utilization, enabling you to reduce costs. It increases IT agility and flexibility by simplifying operations while also extending the platform to include third-party networking and security services.

**Key Benefits**

• Efficiently manages compute resources across cluster and subnet boundaries.

• Scales and moves virtual workloads without physical network or security constraints or the need for specialized appliances.

• Enables integration of third-party network and security solutions through open architecture and standard APIs.

• Streamlines operations through vCenter and vCloud Director integration.

• Provides scalable networking and security while
How It Is Used
vCloud Networking and Security is typically used in the following scenarios.

• Protect and isolate critical applications with adaptive security groups.

• Move security dynamically with the workload for continuous protection and compliance. (When the VM move from one host to another, the security setting follows the VM)

• Increase visibility and control over inter–virtual machine communications. Build an Agile and Trusted Private Cloud Infrastructure

• Secure the edge of the virtual datacenter with the integrated firewall, load balancer and VPN.

• Reduce manual networking provisioning and simplify deployment.

• Optimize management and consumption of compute resources across physical network boundaries. Secure VMware View Virtual Desktop Deployments

• Limit network access for remote or third-party users, and protect sensitive data from unauthorized staff or hackers.

• Limit the spread of malware among virtual machines.

VMware vCloud Networking and Security
How Does It Work?
vCloud Networking and Security abstracts networking and security into a
generalized pool of capacity. It separates the consumption of these services from the
underlying physical infrastructure.

This unified pool of network capacity can be optimally segmented into logical
networks to support specific applications. When the network is associated with an
application, it can move, grow or shrink along with it.

VXLAN networks can span physical boundaries. This optimizes compute resource
utilization across clusters and pods. Because logical networks are decoupled from
physical topology, you can scale VXLAN networks without reconfiguring the
underlying physical hardware. This solves the problem of time-consuming planning
for VLAN provisioning and managing VLAN sprawl.

Greater visibility into traffic flows makes security more effective. As the application is
moved or scaled, it maintains effective internal isolation and perimeter security.

A central point of control for managing, deploying, reporting and logging, as well as
integrating third-party services. The result is simplified operations, efficient resource
utilization and greater agility to scale in response to business needs. This is all
delivered through an integrated and extensible platform
vCloud Networking and Security - Installing vShield Manager 5.1

vShield Manager 5.1:

has been named vCloud Networking and Security
provides firewall protection, traffic analysis, and network perimeter services to
protect your vCenter Server virtual infrastructure.

vShield Manager is the centralized management component of vShield. vShield
Manager is used to monitor and push configurations to vShield App, vShield
Endpoint, and vShield Edge instances. vShield Manager is a virtual appliance
deployed as an OVA file downloaded from VMware.

Once you have installed vShield Manager and linked it to vCenter Server you will
see vCloud Networking and Security appears under the licensing section (which
used to show 3 separate products vShield App, vShield Edge and vShield Endpoint).

1. Download vShield Manager 5.1

2. Import the OVF template into vCenter, Connect to vCenter with vSphere client.
   Select File --> Deploy OVF Template

3. Browse to the path where the OVA file for vShield manager was downloaded to
   Click Next
4. Read and Accept the license agreement
5. Enter a VM name for the vShield Manager VM

Select the datacenter and folder to deploy to, Click Next.
6. Select the Host and Cluster to deploy to

7. Select the datastore to store the VM and click Next
1. Select to Thin or Thick provision the VM storage. This example is using Thin provisioning.

9. Map the network that will be used to manage the vShield Manager VM
10. Review the settings

Tick power on after deployment and Click Finish.

11. You will see a progress dialog and task while the VM is being deployed
12. After the vShield Manager VM has been deployed it will automatically power on (if you ticked the box)

Open a console to the VM and you will see it boot up

13. Login to the vShield Manager with the default username and password

Username: admin

Password: default

14. Enter enable mode, type setup and configure the network settings

15. Type "enable" and hit enter

16. Re-enter the admin password "default"

17. Type "setup" and hit enter

18. Enter the management network settings

(IP address, mask, gateway, DNS and search domain)

Save the new configuration with "y" enter
19. Now open Internet Explorer and browse to the IP you just set e.g.

https://123.123.123.123

Login with the same credentials

Username: admin

Password: default
20. This is the admin interface of vShield Manager (you can also get to it from vSphere client once vCenter server is register)

First configure vShield Manager to register with a vCenter server

Ensure you are under "Settings and Reports"

21. Click the "Configuration" tab

22. Click "Edit" next to vCenter Server,

if you are using vCenter 5.1 you need to use the lookup service. For vCenter Server 5.0 you dont need to/cant use the lookup service for SSO.
23. Enter the vCenter server FQDN and username/password

24. Now the vCenter server will show in the configuration tab
25. Click "Change Password" in the top right of the screen and set a new password for the admin user

![Change Password dialog box]

26. Now click "Backups" under "Configuration"

Setup a backup job for vShield Manager
27. Now open vSphere client and login to vCenter

You will see a vShield Manager icon under Solutions and Applications
28. In the Licensing section of vSphere you will notice vCloud Networking and Security. Add your license key now otherwise it will continue to run in evaluation mode which will expire.

29. Thats vShield Manager deployed! If you click on the datacenter or cluster objects you will see a "vShield" tab like below. This shows information on if vShield endpoint, App is deployed here, they can also be configure from here. The configuration of these will be covered in a separate article.