GROUP 2 - CYANOBAC ENTERPRISE SECURITY FINAL PROJECT

By Connor Reis, Jacob Aragon, Luke Springfield and Tony Winstead

Table of Contents

Cyanobac Password Policy

Effective Date: 5/8/2020

Scope:

This policy applies to anyone (individual, third-party, etc.) that accesses the organization's information resources or digital services in any form.

Policy:

Password policy must at minimum follow the guidelines set by the U.S. Department of Commerce's National Institute of Standards and Technology (NIST).

1. Any changes to the NIST guidelines must be implemented by the organization within 90 days of the change's initial publication.
2. In the event of the obsolescence, decay or removal of NIST password guidelines, the Chief Executive Officer (CEO), Chief Information Officer (CIO) and Chief Security Office (CSO) must decide on a new standard to base the Password Policy on.
3. The new standard must be implemented within 90 days of this decision.

Current Password Guidelines:

1. Minimum Password Length:
    a. 12 characters
2. Maximum Password Length:
    a. 64 characters
3. Types of Characters:
    a. Three of the following: Lowercase Letter, Uppercase Letter, Number, or Special Character (i.e. symbol).
4. Password Change:
    a. Every 180 days from the last password reset.
    b. Passwords can be changed at the user's discretion at any time by contacting the Information Technology Department or following their procedures.
    c. An approved photo ID (driver's license, passport or company ID) is required for an in-person password reset.
5. Lockout Policy:
    a. Incorrectly entering your password 4 times will result in a 30-minute lockout from the organization's information resources and digital services.
6. Additional Password Requirements:
    a. The previous 10 passwords that you have used will not be allowed.

Extraneous Circumstances:

1. If it is suspected that a password has been compromised the Information Technology Department must be notified immediately.
    a. In such cases, the Information Technology Department also reserves the right to change a password without warning.

Enforcement:

1. Human Resources will provide you a digital copy of this form, which you will need to sign and date, and then return. This form will be stored in your employment file.
2. Failure to follow this policy will prevent access to the organizations information resources or digital services.
3. Failure by the organization to follow or update this policy in any form will require that the shareholders be notified within 30 days of this lapse.
4. Users that publicly display or insecurely store their password, will be forced to change their password immediately.
    a. Should this consistently occur Human Resources will be notified, and users will be forced to undergo "Password Protection Training" by a designated third-party at their own expense.
    b. In rare cases, this may result in changes to a person's employment status.

Notices:

The Information Technology Department will not know your password and is unable to provide passwords when requested. However, the IT Department can reset passwords as needed.

Related Policies:
Acceptable Use Policy
System Access Control Policy
Data Classification Policy

Revision History:

Date:	**Made By:**	**Change Description:**
5/7/20	Luke Springfield	Original Policy
5/8/20	Luke Springfield	Edited for Cyanobac corporation

Cyanobac - Data Classification Policy

Effective Date: 5/8/2020

Scope:

This policy is intended to cover any and all Cyanobac company data, as well as all persons associated with the company; including Cyanobac employees, contractors, interns, etc. This policy will be updated on an as-needed basis to best suit the needs of the company.

Policy:

All Cyanobac data will be classified as descripted in the following procedural document. This policy is designed to protect the company by limiting access to confidential data internally, while also minimizing the risk of data leakage in the case of a system breach or willful action of a Cyanobac associate.

Enforcement:

Any employee, contractor or other Cyanobac associate that violates the Cyanobac Data Classification Policy are subject to disciplinary action, including termination and, if necessary, legal action.

Related Policies:

Cyanobac Acceptable Use Policy

Cyanobac Non-Disclosure Agreement

Revision History:

Date:	Made By:	Change Description:
5/8/20	Tony Winstead	Original Policy

Signatories:

____

____

____

____

Cyanobac - Data Classification Procedure

Purpose:

This policy is designed to protect Cyanobac by limiting access to confidential data internally, while also minimizing the risk of data leakage in the case of a system breach or willful action of a Cyanobac associate.

Scope:

The following procedure applies to all Cyanobac staff, contractors, interns, etc. regarding all company-owned or generated data. This also applies to all data residing within or originating from any Cyanobac server.

Procedure:

1. Data Classification
    1. All data generated by Cyanobac staff must be submitted, via secure drop-box, to our designated team or approved staff members for classification immediately upon creation.
    2. Cyanobac Classification staff will classify data accordingly during the same day. Urgent requests may be presented in-person.
    3. All data must be classified by an authorized team member before being stored on Cyanobac shared drives. The classification may dictate where the data is stored.
    4. Data must not be shared or publicized prior to classification without direct approval by our CEO.
2. Approved Classifiers
    1. The Cyanobac Data classification team may classify data in a manner that follows their company-provided training.
    2. Other Cyanobac team members can now classify data for their team, given that they have direct approval by the CEO, and have received the appropriate training from our data classification staff.
3. Data Classes
    1. Level 1 (Classified) – Top secret data to be treated with utmost care. Classified data is only visible by Cyanobac C-level staff and other approved team leaders.
    2. Level 2 (Internal) – Sensitive data like company projects, employee information or lower-level financials that would pose a medium-level risk to the company if compromised. This data is accessible to Cyanobac C-level staff, Finance and HR departments and any other approved team members.

   c. Level 3 (Public) – This is lower-level, general data that is to be accessible by the entire organization, including information that is required by law to be accessible to all employees in order for a company to maintain compliance.

4. Reclassification Procedure
   a. If data requires classification escalation, it may be submitted to any approved classification staff for re-designation.
   b. The CEO is the only person allowed to de-escalate a data classification. All inquiries to do so must go directly to him.

Revision History:

Date:	**Made By:**	**Change Description:**
5/8/20	Tony Winstead	Original Procedure

This procedure document will be revised on an as-needed basis.

Cyanobac Acceptable Use Policy

Effective Date: 05/8/2020

Overview:

This acceptable use policy (hereafter referred to as “AUP”) delineates acceptable practices relating to the use of networks, websites, systems, facilities, products, services, and proprietary information (hereafter referred to as “Company Owned Resources”). This would include, but is not limited to, related equipment such as mobile IT devices, and all other technologies used for conducting business. This policy applies to all Cyanobac employees, contractors, agents and consultants (hereafter referred to as ‘’Individuals”).

Purpose:

This AUP provides rules for the use of information, electronic and computing devices, network resources and any equipment owned or leased that is used for the purpose of conducting business.

Scope:

This AUP applies to all Cyanobac employees. This includes full-time, part-time, technical or nontechnical, vendors, contractors, agents and consultants.

Policy:

Under no circumstances are Individuals authorized to engage in any activity that is illegal under local, state, federal, or international law while using Company Owned Resources.

The following activities while not exhaustive are considered unacceptable.

1. Unauthorized copying of copyrighted material.
2. The unauthorized exporting of Company Owned Resources and information.
3. Accessing data for any purpose other than conducting business.
4. Introduction of malicious programs into the network.
5. Circumventing user authentication or security of any host, network, or account.
6. Sharing or revealing passwords in any way to others.

7. Unauthorized reproduction of company information, client information or contractor information.
8. Displaying and/or viewing any sexually explicit material.

Exceptions:

Exceptions to the policy must be approved by the appropriate management personnel.

Compliance:

Individuals that violate this policy may be subject to disciplinary action which may include termination of employment.

Related Policies:

Password Policy

Revision History:

Date:	**Made By:**	**Change Description:**
5/7/20	Jacob Aragon	Original Policy
5/8/20	Connor Reis	Rework

Signatories:

Cyanobac Acceptable Use Policy Procedures

Accountability:

1. All submissions of employee misconduc-t shall be kept confidential.
2. Any suspected misuse should be reported to the appropriate management personnel.
3. Users/employees are responsible for all activities originating from their employee account/ID.

Monitoring:

1. Users/employees should be aware that management shall monitor bandwidth usage, camera footage, and computer logs.

Equipment:

1. Equipment necessary to perform job related tasks/responsibilities will be provided by the company.
2. Requests for equipment changes/replacements should be given to the appropriate management personnel.

Personal Devices:

1. The use of personal devices should not interfere with job performance and work responsibilities.
2. Wi-Fi is available for use and the password will be provided during job orientation. Future password changes will be communicated to all employees.

Exceptions:

1. All exception requests must be submitted in written format on the appropriate form. These submissions should be given to management as instructed on the from.
2. All approved exceptions shall be given in writing with an expiration date and time when the exception shall be deemed no longer valid.

Revision History:

Date:	Made By:	Change Description:
5/8/20	Connor Reis	Original Procedure

Cyanobac Servers

Physical Server Security Notes:

- All Cyanobac servers will reside in a dedicated, temperature-controlled room.
- An RFID key card and a numeric password are required to enter the room.
- The numeric password is changed every month.
- When the server room is not actively being used by IT staff, the door should be closed and locked.
- Only Cyanobac IT staff is permitted to access the server room.

Domain Controllers

Purpose/Functions:

These servers host Active Directory services, which are necessary to manage all company user accounts and computers that reside within the Cyanobac.com domain. They also host essential networking services by providing DHCP and DNS services.

Domain Controller 1 Configuration:

Hardware Settings:

Machine Name:	CYAN-DC1
OS:	Windows Server 2016 Standard
Processors:	i7-8750H @2.2GHz 2 cores
Memory:	8GB
Hard Disk:	50GB
Network Adapter (1):	NAT
Network Adapter (2):	Bridged
Network Adapter Settings (1):	This will be turned off once inside the VM.
Network Adapter Settings (2):	Bridged. Replicate physical connection state box checked.

Network Settings:

IPv4 Address:	192.168.20.241 (Static)
Subnet:	255.255.255.0
Default Gateway:	192.168.20.1
DNS Servers:	x.x.x.x

Domain Controller 2 Configuration:

Hardware Settings:

Machine Name:	CYAN-DC2
OS:	Windows Server 2016 Standard
Processors:	i7-8750H @2.2GHz 2 cores
Memory:	8GB
Hard Disk:	50GB
Network Adapter (1):	NAT
Network Adapter (2):	Bridged
Network Adapter Settings (1):	This will be turned off once inside the VM.
Network Adapter Settings (2):	Bridged. Replicate physical connection state box checked.

Network Settings:

IPv4 Address:	192.168.20.242 (Static)
Subnet:	255.255.255.0
Default Gateway:	192.168.20.1
DNS Servers:	x.x.x.x

Installation Notes:

The following server roles are installed:

- DHCP Server (DC1)
- DNS Server (DC1)
- Active Directory Domain Services (DC1)
- Print and Document Services (DC2)

Security Notes:

- All external drives on the server have been disabled.

- Remote Access is only permitted to the Server Admin Group

- A second DC Server is created (CYAN-DC2) to operate as a backup in case the primary DC goes down.

- RAID 5 setup is implemented on both domain controllers to ensure redundancy.

Active Directory Domain Services Setup:

1. On the Windows Server 2016, click on Add Roles and Features under Tools.
2. Select the server you want to be the domain controller and then pick Active Directory Domain Services in the Roles window.
3. Install the Active Directory Domain Services role and corresponding Features.
4. Once this role has been installed, you will need to promote the server to be the domain controller.
5. Click on Add a new forest and then input the name of your domain.
6. After further options, you will then be able to install the domain controller.

DHCP Setup (DC1):

1. Click on Add Roles and Features.
2. On the Server Roles window select DHCP Server and add the associated features.
3. Install the DHCP server role.
4. Once the role has been installed, open it by going to DHCP under Tools.
5. Select the server and then right-click on IPv4. Then select New Scope.
6. Type in the name of your scope.
7. Enter the IP address range of your scope.
8. Enter any exclusions if necessary.
9. Enter the duration of for the scope lease.
10. Next, override the server settings and enter in the IP address of the default gateway.
11. Add in the name and the IP address of the DNS server. This allows computers who receive a dynamic address to use the correct DNS server.
12. Finally activate the settings.

DNS Setup (DC1):

1. Click on Add Roles and Features.
2. On the Server Roles window select DNS Server and add the associated features.
3. Install the DNS server role.
4. Once the role has been installed, open it by going to DNS under Tools.
5. Right-click on the server in the DNS Manager window and select Configure a DNS Server.
6. In the wizard, select Create Forward and Reverse Lookup Zones.
7. Select Create the Forward Look Up Zone.
8. Select Primary Zone.
9. Select To All DNS Servers Running on Domain Controllers in this Domain.
10. Enter the zone's name and Allow Only Secure Dynamic Updates.
11. This will complete the creation of the forward lookup zone. You can follow the same steps to create the reverse look up zone.
12. Make sure to select IPv4 Reverse Lookup Zone and then enter in the zone name.
13. Lastly, enter in an external DNS server for queries the internal DNS server cannot resolve.

Print and Document Services Setup (DC2):

1. In the Server Manager click on Add roles and features.
2. On the Server Roles window add the Print and Document Services role.
3. Add the features associated with this role.
4. On the Role Services window select Print Server.
5. Install the Print and Document Services role.
6. After the role is installed, go to Tools in the Server Manager and select Print Management.
7. In the Print Management window select Print Servers and then the CYAN-PRINT server.
8. On the Printers icon, right-click and select Add Printer…
9. The following printers are then added with the associated static IP addresses.

Printers

Printer Name	IP Address
CYANP-FACILITIES	192.168.20.2
CYANP-R&D	192.168.20.3
CYANP-SALES	192.168.20.4
CYANP-SUPPORT	192.168.20.5
CYANP-ACCOUNT	192.168.20.6
CYANP-AUDITING	192.168.20.7
CYANP-CMGMT	192.168.20.8
CYANP-FINSYS	192.168.20.9
CYANP-ITDEV	192.168.20.10
CYANP-DATABASE	192.168.20.11
CYANP-ITSUPPORT	192.168.20.12
CYANP-SYSTEM	192.168.20.13
CYANP-EXECUTIVE	192.168.20.14
CYANP-DIRECT	192.168.20.15

10. Once the printers have been added, right-click on each one and select Add Driver.
11. Then add the corresponding driver for each printer.

IP Addressing, DHCP and DNS Configuration:

DMZ Network:	192.168.10.0/24
DMZ Gateway:	192.168.10.1
DMZ DHCP Scope (Guest Wifi):	192.168.10.2-64
DMZ Servers:	192.168.20.65-70 (Static)

Internal:	192.168.20.0/24
Internal Gateway:	192.168.20.1
Internal Printers:	192.168.20.2.2 – 15 (Static)
Internal DHCP Scope for Computers:	192.168.20.16-240
Servers :	192.168.20.240-254 (Static)

DNS set up on CYAN-DC1 and CYAN-DC2 for internal address look up only.

Global Group Policies

Cyanobac Workstations

Restrict Control Panel: Disables access to the control panel.
Restrict Installs: Disables the ability to install software
Restrict CMD: Disables access to CMD and Powershell.
Restrict Account Creation: Prevents the creation of local and guest accounts
Restrict WIFI: Prevents access to non-approved WIFI network without VPN
Restrict External: Prevents the use of external media
Create Admin: Creation of the CyanAdmin account on each workstation

Password Group Policies:

Minimum Password Length: 12 characters
Maximum Password Length: 64
Enforce Password History: 10
Minimum Password Age: 0
Maximum Password Age: 180
Passwords Must Meet Complexity Requirements: Yes
Account Lockout Threshold: 4
Account Lockout Duration: 30 mins

List of Active Directory Security Groups:

The security groups listed below allow for read, write access on files in the specified folder.

Leadership

Executive: \\CYAN-File\Leadership\Executives
Directors: \\CYAN-File\Leadership\Directors

Facilities

Facilities: \\CYAN-File\Facilities

Finance

Auditing: \\CYAN-File\Finance\Auditing
Accounting: \\CYAN-File\Finance\Accounting
Cash Management: \\CYAN-File\Finance\Cash Management
Financial Systems: \\CYAN-File\Finance\Financial Systems

Sales

Sales NA: \\CYAN-File\Sales\Sales NA
Sales EU: \\CYAN-File\SalesSales EU

R&D
Aqua: \\CYAN-File\R&D\Aqua
IT Research: \\CYAN-File\R&D\IT Research
Pharmacology: \\CYAN-File\R&D\Pharmacology

IT
IT Operations: \\CYAN-File\IT\IT Operations
System Operations: \\CYAN-File\IT\System Operations
IT Development: \\CYAN-File\IT\IT Development
Database Administration: \\CYAN-FIle\Database Administration

Support Systems
Security: \\CYAN-File\Security
Legal: \\CYAN-File\Legal

Admin Security Permissions:

Workstation Admin: Admin and remote access on all Cyanobac workstations.
Database Admin: Admin access on CYAN-LAMP as well as remote access.
Server Admin: Admin access on CYAN-File, CYAN-DC1, CYAN-DC2, CYAN-Backup, CYAN-Firewall and CYAN-Mail as well as remote access.

List of employees and Security Membership:

Title	First	Last	Active Directory Security Groups
CEO	Virginia	Clark	Executive
CIO	Max	Wright	Executive
CFO	Adrian	Campbell	Executive
COO	Jake	Rampling	Executive
Director of Internal Audit	Gordon	Manning	Auditing, Directors
Internal Auditor	Peter	Lawrence	Auditing
Internal Auditor	Ryan	Watson	Auditing
Internal Auditor	Diana	Campbell	Auditing
Director of Accounting	Ava	Buckland	Accounting, Directors
Accountant	Gordon	Wright	Accounting
Accountant	Michelle	Jackson	Accounting
Accountant	Ryan	Mills	Accounting
Accountant	Ella	Springer	Accounting
Accountant	Joshua	Gibson	Accounting

Accountant	Austin	Bailey	Accounting
Accountant	Gabrielle	Bailey	Accounting
Accounting Operator	Harry	Clarkson	Accounting
Cash Management Director	Bernadette	Churchill	Cash Management, Directors
Cash Management Specialist	Peter	Alsop	Cash Management
Cash Management Specialist	Theresa	Lambert	Cash Management
Director of Financial Systems	Samuel	Carr	Financial Systems, Directors
Financial System Development	Karen	Howard	Financial Systems
Financial Systems Support	Amelia	Morrison	Financial Systems
Director of R&D	Kevin	Bower	Aqua, IT Research, Pharmacology, Directors
Chief Researcher	Kevin	Fraser	Aqua, IT Research, Pharmacology
Aqua Project Researcher	Matt	Hudson	Aqua
Aqua Researcher	Jessica	Berry	Aqua
Aqua Researcher	Edward	White	Aqua
Project Researcher - Pharmacology	Dorothy	Hardacre	Pharmacology
Assistant Researcher - Pharmacology	Alexander	Mackay	Pharmacology
Assistant Researcher - Pharmacology	Lauren	Miller	Pharmacology
Director of Facilities	James	Mitchell	Facilities, Directors
Facilities Maintenance-Site 1	Natalie	Metcalfe	Facilities
Facilities Maintenance-Site 1	Luke	Powell	Facilities
Facilities Maintenance-Site 2	Peter	Lawrence	Facilities
Facilities Maintenance-Site 2	Carolyn	Coleman	Facilities
Facilities Maintenance-Site 3	Alan	Anderson	Facilities
Facilities Maintenance-Site 3	Kimberly	Quinn	Facilities
Facilities Maintenance-Site 4	Simon	King	Facilities
Facilities Maintenance-Site 4	Sue	Lewis	Facilities
R&D IT Developer	Sarah	Hudson	IT Research
R&D IT Developer	Colin	McDonald	IT Research
IS Operations Coordinator	Caroline	Ellison	IT Operations, Workstation Admin
Systems Operations Manager	Sean	Martin	System Operations, Server Admin
Network Development	Joe	Welch	System Operations, Server Admin
System Administrator	Elizabeth	Watson	System Operations, Server Admin
System Administrator	Phil	Reid	System Operations, Server Admin
System Administrator	Zoe	Marshall	System Operations, Server Admin
System Administrator	Trevor	MacLeod	System Operations, Server Admin
System Administrator	Ella	Bell	System Operations, Server Admin
Director of IT Development	Jake	Allan	IT Development, Directors
Database Manager	Dan	Watson	IT Development
Database Adminsitrator	Yvonne	Marshall	Database Administration, Database Admin
Database Developer	Evan	Short	Database Administration, Database Admin
Director of Development	Bella	Martin	Database Administration, Directors
IT Development	Frank	Poole	IT Development
IT Development	Steven	Glover	IT Development
IT Development	Rose	Roberts	IT Development
IT Manager	James	Powell	IT Development
IT Systems Support	Samantha	Carr	Systems Operations, Workstation Admin
Security Manager	Harry	Watson	Security, Directors
Business Continuity Manager	Felicity	Carr	Security

Disaster Recovery Analyst	Irene	Hudson	Security
Desktop Support	Simon	Burgess	Systems Operations, Workstation Admin
Head of Legal Counsel	Kimberly	Dyer	Legal
Compliance Specialist	Brian	Ferguson	Legal
Dirctor of Sales & Marketing	Ava	North	Sales NA, Sales EU, Directors
Sales Manager - North America	Thomas	North	Sales NA
Salesperson - Region 1	Sophie	Payne	Sales NA
Salesperson - Region 2	Rebecca	Glover	Sales NA
Salesperson - Region 3	Dorothy	Wilson	Sales NA
Salesperson - Region 4	Jack	Oliver	Sales NA
Sales Manager - Europe	Steven	Lewis	Sales EU
Salesperson - Region 5	Connor	Lyman	Sales EU
Salesperson - Region 6	Bella	Rampling	Sales EU

Please see the attached Cyanobac Active Directory Overview for information on the OU structure.

Cyanobac.com

Computers OU’s

Facilities

CYANC0001
CYANC0002
CYANC0003
CYANC0004
CYANC0005
CYANC0006
CYANC0007
CYANC0008

R&D

CYANC0009
CYANC0010
CYANC0011
CYANC0012
CYANC0013
CYANC0014
CYANC0015
CYANC0016
CYANC0017

Sales

CYANC0018
CYANC0019
CYANC0020
CYANC0021
CYANC0022
CYANC0023
CYANC0024
CYANC0025

Support Services

CYANC0026
CYANC0027
CYANC0028
CYANC0029

Finance

Accounting

CYANC0030
CYANC0031
CYANC0032
CYANC0033
CYANC0034
CYANC0035
CYANC0036
CYANC0037

Auditing

CYANC0038
CYANC0039
CYANC0040
CYANC0041

Cash Management

CYANC0042
CYANC0043

Financial Systems

CYANC0044
CYANC0045

IT

IT Development

CYANC0046
CYANC0047
CYANC0048
CYANC0049

Database Administration

CYANC0050
CYANC0051
CYANC0052

IT Support Operations

CYANC0053
CYANC0054

Systems Operations

CYANC0055
CYANC0056
CYANC0057
CYANC0058
CYANC0059
CYANC0060
CYANC0061

Leadership

CYANCL0062
CYANCL0063
CYANCL0064
CYANCL0065
CYANCL0066
CYANCL0067
CYANCL0068
CYANCL0069
CYANCL0070
CYANCL0071
CYANCL0072
CYANCL0073
CYANCL0074

Servers

CYAN-DC1
CYAN-DC2
CYAN-MAIL
CYAN-FILE
CYAN-LAMP
CYAN-BACKUP
CYAN-FIRE

Cyanobac.com

Users OU’s

Facilities

Natalie Metcalfe
Luke Powell
Peter Lawrence
Carolyn Coleman
Alan Anderson
Kimberly Quinn
Simon King
Sue Lewis

Sales

North America
Thomas North
Sophie Payne
Rebecca Glover
Dorothy Wilson
Jack Oliver

Europe
Steven Lewis
Connor Lyman
Bella Rampling

Support Services

Legal
Kimberly Dyer
Brian Ferguson

Security
Felicity Carr
Irene Hudson

Finance

Accounting
Gordon Wright
Michelle Jackson
Ryan Mills
Ella Springer
Joshua Gibson
Austin Bailey
Gabrielle Bailey
Harry Clarkson

Auditing
Gordon Manning
Peter Lawrence
Ryan Watson
Diana Campbell

Cash Management
Peter Alsop
Theresa Lambert

Financial Systems
Karen Howard
Amelia Morrison

IT

IT Development
James Powell
Frank Poole
Steven Glover
Rose Roberts

Database Administration
Dan Watson
Yvonne Marshall
Evan Short

IT Support Operations
Samantha Carr
Simon Burgess

Systems Operations
Sean Martin
Joe Welch
Elizabeth Watson
Phil Reid
Zoe Marshall
Trevor MacLeod
Ella Bell

Leadership

Chiefs
Virginia Clark
Max Wright
Adrian Campbell
Jake Rampling

Directors
Gordon Manning
Ava Buckland
Bernadette Churchill
Samuel Carr
Kevin Bower
James Mitchell
Caroline Ellison
Ava North
Harry Watson
Bella Martin

R&D

Aqua
Matt Hudson
Jessica Berry
Edward White

Chief Researcher
Kevin Fraser

IT
Sarah Hudson
Colin McDonald

Pharmacology
Dorothy Hardacre
Alexander Mackay
Lauren Miller

Backup Server

Purpose/Functions:

The backup server automatically creates and stores copies of all company drives and databases to prevent the loss of any user work or company data. Backups are ran according to the schedule specified below.

Hardware Settings:

Machine Name:	CYAN-BACKUP
OS:	Windows Server 2016 Standard
Processors:	i7-8750H @2.2GHz 2 cores
Memory:	8GB
Hard Disk:	50GB
Attached Drives (RAID 10):	8x2TB HDD's
Network Adapter (1):	NAT
Network Adapter (2):	Bridged
Network Adapter Settings (1):	This will be turned off once inside the VM.
Network Adapter Settings (2):	Bridged. Replicate physical connection state box checked.

Network Settings:

IPv4 Address:	192.168.20.243 (Static)
Subnet:	255.255.255.0
Default Gateway:	192.168.20.1
DNS Servers:	x.x.x.x

Notes:

Redundancy was planned for the backup server with a RAID 10 configuration. The redundancy setup with RAID 10 allows for strong protection against data loss, quick transfer times as well as quick rebuild times if a drive fails.

Backup Schedule:

Full Back up: Saturday 11:30pm.
Incremental Backups: Sunday – Friday at 11:30pm

Installation Notes:

1. In the Windows Server Manager, go to Computer Management.
2. Under Storage select Disk Management.
3. Under Actions go to Attach VHD.
4. Go through and create a VHD for every server on the network that needs to be backed up.
5. Ensure that the Windows Server Backup role and featured are installed on the Windows 2016 server.

6. In the Server Manager go to Tools and select Windows Server Back.
7. Click Schedule Backup and then Customize Backup.
8. The different VHDs (servers) can then be scheduled to backup. The type of back up can also be selected.

Database Server

Purpose/Functions

The database server uses MS SQL to host all company databases required for various business functions and applications.

Hardware Settings:

Machine Name:	CYAN-DB
OS:	Windows Server 2016 Standard
Processors:	i7-8750H @2.2GHz 2 cores
Memory:	8GB
Hard Disk:	60GB
Network Adapter (1):	NAT
Network Adapter (2):	Bridged
Network Adapter Settings (1):	This will be turned off once inside the VM.
Network Adapter Settings (2):	Bridged. Replicate physical connection state box checked.

Network Settings

IPv4 Address:	192.168.20.243 (Static)
Subnet:	255.255.255.0
Default Gateway:	192.168.20.1
DNS Servers:	x.x.x.x

Installation Notes

- No additional features/roles were installed.
- Installed Microsoft SQL 2019.
- All databases are stored locally and are backed up according to the previously-mentioned schedule.

File Server

Purpose/Functions:

The file server stores company data for all departments and users. Network shares are utilized to organize the data by department. Users are granted access to these drives by Group Policy as well as Security Group memberships.

Hardware Settings:

Machine Name:	CYAN-FILE
OS:	Windows Server 2016 Standard
Processors:	i7-8750H @2.2GHz 2 cores
Memory:	8GB
Hard Disk:	60GB
Additional Drives (RAID 5 Array):	5x2TB HDD’s
Network Adapter (1):	NAT
Network Adapter (2):	Bridged
Network Adapter Settings (1):	This will be turned off once inside the VM.
Network Adapter Settings (2):	Bridged. Replicate physical connection state box checked.

Network Settings:

IPv4 Address:	192.168.20.244 (Static)
Subnet:	255.255.255.0
Default Gateway:	192.168.20.1
DNS Servers:	x.x.x.x

Storage Pool Configuration:

1. Configure RAID Array (Assigned letter D:)
2. Go to Server Manager > Volumes > Storage Pools
3. Go to Physical Disks > Tasks > New Storage Pool.
4. Name: CyanStorage1, then click Next.
5. Select the previously-created RAID (D:) drive, then click Next.
6. Double-check configuration details, then click Create.

Network Shares Configuration:

1. Go to Server Manager > Shares
2. Go to Tasks > New Share
3. Select SMB Share – Quick.
4. Select D: Drive
5. Name the Share, then click Next.
6. Check boxes for Allow caching of share and Encrypt data access, then click Next.
7. Accept default permissions, then click Next.
8. Double-check configuration details, then click Create.

Company Shared Drives:

- R&D (R: Drive)
- Finance (F: Drive)
- IT (I: Drive)
- Sales (S: Drive)
- Marketing (M: Drive)

Email Server

Purpose/Functions:

This server's main purpose is to allow company personnel to communicate securely within the network. Only company information should be transmitted and employees should avoid personal use.

Hardware Settings:

Machine Name:	CYAN-MAIL
OS:	Linux 64-bit (Ubuntu Server 20.04)
Processors:	i7-8750H @2.2GHz 2 cores
Memory:	8GB
Hard Disk:	60GB
Network Adapter (1):	NAT
Network Adapter (2):	Bridged
Network Adapter Settings (1):	This will be turned off once inside the VM.
Network Adapter Settings (2):	Bridged. Replicate physical connection state box checked.

Network Settings:

IPv4 Address:	192.168.10.68 (Static)
Subnet:	255.255.255.0
Default Gateway:	192.168.10.1
DNS Servers:	x.x.x.x

Software Installations:

- Postfix (Release 3.5.1)
- Dovecot (Release 2.3.9.2)

Ubuntu Installation:

1. Choose language: English
2. Keyboard Config: Detect layout automatically.
3. Network connections: eth0
4. Configure proxy: blank.
5. Archive mirror: blank.
6. Guided storage configuration: local disk (/dev/sda)
7. Profile setup:
    a. Your name: CYAN-MAIL
    b. Servers name: mail-cyanobac-com
    c. Username: cyanobac
    d. Password: CY4N0bac!
8. SSH setup: yes.
9. Install and reboot.

Postfix Configuration:

1. *Sudo apt install postfix - Installation*
2. *Sudo dpkg-reconfigure postfix- Basic Config*
3. Internet site
4. Mail.cyanobac.com
5. CYAN
6. Mail.cyanobac.com, localhost.cyanobac, localhost
7. No
8. 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128 192.168.0.0/24
9. 0
10. +
11. All

Dovecot Configuration:

```
Sudo apt install dovecot-imapd
```

## This server will be using IMAP so the installation of POP3 isn’t necessary.

-Configuration

```
! include_try / usr / share / dovecot / protocols . d /*. protocol
```

## To use the self-signed certificate for dovecot that was created for postfix, amend the cert by adding it to the dovecot configuration file.

```
    Sudo nano /etc/dovecot/conf.d/10-ssl.conf
```

ADD:

```
    ssl_cert = </etc / dovecot / private / dovecot . pem
    ssl_key = </etc / dovecot / private / dovecot . key
```

SMTP Authentication Configuration:

SMTP-AUTH allows the client to identify itself through the SASL authentication mechanism, using Transport Layer Security (TLS) to encrypt the authentication process. Once authenticated the client can proceed to relay mail.

```
    sudo postconf −e ’ smtpd_sasl_type = dovecot ’ sudo postconf −e ’ smtpd_sasl_path = priva te
    /auth ’ sudo postconf −e ’ smtpd_sasl_local_domain =’ sudo postconf −e ’
    smtpd_sasl_security_options = noanonymous ’ sudo postconf −e ’ broken_sasl_auth_clients = yes
    ’ sudo postconf −e ’ smtpd_sasl_auth_enable = yes ’ sudo postconf −e ’
    smtpd_recipient_restrictions = \ permit_sasl_authenticated , permit_mynetworks ,
    reject_unauth_destination ’
```

*Note: The *smptd_sasl_path* config parameter is a path relative to the postfix queue directory. Next, generate or obtain a digital certificate for TLS.

Security Configuration:

1. Generating a Certificate Signing Request (CSR).

   a. *Openssl genrsa -des3 -out server.key 2048*
   b. *Generating RSA private key , 2048 bit long modulus ....+++ +++ ....++++++ e is 65537 (0 x10001)*
   c. *Enter passphrase for server.key: CYAN*
   d. *Reenter:*
   e. *##* The server key is now created and stored in the server.key file. Now an insecure key was created, without a passphrase, and shuffled.
   f. *openssl rsa -in server.key -out server.key.insecure*
   g. *my server.key server.key.secure*
   h. *my server.key.insecure server.key*

2. Creating the CSR
   a. *Openssl req -new -key server.key -out server.csr*
   b. *Company Name: Cyanobac*
   c. *Site Name: mail.cyanobac.com*
      d. *Email Id: localhost*
   e. *##* The CSR is now stored in the server.csr file.

3. Creating a self-signed certificate.
   a. *##* Running this command required a passphrase (CYAN). Once the passphrase was entered then the certificate was created and stored in a file named server.crt. This passphrase will provide more security because every service (dovecot or postfix) will require the passphrase every time it's being used. Not incorporating a passphrase will eliminate the extra security, but increase the convenience of not having to be bothered with entering the passphrase.
   b. *openssl x509 −req −days 365 −in server.csr −signkey server.key −out server.crt*

4. Installing the certificate.
   a. *sudo cp server.crt /etc/ssl/certs*
   b. *sudo cp server.key /etc/ssl/private*
   c. *##* Now applications that can be configured to use the public-key cryptography, can use the certificate and key generated above. Ie) Dovecot can provide IMAP3 and POP3.

Additional Information:

The following PDF is beneficial for future admins of Cyanobac Pharmaceuticals and can be used to leverage higher security by incorporating additional utilities such as eCryptfs and referring to guides on Ubuntu server configuration:

https://assets.ubuntu.com/v1/0032cef9-ubuntu-server-guide.pdf

Firewall Server

Purpose/Functions:

The purpose of this firewall server is to allow or block incoming and outgoing packets of information traveling across or around the network. It's job is to control unwanted traffic into the network while allowing legitimate traffic to flow freely.

Hardware Settings:

Machine Name:	CYAN-FW
OS:	Windows Server 2016 Standard
Processors:	i7-8750H @2.2GHz 2 cores
Memory:	8GB
Hard Disk:	60GB
Network Adapter (1):	NAT
Network Adapter (2):	Bridged
Network Adapter Settings (1):	This will be turned off once inside the VM.
Network Adapter Settings (2):	Bridged. Replicate physical connection state box checked.

Network Settings:

IPv4 Address:	192.168.10.69 (Static)
Subnet:	255.255.255.0
Default Gateway:	192.168.10.1
DNS Servers:	x.x.x.x

Software Installations:

- Pfsense 2.4.4
- Winzip

Installation Notes:

1. Navigate to Pfsense website. (https://www.pfsense.org/download/)
2. Download V 2.4.4 AMD 64 bit ISO.
3. Download saved as a .gz (GZIP) file.
4. Extract ISO from the zipped file using the application winzip.

pfSense Configuration:

1. Should VLANs be set up now [y/n]?
   - No
2. Enter the WAN interface name or 'a' for auto-detection (em0 or a):
   -em0
3. Enter the LAN interface name or 'a' for auto-detection:

   -(blank)

4. The interfaces will be assigned as follows: WAN -> em0   [y/n]?
   -y
5. Would you like to remove the LAN IP address andn unload the interface now [y/n]?
   –n

Web Configurator Access:

Use Google Chrome to enter the web configurator by entering the WAN IP address into the search box after http:// (http://192.168.88.138).

Default Login Credentials:

Username: admin
Password: pfsense

Firewall Server Configuration:

1. Navigate to the user manager and create a new user called CYAN_FW. Proceed to add it to the group 'admins' to adopt the permissions.
   - Change the password so that it follows Cyanobac password policy guidelines.
   - Set an expiration date for 1 month so that the admin will have to reset password every month starting May 7, 2020.
   - Save.
   - New credentials-
     - Firewall
     - B8!$nsd*hfHikS^
2. To make sure that there is only one active admin account, logout and login to the new account. Navigate back to the user manager and check the box "user not allowed to logon".

Main Firewall Configuration:

1. Under the interfaces tab change change the name WAN to "Enterprise LAN"
   - Change to static IPv4
   - IPv6 type- none
   - Change IP address to 192.168.88.2/24
2. That is the IP address of the firewall server in the DMZ.
   - Leave the reserved networks at default.
   - Save
3. Under the interfaces tab change the name LAN to "DMZ".
   - Change to static IPv4
   - IPv6- none
   - Change the IP address to 192.168.88.3/24
   - Leave the reserved networks at default.
   - Save
4. To change the rules for the **main firewall** then navigate to the "Rules" in the dropdown menu.

SMTP

- Action- Pass
- Interface- ENTERPRISELAN
- Direction- any
- Address Family- IPv4
- Protocol- TCP/UDP
- Source- ENTERPRISELAN net
- Destination Port Range 192.168.88.2
- Port range- 25
- Description- Outbound mail

IMAP

- Action- Pass
- Interface- ENTERPRISELAN
- Direction- any
- Address Family- IPv4
- Protocol- TCP/UDP
- Source- ENTERPRISELAN net
- Destination Port Range 192.168.88.2
- Port Range- 143
- Description- Inbound mail

HTTPS

- Action- Pass
- Interface- ENTERPRISELAN
- Direction- any
- Address Family- IPv4
- Protocol- TCP/UDP
- Source- ENTERPRISELAN net
- Destination Port Range 192.168.88.2
- Port Range- 443
- Description- Safe web traffic

Server Protection:

- Changing the login credentials is important to prevent malicious acts like dictionary attacks or brute force. By adhering to the Cyanobac password policy, the new login information is:

  Username: Firewall
  Password: B8!$nsd*hfHikS^

Remote Access (VPN) Servers

Hardware Configuration:

Machine Name:	CYAN-VPN
Machine Name:	CYAN-CA
OS:	Linux 64-bit (Ubuntu 18.04.4 LTS)
Processors:	i7-8750H @2.2GHz 2 cores
Memory:	8GB
Hard Disk:	20GB
Network Adapter (1):	NAT
Network Adapter (2):	Bridged
Network Adapter Settings (1):	This will be turned off once inside the VM.
Network Adapter Settings (2):	Bridged. Replicate physical connection state box checked.

Network Settings CA server

DHCP:	
IPv4 Address:	192.168.10.67
Subnet:	255.255.255.0
Default Gateway:	192.168.10.1
DNS Servers:	x.x.x.x

Network Settings VPN server

DHCP:	
IPv4 Address:	192.168.10.66
Subnet:	255.255.255.0
Default Gateway:	192.168.10.1
DNS Servers:	x.x.x.x

Installation Notes

Ubuntu is the underlying operating system and the OpenVPN software is what the remote access server and CA server will be using. The remote access server will be paired with a CA server to sign the certificates for the clients.

Purpose/Functions

The purpose of the remote access server is to provide a remote capable session for employees of Cyanobac to be able to log on from different locations. The purpose of the CA server is to sign certificates for the clients so they can use the remote access server.

Configuration:

1. Download Ubuntu 18.04.4 LTS from https://ubuntu.com/download/desktop then install it on VMware.

2. Installing OpenVPN and EasyRSA. This first part is for both the CA server and the OpenVPN server:

3. Update your system and then install OpenVPN

4. To begin building the CA and PKI you need to DL the latest version of EasyRSA. This will need to be installed on both the CA machine and the OpenVPN server.

5. Now extract the tarball

6. Now Configuring the EasyRSA Variables and Building the CA. This step is only for the CA machine

7. Go to the EasyRSA directory

8. Now copy the file named vars.example

9. Open this file using your preferred text editor

10. Now you need to find the settings that set the defaults for new certificates.

11. You will need to uncomment them and update them to the correct values.

12. Make sure to save the file after you have made your changes.

13. Now still within the EasyRSA directory is a script called easyrsa. Run this script to initiate the PKI on the CA server

14. Now you need to call the script again this will build the CA and create two important files ca.crt and ca.key

15. In the output you will be asked to confirm the common name for the CA if you want to keep this simple just hit enter to accept the default name. Otherwise give it a name.

16. Now on to Creating the Server Certificate, Key, and Encryption Files. Move to the Remote Access Machine (VPN Server)

17. Move to the EasyRSA directory

18. Now run the easyrsa script with init-pki

19. Now run that again this time with gen-req option followed by a common name for the machine:

20. That will have created a private key for the server and a certificate request file called cyanobacVPNserver.req this file needs to be copied to the /etc/openvpn/ directory.

21. Now we need to transfer the file over to the CA server by secure means

22. Now on the CA server move to the EasyRSA directory

23. Now run the easyrsa script to import the cyanobacVPNserver.req

24. Run the script again with the sign-req option followed by the request type (i.e. server, client)

25. Once you have verified that the request comes from a trusted source type yes and hit enter.

26. Now you will need to transfer the now signed certificate back to the VPN server along with the ca.crt file

27. Now back on the OpenVPN server copy the server.crt and the ca.crt file into the /etc/openvpn/ directory

28. Move to the easyrsa directory

29. Now create a diffie-hellman key

30. Now generate a HMAC to strengthen the servers TLS

31. Now copy the two new files to your /etc/openvpn/ directory

32. All the certificates and keys needed by your server have been generated.

Securing the VPN and CA server

Since we are using OpenVPN for our VPN/CA servers we don't have to do much to secure it. However, there are still things we need to secure like our firewall, SSH, and removing unused network facing services.

For the firewall make sure you can log in by enabling SSH, HTTP, HTTPS and others if needed, but you will want to deny any protocol that is not needed for the servers to function. Along with the fire wall we will want an application like Fail2ban that examines server logs looking for repeated or automated attacks. If any attacks are found this application can alter the firewall to block the attacker's IP permanently or for a specified amount of time.

For SSH you will want to prevent remote logins from accounts with empty passwords. Next you will want to configure an idle timeout to avoid having an unattended SSH session. Limit the SSH access to provide another layer of security, you should limit your SSH logins to only certain users who need remote access. You will want to disable root logins through SSH. Changing the port and using a non-standard port is a way to avoid being seen by casual scans. Other things you should do for SSH are enable two-factor authentication and use strong usernames and passwords.

Since almost all Linux servers come with a few network facing services enabled. There are a few that you will want to remove.

LAMP Server

Purpose/Functions:

The purpose of the LAMP server is to provide a web server for Cyanobac.

Hardware Settings:

Machine Name:	CYAN-LAMP
OS:	Linux 64-bit (Ubuntu 18.04.4 LTS)
Processors:	i7-8750H @2.2GHz 2 cores
Memory:	4GB
Hard Disk:	20GB
Network Adapter (1):	NAT
Network Adapter (2):	Bridged
Network Adapter Settings (1):	This will be turned off once inside the VM.
Network Adapter Settings (2):	Bridged. Replicate physical connection state box checked.

Network Settings:

DHCP:	
IPv4 Address:	192.168.10.65
Subnet:	255.255.255.0
Default Gateway:	192.168.10.1
DNS Servers:	x.x.x.x

Installation Notes:

Ubuntu is the underlying operating system with a LAMP stack installed on top of it. LAMP stands for Linux, Apache, MySQL, and PHP.

Users/Access

Any employee in the internal network can access the default Apache web page. Access to the web page outside of the internal network is dependent on the Firewall’s ACL. Nevertheless, as this is a web server residing in the DMZ, limitations are less stringent to any attempts trying to access the internal network from the outside.

Configuration:

1. Download Ubuntu 18.04.4 LTS form https://ubuntu.com/download/desktop then install it on VMware.

2. Open the terminal to install any updates, the LAMP stack, and to configure Apache.

3. Update your system

4. Install Apache, MySQL, PHP

5. Configure Apache. Open the apache2.conf

6. Open the mpm_prefork.conf file located in /etc/apache2/mods-available and edit the configuration.

7. Check to make sure the ports 80 and 443 are enabled for Apache

8. To allow incoming HTTP and HTTPS traffic

9. Disable the event module and enable prefork

10. Restart Apache

Securing the LAMP server

When it comes to securing the lamp server it is relatively quick and simple, to start off you will want to configure the firewall to allow basic services like openSSH and Apache. We will want to disable unused or unwanted services. Fail2ban is a service that we will want to put on this server for the case that there are many login failures, faill2ban will block the IP address that is showing malicious signs.

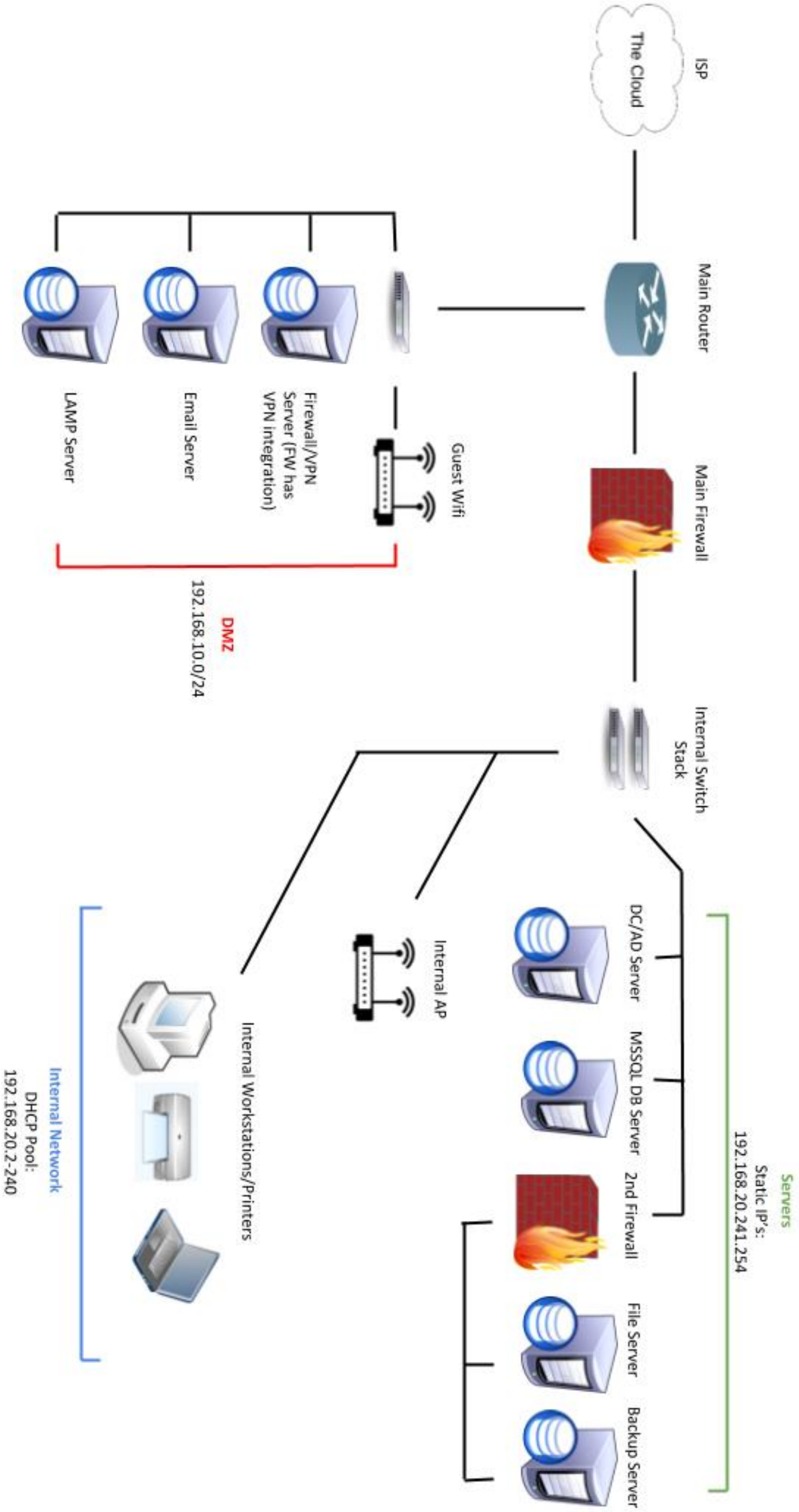
Next we will hide Apache's sensitive information since it provides much information that can be used against the server. Another way we will secure the server is by setting up and web application firewall (WAF) with Mod_security. Mod_security provides protection against attacks like SQL injections, session hijacking, cross site scripting, bad user agents along with many others. We will use Apaches module called mod_evasive this will be used to protect the web server form DoS, DDoS, and brute-force attacks.

We will want to create separate MySQL users for each database and application. We will want to disable the LOCAL INFILE since we don't use it.

To secure PHP we will hide the basic information, disable functions that could be harmful to your system, restrict file uploads by creating a max file size that can be uploaded and set a maximum execution time that set the maximum time a script is allowed to run and maximum amount of memory it is allow to use. Lastly, we will want to enable open_basedir this allows you to set the location from which PHP is allowed to access files.

Since the server uses SSH you will want to prevent remote logins from accounts with empty passwords. Next you will want to configure an idle timeout to avoid having an unattended SSH session. Limit the SSH access to provide another layer of security, you should limit your SSH logins to only certain users who need remote access. You will want to disable root logins through SSH. Changing the port and using a non-standard port is a way to avoid being seen by casual scans. Other things you should do for SSH are enable two-factor authentication and use strong usernames and passwords.

Cyanobac Network Map



ISP
The Cloud
Main Router
Main Firewall
Internal Switch Stack
Guest Wifi
Firewall/VPN Server (FW has VPN integration)
Email Server
LAMP Server
DMZ
192.168.10.0/24
Servers
Static IP's:
192.168.20.241.254
DC/AD Server
MSSQL DB Server
2nd Firewall
File Server
Backup Server
Internal AP
Internal Workstations/Printers
Internal Network
DHCP Pool:
192.168.20.2-240