Small Home Office (SOHO)
Private Email
Proposal

December 2019

Western Governors University (WGU)

B.S.I.T. Capstone Project

Revision History

Date	Revision	Description	Author
12/25/2019	1.0	Initial Release, Final Exam	K.L. Geels, Student

Table of Contents

1 Overview

As part of its small office home office business launch, Figchen, Inc planned to establish a Local Area Network (LAN) connected to the internet via Internet Service Provider (ISP). To operate within a secretive and competitive research and development (R&D) sector, the company intended to prioritize end-to-end communications security and the ability to exchange emails in a confidential manner that obscures visibility into its corporate activities and instills customer confidence, while maintaining simplicity and low costs. The SOHO LAN solution for Figchen, Inc. was based on delivery of a secure private email server designed around inexpensive hardware and software that could be easily maintained and monitored for a period of a few years prior to reaching obsolescence. The project evolved as expected, with all project activity taking place in a live environment without interrupting unrelated internet activity.

The initial selection of the host environment was based on a comparison of the pros and cons of a virtual environment compared to purchasing an appliance. Quick experimentation ended in selection of the hardware purchase. The domain name www. Figchen.online was registered, and the operating system was installed with a few minor disruptions, including the unexpected revelation that ethernet ports are no longer “out of the box” components on modern PCs. Apparently, based on advances in wireless technology, the trend is to rely on wireless as the primary means of connecting to the internet, with a physical cable considered non-standard. This fact caused a reinstallation of the OS, since that process is mainly automatically configured, so that the first installation from the USB and without the ethernet adapter resulted in a failure of the OS to recognize and label the add-on converter port. The re-install resolved the issue and the Ubuntu environment was established.

After the Ubuntu OS was installed and network connectivity verified with a ping, basic OS security measures (updates and firewall) commenced without mishap. Initial port testing confirmed that the ISP had blocked a port required for email communications (SMTP port 25), causing a project pause to compare alternative solutions (relay host or block removal), ultimately resolved by a flat fee to the service provide for removal of the port block. After lengthy consultation with the ISP, the block removal was verified instantly. Project resumed with installation of the mail server, which successfully passed connectivity tests, completing functional implementation. The project concluded with a detailed markup of the documentation package to include account numbers, user ids and passwords, and detailed command line instructions for key functional tests.

2 Review of Other Work

2.1 Build Your Own Email Server on Ubuntu: Basic Postfix Setup

Having discovered the abundance of guide material on setting up a private Ubuntu Postfix server, the challenge became selection for actual implementation. The multi-part webzine series on the topic (Guoan, 2019) proved to have the advantages of being succinct and well-organized. In following the brief, simple, clear procedures, the server installation itself took only moments. Additionally, the article provided guidance and procedures on firewall settings and add-on software installations during the procedures, so that confusing cross-referencing was avoided.

2.2 DNS Management: Record Types and When to Use Them

Due to the offerings of the registrar service used to host the domain, DNS records maintenance was especially confusing. Much of the documentation on the web was full of self-referencing explanations that did little to clarify and much to confuse. DNS records updating is a very simple, short process with updating of only a few fields required. However, if the wrong field is updated, or the wrong information supplied, the email server would be unavailable. A tutorial offered as part of a series on DNS management (Pressable Knowledge Base, 2014) was especially helpful in achieving the proper DNS record changes were made for Figchen.online.

2.3 Web install

During the security certificate portion of the project, an unexpected requirement emerged to rely on a personal webserver as part of the certificate application process. The certificate application process is extremely complex, so that the requirement to apply from a personal web server was only apparent after multiple reviews of the procedures for obtaining the certificate. In the course of comparing the certificate procedures across multiple guides, one of the more complicated tutorials included a direct link to a separate stand-alone process guide for setting up a personal webserver. In that separate web-server tutorial (Hutchinson, 2012), the author delivered a detailed summary of different webserver advantages, as well as recommendation for which software to choose, and importantly, the Linux installation procedures. The process for standing up a personal email server was lengthy and complicated, due to being based on multiple complex IT topics, such as Domain Naming (DNS), SSL/TLS security, port blocking, OS installation, and finally – installing a webserver. The stand-alone tutorial for setting up a webserver was a really brief guide embedded in a highly convoluted tutorial for the email server. The two were completely unrelated to each other in terms of publication dates, and the author went into detail, providing a significant amount of research summarizing several different categories of information about the webserver installation process (software performance comparisons, software recommendations, and Linux webserver installation procedures). Following this guide (which was absent from the other detailed guides on email server SSL/TLS certificates allowed the project's scheduled to remain largely intact, with a delay of less than an hour to read the guide and complete the server installation.

3 Changes to the Project Environment

Figchen, Inc. was previously reliant on email service providers for email communications. Although higher service levels were available through higher fees for increased security, privacy, and confidentiality, all solutions lacked the key feature of providing Figchen with direct control over its own email server, configuration, and confidential email data. The designed solution consisted of establishing a domain and private email hosting server connected to the internet via traditional Internet Service Provider (ISP). A hardware appliance was purchased and added to the internal LAN in order to physically host the email server within the physical premises of the organization. A domain was registered in the company name, and DNS records updated to point to the installed webserver at www.Figchen.online and MX record updated to point to the mail server host. The ISP modified account settings for Figchen's internet connection to allow use of TCP port 25, which is essential for email communications to and from the premise. A web server was also installed on the host appliance, to meet basic requirements for certificates. This adds an element of vulnerability that must be handled with care through the firewall settings until the entire system is hardened for security.

4 Methodology

Plan Do Check Act (PDCA) was employed for this project, providing a simple framework that allowed the project to build layer on layer for testing purposes, and easily go backwards to isolate problems and solutions as necessary without affecting the entire project plan. The planning phase analyzed the technical requirements for the email system from the perspective of key considerations: security, availability of support, performance, and expense. Physical security and hardware performance of the appliance required less emphasis and rigor, compared to proven design security and low cost., because the hardware requirements can easily be met for this system (low usage), and physical security lacks the complexity of a large company with multiple locations and numerous personnel. Based on these facts, a physical appliance was chosen, due to lack of complexity and expense compared to virtual system (via a cloud service provider). Moving beyond the planning phase, implementation was an iterative process of “doing, checking, then acting”. After “doing” the OS installation, a check revealed the need to go backwards. The installation process itself was very speedy, however, network functionality failed during a “check” with a network PING test. The “act” phase consisted of attempting an OS restoration from the install disk. The 2nd check based on this solution failed, so that the “act” phase consisted of going backwards and uninstalling the OS completely, then reinstalling. A PING test to check the 3rd installation passed. The Postfix email server was installed, but a relay test failed. Troubleshooting checks revealed an ISP block. After comparing the options for resolution, the action was taken to pay a one-time fee to the ISP to unblock the port (essential to email communications, port 25/TCP) and a port test passed. Advancing to the SSL/TLS certificate phase to implement security, a review of the highly detailed procedures revealed that installation of a webserver was the easiest method to implement the certificate process on the email server. The webserver was installed, and then used to test the DNS records on the host server, which verified the A record was accurate. Additional testing concluded with a successful transmission of an email in the configured system to an email account, thereby concluding the Do, Check, Act portion of the project. As all phases of the testing were completed, the documentation was marked with the final procedures necessary for achieving a successful configuration.

5 Project Goals and Objectives

	Goal	Supporting objectives	Deliverables enabling the project objectives
1	Protect client and organizational confidentiality by	Register a company domain name	Company domain IP obtained through registrar service
			Security of access to registrar account verified

	Goal	Supporting objectives	Deliverables enabling the project objectives
	implementing a sustainable private email system	Configure a Linux host for the email server software	Host for email server designated
			Linux Ubuntu installed
			OS functionality verified
		Install an email server software on private email host	Linux Postfix email server (MTA) software installed
			Email functionality verified
		Configure email host with authentication for security	Host login permissions configured
			Email server SSL certificate configured
		Ensure encryption of all sessions to and to and from the server	Configure firewall with implicit SSL/TLS encryption for outbound SMTP traffic (port 465)
			Configure firewall with implicit SSL/TLS encryption for inbound IMAP traffic (port 993)
			Configure Postfix to enforce mandatory session encryption for all mail traffic
		Ensure knowledge transfer of system to allow client to use and maintain private email system	Document all software version and configuration information
			Document all procedures

With successful implementation of this project, Figchen, Inc. attained the goal of organizational confidentiality by implementing a sustainable private email system.

The first objective was met by registering a company domain name for the system and update the related DNS records so that emails could ultimately arrive at the IP server as designated. The selected registrar optionally offered the free service of account privacy related to the domain as an added safeguard, which provides a barrier to access to the account itself, in order to prevent that information in the account from tampering, and malicious hacking purposes to redirect the emails, take control of aspects of the host system, etc. The domain was registered and the privacy guard option selected in order to prevent visibility of the account owner and/or potential hacking into the account. Having verified the privacy guard option in the registrar's control panel, domain account privacy is established to prevent malicious hacking into the DNS MX record for the purpose of redirecting emails to a different email server.

The second objective was met by implementing a Linux Ubuntu OS on the host server. Linux was selected as an Operating System (OS) for the environment designated to host the email server, to best ensure physical control over the email system. It offers many performance and security advantages and is an open-source OS that is free to use. Version 18.04 LTS for Ubuntu Server was selected as the OS to run on the host environment because free support of this version has been scheduled for the next three years by the developer. It has the benefit of being more secure and requiring less memory and storage than a Windows OS, so that when operating under a similar hardware environment, performance outcomes are better from the Linux system. By meeting the objective of configuring a Linux host environment for the privately controlled emails system, a sustainable OS solution for the host was successfully implemented that is planned to last for a period of at least three years without requiring time-consuming or expensive upgrades.

The objective of installing an email server software on the private email host, to meet the confidentiality and sustainability goals of the project, Postfix is the email server software selected for this project, due to high ratings as an email server software compatible with Linux Ubuntu. Email configuration settings are potentially complex, so selecting a software that is well-documented and praised by the user audience supports the goal of a sustainable system offering widely available user support for the mail software portion of the email system. The risk of compatibility concerns were minimized, and the baseline email utility was successfully configured in minutes.

The goal of a confidential system is met by objectives that apply security of the email system to two security layers: the first layer is the permission required to login to the email host in order to send an email. The second form of authentication is an SSL certificate obtained and configured on the host email server to allow encrypted tunneling. Both objectives were met, ensuring the objectives of security to meet the goal of preserving privacy and intellectual property, and minimize the risk of impersonation and the ability to intrude into the host email server.

Once the host is configured with SSL/TLS certificates, the objective of enforcing encryption for all sessions was met by configuring the firewall of the email system to transmit across ports 465 and 993, and configuring the Postfix server software to deny communications with remote hosts unless the remote host accepts the request to encrypt the session tunnel. The goal of confidentiality is met by meeting this objective, so that man-in-the-middle threats to host security are eliminated, and all traffic leading into and out of the host must be sent across an encrypted tunnel. The end-to-end encryption ensures privacy of the credentials used to access the host system, which needs to be protected to avoid hacks into the host. Ports 465 and 993 are designated for transmitting email traffic across the encrypted tunnel.

Because Figchen, Inc. is a small organization attempting to establish its credibility, and does not yet have steady revenue streams, an accurate and complete documentation package is essential to a successful handoff to the client. By meeting the objective of delivering an accurate and thorough documentation package that is well-organized and easy to reference, the goal of sustainability is met, potential time for maintenance and repair is greatly minimized, compared to the absence of system configuration and user procedures. If troubleshooting is required, the system itself is clearly documented to minimize necessary time and effort. Documented usage and maintenance of the system was captured at a detailed procedural level.

6 Project Timeline

Milestone or deliverable	Planned Duration (hours)	Actual Duration (hours)	Actual start date	Actual end date
Host for email server designated	2	4	12/18/19	12/18/19
Linux Ubuntu installed	4	4	12/19/19	12/19/19
OS functionality verified	1	1	12/19/19	12/19/19
Linux Postfix email server (MTA) software installed	3	1	12/20/19	12/20/19
Email functionality verified	4	1	12/20/19	12/20/19
Host login permissions configured	2	1	12/18/19	12/18/19
Email server SSL certificate configured	4	6	12/21/19	12/21/19
Configure firewall with implicit SSL/TLS encryption for outbound SMTP traffic (port 465)	1.5	.5	12/22/19	12/22/19
Configure firewall with implicit SSL/TLS encryption for inbound IMAP traffic (port 993)	1.5	.5	12/22/19	12/22/19
Configure Postfix to enforce mandatory session encryption for all mail traffic	5	1	12/22/19	12/22/19
Document all software version and configuration information	7	4	12/23/19	12/23/19
Document all procedures	7	4	12/23/19	12/23/19

The project started and finished earlier than planned by four days. Although unexpected events occurred, the schedule had been built upon unplanned events occurring. Such events included the extra time it took to purchase an additional hardware device, due to an unmet requirement during initial hardware selection. Another delay occurred during OS installation, due to the OS having to be installed three different times before passing the OS tests. Since ample time was scheduled for the OS installation, this did not adversely impact the schedule. The third unexpected requirement emerged during the SSL/TLS certification process, due to the previously unrecognized recommendation to rely on a personal webserver for the process, to make it simpler. Since the requirement was not visible during the planning phase, it took a small amount of time to research and complete the webserver install. However, due to the known complexity of SSL/TLS certification, ample time had been scheduled, so this did not adversely impact delivery either. Due to the complexity of the project, the duration of the task was doubled and sometimes tripled, to accommodate the need for research and unexpected complications. Time was also made up in areas where complications were expected but did not occur due to the well-written procedures used for the project. In particular, the Postfix installation and encryption installation went more quickly than expected due to clearly written procedures. The documentation package was also less time-consuming due to having been maintained as the project was developing, instead of saved until the end. All in all, the project tempo went as expected, because it was planned around the likelihood that many things would not go as expected.

7 Unanticipated Requirements

As expected, requirements emerged in the course of the project that required additional investigation, decision-making, and expense:

Initially, Amazon Cloud’s virtual services were selected for the email server’s host environment. However, the interface and billing environment proved too complex, so the physical hardware option for on-premise server was chosen.

Upon purchasing an inexpensive appliance and installing Ubuntu via USB, it was realized that the appliance was defaulted to wireless internet and did not have an on-board ethernet (recommended for email security). Although ethernet adapters are relatively inexpensive, it did cause a delay, and caused Ubuntu to have to be re-installed, due to the complexity of ethernet port assignments in the OS.

Port testing revealed that the ISP blocks port 25 by default to prevent email abuses such as high-volume sending. The fix turned out to be removal of the block for a flat fee. This was elected as the preferred option, after researching availability of a relay host service. The relay host was deemed less secure, since the service provider maintains a duplicate copy of the email data.

Installation of a webserver turned out to be the path of least resistance for obtaining the encryption certificates (SSL/TLS). A last-minute install of Linux’s Apache2 webserver was a simple solution but does alter the host environment. Maintenance of a web server on the same host as the email server is ill-advised for security reasons, therefore it’s advised to relocate the web server to a different appliance, once additional consideration has been given to the overall security of the Figchen LAN. For now, the firewall will be used to limit access via the web server.

8 Conclusion

The outcome of this project is a private email system for the SOHO Figchen, Inc., and a documentation package that allows the small company to sustain the email system in an efficient way. The documentation package proactively describes maintenance procedures (such as vulnerability patching) and includes all the necessary the system configuration, software versions, and account information (registrar and ISP) so that if an external consultant is required for technical support, the topic can be addressed with as little time and energy as possible. The completed system provides Figchen the assurance of security and privacy desired by the company in order to protect all intellectual property exchanged by email. It masks the organization's activity so that its data cannot be harvested, nor is it a vulnerable target of marketers and/or malicious competitors based on visibility into its activity and protection of intellectual property. The success of the project was measured by functionality tests at each stage of the configuration, and a final functionality test demonstrating emails can be securely and confidentially sent and received via the internet.

9 Project Deliverables

The items described in this section are those deliverables that were captured as key demonstrations of the success of the project. Actual artifacts are included in the appendices, and linked directly from within the description of each deliverable.

9.1 Privacy Guard Verified (Protects Privacy of Account Information to Prevent Malicious Intrusion)

Upon completing domain registration, the privacy guard option was enabled on the account (*see* **Error! Reference source not found.** *Artifact*). This option redirects domain inquiries to the registrar information (in this case Namecheap), and blocks visibility into the individual registrant (in this case, Figchen, Inc.). It's an essential element of the email system environment to prevent account intrusion and DNS MX record modification that could redirect email communications to a malicious host.

9.2 Successful Boot and Network Ping (OS Installation)

The successful installation of the Linux Ubuntu Operating System was demonstrated by a screen capture of the boot screen upon successful load, and then successful execution of the OS configuration by capturing a screenshot of the network PING, which was achieved at the command line from within the Ubuntu OS (*see artifact in* **Error! Reference source not found.**). Initially, the PING command failed due to the lack of ethernet port identification when connected via physical cable (versus wireless). A 3rd installation of the Operating System (the 2nd failed) resolved the issued, and the PING command successfully communicated with an external network.

9.3 Successful Email Transmission

Upon successful configuration, functionality of the completed system and its ability to communicate with external email systems was verified by capturing a screenshot of an email sent from Figchen's new installed email server and received by an external email system (*see artifact in* **Error! Reference source not found.**).

9.4 Thorough Documentation Package

Delivering thorough documentation was included as a key deliverable to sustain a successful project. Figchen is a small company that cannot afford interruptions and delays in critical services. Maintenance and service times will be kept within reasonable and efficient timelines based on delivery of a thorough and organized documentation package. The table of contents for the package is shown in **Error! Reference source not found.**.

10 References

Guoan, X. (2019, December 11). *Build Your Own Email Server on Ubuntu.* Retrieved from Linuxbabe: https://www.linuxbabe.com/mail-server/setup-basic-postfix-mail-sever-ubuntu

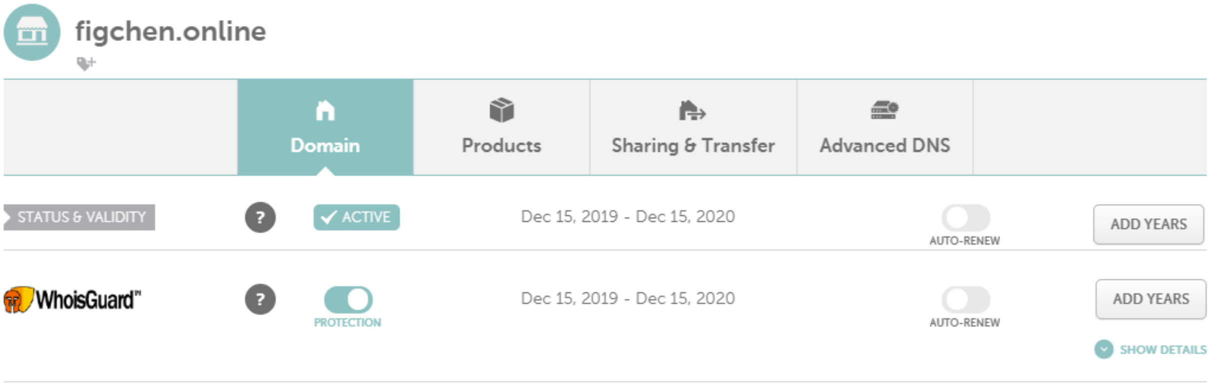
Hutchinson, L. (2012, November 27). *ARS Technica.* Retrieved from How to set up a safe and secure Web browser: https://arstechnica.com/gadgets/2012/11/how-to-set-up-a-safe-and-secure-web-server/

Pressable Knowledge Base. (2014, December 23). *DNS MANAGEMENT: RECORD TYPES AND WHEN TO USE THEM.* Retrieved from Pressable: https://kb.pressable.com/article/dns-record-types-explained/

Appendix A. Acronyms and Abbreviations

Appendix B. Artifacts

B.1 DNS Records and Privacy Guard

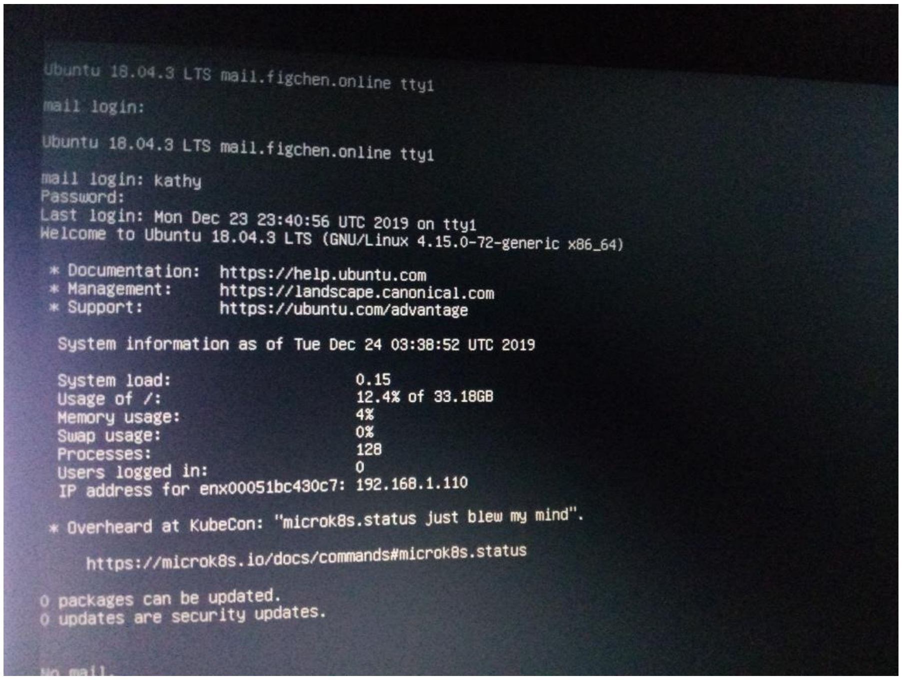

figchen.online

STATUS & VALIDITY ? ✓ ACTIVE Dec 15, 2019 - Dec 15, 2020 AUTO-RENEW ADD YEARS

WhoisGuard™ ? PROTECTION Dec 15, 2019 - Dec 15, 2020 AUTO-RENEW ADD YEARS

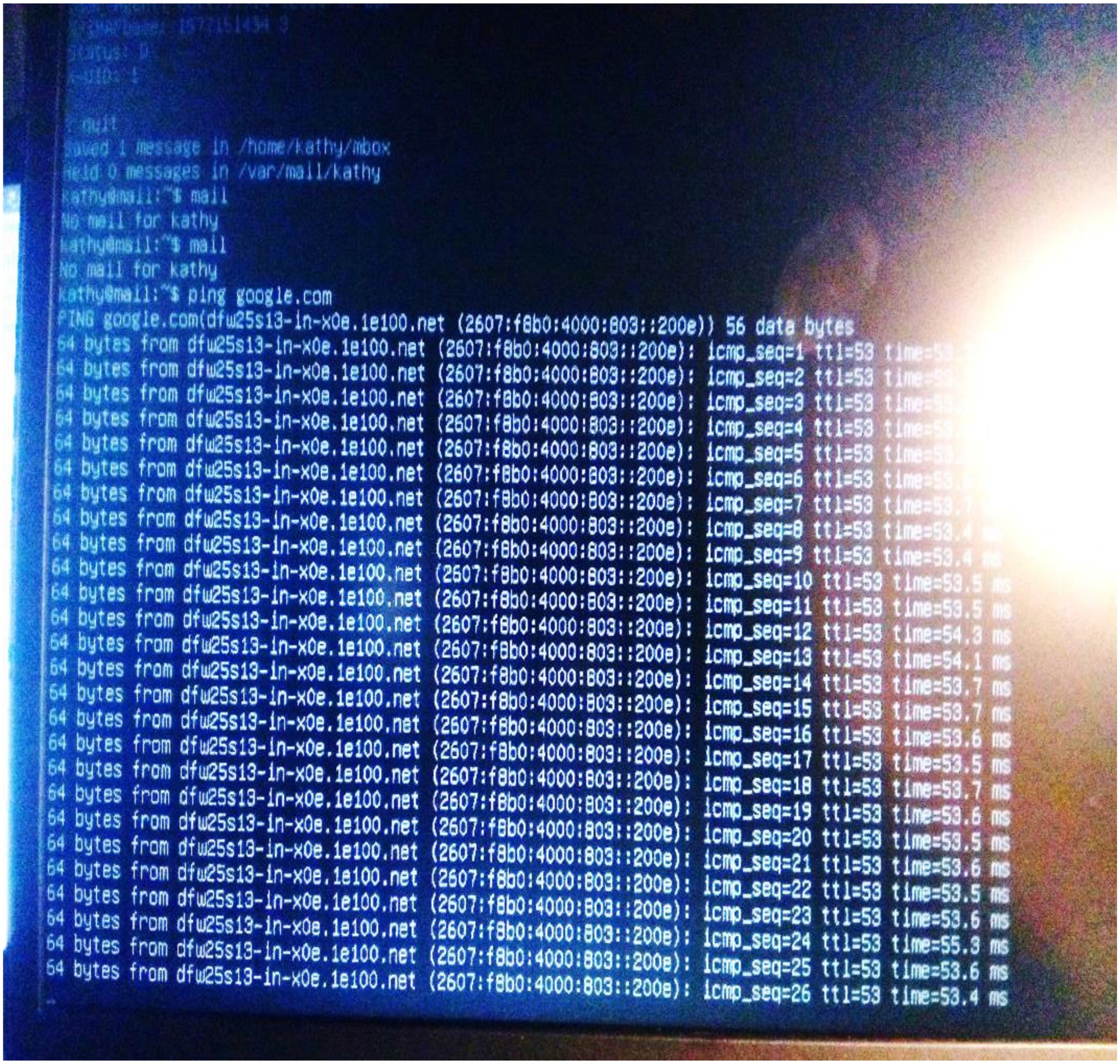
Figure 1 Privacy Guard option (Shown on Registrar's Domain Management Panel)

B.2 Successful Boot and Network PING after Ubuntu 18.04 reinstall



```
Ubuntu 18.04.3 LTS mail.figchen.online tty1

mail login:

Ubuntu 18.04.3 LTS mail.figchen.online tty1

mail login: kathy
Password:
Last login: Mon Dec 23 23:40:56 UTC 2019 on tty1
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-72-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue Dec 24 03:38:52 UTC 2019

  System load:                    0.15
  Usage of /:                     12.4% of 33.18GB
  Memory usage:                   4%
  Swap usage:                     0%
  Processes:                      128
  Users logged in:                0
  IP address for enx00051bc430c7: 192.168.1.110

 * Overheard at KubeCon: "microk8s.status just blew my mind".

     https://microk8s.io/docs/commands#microk8s.status

0 packages can be updated.
0 updates are security updates.


No mail.
```

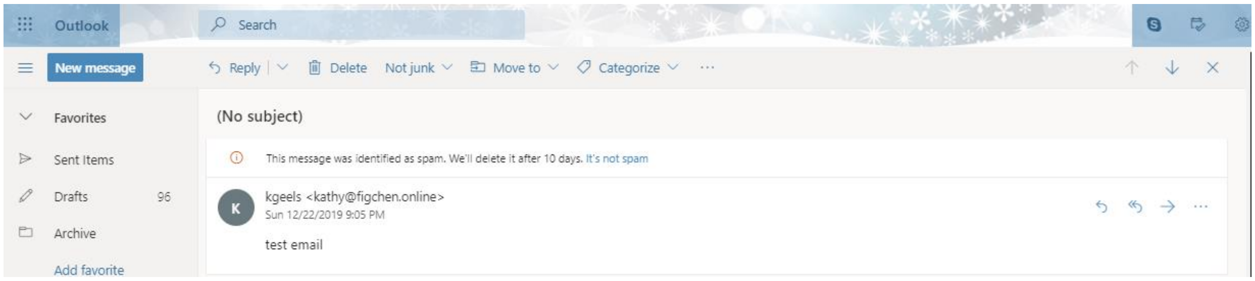
Figure 2 Boot screen after Successful Ubuntu Server Installation



```
X-IMAPbase: 1577151434 3
Status: O
X-UID: 1

? quit
Saved 1 message in /home/kathy/mbox
Held 0 messages in /var/mail/kathy
kathy@mail:~$ mail
No mail for kathy
kathy@mail:~$ mail
No mail for kathy
kathy@mail:~$ ping google.com
PING google.com(dfw25s13-in-x0e.1e100.net (2607:f8b0:4000:803::200e)) 56 data bytes
64 bytes from dfw25s13-in-x0e.1e100.net (2607:f8b0:4000:803::200e): icmp_seq=1 ttl=53 time=53
64 bytes from dfw25s13-in-x0e.1e100.net (2607:f8b0:4000:803::200e): icmp_seq=2 ttl=53 time=53
64 bytes from dfw25s13-in-x0e.1e100.net (2607:f8b0:4000:803::200e): icmp_seq=3 ttl=53 time=5
64 bytes from dfw25s13-in-x0e.1e100.net (2607:f8b0:4000:803::200e): icmp_seq=4 ttl=53 time=53
64 bytes from dfw25s13-in-x0e.1e100.net (2607:f8b0:4000:803::200e): icmp_seq=5 ttl=53 time=53
64 bytes from dfw25s13-in-x0e.1e100.net (2607:f8b0:4000:803::200e): icmp_seq=6 ttl=53 time=53.
64 bytes from dfw25s13-in-x0e.1e100.net (2607:f8b0:4000:803::200e): icmp_seq=7 ttl=53 time=53.7
64 bytes from dfw25s13-in-x0e.1e100.net (2607:f8b0:4000:803::200e): icmp_seq=8 ttl=53 time=53.4 ms
64 bytes from dfw25s13-in-x0e.1e100.net (2607:f8b0:4000:803::200e): icmp_seq=9 ttl=53 time=53.4 ms
64 bytes from dfw25s13-in-x0e.1e100.net (2607:f8b0:4000:803::200e): icmp_seq=10 ttl=53 time=53.5 ms
64 bytes from dfw25s13-in-x0e.1e100.net (2607:f8b0:4000:803::200e): icmp_seq=11 ttl=53 time=53.5 ms
64 bytes from dfw25s13-in-x0e.1e100.net (2607:f8b0:4000:803::200e): icmp_seq=12 ttl=53 time=54.3 ms
64 bytes from dfw25s13-in-x0e.1e100.net (2607:f8b0:4000:803::200e): icmp_seq=13 ttl=53 time=54.1 ms
64 bytes from dfw25s13-in-x0e.1e100.net (2607:f8b0:4000:803::200e): icmp_seq=14 ttl=53 time=53.7 ms
64 bytes from dfw25s13-in-x0e.1e100.net (2607:f8b0:4000:803::200e): icmp_seq=15 ttl=53 time=53.7 ms
64 bytes from dfw25s13-in-x0e.1e100.net (2607:f8b0:4000:803::200e): icmp_seq=16 ttl=53 time=53.6 ms
64 bytes from dfw25s13-in-x0e.1e100.net (2607:f8b0:4000:803::200e): icmp_seq=17 ttl=53 time=53.5 ms
64 bytes from dfw25s13-in-x0e.1e100.net (2607:f8b0:4000:803::200e): icmp_seq=18 ttl=53 time=53.7 ms
64 bytes from dfw25s13-in-x0e.1e100.net (2607:f8b0:4000:803::200e): icmp_seq=19 ttl=53 time=53.6 ms
64 bytes from dfw25s13-in-x0e.1e100.net (2607:f8b0:4000:803::200e): icmp_seq=20 ttl=53 time=53.5 ms
64 bytes from dfw25s13-in-x0e.1e100.net (2607:f8b0:4000:803::200e): icmp_seq=21 ttl=53 time=53.6 ms
64 bytes from dfw25s13-in-x0e.1e100.net (2607:f8b0:4000:803::200e): icmp_seq=22 ttl=53 time=53.5 ms
64 bytes from dfw25s13-in-x0e.1e100.net (2607:f8b0:4000:803::200e): icmp_seq=23 ttl=53 time=53.6 ms
64 bytes from dfw25s13-in-x0e.1e100.net (2607:f8b0:4000:803::200e): icmp_seq=24 ttl=53 time=55.3 ms
64 bytes from dfw25s13-in-x0e.1e100.net (2607:f8b0:4000:803::200e): icmp_seq=25 ttl=53 time=53.6 ms
64 bytes from dfw25s13-in-x0e.1e100.net (2607:f8b0:4000:803::200e): icmp_seq=26 ttl=53 time=53.4 ms
```

Figure 3 Network connectivity PING results after OS configuration

B.3 Successful Email Transmission



(No subject)

This message was identified as spam. We'll delete it after 10 days. It's not spam

kgeels <kathy@figchen.online>
Sun 12/22/2019 9:05 PM

test email

Figure 4 Email Successfully Between Figchen.online Email Server and External (Microsoft) Email

B.4 Thorough Documentation Package

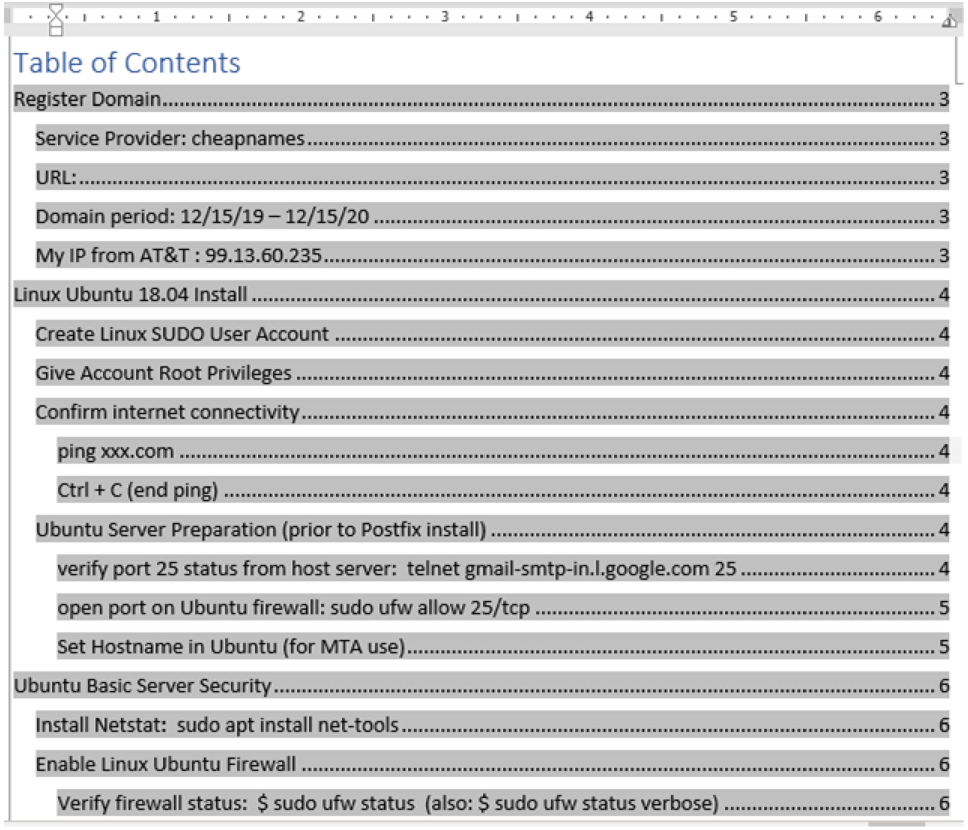


Table of Contents

Figure 5 Table of Contents of Documentation Package