

Test Project

Module A Linux Environment

IT Network Systems Administration

Independent Test Project Designer: Fabian Flückiger
Independent Test Project Validator: Troy Pretty

Contents

Introduction	3
<i>Login</i>	<i>3</i>
<i>System Configuration</i>	<i>3</i>
<i>Important: Grading.....</i>	<i>3</i>
<i>Software</i>	<i>3</i>
<i>Networking & SSH.....</i>	<i>3</i>
Description of project and tasks	4
<i>Intro</i>	<i>4</i>
<i>General Configuration</i>	<i>4</i>
<i>Servers and Clients.....</i>	<i>4</i>
<i>DNS-Zone notes</i>	<i>5</i>
<i>LDAP Users.....</i>	<i>5</i>
<i>Samba Users</i>	<i>5</i>
<i>Topology.....</i>	<i>6</i>
<i>Part 1: Internal Network</i>	<i>7</i>
<i>int-srv01.int.worldskills.org</i>	<i>7</i>
<i>Part 2: Firewall</i>	<i>8</i>
<i>fw.worldskills.org.....</i>	<i>8</i>
<i>Part 3: DMZ</i>	<i>9</i>
<i>mail.dmz.worldskills.org.....</i>	<i>9</i>
<i>ha-prx01.dmz.worldskills.org and ha-prx02.dmz.worldskills.org</i>	<i>10</i>
<i>web01.dmz.worldskills.org and web02.dmz.worldskills.org</i>	<i>10</i>
<i>Part 4: Client (jamie-ws01)</i>	<i>11</i>

Introduction

Welcome to module A!

To successfully complete this module, please **read** the following instructions **carefully**!

The competition has a fixed start and finish time. It's up to you to allocate your time wisely.

Login

Unless otherwise specified within this document, use the following information for all servers and services:

Username: root / user

Password: Skill39@Lyon

System Configuration

Region/Timezone: Europe/Paris

Locale: English US (UTF-8)

Key Map: English US

Important: Grading

The majority of assessment performed are functional marking, you are allowed to choose any package you prefer for task completion, such as Apache or NGINX. However, if a particular package is specified, ensure to install the one.

Please note that we will not modify your configurations or restart any services or virtual machines unless specifically stated, so ensure they remain operational/running at the end of the competition. Services that are non-functional at the end of the competition, even if nearly fully configured, will not earn you points.

To run our checks, we will use ssh connections and the ssh key mentioned below in "Networking and SSH".

There might be several ways to complete a specific task.

Software

For testing purpose, all Linux hosts have been installed with the following test tools: smbclient, curl, lynx, dnsutils, ldap-utils, ftp, lftp, wget, ssh, nfs-common, rsync, telnet, traceroute, tcptraceroute, tcpdump

All VMs are equipped with all Debian Blu-ray discs. This allows you to install software using APT.

In addition, the VM **ha-prx01** is equipped with GNOME, Visual Studio Code and Zeal Docs (offline documentation) for Python3, Ansible, NGINX and Bash

Networking and SSH

Unless otherwise specified, all services should be accessible through IPv4 and IPv6 (Dual Stack).

To make your life a bit easier, networking has been preconfigured on all machines.

Every host is equipped with a ssh key for root located at /root/.ssh/id_ed25519. It is also included in the authorized_keys file of root on all hosts. You are allowed to use it to connect to other hosts. Do **NOT** modify it!

Description of project and tasks

Intro

The IT-startup ClearSky (no clouds) hired you to setup their new IT-infrastructure. After their CFO saw their last cloud bill, they decided to leave the cloud and move their IT back onto local hardware.

General Configuration

Table 1: Servers and Clients

FULLY QUALIFIED DOMAIN NAME	IPV4	IPV6	SERVICES
fw.worldskills.org	WAN: 1.1.1.10/24 INT: 10.1.10.1/24 DMZ: 10.1.20.1/24 VPN: 10.1.30.1/24	WAN: 2001:db8:1111::10/64 INT: 2001:db8:1001:10::1/64 DMZ: 2001:db8:1001:20::1/64 VPN: 2001:db8:1001:30::1/64	Transparent proxy (squid), Firewall (nftables) VPN Server (WireGuard)
int-srv01.int.worldskills.org	INT: 10.1.10.10/24	INT: 2001:db8:1001:10::10/64	CA, LDAP, Samba, DNS Server (BIND9)
mail.dmz.worldskills.org	DMZ: 10.1.20.10/24	DMZ: 2001:db8:1001:20::10/64	Mail server (Dovecot + Postfix)
prx-vrrp.dmz.worldskills.org	DMZ: 10.1.20.20/24	DMZ: 2001:db8:1001:20::20/64	Reverse proxy virtual IP
ha-prx01.dmz.worldskills.org	DMZ: 10.1.20.21/24	DMZ: 2001:db8:1001:20::21/64	Reverse Proxy, DNS Server (BIND9)
ha-prx02.dmz.worldskills.org	DMZ: 10.1.20.22/24	DMZ: 2001:db8:1001:20::22/64	Reverse Proxy, DNS Server (BIND9)
web01.dmz.worldskills.org	DMZ: 10.1.20.31/24	DMZ: 2001:db8:1001:20::31/64	Web server
web02.dmz.worldskills.org	DMZ: 10.1.20.32/24	DMZ: 2001:db8:1001:20::32/64	Web server
jamie-ws01.ext.worldskills.org	WAN: 1.1.1.20/24 VPN: 10.1.30.2/24	WAN: 2001:db8:1111::20/64 VPN: 2001:db8:1001:30::2/64	E-Mail Client, VPN-Client, Browser

DNS-Zone notes

When discussing on how to configure the DNS servers with the customer, you made the following notes:

Internal network

- Create both forward and reverse lookup zones and dns records for all devices in the network (see “Servers and Clients” above)
- Create a service record for LDAP. Make sure it points to int-srv01 when auth.int.worldskills.org is queried.
 - Protocol is TCP, port is 389, priority 10 and weight is 50.

DMZ network

- Create both forward and reverse lookup zones and dns records for all devices in the network (see “Servers and Clients” above)
- Add an alias for www.dmz.worldskills.org to prx-vrrp.dmz.worldskills.org (you are not allowed to create an A record for this!)

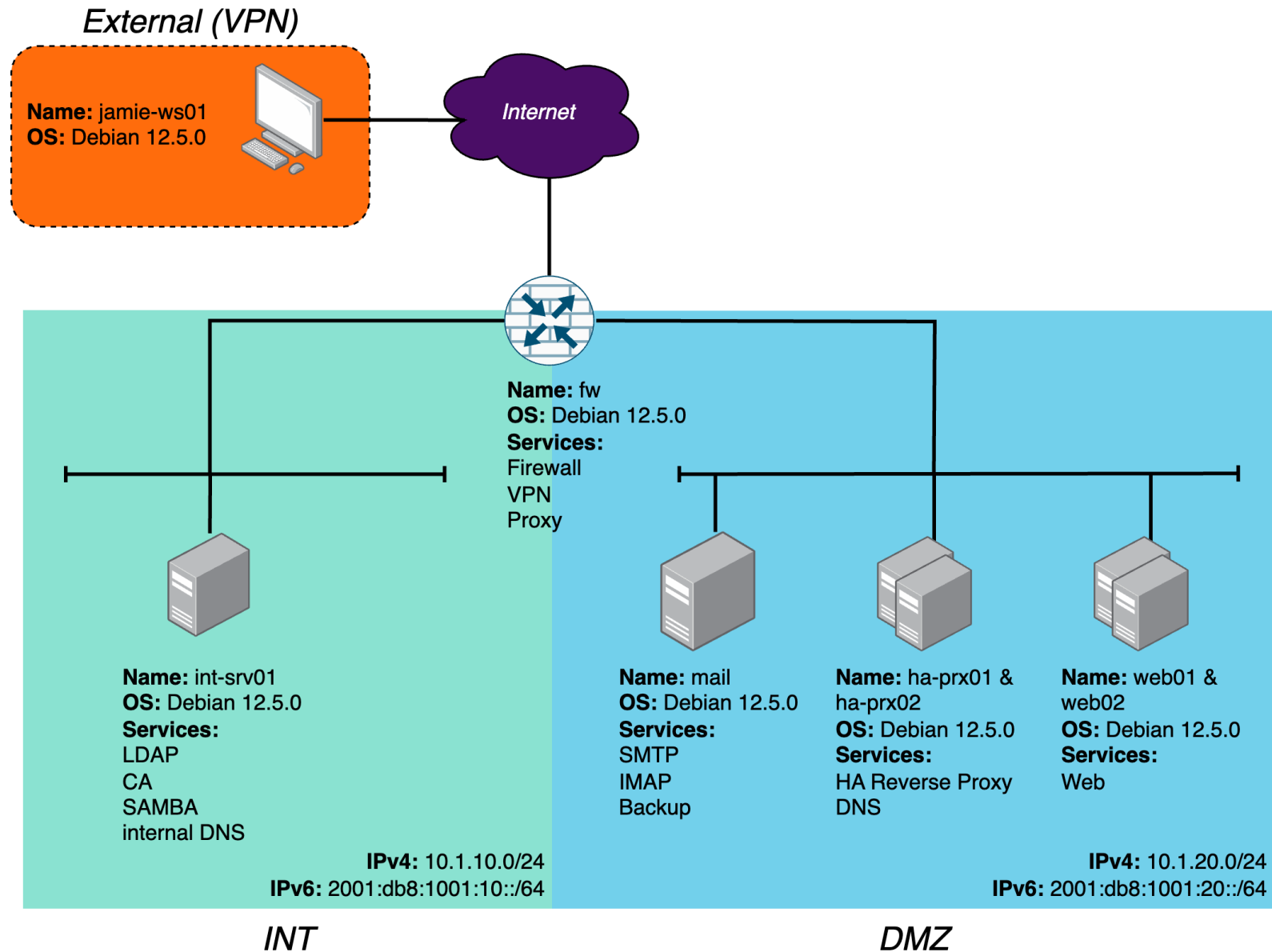
Table 2: LDAP Users

FULL NAME	USERNAME (UID)	PASSWORD	OU	E-MAIL ADDRESS
Jamie Oliver	jamie	Skill39@Lyon	Employees	jamie.oliver@dmz.worldskills.org
Peter Fox	peter	Skill39@Lyon	Employees	peter.fox@dmz.worldskills.org
Administrator	admin	Skill39@Lyon		

Tables 3: Samba Users

USERNAME	PASSWORD
jamie	Skill39@Lyon

Topology



Part 1: Internal Network

int-srv01.int.worldskills.org

This server will act as internal server providing authentication, certificate authority (CA), file and DNS services

LDAP

Install a LDAP server.

1. The LDAP server will be used for authentication for users to log in to the mail server. Add the domain int.worldskills.org and all users including the attributes specified in the Table 2 to the LDAP database.

CA

Using OpenSSL, create a root CA and one sub-CA:

1. Root CA:
 - (a) Use “ClearSky Root CA” as the name (CN) for the root CA.
 - (b) For unspecified fields (i.e. CN, Country, etc.) you may use any value.
2. Sub-CA Services:
 - (a) Create a certificate for your web servers which is valid for www.dmz.worldskills.org
 - (b) Create a certificate for the mail server valid for mail.dmz.worldskills.org
3. Ensure a copy of each certificate is located in /opt/grading/ca, so our experts can find them during marking:
 - (a) CA: ca.pem
 - (b) Sub-CA Services: services.pem
 - (c) Certificate webserver: web.pem
 - (d) Certificate mailserver: mail.pem

Samba

Configure a file server using Samba.

1. Create users according to the Table 3 Samba Users in the General Configuration section (Note: you are allowed to create local users for this. You don't have to connect Samba to LDAP)
2. Configure the following shares:
 - (a) /public: everybody (even guests without user) should be able to read files, only logged-in users are allowed to write files
 - (b) /internal: only authenticated users are allowed to read and write, guests are not allowed to access this share

Internal DNS

Install and configure BIND9.

1. Create the zone int.worldskills.org and the corresponding reverse zones.
2. Add the DNS records according to the DNS zone notes in the General Configuration section.
3. Make sure the zone dmz.worldskills.org, as well as its reverse zones, get synced from the DMZ DNS servers. (You are not allowed to manually transfer them!)
4. As this will be the DNS server used by the employee-devices, enable recursion.

Part 2: Firewall

fw.worldskills.org

This host will act as a router, firewall and transparent proxy.

Packet Forwarding

Configure Linux to forward both IPv4 and IPv6 packets

Firewall & NAT

Using nftables, configure the following rules:

1. IPv4
 - (a) Traffic originating from INT and DMZ to the internet should be allowed.
 - (b) Traffic originating from INT to the DMZ should be allowed
 - (c) Any traffic leaving the firewall on the WAN interface should use the firewall's WAN-IP as source (Masquerade NAT)
 - (d) Configure the following port forwardings:
 - (i) HTTP (80/tcp) should get forwarded to the high available reverse proxy in the DMZ
 - (ii) HTTPS (443/tcp) should get forwarded to the high available reverse proxy in the DMZ
 - (iii) DNS (53/udp, 53/tcp) should get forwarded to the high available DNS server (reverse proxy) in the DMZ
 - (e) Clients connected to the VPN should have access to both internal and DMZ networks
 - (f) The mail server should be able to query LDAP on the int-srv01 server
 - (g) Any other traffic should be dropped (default deny)
2. IPv6
 - (a) Traffic originating from INT and DMZ to the internet should be allowed.
 - (b) Traffic originating from INT to the DMZ should be allowed
 - (c) Clients connected to the VPN should have access to both internal and DMZ networks
 - (d) Allow HTTP (80/tcp) and HTTPS (443/tcp) from WAN to the high available reverse proxy in the DMZ

WireGuard VPN

Configure WireGuard as VPN solution to establish a secure connection from the external workstation to the internal network. You should route any traffic from the client through the tunnel. As an additional security measure, configure a pre-shared key for the tunnel. The external workstation should use the internal DNS server to resolve DNS hostnames. For the tunnel network, use the IP addresses mentioned in the general configuration table

Make sure to place the configuration file (wg0.conf) in /etc/wireguard and use wg-quick to run it as a system service.

Transparent proxy

Configure a transparent proxy service.

1. Any traffic originating from the internal network as well as from the VPN network with the destination port 80 should get intercepted by the transparent proxy
2. The proxy should add the following header to any proxied HTTP response: x-secured-by: clearsky-proxy

Part 3: DMZ

mail.dmz.worldskills.org

This host will act as IMAP (Dovecot) and SMTP- (Postfix) server.

Mail server

Configure a mail server using dovecot and postfix.

1. Install dovecot and postfix and configure them to fulfil the requirements below.
2. Configure the server to send and receive emails for **dmz.worldskills.org**
 - (a) The users should be able to access their mailbox via IMAP (tcp/143) & IMAPS (tcp/993).
 - (b) All communication between this server and the clients should be secured with TLS. If you completed the task “CA”, use the certificate you created for the mail server. Ensure a client which only trusts the “ClearSky Root CA” is able to validate the entire chain. Otherwise, generate a self-signed certificate.
3. Make sure the LDAP user jamie created in the LDAP task can login using his username and access his mailbox. The mail attribute of the LDAP user should be used as the mail address.
4. Upon receiving an email at echo@dmz.worldskills.org, the system should automatically respond to the sender with either the original email content (echo) or a custom thank-you message. (Note: A non-delivery report does not qualify as a response.)

Backup

Due to space and budget constraints, it is currently not possible to do an automated off-site backup to a secure location. To prevent a total loss of data in case the server-room burns down, you decided to setup a backup to an external disk (The external disk is being simulated by the disk /dev/sdb attached to the VM)

1. Create a mount point at /opt/backup and mount the disk to it.
2. Ensure the backup disk is mounted automatically during server startup.
3. Create a script to automatically backup the mailbox data, as well as important mail server configurations to /opt/backup. You should be able to re-create the mailserver in case of complete loss using your backup! save the script as /opt/backup.sh

SSH key management

To simplify SSH key management, your team decided to instead of putting all ssh public keys on all servers, you will make use of the SSH user certificate functionality. As a proof of concept, this technology should be used to access the mail server only.

1. Configure this server to accept SSH logins using SSH user certificates.
2. Configure ssh on ha-prx01 to use an SSH certificate to login when connecting to the mail server as user root.

ha-prx01.dmz.worldskills.org and ha-prx02.dmz.worldskills.org

These two servers will act as a high-available reverse proxy and DNS

Reverse proxy

Configure a **high-available** reverse proxy on the VMs ha-prx01 and ha-prx02.

1. The services should always be available via the virtual IP 10.1.20.20/24 and 2001:db8:1001:20::20/64
2. Requests sent via HTTP should be redirected to HTTPS
3. If one web server goes down, requests should get forwarded to the other web server
4. To make troubleshooting easier, the proxies should add the header “via-proxy: hostname” (replace hostname with the proxy hostname) to the response
5. The proxy should do TLS termination.
6. If you completed the CA task, use the generated “web” certificate. Ensure that a client which only trusts the root CA is able to validate the entire chain.
7. If you did not complete the CA task, create a self-signed certificate.
8. In case the reverse proxy process is not running, the other VM should take over the IP 10.1.20.20/24 / 2001:db8:1001:20::20/64 and provide the services there

DNS server

Configure a primary and secondary DNS Server on the VMs ha-prx01 and ha-prx02.

1. use ha-prx01 as primary DNS server. The DNS zones should be transferred to ha-prx02 via DNS zone transfer.
2. create the DNS zone dmz.worldskills.org, the corresponding reverse zones and records according to the DNS-zone note in the general section
3. make sure the server only answers queries for its authoritative DNS zones

web01.dmz.worldskills.org and web02.dmz.worldskills.org

These two servers will act as the web servers.

Web server

Install a web server on the VMs web01 and web02. As you expect a higher load in the future, your team has decided to use Ansible to configure the web servers.

Note: For grading, the experts will restore the initial state of the VM “web02” and then try to apply your Ansible playbook from the VM ha-prx01 by running the command `ansible-playbook /opt/ansible/configure-web02.yml`. Make sure this exact command will work, as they will not be allowed to adapt/change it.

1. The web servers will host the website www.dmz.worldskills.org
2. As TLS gets terminated at the reverse proxy in front of the web servers, they only listen to port 80 (HTTP)
3. The web servers should serve the content of /opt/wwwroot/. A colleague from the web team already put all the necessary files there.
4. If no file is specified, serve main.html (you are not allowed to rename this file)
5. To make troubleshooting easier, make sure the server returns his hostname when /whoami is being accessed.
6. If a page is not found, return the file 404.html located in /opt/wwwroot/

Part 4: Client (jamie-ws01)

This host acts as remote workstation for the ClearSky CEO.

General configuration

Install GNOME as desktop environment and create a new local user Jamie Oliver (jamie) with the password “Skill39@Lyon”. To facilitate the management of the VPN, setup the wireguard-connection in networkmanager and connect to it.

Browser & mail client

Install Thunderbird and Firefox, import the root-CA certificate into the according CA stores

1. In Firefox, define <https://www.dmz.worldskills.org> as homepage
2. In Thunderbird, setup e-mail for Jamie.