Virtualized Open-Source Network Security Appliance

By

Daniel Secrist

Submitted to
the Faculty of the Information Technology Program
in Partial Fulfillment of the Requirements for
the Degree of Bachelor of Science
in Information Technology

University of Cincinnati
College of Applied Science

May, 2008
Virtualized Open-Source Network Security Appliance

By

Daniel Secrist

Submitted to
the Faculty of the Information Technology Program
in Partial Fulfillment of the Requirements
for
the Degree of Bachelor of Science
in Information Technology

© Copyright 2008 Daniel Secrist

The author grants to the Information Technology Program permission
to reproduce and distribute copies of this document in whole or in part.

___________________________________________________ __________________
Daniel Secrist        Date

___________________________________________________ __________________
Professor Mark Stockman, Faculty Advisor    Date

___________________________________________________ __________________
Hazem Said, Ph.D. Department Head     Date
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table of Contents</td>
<td>i</td>
</tr>
<tr>
<td>List of Figures</td>
<td>ii</td>
</tr>
<tr>
<td>Abstract</td>
<td>iv</td>
</tr>
<tr>
<td>1. Statement of the Problem</td>
<td>1</td>
</tr>
<tr>
<td>2. Description of the Solution</td>
<td>2</td>
</tr>
<tr>
<td>2.1. User Profiles</td>
<td>3</td>
</tr>
<tr>
<td>2.2. Design Protocols</td>
<td>3</td>
</tr>
<tr>
<td>2.2.1. VMWare Server</td>
<td>4</td>
</tr>
<tr>
<td>2.2.2. Vyatta Router</td>
<td>6</td>
</tr>
<tr>
<td>2.2.3. Smoothwall Firewall</td>
<td>7</td>
</tr>
<tr>
<td>2.2.4. Monowall VPN Server</td>
<td>8</td>
</tr>
<tr>
<td>2.2.5. Management Server</td>
<td>10</td>
</tr>
<tr>
<td>3. Deliverables</td>
<td>11</td>
</tr>
<tr>
<td>4. Design and Development</td>
<td>11</td>
</tr>
<tr>
<td>4.1. Budget</td>
<td>11</td>
</tr>
<tr>
<td>4.2. Timeline</td>
<td>13</td>
</tr>
<tr>
<td>4.3. Testing Plan</td>
<td>13</td>
</tr>
<tr>
<td>5. Proof of Design</td>
<td>15</td>
</tr>
<tr>
<td>5.1. Open-Source Small-Business Class Routing Functionality</td>
<td>15</td>
</tr>
<tr>
<td>5.2. Open-Source Configurable Firewall Functionality</td>
<td>16</td>
</tr>
<tr>
<td>5.3. Open-Source Dynamic Host Control Protocol Server Functionality</td>
<td>19</td>
</tr>
<tr>
<td>5.4. Open-Source Virtual Private Network Server Functionality</td>
<td>21</td>
</tr>
<tr>
<td>5.5. Open-Source Intrusion Detection System Functionality</td>
<td>22</td>
</tr>
<tr>
<td>5.6. Simple and Unified Web-Interface for Configurations\Unified Viewing of Log Files</td>
<td>24</td>
</tr>
<tr>
<td>5.7. Basic Scripts to Aid in Setup</td>
<td>25</td>
</tr>
<tr>
<td>5.8. Virtualized Open-Source Network Security Appliance saved to a DVD</td>
<td>29</td>
</tr>
<tr>
<td>6. Conclusions and Recommendations</td>
<td>30</td>
</tr>
<tr>
<td>6.1 Conclusions</td>
<td>30</td>
</tr>
<tr>
<td>6.2 Recommendations</td>
<td>30</td>
</tr>
<tr>
<td>Appendix A</td>
<td>31</td>
</tr>
<tr>
<td>References</td>
<td>33</td>
</tr>
</tbody>
</table>
## List of Figures

<table>
<thead>
<tr>
<th>Figure Number</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1</td>
<td>Virtualized Open-Source Security Appliance layout</td>
<td>4</td>
</tr>
<tr>
<td>Figure 2</td>
<td>VMWare Virtual Machines</td>
<td>5</td>
</tr>
<tr>
<td>Figure 3</td>
<td>Vyatta GUI configuring Interface eth0</td>
<td>6</td>
</tr>
<tr>
<td>Figure 4</td>
<td>Smoothwall GUI configuring firewall</td>
<td>7</td>
</tr>
<tr>
<td>Figure 5</td>
<td>m0n0wall GUI configuring VPN</td>
<td>9</td>
</tr>
<tr>
<td>Figure 6</td>
<td>Unified management Web site</td>
<td>10</td>
</tr>
<tr>
<td>Figure 7</td>
<td>Itemized budget</td>
<td>12</td>
</tr>
<tr>
<td>Figure 8</td>
<td>Timeline</td>
<td>13</td>
</tr>
<tr>
<td>Figure 9</td>
<td>Test environment</td>
<td>14</td>
</tr>
<tr>
<td>Figure 10</td>
<td>Proof pings are routing through the Vyatta Router</td>
<td>16</td>
</tr>
<tr>
<td>Figure 11</td>
<td>Firewall configurations page before exceptions</td>
<td>17</td>
</tr>
<tr>
<td>Figure 12</td>
<td>Ping unsuccessful, before exceptions</td>
<td>17</td>
</tr>
<tr>
<td>Figure 13</td>
<td>Exceptions created</td>
<td>18</td>
</tr>
<tr>
<td>Figure 14</td>
<td>Ping successful, exceptions work</td>
<td>18</td>
</tr>
<tr>
<td>Figure 15</td>
<td>DHCP server settings</td>
<td>19</td>
</tr>
<tr>
<td>Figure 16</td>
<td>User is using DHCP to obtain an IP address</td>
<td>20</td>
</tr>
<tr>
<td>Figure 17</td>
<td>User was assigned an IP address through DHCP</td>
<td>20</td>
</tr>
<tr>
<td>Figure 18</td>
<td>Ping unsuccessful without VPN</td>
<td>21</td>
</tr>
<tr>
<td>Figure 19</td>
<td>Ping successful after authenticating through VPN server</td>
<td>22</td>
</tr>
<tr>
<td>Figure 20</td>
<td>Creating an extremely large ping packet</td>
<td>23</td>
</tr>
</tbody>
</table>
Figure 21: Snort rule detecting large ping packets

Figure 22: The warnings in the IDS logs, created from the ping

Figure 23: The unified Web-GUI for central management

Figure 24: The various links for the log files on the unified Web-GUI

Figure 25: InstallVOSNSA.bat

Figure 26: First half of InstallVOSNSA.bat successfully running

Figure 27: Last half of InstallVOSNSA.bat successfully running

Figure 28: Contents of ReadMe.txt
Abstract

The Virtualized Open-Source Network Security Appliance is a powerful piece of networking equipment that was designed to give the small-business owner an alternative to pricey, name-brand networking equipment. This device combines many powerful utilities and services onto one physical piece of hardware, which includes a business class router, a stateful firewall, a VPN server, a DHCP server, an Intrusion Detection System, detailed logging and management, and much more. This is accomplished by utilizing several of the most robust open-source programs and integrating them to communicate efficiently on the same device through the use of virtualization. All of the utilities and services will be easily managed through a Web-GUI, which will tie the components together and allow them to be centrally administrated. Running on the device are four separate virtual machines, with each controlling a level of functionality inside the device. Some of the specific open-source programs that were used to create this project are VMWare Server, CentOS Linux,Vyatta router, Smoothwall firewall and m0n0wall VPN. A name brand piece of hardware with the same functionality could easily cost a small-business owner thousands of dollars. However, by going open-source, it will be completely free. Small-business owners will now never have to sacrifice functionality due to budget concerns.
Virtualized Open-Source Network Security Appliance

1. Statement of the Problem

In today’s fast-paced business environment, it is becoming harder and harder for small business owners to get the hardware they need. Almost all small businesses are turning to Information Technology to power their businesses. To do this, they are going to need powerful hardware and software to enable them to sell their business on the Internet or traditionally. All of this Information Technology equipment is very expensive and can be very challenging for small businesses to acquire due to the cost. Some expensive components that all successful small businesses require are routers, firewalls VPN servers, etc. Cisco is a well established company that is the standard when it comes to networking components, commanding the majority of the market share in networking equipment (2). Cisco and other name-brand networking equipment manufacturers offer validated and powerful network appliances for businesses; the problem is the cost. A Cisco 1841 Router, which is designed for small businesses, can cost over $2,000 (4). This is a great deal of money that small businesses would rather use for other endeavors. Most small businesses do not like spending money on Information Technology. These companies view Information Technology as a money pit. They feel that they invest the money into Information Technology, but that they get no return on their investment (3).

Another problem related to using Cisco or other expensive brand-name networking equipment is that they are not very flexible. What this means is that one has to use the manufacturer’s operating system and built-in tools when managing the equipment. These manufacturer-created operating systems and built-in tools drive up the
price for this already expensive equipment. Another problem with name brand networking equipment is that the company has to rely on the manufacturer to support and produce the software that will run on the appliance. This leads to a lack of flexibility because the appliance is stuck using only the tools that the manufacturers develop for it (5).

2. Description of the Solution

The solution to the above problem is to create a Virtualized Open-Source Network Security Appliance that the small business owner would be able to use at a minimum cost. The open-source network appliance would be based on a Linux operating system and would feature many security tools also for Linux. Since Linux is open source under the GNU license, there will be no cost associated with it (1). Using Linux would be 100% free and offer many flexible options for routing and security tools. Any program written in Linux could be used to add new functionality to the appliance. This will give the small business owner thousands of Linux programs from which to be able to choose on top of what is included with the Virtualized Open-Source Network Security Appliance. This will eliminate the problem of the small business being forced to use the manufacturer’s software applications on their networking equipment and will add a superior level of flexibility (5). Essentially, the small business owner will connect one NIC on the Virtualized Open-Source Network Security Appliance to their ISP and the other NIC to their Internal LAN. After minor configurations, they will then have a powerful and robust Network Security Appliance with the following functionality: Small-business routing, Firewall, DCHP, Intrusion Detection, VPN and Detailed Logging.
2.1. User Profiles

The Virtualized Open-Source Network Security Appliance would play a very important role in the small-business owner’s network. It would be responsible for all network traffic entering and leaving their network. Due to the importance of this device only one user group has been created: the administrator user group. There is no need for other user groups, because the only user that should ever need to make changes within the Virtualized Open-Source Network Security Appliance would be the small-business owner or network administrator.

2.2. Design Protocols

The Virtualized Open-Source Network Security Appliance is an integration of several powerful open-source networking virtual systems all onto one physical machine. This is accomplished through the use of VMWare Virtual Server. Using VMWare, the physical computer that is the Virtualized Open-Source Network Security Appliance can be hosting multiple virtual networking components, each one with a specialized role. The virtual networking components that will be making up the Virtualized Open-Source Network Security Appliance are:

- **Vyatta Open-Source Router:** The Vyatta router virtual machine will function as the gateway router.

- **Smoothwall Open Source Firewall:** The Smoothwall firewall will function as a firewall, as well as the Intrusion Detection System and the DHCP Server.

- **m0n0wall Open Source VPN server:** The m0n0wall VPN server will provide VPN functionality to the users.
• **Open-Source Management Server:** The management server will host the Unified Web site and will also host the scripts that will aid in configuration of the Virtualized Open-Source Network Security Appliance.

See Figure 1 below for a diagram of how all of the components will come together to create the Virtualized Open-Source Network Security Appliance.

![Figure 1: Virtualized Open-Source Security Appliance layout](image)

2.2.1. VMWare Server

VMWare Server is a very powerful open-source virtualization program that gives the ability to combine several pieces of networking equipment on to one physical machine. Each piece of networking equipment is its own virtual machine in VMWare. In
total, there are four virtual machines that make up the Virtualized Open-Source Network Security Appliance. Without VMWare the small business owner would have to have a physical server for each piece of networking equipment. Using VMWare is a much better solution for the small business owner because all of the networking components are centralized in one location. This provides a much greater level of management: having all of the networking equipment on one piece of hardware as opposed to being spread out over four separate pieces of networking equipment. Having all of the pieces of networking equipment consolidated saves the small business owner money by only having to purchase one server instead of four servers. Also by using four separate virtual machines gives the small business owner much more scalability. If network demands increase, the small business owner could eventually port all of the four virtual machines over to their own physical hardware. See Figure 2 below for a view of the various virtual machines that will be running on the Virtualized Open-Source Network Security Appliance.

Figure 2: VMWare Virtual Machines
2.2.2. Vyatta Router

In the Virtualized Open-Source Network Security Appliance, the Vyatta Router would act as the small business owner’s gateway router. Vyatta router includes support for most commonly used network interfaces, industry-standard routing and management protocols, and all of these features are configurable through a single command-line interface or Web-based GUI. See Figure 3 below for an image of the Web-based GUI.

![Figure 3: Vyatta GUI configuring Interface eth0](image)

On top of supporting industry-standard routing the Vyatta router has many other features that the small business owner can utilize if they choose, such as network to network VPN or DHCP functionality. However, for the Virtualized Open-Source Network Security Appliance, the Vyatta router will only be responsible for gateway
routing, because the other modules in the Virtualized Open-Source Network Security Appliance can do a much better job at providing these services.

2.2.3. Smoothwall Firewall

The Smoothwall firewall is the next component to make up the Virtualized Open-Source Network Security Appliance. Smoothwall is an open-source firewall based on a Linux operating system that is manageable through an easy to use Web-based GUI. See Figure 4 below for an image of the Web-based GUI.

![Smoothwall GUI configuring firewall](image)

**Figure 4: Smoothwall GUI configuring firewall**

In the Virtualized Open-Source Network Security Appliance, Smoothwall will be responsible for the Stateful Firewall, Intrusion Detection, and it will host the DHCP Server for all of the users on the LAN. Smoothwall will come preconfigured with some
basic firewall rules already in place. It will be up to the small business owner to provide any other rules that they would deem necessary on their network. The firewall will come preconfigured to block all traffic except for the most commonly used protocols, such as Web Traffic, VPN, SSL and others.

DHCP will also be running on Smoothwall and will be able to automatically assign IP addresses to all of the clients on the LAN side of the Virtualized Open-Source Network Security Appliance. The DHCP settings will be configured to a 10.1.1.0/24 type addressing scheme. This may not work for every small business owner, but is easily changed in the DHCP portion of the Smoothwall GUI.

The final component that makes up the Smoothwall virtual machine is the Intrusion Detection System. For its Intrusion Detection System, Smoothwall uses Snort. Snort is an open source network Intrusion Detection System that uses a rule-driven method to detect potential network breaches. Snort connects to the Snort server on the Internet to guarantee it has the latest rules. To be able to connect to the Snort server and begin downloading rules one must have an “Oink Code” which I have provided and already configured on the Smoothwall virtual machine. Once configured, when Snort detects suspicious activity it will be recorded in the IDS Log file for Smoothwall.

2.2.4. Monowall VPN Server

In the Virtualized Open-Source Network Security Appliance m0n0wall will be the VPN server. M0n0wall also has some functionality for some basic firewall settings. Like all of the other virtual machines, m0n0wall is configured through an easy to use Web interface. See Figure 5 on the next page for an image of m0n0wall’s Web-GUI.
Users can be authenticated either through a database saved on the m0n0wall virtual machine or the small business owner can opt to use a separate RADIUS server for their authentication. Also, the small business owner can choose other values such as the IP address range for the VPN clients and encryption settings.

**Figure 5: m0n0wall GUI configuring VPN**
2.2.5. Management Server

The Management Server will be the centralized management for the whole Virtualized Open-Source Network Security Appliance. The management server is run on CentOS, which is a stable server distribution of Linux. The management server will be running Apache in order to host the unified Web site. The unified Web site is custom-made for the Virtualized Open-Source Network Security Appliance. The unified Web site will tie together the Web-based GUIs for the other three virtual machines. The Website will have links to the Vyatta, Smoothwall and the m0n0wall Web-based GUI. See Figure 6 below.

Figure 6: Unified management Web site

On the unified Web site there will also be direct links to functions that network administrators will use often, such as adding VPN clients, configuring DHCP settings,
changing the router interface settings, adding firewall rules, just to name a few. Also, from the unified Web site, the network administrator will have the ability to run preconfigured scripts to aid in basic setup.

3. Deliverables

For the Virtualized Open-Source Network Security Appliance there are a total of nine deliverables that have been met and made available to the small-business owner.

1. Open-Source Small-Business class routing functionality
2. Open-Source Configurable Firewall
3. Open-Source Dynamic Host Control Protocol Server Functionality
4. Open-Source Virtual Private Network Server Functionality
5. Open-Source Intrusion Detection System Functionality
6. A simple and unified Web-interface for configurations
7. Unified viewing of the different log files created by the different modules
8. Virtualized Open-Source Network Security Appliance saved to a DVD
9. Basic scripts to aid in setup

4. Design and Development

4.1. Budget

The budget for this project, including the items listed above in the Technical Details section, is described below in Figure 1 on the next page. The total retail cost of the project would be $1,643.77. The only components of this project that will cost money are the hardware components. All of the software components are under an open source license agreement and, therefore, are free for use. It is important to note that the proposed retail cost would not be the cost that a small business owner would pay. The total retail cost is the price required to create the Virtualized Open-Source Security Appliance. The
only price the business owner would have is the cost of the workstation on which the
Virtualized Open-Source Security Appliance is running. See Figure 7 below for an
itemized budget.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Retail Cost</th>
<th>Cost Incurred</th>
</tr>
</thead>
<tbody>
<tr>
<td>80 Gb Portable Hard Drive</td>
<td>Have</td>
<td>$89.95</td>
<td>$0.00</td>
</tr>
<tr>
<td>VMWare Server</td>
<td>“Provided free, as open-source software, and licensed under a GNU-style agreement.”</td>
<td>$0.00</td>
<td>$0.00</td>
</tr>
<tr>
<td>CentOS Linux</td>
<td>“Provided free, as open-source software, and licensed under a GNU-style agreement.”</td>
<td>$0.00</td>
<td>$0.00</td>
</tr>
<tr>
<td>Vyatta</td>
<td>“Provided free, as open-source software, and licensed under a GNU-style agreement.”</td>
<td>$0.00</td>
<td>$0.00</td>
</tr>
<tr>
<td>Smoothwall</td>
<td>“Provided free, as open-source software, and licensed under a GNU-style agreement.”</td>
<td>$0.00</td>
<td>$0.00</td>
</tr>
<tr>
<td>Snort</td>
<td>“Provided free, as open-source software, and licensed under a GNU-style agreement.”</td>
<td>$0.00</td>
<td>$0.00</td>
</tr>
<tr>
<td>m0n0wall</td>
<td>“Provided free, as open-source software, and licensed under a BSD-style agreement.”</td>
<td>$0.00</td>
<td>$0.00</td>
</tr>
<tr>
<td>Lenovo T61 Laptop</td>
<td>Have</td>
<td>$1,553.82</td>
<td>$0.00</td>
</tr>
<tr>
<td>Dual-Layer DVD</td>
<td>Have</td>
<td>$1.99</td>
<td>$0.00</td>
</tr>
</tbody>
</table>

**Retail Total:** $1,645.76

**My Total:** $0.00

Figure 7: Itemized budget
4.2. Timeline

There were a number of tasks involved in completing this project. The project was broken down into several different modules and then completed piece by piece. See Figure 8 below.

Figure 8: Timeline

### Senior Design II

<table>
<thead>
<tr>
<th>WEEK OF:</th>
<th>MILESTONE \ TASK:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/7/2008</td>
<td>Create Vyatta Router</td>
</tr>
<tr>
<td>1/14/2008</td>
<td>Get Vyatta Router Functioning</td>
</tr>
<tr>
<td>1/21/2008</td>
<td>Create Smoothwall Server</td>
</tr>
<tr>
<td>1/28/2008</td>
<td>Get DHCP functioning in Smoothwall</td>
</tr>
<tr>
<td>2/4/2008</td>
<td>Create Management Server</td>
</tr>
<tr>
<td>2/11/2008</td>
<td>Create Centralized Web site</td>
</tr>
<tr>
<td>2/18/2008</td>
<td>Create m0n0wall VPN Server</td>
</tr>
<tr>
<td>2/25/2008</td>
<td>Get VPN functioning in m0n0wall. Create Design Freeze.</td>
</tr>
<tr>
<td>3/10/2008</td>
<td>Get IDS functioning in Smoothwall</td>
</tr>
</tbody>
</table>

### Senior Design III

<table>
<thead>
<tr>
<th>WEEK OF:</th>
<th>MILESTONE \ TASK:</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/31/2008 –</td>
<td>Begin Testing of Complete Appliance</td>
</tr>
<tr>
<td>4/14/2008</td>
<td>Create Scripts</td>
</tr>
<tr>
<td>4/21/2008</td>
<td>Update Centralized Web site</td>
</tr>
<tr>
<td>4/28/2008 –</td>
<td>Complete Documentation</td>
</tr>
<tr>
<td>5/12/2008</td>
<td>Place Project on DVD</td>
</tr>
<tr>
<td>5/19/2008</td>
<td>Project Complete</td>
</tr>
<tr>
<td>5/22/2008</td>
<td>Tech Expo</td>
</tr>
</tbody>
</table>

4.3. Testing Plan

Testing for the Virtualized Open-Source Security Appliance will be continuous throughout the projects’ development. The Virtualized Open-Source Security Appliance is broken into four major components: Vyatta Router, Smoothwall Firewall, m0n0wall VPN and the Management Server. Testing will be conducted first on each individual
After the Virtualized Open-Source Security Appliance has passed all of the usability testing in a “real-world” environment, user acceptance testing will begin. The
user acceptance testing will determine how user-friendly the Virtualized Open-Source Security Appliance is to its intended user base, in this case, the small business owner. The user acceptance testing will be performed on the owner of CincyCyberKnights: a local Information Technology company (3). Any feedback from the user acceptance test will be collected and incorporated into the Virtualized Open-Source Security Appliance if possible.

5. Proof of Design

There are many different levels of functionality in the Virtualized Open-Source Network Security Appliance the sections below will demonstrate that each component of the Virtualized Open-Source Network Security Appliance is functioning as stated in the deliverables section. To do this, a test network has been set up, complete with a simulated Internet.

5.1 Open-Source Small-Business Class Routing Functionality

One of the primary components of the Virtualized Open-Source Network Security Appliance is a simple router. Small-businesses need to be able to route their information from their internal networks out to the Internet. In the Virtualized Open-Source Network Security Appliance this is achieved with an open-source business router program called Vyatta. Network traffic cannot pass between different networks unless there is a router. To prove that the Vyatta router is working in the Virtualized Open-Source Network Security Appliance, traffic would simply have to pass through the Vyatta router, with a different network on each side of the device. See figure 9 on the previous page.

To prove traffic is flowing through the Vyatta router successfully, a simple ICMP Ping can be done from a host on one side of the Vyatta router, to a network on the other
side of the Vyatta router. If the ping is successful, then we know that the router is successfully routing packets for the Virtualized Open-Source Network Security Appliance. See figure 10 below.

![Ping results]

**Figure 10: Proof pings are routing through the Vyatta Router**

### 5.2. Open-Source Configurable Firewall Functionality

The open-source configurable firewall allows the small-business owner to fine tune what traffic will be allowed into their network. This adds another layer of security to protect the network from malicious attacks. In the Virtualized Open-Source Network Security Appliance, the firewall that is being used is Smoothwall. Firewalls work by blocking all traffic by default, and only allowing in traffic that has been approved by the network administrator. Traffic that has not been specifically allowed entrance or exit from the network will be dropped.
To prove that the configurable firewall is working the test network in figure 7 will be used again. In the first example traffic will be passed through the Smoothwall firewall with no allow traffic rules. This will show that no traffic is making it through the Smoothwall firewall and the firewall is not allowing unauthorized traffic on to the network. See Figures 11 and 12 below.

![Figure 11: Firewall configurations page before exceptions](image1)

![Figure 12: Ping unsuccessful, before exceptions](image2)
In the next example, all exception rules will be set up to allow traffic through the Smoothwall firewall, and show that the created exceptions and the firewall do indeed function correctly. See Figures 13 and 14 below.

Figure 13: Exceptions created

Figure 14: Ping successful, exceptions work
5.3. Open-Source Dynamic Host Control Protocol Server Functionality

The Dynamic Host Control Protocol is a very important part of any network that allows the network administrator to automatically assign IP addresses to hosts as they connect to the Local Area Network. In the Virtualized Open-Source Network Security Appliance, the Smoothwall device has Dynamic Host Control Protocol functionality built into it.

To prove that the Dynamic Host Control Protocol component is working in the Virtualized Open-Source Network Security Appliance is a very simple task. If a host can enter the LAN with its network setting set to automatically pick up an IP, and it has an IP address assigned to it from the Dynamic Host Control Protocol Server, then one knows that the server is assigning IP addresses correctly. On the Dynamic Host Control Protocol Server, the network administrator creates the range of useable IP address. See Figure 15 below.

![Figure 15: DHCP server settings](image-url)
Once the Dynamic Host Control Protocol Server has been correctly configured, the user needs to enter their network configuration settings, and allow the server to configure and IP address automatically. See Figure 16 below.

**Figure 16: User is using DHCP to obtain an IP address**

The a simple check of the IP address shows that the user was assign an IP address in the specified range from the Dynamic Host Control Protocol Server. See Figure 17 below.

**Figure 17: User was assigned an IP address through DHCP**
5.4. Open-Source Virtual Private Network Server Functionality

The Virtual Private Network Server allows users that are outside of the internal network to authenticate through the server and gain access to all of the resources inside the internal network. In the Virtualized Open-Source Network Security Appliance an open-source program known as m0n0wall is acting as the Virtual Private Network Server. Users that are sitting outside of the network will not be able to use any of the resources inside the network, unless they can VPN in.

To prove that the Virtual Private Network Server is working, the “Simulated Internet” host outside the test network in figure 7 above will try to communicate to users inside the internal network through a simple ICMP Ping. Without VPN’ing into the network the outside host will not be successful. See Figure 18 below.

![Figure 18: Ping unsuccessful without VPN](image-url)
Now that same user will connect into the internal network through the Virtual Private Network Server that is being run on the m0n0wall device. Once that host has authenticated through the Virtual Private Network Server, that host will be treated as if it is part of the internal network, and therefore will be able to ICMP Ping other devices on the internal network, unlike before. See Figure 19 below.

![Image](image_url)

**Figure 19:** Ping successful after authenticating through VPN server

### 5.5. Open-Source Intrusion Detection System Functionality

The Intrusion Detection System that is included in the Virtualized Open-Source Network Security Appliance is an open-source program called Snort. Snort is installed on the Smoothwall device. The Intrusion Detection System analyzes network traffic and will warn the network administrator of potentially malicious or harmful traffic. Snort does this based off of rule files that have been created by the Snort community. If network traffic meets the criteria described in the rules files, then Snort will throw an exception, and make note of the traffic in its log files. These log files can then be viewed by the network administrator and action can then be taken to protect the network.
To prove the Intrusion Detection System is working in the Virtualized Open-Source Network Security Appliance, suspicious traffic will be created on the network in the form of an extremely large ICMP Packet. See Figure 20 below.

![Figure 20: Creating an extremely large ping packet](image)

Figure 20: Creating an extremely large ping packet

The Intrusion Detection System will then detect this overly large packet based off of the criteria specified in the rules files. See Figure 21 below.

![Figure 21: Snort rule detecting large ping packets](image)
Once the traffic matches the criteria specified in the rules files, then a warning will be created and added to the Intrusion Detection System Log files. See Figure 22 below.

![Log]

*The 50000 byte ICMP packet created an IDS alert.*

Figure 22: The warnings in the IDS logs, created from the ping

5.6. Simple and Unified Web-Interface for Configurations

One main component of this project is having the ability to centrally manage all of the different devices. The unified Web-GUI that was created for this project ties all of the pieces together and gives the network administrator greatly enhanced control over the different modules. The Unified Web-Interface is an HTML file that links to the other management and logging pages of the different components. See Figures 23 and 24 on the next page.
Virtualized Open-Source Appliance Management

Figure 23: The unified Web-GUI for central management

Figure 24: The various links for the log files on the unified Web-GUI

5.7. Basic Scripts to Aid in Setup

The final component of the Virtualized Open-Source Network Security Appliance is having it be easy for the end-user to install and implement. This has been accomplished by writing a script to install all of the components of the project onto the end-users
computer. The script is a batch file called “InstallVOSNSA.bat” that first copies the necessary files over to install VMWare Server to the “C:\Temp” directory. After that is done, the script then silently installs the VMWare without any input from the user. The script then copies over all four of the virtual machines that make up the Virtualized Open-Source Network Security Appliance. After that, the only thing the user will need to do is run VMWare, add the virtual machines, and begin using the Virtualized Open-Source Network Security Appliance. See Figure 25 below for the code of the script.

```batch
@ECHO OFF
ECHO This will install the Virtualized Open-Source Network Security Appliance on your computer!!!
pause
@ECHO ON
XCOPY *.* C:\Temp
C:\Temp\VMware-server-installer-1.0.4-56528.exe /a /s /v"/qn TARGETDIR=C:\Temp"
msiexec -i "C:\temp\VMware Server Standalone.msi" ADDLOCAL=ALL DESKTOP_SHORTCUT=1 SERIALNUMBER="9A5FX-YDF0U-115FM-49H2T" /qn
msiexec -i "C:\temp\VMware Management Interface.msi" ADDLOCAL=ALL /qn
msiexec -i "C:\temp\VMware VmCOM Scripting API.msi" ADDLOCAL=ALL /qn
msiexec -i "C:\temp\VMware VmPerl Scripting API.msi" ADDLOCAL=ALL /qn
MKDIR C:\VOSNSA1.0
MKDIR C:\VOSNSA1.0\Management Server
MKDIR C:\VOSNSA1.0\m0n0wall VPN
MKDIR C:\VOSNSA1.0\Smoothwall Firewall
MKDIR C:\VOSNSA1.0\Vyatta Router
```

Figure 25: InstallVOSNSA.bat (continued on next page)
COPY ".\CentOS-Internal\*.*" "C:\VOSNSA1.0\Management Server"
COPY ".\m0n0wall\*.*" "C:\VOSNSA1.0\m0n0wall VPN"
COPY ".\Smoothwall TEST\*.*" "C:\VOSNSA1.0\Smoothwall Firewall"
COPY ".\Vyatta-VC2.2\*.*" "C:\VOSNSA1.0\Vyatta Router"

@ECHO OFF
ECHO The Virtualized Open-Source Network Security Appliance has been successfully installed on your computer. See Readme.txt for additional information.

Daniel Secrist 2008
pause
@ECHO ON
ReadME.txt

Figure 25: InstallVOSNSA.bat

Figures 26 and 27 the next pages show the script successfully running on a machine.
Figure 26: First half of InstallVOSNSA.bat successfully running
5.8. Virtualized Open-Source Network Security Appliance saved to a DVD

All of the projects files and install scripts have been saved to a DVD. The DVD is enclosed at the end of this document for anyone who would be interested in installing the Virtualized Open-Source Network Security Appliance.
6. Conclusion and Recommendations

6.1. Conclusion

In conclusion, the Virtualized Open-Source Network Security Appliance has been developed, tested, and completed according to the deliverables. The Virtualized Open-Source Network Security Appliance has been created to give the small-business owner a cost-free option when considering their networking hardware. Small-Business owners will not longer have to sacrifice functionality due to budget concerns.

6.2. Recommendations

Anyone who owns a small business should use the Virtualized Open-Source Network Security Appliance. This project is also ideal for use on a home network. However, I think that it is important that the users have at least a basic understanding of computers and networking.
Appendix A

Figure 28 below shows the contents of the ReadMe.txt file that opens successful installation of InstallVOSNSA.bat.

To run the Virtualized Open-Source Network Security Appliance first:

1: Run VMWare Server from the Icon located on the desktop.

2: Once load select Local for the Host

3: Select Open Existing Virtual Machine

4: Select browse and load the following machines:

   C:\VOSNSA1.0\CentOS-Internal
   C:\VOSNSA1.0\m0n0wall
   C:\VOSNSA1.0\Smoothwall
   C:\VOSNSA1.0\Vyatta-VC2.2

5: After that, start the virtual machines, and then the Virtualized Open-Source Network Security Appliance is Operational.

It is important to note that you should not change any of the Virtual Network Settings within VMWare Server.

If you have any other questions regarding configurations see the enclosed documentation on the DVD.

DEFAULT PASSWORDS:
SMOOTHWALL:
   LOGON:     admin
   PASSWORD:  password

MONOWALL:
   LOGON:     admin
   PASSWORD:  mono

VYATTA:
   LOGON:     vyatta
   PASSWORD:  vyatta

Thanks for reading!!!

Dan Secrist 2008

Figure 28: Contents of ReadMe.txt
References


3. **Lipps, John.** Small Business Owner: CincyCyberKnight. Personal Interview. 23 November 2007
