**Testing Document and Specification**

Test Specification

Team 16

CS 451R

|  |  |  |
| --- | --- | --- |
| Tyler DeWitt |  | Zach Foss |
|  |  |  |

|  |  |
| --- | --- |
| Test Case ID: | 4.1.1 |
| Title: | Fortigate Firewall |
| Feature/Subfeature: | Firewall configuration |
| Purpose: | To ensure that the firewall is working as intended |
| Initial Conditions: | Users must have already had a firewall installed or are currently installing it. |
| Test Data: | Test Data will include invalid usernames like georgeWash and AbeLincoln and invalid passwords as in 123456789 and 098765432. Valid usernames and passwords will also be used but will not be listed here for security and confidentiality reasons. |
| Test Actions: | 1. Go to <http://www.fortiguard.com/antivirus/eicartest.html> to download the test file (eicar.com) or the test file in a ZIP archive (eicar.zip). 2. If the antivirus profile applied to the security policy that allows you access to the Web is configured to scan HTTP traffic for viruses, any attempt to download the test file will be blocked. This indicates that you are protected. |
| Expected Results: | AAgvgghhaaa The Fortigate will not allow you to download the file |

|  |  |
| --- | --- |
| Test Case ID: | 4.1.2 |
| Title: | Switch configurations |
| Feature/Subfeature: | System User Validation/Availability of Survey |
| Purpose: | To ensure the switches are operational |
| Initial Conditions: | Users must have had the switches previously installed. |
| Test Data: | Test Data will include names of computers connected to the switch and their IP addresses |
| Test Actions: | 1. Check LEDs    1. The Power LED should be solid green (or blue, if clients are connected). If it is ﬂashing blue, the ﬁrmware is automatically upgraded and the LED should turn green when the upgrade is completed (normally within a few minutes). See the "LED Indicators" section for more details. .    2. Note: Your MR42 must have an active route to the Internet to check and upgrade its ﬁrmware. 2. Verify access point connectivity    1. Use any 802.11 client device to connect to the MR42 and verify proper connectivity using the client’s web browser. 3. Check network coverage 4. Conﬁrm that you have good signal strength throughout your coverage area. You can use the signal strength meter on a laptop, smart phone, or other wireless device. |
| Expected Results: | Each user computer will be able to connect to the network |

|  |  |
| --- | --- |
| Test Case ID: | 4.1.3 |
| Title: | FireEye & Inky |
| Feature/Subfeature: | Email Threat Prevention |
| Purpose: | To ensure company emails are secured both in offices and on the go. |
| Initial Conditions: | Employee computer must be equipped with the software |
| Test Data: | The data available will include employee email addresses |
| Test Actions: | 1. Perform a penetration test against the software |
| Expected Results: | Access to email is not given to penetration tester |

|  |  |
| --- | --- |
| Test Case ID: | 4.1.4 |
| Title: | FortiClient VPN |
| Feature/Subfeature: | Capability of working from home |
| Purpose: | This is to allow employees to work from home so they can access information that would be on the company network. |
| Initial Conditions: | Employees computer must have the FortiClient VPN and set to the locations network information |
| Test Data: | The data will include employees username and password |
| Test Actions: | 1. End user sign in from home 2. End user sign in using a hotspot 3. Verify user can access company information while connected to VPN |
| Expected Results: | The end user should be able to connect to the VPN using their username and password. Once connected they should be able to access company information that typically is only accessible if they were in the office. |