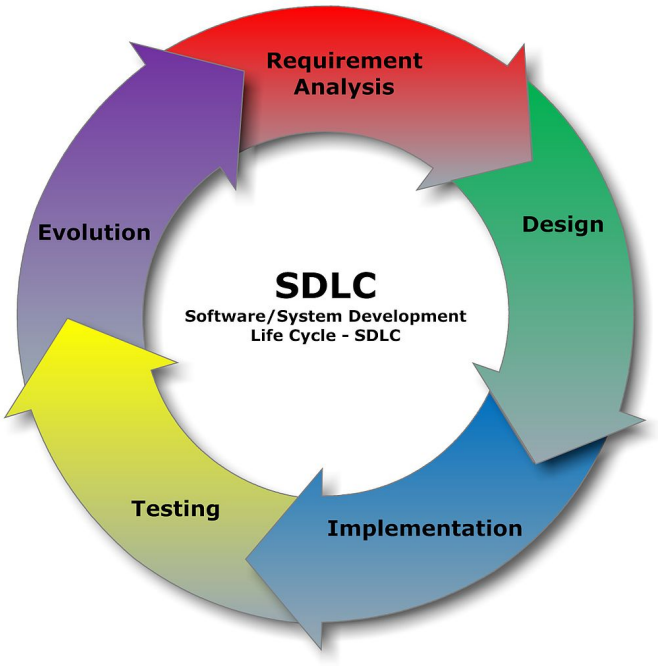
SEENPAY

Seen it, and pay it

Department of IT Development

SYSTEM DEVELOPMENT LIFE CYCLE (SDLC) PLANNING

Third Revision
1st of June 2015



INDEX

About the Team

Team Leader

Zen Le

IT Team Leader

Slack: #zenle311

Team Member

Huy Le

Founder/Project Leader

Slack: #huyle

Jimmy Vo

Database and Hardware

Slack: #truongthinh1987

Phuc Le

IT Advisor

Slack: #phuclt2710

Channel of Communication

Download

- **Apple AppStore**:

  https://itunes.apple.com/au/app/slack/id803453959?mt=12

- **Google Play**:

  https://play.google.com/store/apps/details?id=com.Slack&hl=en

- **Webpage**:

  https://slack.com

Team Address

SeenPay.com

Team Channel

#tech-team

Recommend Developer Tool

Browser

- Google Chrome
- Apple Safari

Coding

- Adobe Dreamweaver CS6 or above
- Notepad++
- PHPStorm

Communication

- Slark Mobile Application
- Facebook Messenger
- Google Hangouts

Database

- MySQL
- Microsoft SQL Server

Design

- Adobe Photoshop CS6 or above
- Adobe Illustration
- JustInMind Prototype

Documentation

- Microsoft Office 2003 or above

Networking

- Cisco Packet Tracer

Server Hosting

- Xampp Apache + MySQL + PHP + Perl (local hosting)

Current mission

- Complete Interaction Diagram between B2C & C2C using Lucid Chart
- Complete Network Hardware planning
- Complete Network Topology using Diagram or Cisco Packet Tracer
- Complete Network Topology configuration in Cisco Packet Tracer

Proposal

Dell PowerEdge T20 Mini-tower Server System

Overview

What it use for?

- Webpage testing
- Hosting testing
- Intranet testing
- VPN testing
- Data Storage

Back view

Side view

Specification

MAIN

Brand	DELL
Series	PowerEdge T20
Model	462-0993
Type	Mini-tower

PROCESSOR

CPU Type	Intel Xeon E3-1225 v3 3.2GHz
Cache Memory	8MB L3 Cache
CPU Features	Quad-core Processor Max Turbo Frequency 3.6GHz
MAX Processors	1

MEMORY

Installed Memory Type	2 x 4GB
Memory Type	DDR3 1600
Memory Features	Dual Ranked UDIMM

STORAGE

Hard Drive (Installed)	2 x 1TB 7200RPM
Storage Controller	Onboard SATA, HDD connected to onboard SATA Controller
HDD Interface	SATA
Raid Level	No RAID
Media Drives	No Internal Optical Drive

EXPANSION

Other Ports	Up to 12 USB (four USB 3.0) ports

SOFTWARE

Software	No

FEATURES

Features	1 Year Basic Hardware Warranty Repair: 5x10 HW-Only, 5x10 NBD Parts

Estimate Price: 667.48 USD*

**base on dell.com*

Synology DiskStation DS214play 2-Bay NAS Server

What it use for?

- Cloud Data Testing
- Automatic Backup testing
- Data Storage

Specification

Hardware Specification

CPU Frequency	Dual Core 1.6 GHz
Floating Point	Yes
Hardware Transcoder	H.264 (AVC), MPEG-4 Part 2, MPEG-2, VC-1

Memory

System Memory	1 GB DDR3

Storage

Drive Bays	2
Drive Type	3.5" SATA(III) / SATA(II) HDD 2.5" SATA(III) / SATA(II) HDD 2.5" SATA(III) / SATA(II) SSD
Max Internal Capacity	12 TB (6 TB HDD X 2) (Capacity may vary by RAID types)
Hot Swap Support	Yes

External Ports

USB 2.0 Port	1
USB 3.0 Port	2
eSATA Port	1
LAN Ports	1 x Gigabit LAN (RJ45) port
SD Card Slot	Yes
USB/SD Copy	Yes

File System

Internal Drives	EXT4
External Drives	EXT4, EXT3, FAT, NTFS, HFS+

Other Specification

Wake on LAN/WAN	Yes
System Fan	1 x fan (92 x 92 mm)
Wireless Support	Yes (with optional wireless dongle)
Noise Level	19.8 dB(A)
Power Recovery	Yes
Power Supply	65 W
AC Input Power Voltage	100 V to 240 V AC
Power Frequency	50/60 HZ, single phase
Power Consumption	28.74 W (Access) 11.5 W (HDD hibernation)
Certifications	FCC Class B, CE Class B, BSMI Class B

Storage Management	Max File System Size: 16 TB Max Internal Volume Number: 256 Max iSCSI Target Number: 10 Max iSCSI LUN: 10 Supported RAID Type: Synology Hybrid RAID, Basic, JBOD, RAID 0, RAID 1
RAID Level Migration	Basic to RAID 1
Volume Expansion	With Larger HDDs: Synology Hybrid RAID, RAID 1 By Adding a HDD: Synology Hybrid RAID
File Sharing Capacity	Max User Accounts: 2,048 Max Groups: 256 Max Shared Folder: 256 Max Shared Folder Sync Tasks: 4 Max Concurrent CIFS/AFP/FTP Connections: 256 Windows Access Control List (ACL) Integration
Dimensions (HxWxD)	6.5 x 4.3 x 9.2" / 165 x 108 x 233.2 mm
Weight	2.789 lb / 1.265 kg

Environment Conditions

Operating Temperature	40 to 95°F / 5 to 35°C
Storage Temperature	15 to 155°F / -10 to 70°C
Relative Humidity	5 to 95%
Maximum Operating Altitude	6,500 ft / 1,981 m
RoHS Compliant	Yes

Estimate Price: 359.94 USD*

**Base on bhphotovideo.com*

Team Data Cloud Storage Explanation

Dropbox for Business

This will be main *cloud storage system* for the IT Department. Each IT members will have their own User Account.

Getting Your Account

Please contact IT Department or your Team Leader for account information.

Marketing & Business Department

Huy Le
Founder/Project Leader
Slack: #huyle

IT Department:

Zen Le
IT Team Leader
Slack: #zenle311

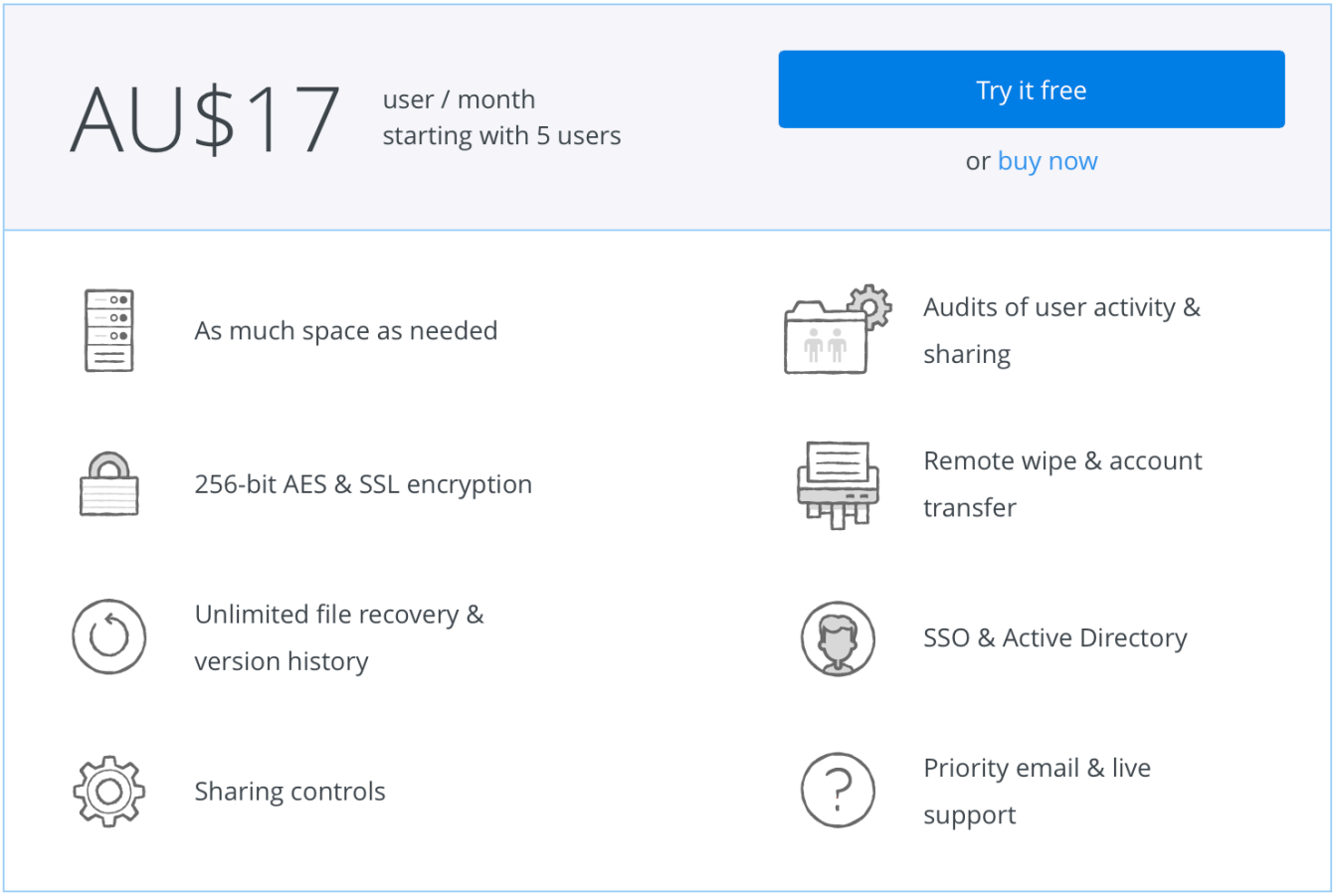
What does it use for?

Mostly *reports* and ***non-classified*** files

Example:

- Marketing Report
- User Growing Report
- Webpage template
- Coding irrelevant to page function (PHP, HTML, CSS, ASP.NET…)

Basic Feature



- Each user will have 1TB (1000 GB) of storage
- Dropbox offer 256-AES & SSL Encryption to ensure data protection and privacy
- File history will help to recover accidentally deleted files or modified files
- Dropbox will offer features to share file control (Read/Write/Execute)
- User action will be log with Dropbox activity log
- Data of user can be Remote Wipe and can transfer to another account
- SSO (Single Sign On) will make user only need to sign in one single time.
- Active Directory is a directory service that helps System determined whether login user is system administrator or normal user
- Live Support with Dropbox will be available with priority

Google Drive

A second base storage system in case Dropbox has problems

Getting Your Account

Please contact IT Department or your Team Leader for account information.

Marketing & Business Department

Huy Le
Founder/Project Leader
Slack: #huyle

IT Department:

Zen Le
IT Team Leader
Slack: #zenle311

What does it use for?

Mostly *reports* and ***non-classified*** files.

Furthermore, please make a backup of your important documents on Dropbox weekly using Google Drive to ensure 100% data availability.

Example:

- Marketing Report
- User Growing Report
- Webpage template
- Coding irrelevant to page function (PHP, HTML, CSS, ASP.NET…)

Network Attachment Storage (NAS)

This will be the second ***local and cloud storage system*** for Project members.

Getting Your Account

Please contact IT Department or your Team Leader for account information.

Please acknowledge that very few people have access to the NAS System as it contents top confidential files that will not affect working experiences of other members.

Marketing & Business Department

Huy Le
Founder/Project Leader
Slack: #huyle

IT Department:

Zen Le
IT Team Leader
Slack: #zenle311

What does it use for?

This will be used to store *backups*, *coding* and *data* that need **a very high level of confidential**. (TOP SECRET)

Example: (will be updated)

- User Login Database.
- User Banking Database.
- System Architecture Details.
- All data and coding that relevant to interaction between Bank system and SeenPay system.
- Security System Details.
- Security Bug Reports.
- Web Application bugs and Patches.

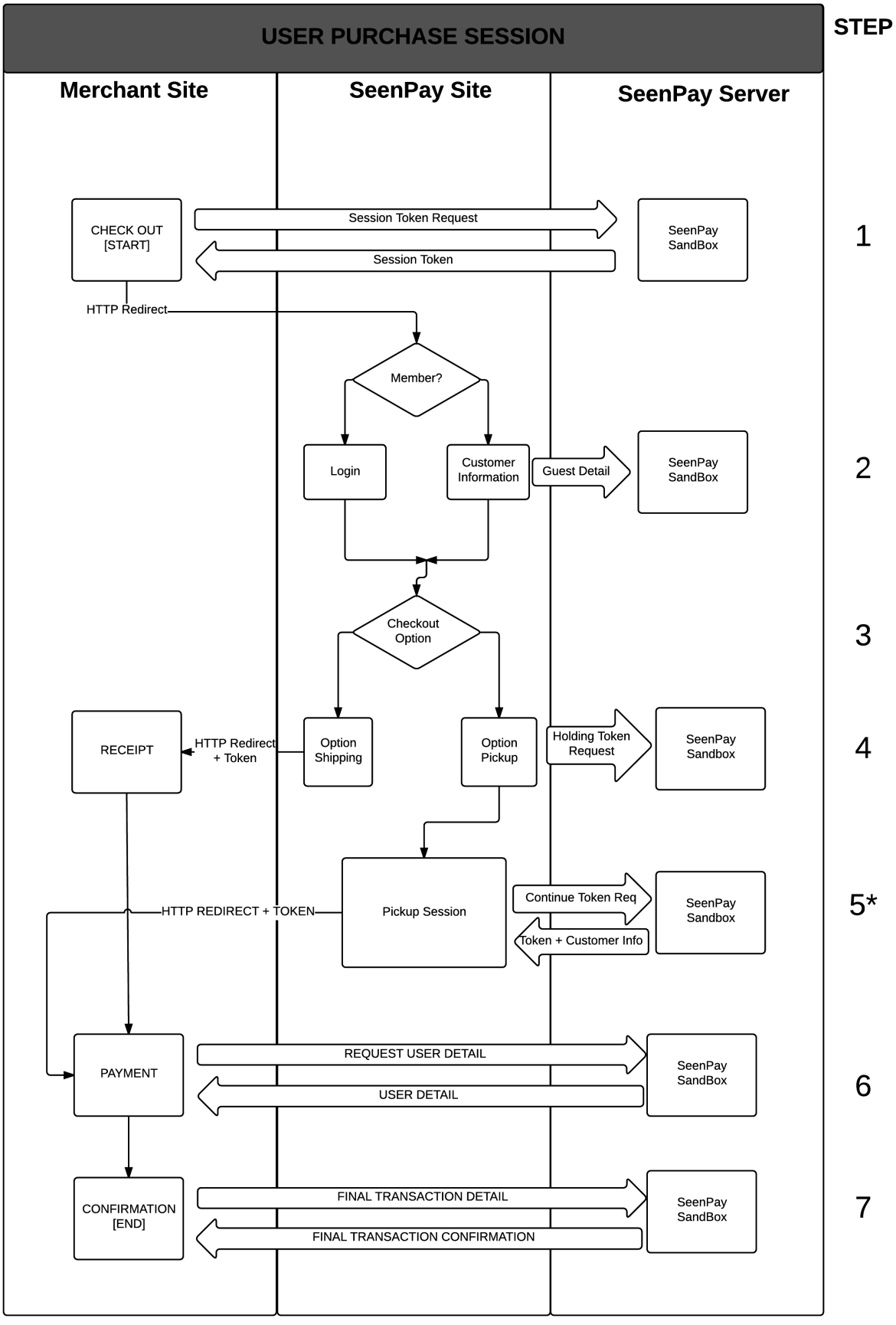
Basic Feature (will be updated)

- Windows Server 2012
- ~12TB of Storage
- Dedicated high-speed fibre cable
- Active Directory
- Folder Sharing and Permission
- Auto Backup
- Using RAID 1+0

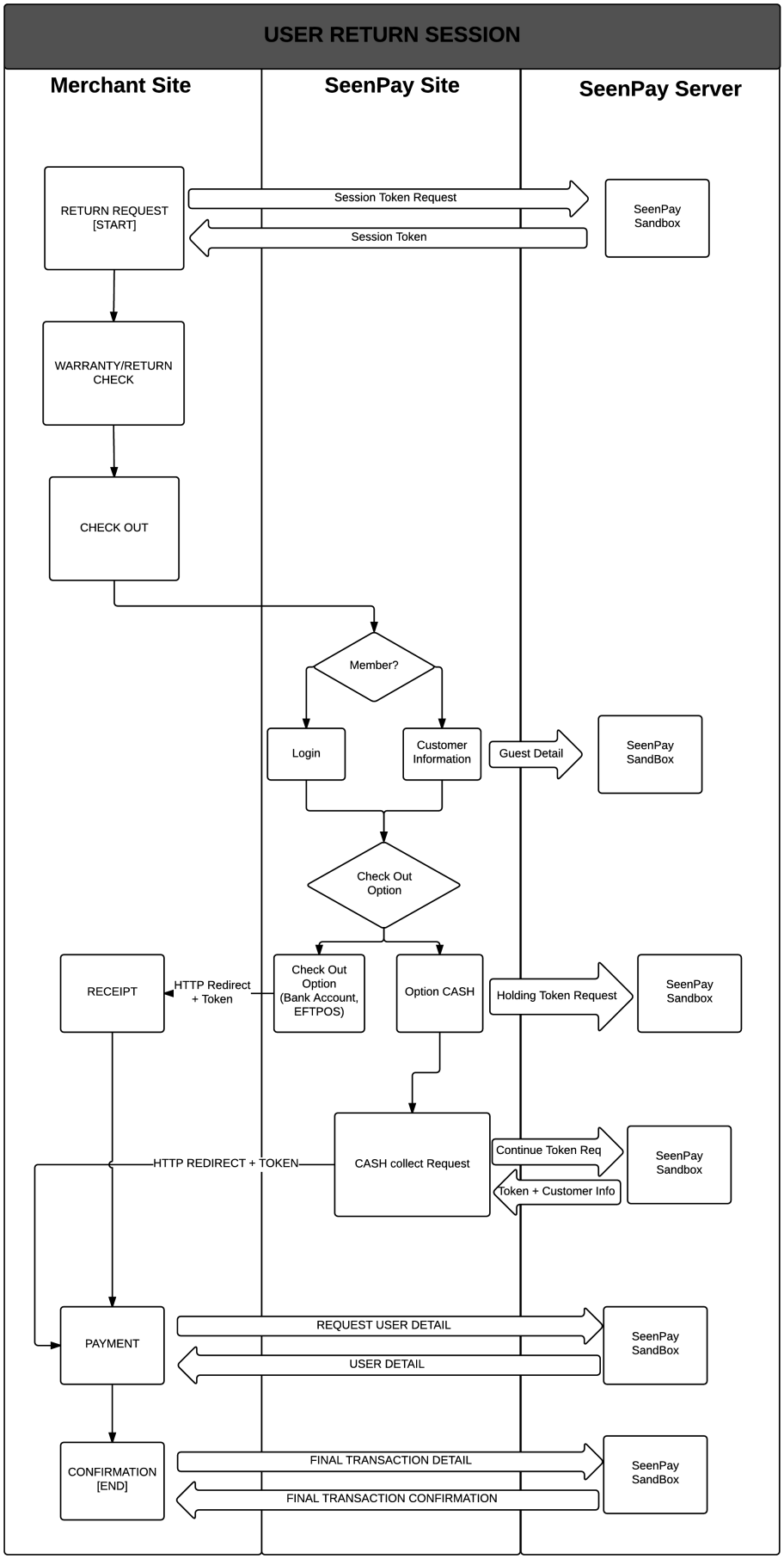
Web Application Explanation

Interaction Diagram B2C

User Purchase Session



User Return Session



Server Application Explanation

Operating System

Windows Server 2012 R2 Standard Edition

Database

Microsoft SQL Server 2012

Control Panel

Windows 2012 R2 STD Plesk 12
ISPconfig3
DirectAdmin

Network Topology Explanation

Server Network

Connection and protection

Capacity	1 Gbps Lossless
Device	Cisco Nexus
Anti-DDoS	Professional Anti-DDoS included

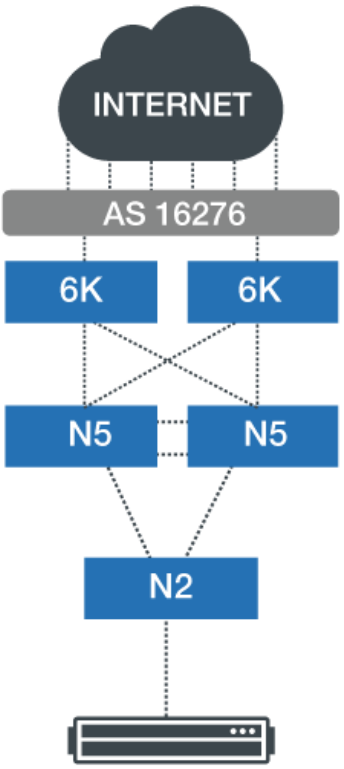
Guaranteed bandwidth

Outgoing (OVH to the internet)	500 Mbps
Burst ⓘ	1 Gbps
Internal (OVH to OVH)	1 Gbps
Incoming (The internet to OVH)	1 Gbps

More bandwidth? Check out our offers.

IP with no monthly fees*

IPv4	1
IPv6	/64



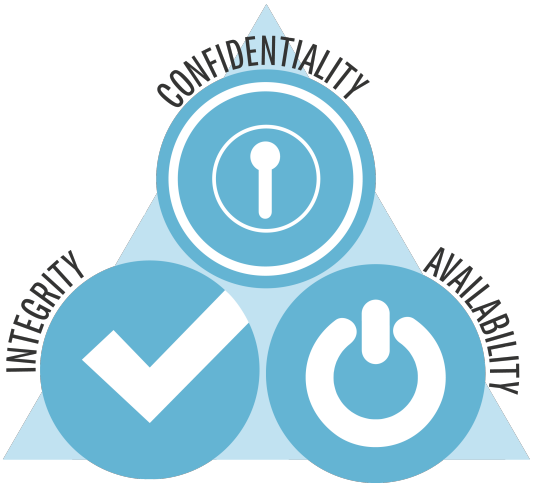
NAS Network

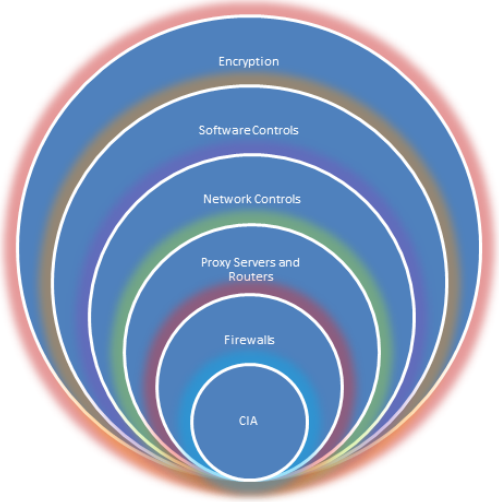
Database Explanation

(to be updated)

Security Policy Explanation

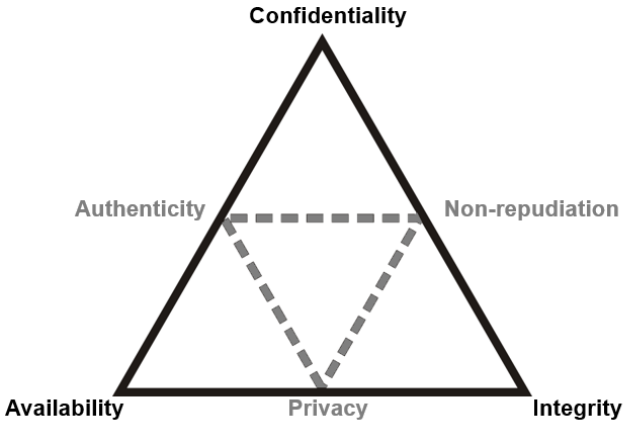
Confidentiality, Integrity, and Availability Triad





What is it?

This is one of a basic Internet security knowledge. **C**onfidentiality, **I**ntegrity, and **A**vailability or also known as CIA.



- **Confidentiality** – data is secured to authorized parties
- **Integrity** – data is trusted
- **Availability** – data is accessible when and where needed
- **Non-repudiation** – service provides a trusted audit trail
- **Authenticity** – components can prove their identity
- **Privacy** – service does not automatically see customer data

- Confidentiality is a set of rules that limits access to information.
- Integrity is the assurance that the information is trustworthy and accurate.
- Availability is a guarantee of reliable access to the information by authorized people.

More Details and Explanation

Adopted from: http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

Confidentiality:

Confidentiality is roughly equivalent to privacy. Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it: Access must be restricted to those authorized to view the data in question. It is common, as well, for data to be categorized according to the amount and type of damage that could be done should it fall into unintended hands. More or less stringent measures can then be implemented according to those categories.

Sometimes safeguarding data confidentiality may involve special training for those privy to such documents. Such training would typically include security risks that could threaten this information. Training can help familiarize authorized people with risk factors and how to guard against them. Further aspects of training can include strong passwords and password-related best practices and information about social engineering methods, to prevent them from bending data-handling rules with good intentions and potentially disastrous results.

A good example of methods used to ensure confidentiality is an account number or routing number when banking online. Data encryption is a common method of ensuring confidentiality. User IDs and passwords constitute a standard procedure; two-factor authentication is becoming the norm. Other options include biometric verification and security tokens, key fobs or soft tokens. In addition, users can take precautions to minimize the number of places where the information appears and the number of times it is actually transmitted to complete a required transaction. Extra measures might be taken in the case of extremely sensitive documents, precautions such as storing only on air gapped computers, disconnected storage devices or, for highly sensitive information, in hard copy form only.

Integrity:

Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people (for example, in a breach of confidentiality). These measures include file permissions and user access controls. Version control maybe used to prevent erroneous changes or accidental deletion by authorized users becoming a problem. In addition, some means must be in place to detect any changes in data that might occur as a result of non-human-caused events such as an electromagnetic pulse (EMP) or server crash. Some data might include checksums, even cryptographic checksums, for verification of integrity. Backups or redundancies must be available to restore the affected data to its correct state.

Availability:

Availability is best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed and maintaining a correctly functioning operating system environment that is free of software conflicts. It's also important to keep current with all necessary system upgrades. Providing adequate communication bandwidth and preventing the occurrence of bottlenecks are equally important. Redundancy, failover, RAID even high-availability clusters can mitigate serious consequences when hardware issues do occur. Fast and adaptive disaster recovery is essential for the worst case scenarios; that capacity is reliant on the existence of a comprehensive disaster recovery plan (DRP). Safeguards against data loss or interruptions in connections must include unpredictable events such as natural disasters and fire. To prevent data loss from such occurrences, a backup copy may be stored in a geographically-isolated location, perhaps even in a fireproof, waterproof safe. Extra security equipment or software such as firewalls and proxy servers can guard against downtime and unreachable data due to malicious actions such as denial-of-service (DoS) attacks and network intrusions.

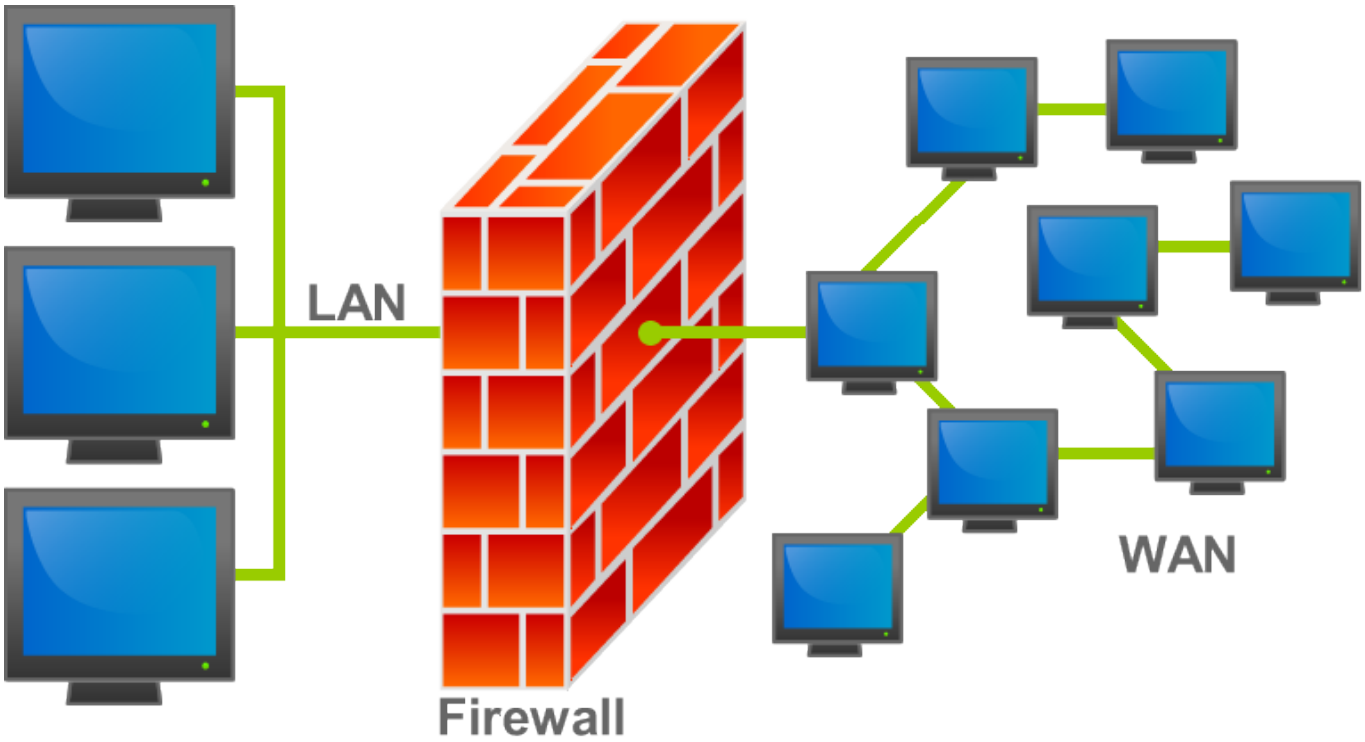
Top 5 Layer of Information Security

Adopted from: http://resources.infosecinstitute.com/guiding-principles-in-information-security/

Information security is a protection mechanism. It starts with physical security and goes up to software and network security. By protecting the source of information at different levels, security administrators are able to develop a complete defensive model for the organization.

Firewalls

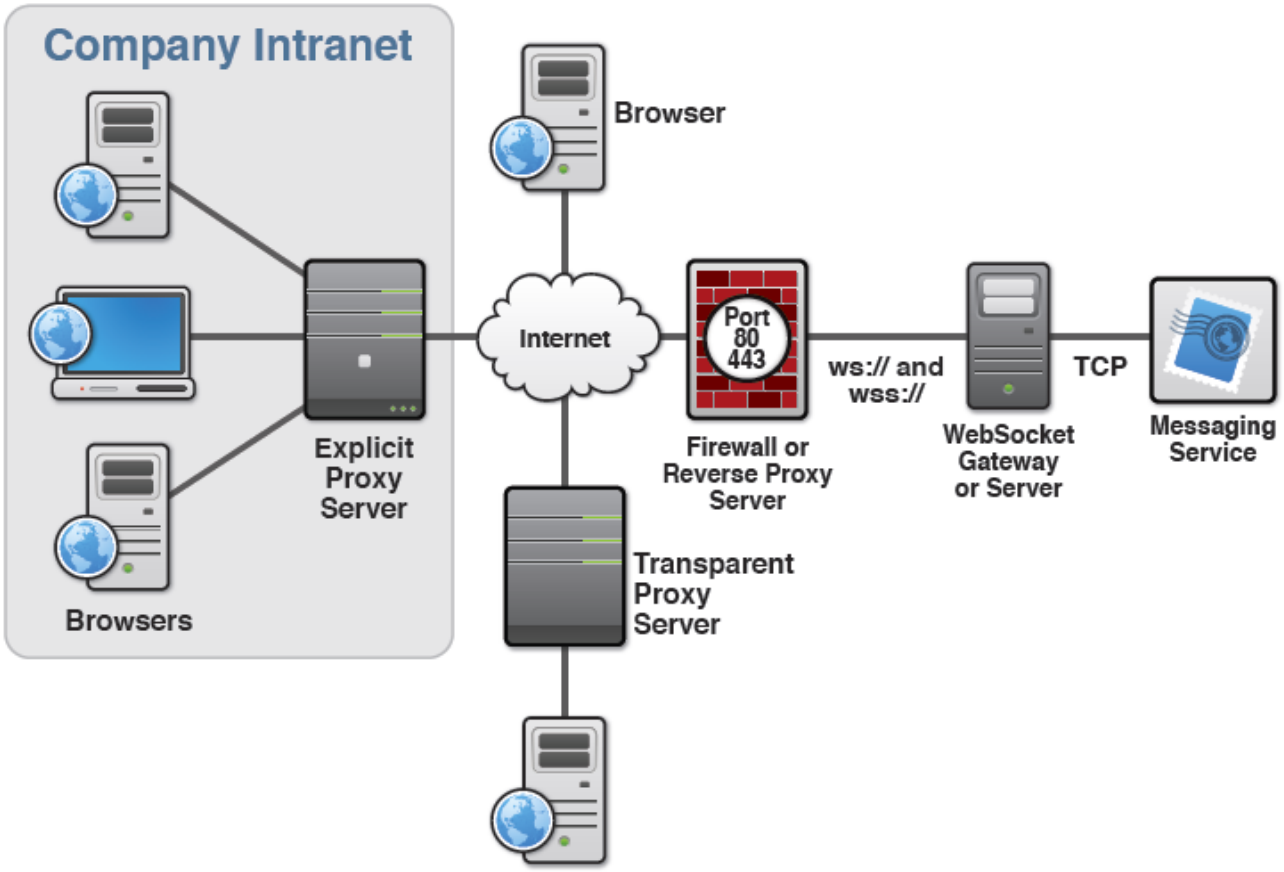
Hardware firewalls are appliances used to keep programs from entering the network. A firewall uses access lists, which are summaries of networks that have or do not have access to the system. For example, a network with an IP address of 150.31.x.x may be allowed in, but all other networks may be denied entrance into the network. Hardware firewalls also can be used to set up VPNs and free servers for other duties.



Proxy Servers and Routers

Two other hardware devices can control information security for an organization. A server, via hardware such as a proxy server (pretending to be something else) can control what the outside world sees of the network. Since the Internet is an open system, anyone can have access to any device that has connections and access. So one way that protection comes about is by putting up a "smoke screen" on the network. That would be the proxy server. It hides the real network, by showing a minimal connection to the Internet.

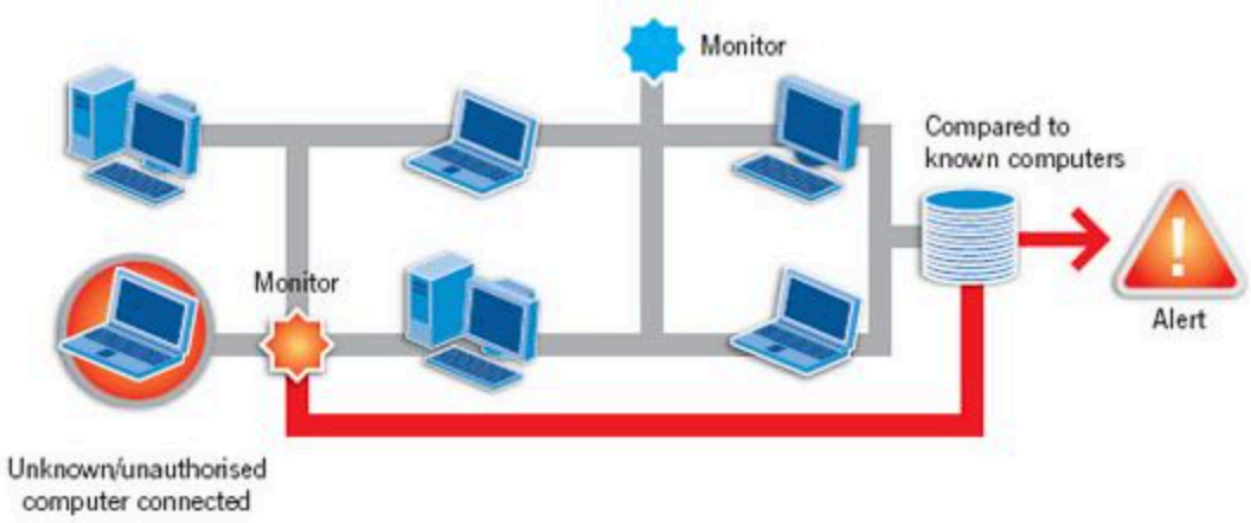
A router is a different device that can control access to the network. Like a firewall, it can have access lists that allow or prevent access into a network. They are like a firewall; however, they do more than just monitor access: They route IP packets to other networks. No other device on the network or the Internet does that.



Both of these devices work to control access into the network, one direct (the router) and the other indirect (proxy server).

Network Controls

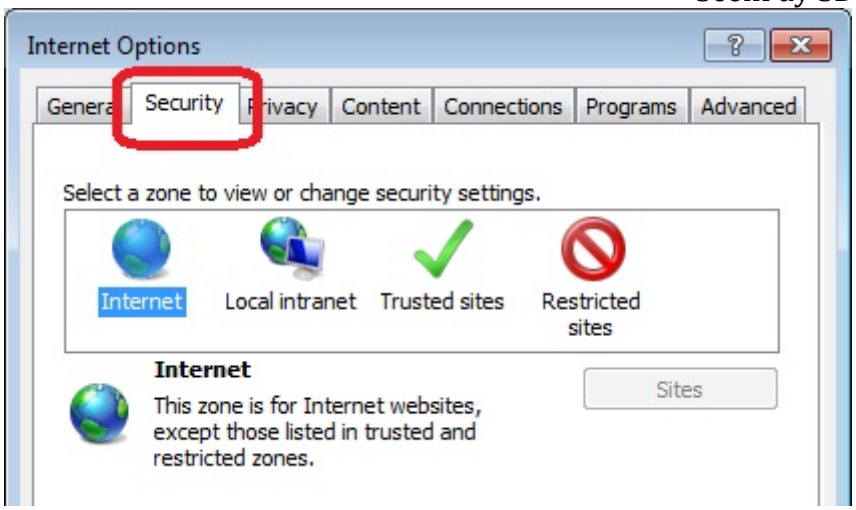
Network controls can provide information security for an organization. This type of control occurs at the local level. Authentication involving logins and passwords are key. Every user must have an account that allows him to access the network. Furthermore, the user must have a password, structured with a sophisticated protocol, like a minimum of ten characters, no common names, like "password," and a combination of letters and numbers. These network controls can affirm that only legitimate users will gain entrance to the network.



Sophos NAC Informant: identifying unauthorised computers

Software Controls

Software Controls add another layer to information security by preventing viruses, spam, and other forms of malware from penetrating the system. If penetration does occur, then the controls should remove the infections and return the system to the pre-infestation state.

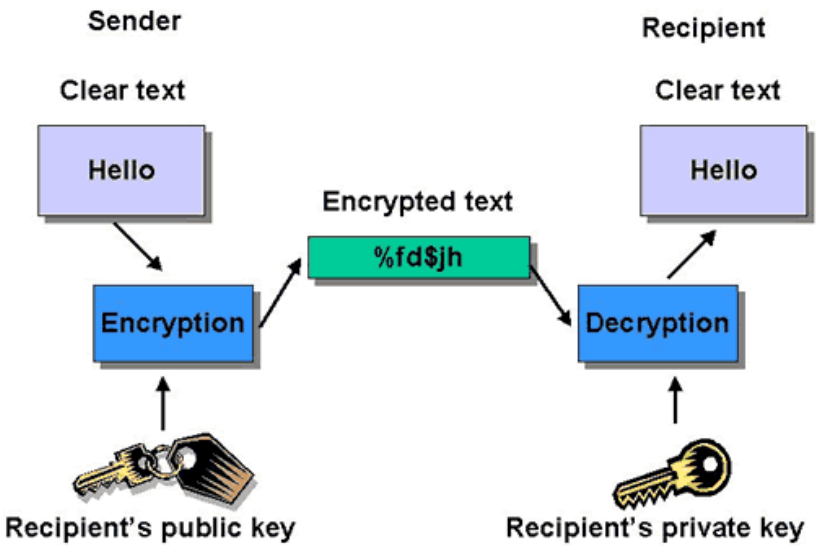


Encryption

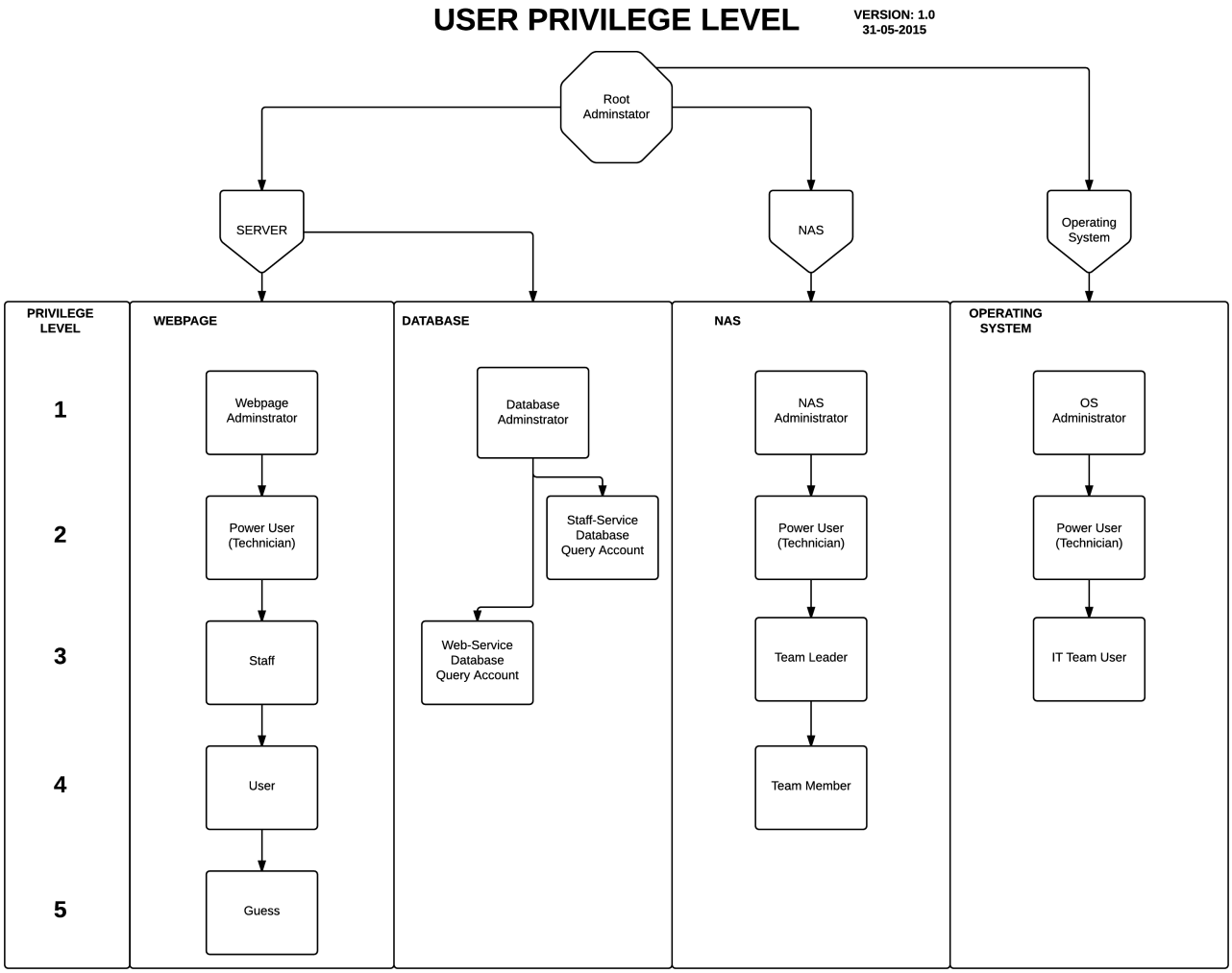
The final layer of security information is encryption. This involves changing the characters of a file to make them unreadable unless a key to decipher the information is available.

Encryption comes in different formats as encryption tools have become more sophisticated. There is manual encryption, which uses software, and a user must initiate the encryption. Transparent encryption occurs automatically without the user intervention.

Symmetric encryption occurs by using character substitution with a key that is used to decrypt the information. On the other hand, asymmetric encryption occurs when two keys are used, a public and a private. Anyone can encrypt using the public key, but only the person with the private key can decrypt the information.



User Privilege Level



Maintenance Policy Explanation

(to be updated)

Backup

Backup will be automatically done at the end of each day at 0:00 (GMT +7).
Backup will use a Dedicated Device/Disk (NAS or Hard Disk Drives)

Restore

Restore will only use in ***critical event*** to avoid data losses.

Example Critical Event:

- Data Loss (50GB or above).
- System Error (Fixing may take more than 2 day).
- Security Compromise (Administrator loss control of system).

Server Hardware Explanation

(to be updated)

Basic Information

Link: https://www.ovh.com/us/dedicated-servers/range-2013/2013-SP-64-PLUS-3HD.xml

Dedicated server SP-64 + 2013 3HD

$124.59* /month

CPU:	Intel Xeon E5-1650 6c/12t 3,2 GHz+/3,8 GHz+
RAM:	64 GB DDR3 ECC 1333MHz
Disks:	3x 2 TB SATA3
IP with no monthly fees*	256 IPs
Public network card:	1x 1 Gbps
Availability:	

Order

*Setup fees FREE.

Setup Fee WAIVED for the BHS datacentre.

Hardware

Chassis	1U/T3
CPU	Intel Xeon E5-1650
Cores/threads	6/12t
Frequency/burst	3,2 GHz+/3,8 GHz+
Intel Smart Cache	10 MB
RAM	64 GB DDR3 ECC 1333MHz
Disks	3x 2 TB SATA3
RAID	SOFT/JBOD
Bandwidth	500 Mbps
Traffic	Unlimited
Burst	1 Gbps
IP with no monthly fees*	256 IPs