

ix/IN/IS/IM Mailing Systems

Network Security

Author: Jose Valle
Valid from: 04-13-2020
Version No.: V4.0

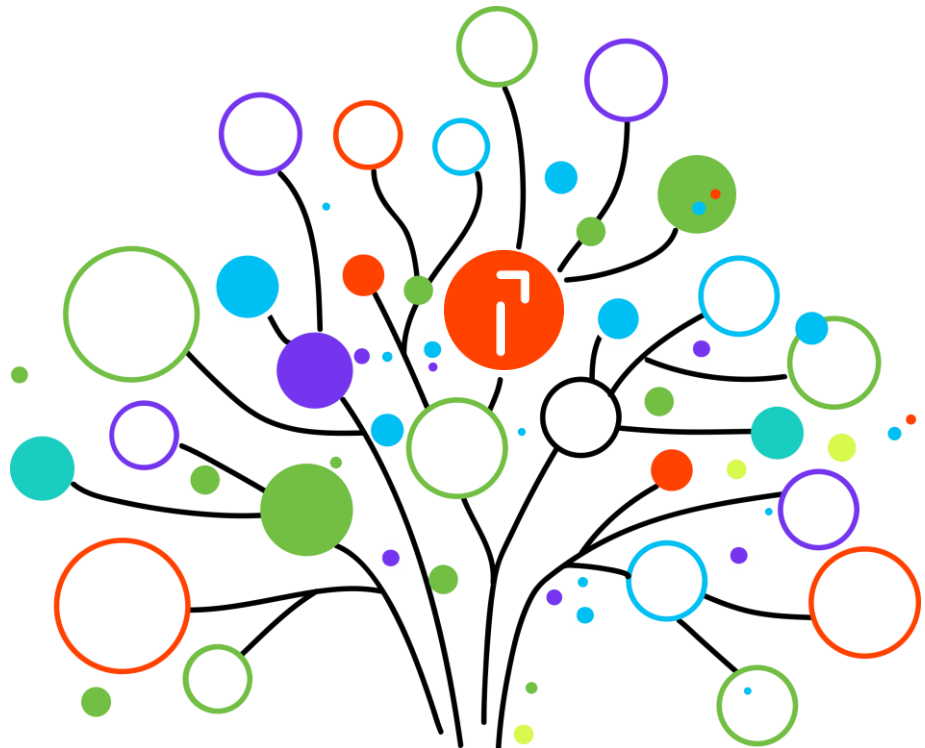




Table of Contents

1 Purpose of this document..... 3

2 Quadient Inc. Meter Security Information..... 3

 2.1 Meter/Server Communications..... 3

 2.2 Cipher Suite Used 4

 2.2.1 Cipher for the IN/IM/IS Systems 4

 2.2.2 Cipher for the iX Systems 4

 2.3 Mailing System OS..... 4

3 Whitelist..... 5

 3.1 Legacy Systems..... 5

 3.2 iX Systems..... 5

 3.3 Troubleshooting..... 6

4 TLS 1.0 Vulnerabilities & Mitigations 7

 4.1 POODLE Attack CVE-2014-3566 7

 4.2 BEAST Attack CVE-2011-3389..... 8

5 Mailing System Connection Overview 9

 5.1 Scenario 1 – Downloading Funds 9

 5.2 Scenario 2 – Automatic Monthly Connection to OLS 10

6 Alternative Network Configurations 11

 6.1 VLANs 11

 6.2 DMZ..... 12

Revision History 14



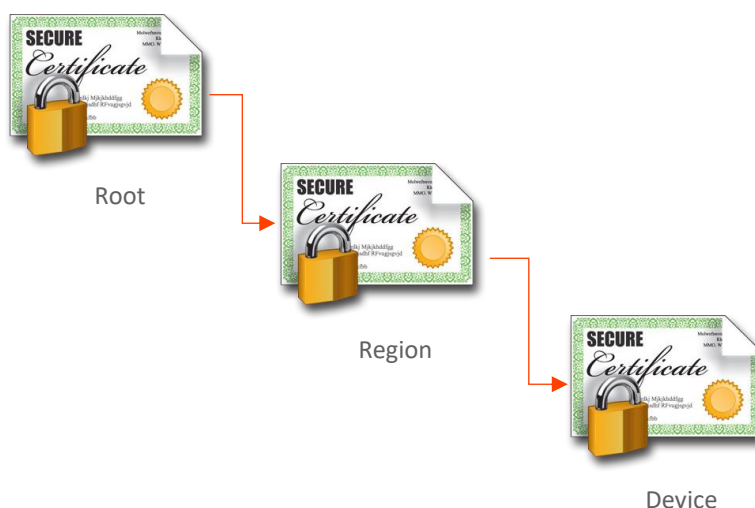
1 Purpose of this document

This White Paper was created to provide customers, and their IT, with specific details on the software that runs Quadient Inc. Mailing Systems (e.g. iX/IS/IM & IN models) and how it interfaces with their networks. Furthermore, this document will provide solutions to customers that feel uncomfortable about attaching our mailing systems to their network.

2 Quadient Inc. Meter Security Information

2.1 Meter/Server Communications

Quadient Inc. maintains its own 3-tier certificate system that enables our meters to connect to our infrastructure. Since we only communicate with our meters and our meters only communicate with our infrastructure, there is no need for a 3rd party certificate.



The Mailing Systems connect to our Infrastructure using TLS Mutual Authentication. Therefore, our server will not accept any device posing as one of our systems. Further, the mailing systems will not honor any “rogue” servers posing as our infrastructure.

NOTE: Since our server and mailing systems do not accept other certificates, SSL inspection *cannot be used* to monitor encrypted traffic. The mailing systems would see it as a man-in-the-middle attack and disconnect.



2.2 Cipher Suite Used

2.2.1 Cipher for the IN/IM/IS Systems

- ❖ Diffie-Hellman Key Exchange (DHE)
- ❖ RSA Certificate Identification
- ❖ AES 128 bit encryption
- ❖ SHA-1 hashing

2.2.2 Cipher for the iX Systems

- ❖ Diffie-Hellman Key Exchange (DHE)
- ❖ RSA Certificate Identification
- ❖ AES 128 bit encryption
- ❖ SHA256 hashing

2.3 Mailing System OS

The Mailing Systems (MS) use two proprietary versions (locked) of operating system software:

Model	Windows CE 5.0	Linux
IS/IM 280	✓	
IS/IM 330/350	✓	
IS/IM 400 series	✓	
IS/IM 5000/6000	✓	
IN-360/600/700/750*	✓	✓
iX-3/5/7/7Pro		✓

**Systems after July 2017 arrive with a Linux board*

Both operating systems *do not* allow any third-party software to be loaded. Any drivers must be signed and incorporated into a software release by Quadient Inc. R&D. All software updates are in a special format that cannot be read by any other computer or software. New software is only released by Quadient Inc. through our service organization.



*Additional functions the OS software will **NOT** do:*

- ❖ Does *not* connect to or embed an email client or server
- ❖ Does *not* include or allow a web server or browser
- ❖ Does *not* offer access to the BIOS
- ❖ Does *not* offer access to a command prompt, root directory or registry
- ❖ Will *not* download or propagate a virus or worm (all ports closed)
- ❖ Is *not* susceptible to a man-in-the-middle attack due to TLS protocol

3 Whitelist

3.1 Legacy Systems

Please add the new URIs (below) to the firewall Whitelist and create any rules for allowing traffic that are necessary.

- ❖ Us-r1-meterservices.neopost.com (146.20.53.70)
- ❖ Us-r1-olsservices.neopost.com (146.20.53.70)

When creating the rule please allow the IP to be dynamically resolved since it may change in the future due to load balancing.

NOTE: There are many network appliances that have different rules so please be aware that each may treat the Mailing System communications differently.

3.2 iX Systems

Please add the new URIs (below) to the firewall Whitelist and create any rules for allowing traffic that are necessary.

- ❖ us-imi-meterservices.neopost.com
 - 40.141.82.122
 - 40.141.63.122
 - 198.105.7.204
- ❖ us-imi-olsservices.neopost.com
 - 23.253.147.97

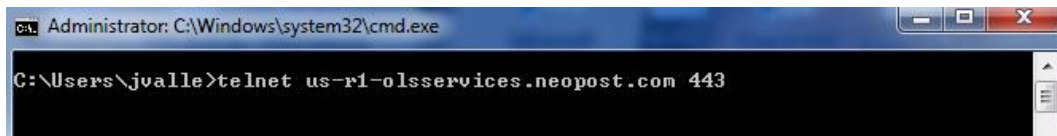
When creating the rule please allow the IP to be dynamically resolved since it may change in the future due to load balancing.



3.3 Troubleshooting

Using ping to test the connection can work. However, we recommend using Telnet to test the connection to all URIs on port 443.

1. Below is an image of a Command Prompt ready for the Telnet test:



```
C:\Users\jvalle>telnet us-r1-olsservices.neopost.com 443
```

2. Once the Telnet session is established the port communication is confirmed:



3. Type some characters and the connections will be terminated:



NOTE: if the command fails after the first step then check the firewall whitelist.



4 TLS 1.0 Vulnerabilities & Mitigations

4.1 POODLE Attack CVE-2014-3566

The POODLE attack or 'Padding Oracle On Downgraded Legacy Encryption' is a vulnerability for TLS 1.0 using web browsers and web servers. The vulnerability requires the use of cipher-block chaining mode (CBC) and SSL 3.0 between the target device (PC with web browser) and the web server.

The attack complexity is high and requires the attacker to have some control over the web browser. Further, they have to establish an effective man-in-the-middle (MITM) exploit. In addition, multiple failed connection attempts have to be sent to the server to 'downgrade' to SSL 3.0 (or lower).

Mitigation

First, the Quadient Inc. Spine server does not offer the ability to downgrade to any SSL protocol. Second, our mailing systems/server do not use RC4 in the cypher suite. Third, our mailing systems do not have a web browser and will not allow any third-party devices/sites to connect. Lastly, our server and the mailing system use mutual authentication – this prevents a MITM attack.

More information:

<https://nvd.nist.gov/vuln/detail/CVE-2014-3566#vulnDescriptionTitle>

<https://www.us-cert.gov/ncas/alerts/TA14-290A>



4.2 BEAST Attack CVE-2011-3389

The Beast attack is a client-side SSL attack that uses a Man-in-the-middle (MITM) attack to decrypt HTTPS (SSL) sessions using browser components such as JavaScript, HTML5 Websocket API, Java URLConnection API, or the Silverlight WebClient API.

Mitigation

First, our mailing systems do not have a web browser and will not allow any third-party devices/sites to connect. Further, neither JavaScript nor any Web API can be run on the mailing systems. Lastly, our server and the mailing system use mutual authentication – this prevents a MITM attack.

More information:

<https://nvd.nist.gov/vuln/detail/CVE-2011-3389#vulnCurrentDescriptionTitle>

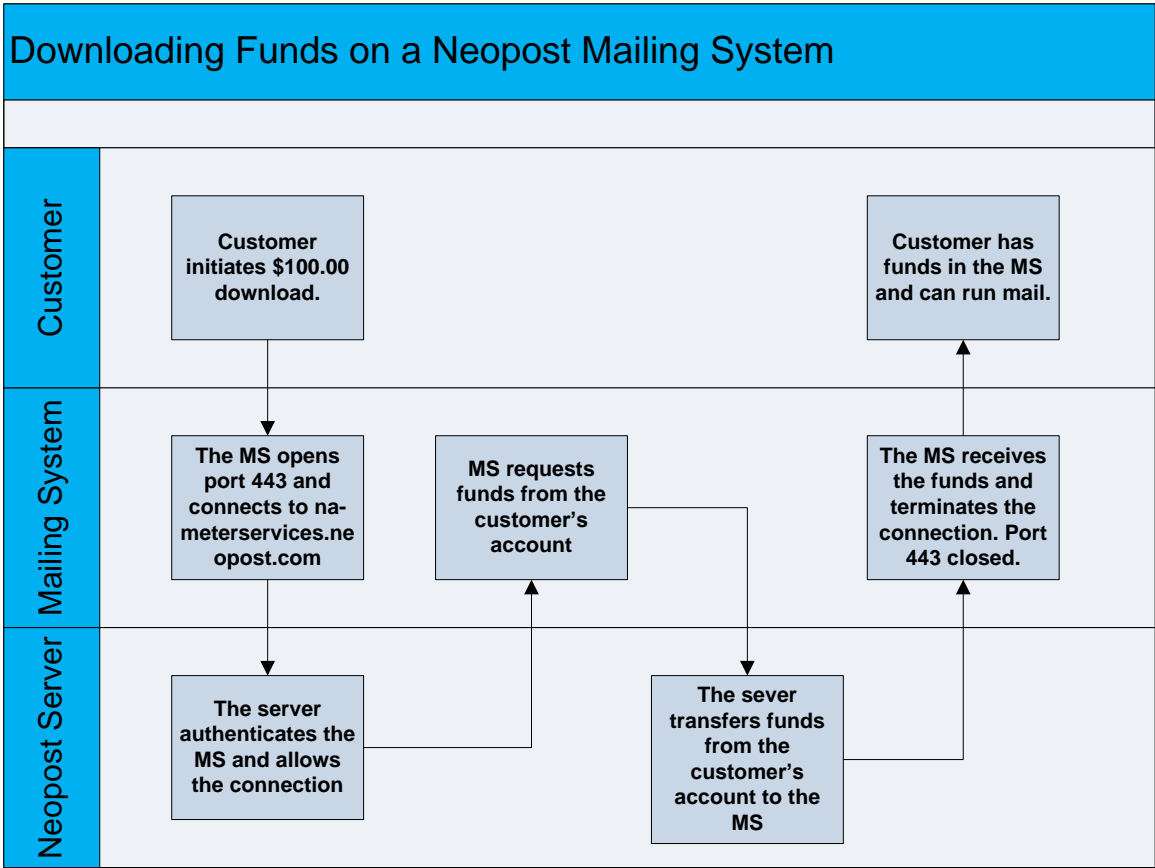


5 Mailing System Connection Overview

When a call is initiated on a Mailing System, to communicate with the Quadient Inc. servers, the MS opens a secure link using Transport Layer Security 1.0 for legacy systems and TLS 1.2 for iX systems. The two most common connection scenarios are described in the following sub sections.

5.1 Scenario 1 – Downloading Funds

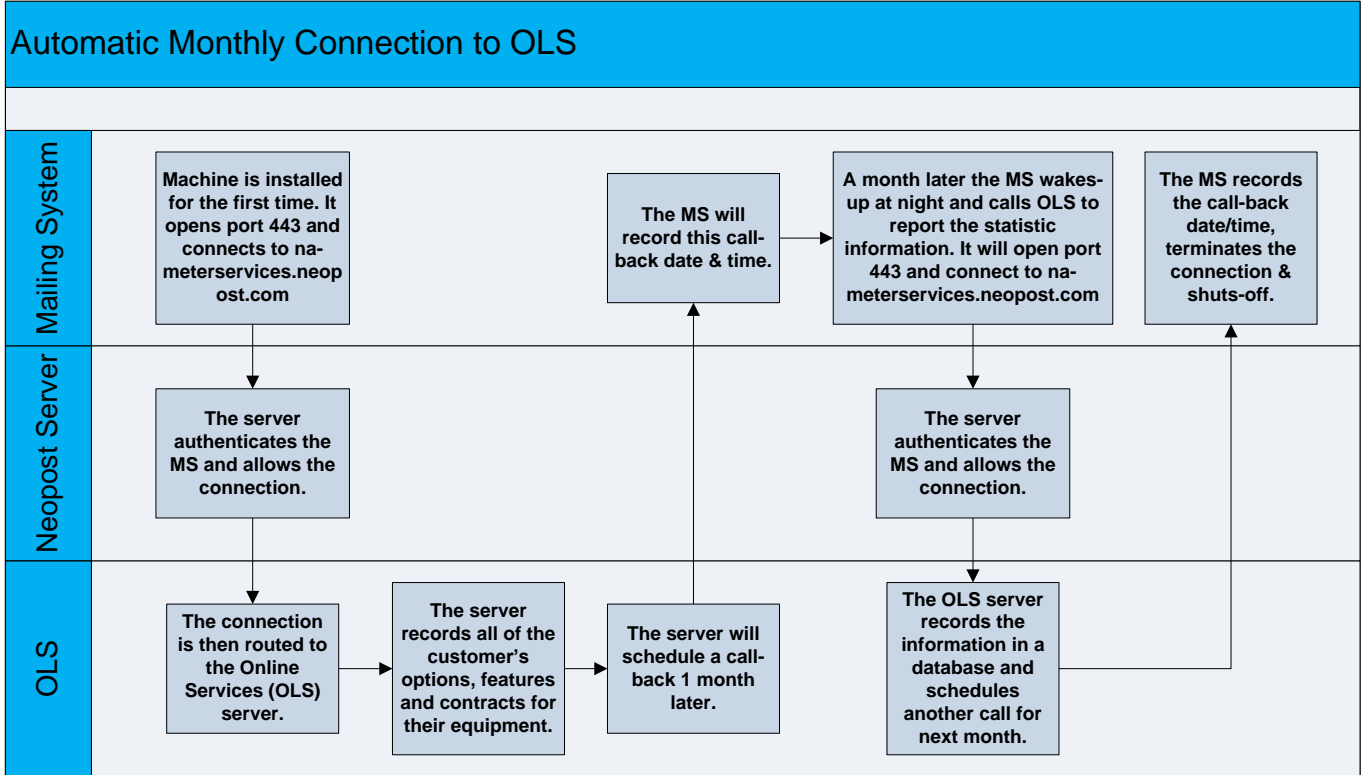
When a Mailing System (MS) user needs funds they perform the funds download procedure on the machine. The MS will open port 443 (SSL, TLS) and establish a secure connection with our server. After the transaction has completed the MS will terminate the connection and close port 443.





5.2 Scenario 2 – Automatic Monthly Connection to OLS

The USPS requires Quadient Inc. to provide them with postage statistics from our Mailing Systems (MS). Therefore, the MS will automatically connect to the Quadient Inc. Online Services (OLS) server to upload postage usage information on a monthly basis. See diagram below.



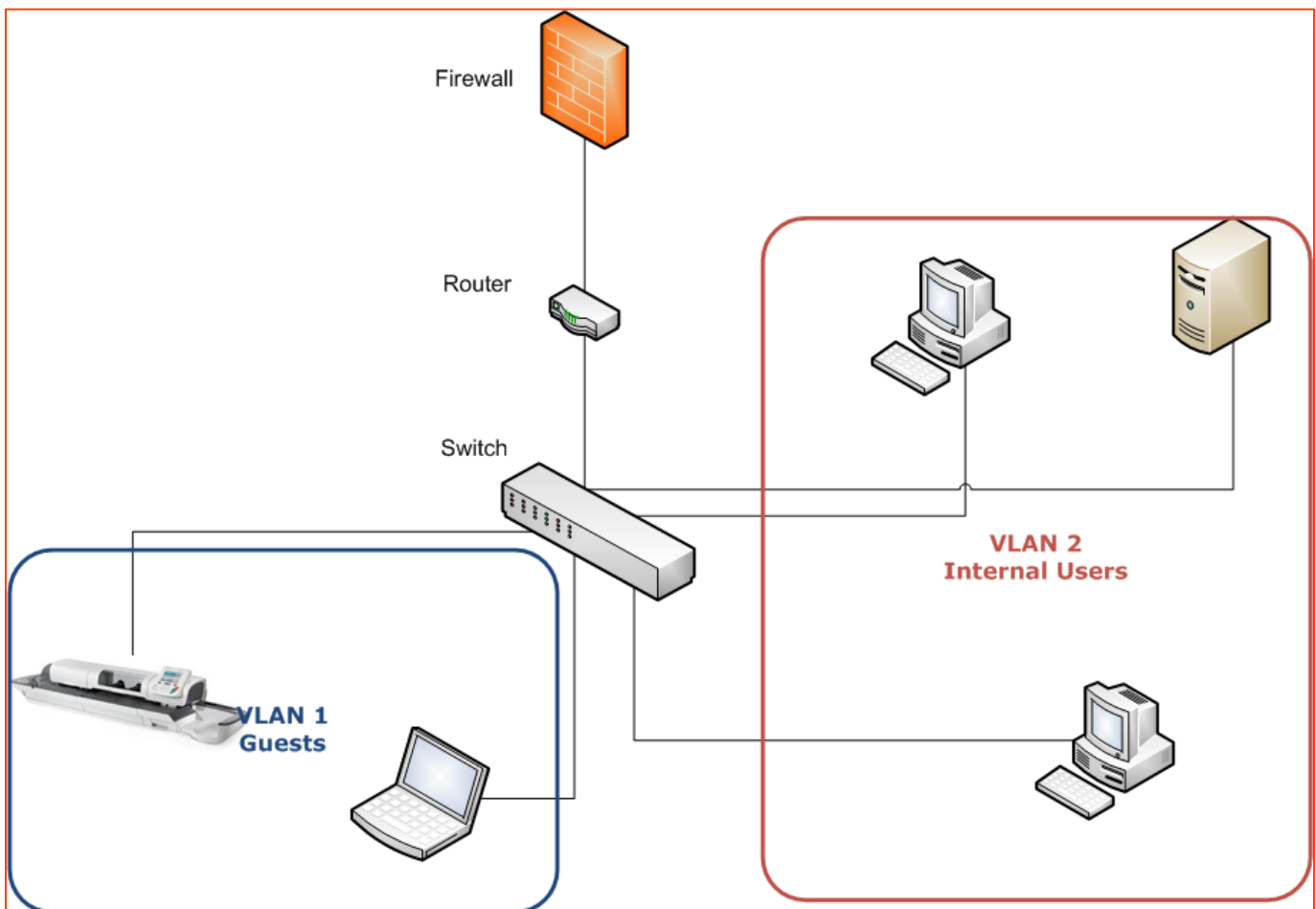


6 Alternative Network Configurations

Some IT managers may not feel comfortable allowing our meters on their network for fear of infiltration by a virus or hacker. Therefore, we offer a solution that can allow our Mailing Systems on the customer network and alleviate some of the concerns that IT may have.

6.1 VLANs

The use of a VLAN is a known way of segmenting a network. Moreover, it is an effective way of securing internal servers and data. By creating a VLAN that only has access to the internet an IT manager mitigates the risk of successful breach of internal company resources. Many of our customers have setup “Guest” networks that allow our Mailing Systems (MS) to connect to our servers without giving the MS access to internal customer resources. See network diagram below.





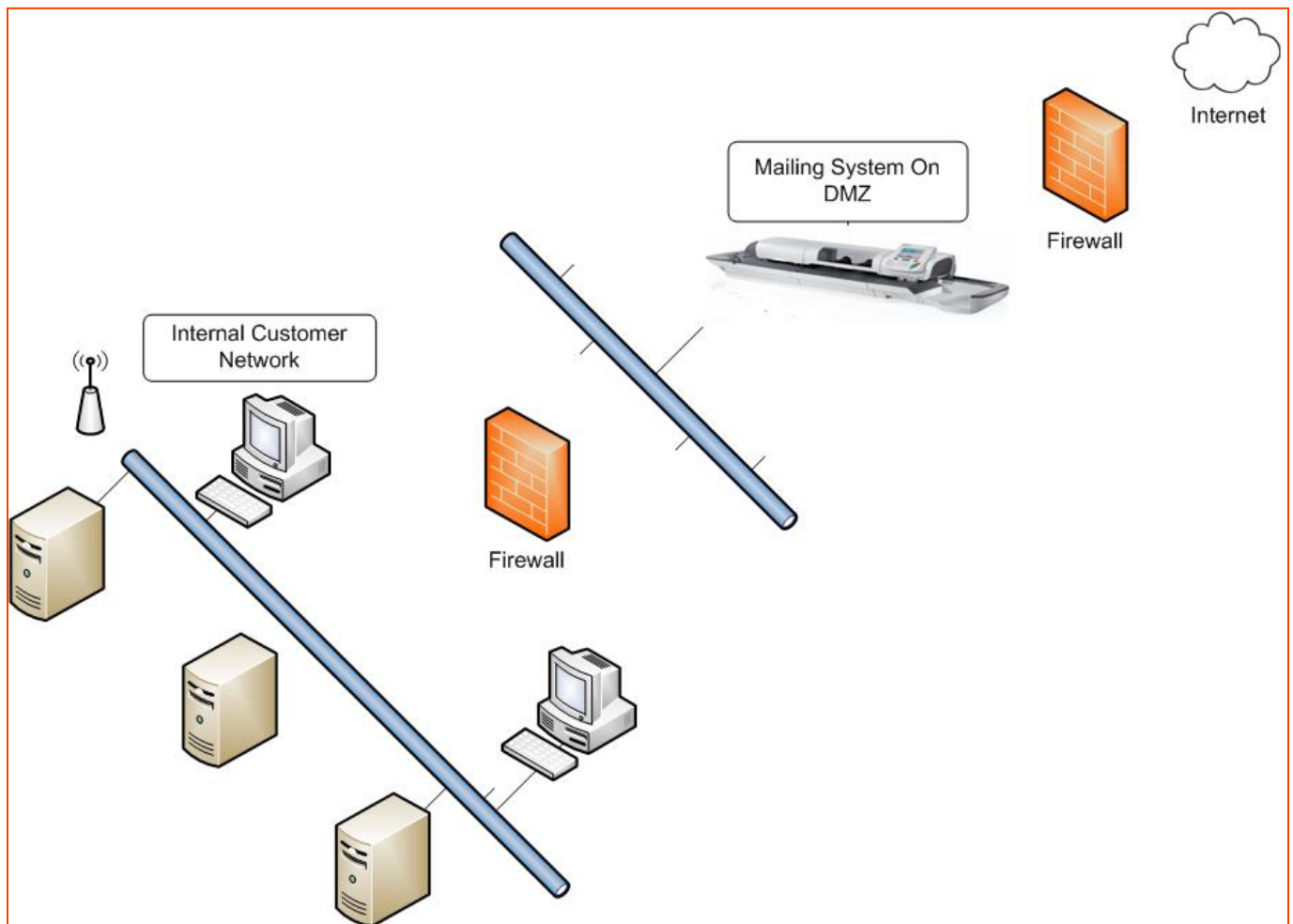
As shown in the previous diagram, allocating a network segment for the Mailing System assures that network resources are shielded from possible intrusion by malicious software or users.

6.2 DMZ

This method is very similar to creating a VLAN, however, instead of using switches it is accomplished with routers. A DMZ is a “De-militarized Zone” and is a borrowed term from the military. It designates a danger zone where there is little security. In networking, a DMZ is created to allow a server or system to be seen by the internet with only a firewall to limit access and provide security. Most web servers operate in this fashion.

So, the suggestion is to put our Mailing System on the DMZ and allow it to be seen externally. The machine will not accept requests or load any software so the chances that it will get compromised are slim. In the event that it does get compromised, it has been shielded from the rest of the internal network.

See the network diagram on the next page.



Both methods offer similar results and further protection can be achieved by combining them. It is beyond the scope of this article to describe how to setup any of these configurations. Since different networks are configured using different equipment, steps to any of these solutions may vary.

It Is up to IT managers to investigate and determine the best configuration for their network.



Revision History

Version	Date	Author	Description
3.0	5/2/2018	Jose Valle	Document Created Removed ports information and added it to Spec sheet document
4.0	4/13/20	Jose Valle	Converted to Quadiant branding. Added iX systems to document.