|  |  |  |
| --- | --- | --- |
| Qualification Code: | ICT60515 | |
| Qualification Title: | Advanced Diploma of Computer Systems Technology | |
| Unit Code/s: | ICTNWK509 | |
| Unit Title/s: | Design and implement a security perimeter for ICT networks | |
| Student Id | Cal14385330 | |
| Student Name | Benjamen Calleja | **Signature** |
| Assessment Due Date: |  | |
| Assessment Name: | Assessment Item 3 Project | |
| Teacher’s name: | Murad Quazi | |
| Teacher’s email: | mquazil@kangan.edu.au | |

|  |
| --- |
| 1. Task Instructions |

This Project requires students to work in team and address all requirements as per Assessment item Description. Students are required to accomplish their task professionally and in time. Students must submit this project by due date. This assessment is group project and group leader must clearly identify his team members work.

|  |
| --- |
| 1. Submission instructions |

All items submitted must be clearly marked with the following details:

• Your full name

• Your student number

• Your class group

• The date

This cover sheet must accompany all items submitted.

Student’s Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Marking Criteria

|  |  |
| --- | --- |
| **Grade** |  |
| NP | * Assessment aims have not been met |
| CA | * All requirements mentioned in Part A, Part B and Part C are correctly addressed. * Graphics are accurate, well presented and clearly reference if required * Comparison is done wherever required * OHS Risks are identified and documented * OHS Risk control measure are taken * Contents are comprehensive, accurate and professionally presented * Requirements are explained with Graphics. * Proper Documentation is done |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Comments: |  | | | |
| Teachers Signature: | |  | Date: |  |

# Assessment Item Description

**Students are required to create instructions/Step by Step tutorial for Installation and Configuration of Firewall , VPN and Backup**

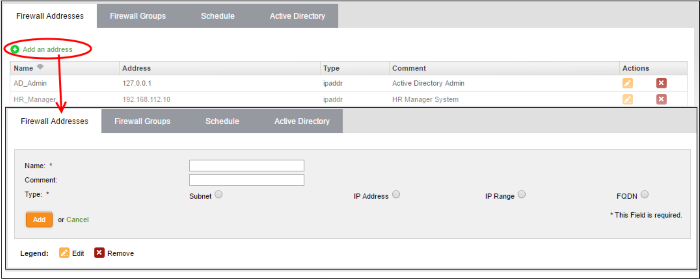
This project requires students to work in a team and accomplish their task professionally and on time. It is team leader’s responsibility to inform teacher about individual student’s responsibility. Students are required to research their own component. This assessment has three Parts.

**Part A**

* How to configure Firewall

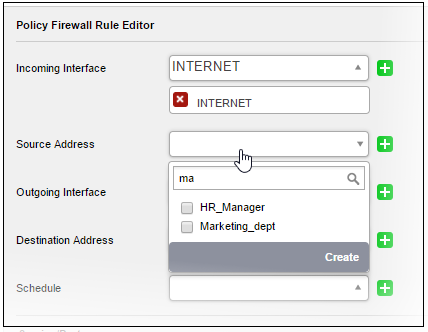
The firewall address object can be created in two ways:

* **From the 'Add an Address' pane. Define a name for the object and the IP address, IP range or subnet of the host(s) to be included in the object. See section below for more details.**
* **By importing users from Active Directory. See '**[**Active Directory**](https://help.comodo.com/topic-451-1-938-12953-.html#fw_ad)**' for more information.**
* **Click 'Firewall' > 'Objects' on the left menu and click the '**[**Firewall**](https://cdome.comodo.com/firewall/)**Addresses' tab**
* **Click 'Add an address' at top left**



* **Enter the parameters for the new object as shown below:**
* **Name - Specify a name for the object (15 characters max) representing the host(s) included in the object.**
* **Comment - Enter a short description of the object.**
* **Type - Select the type by which the hosts are to be referred in the object. The available options are:**
* **Subnet - Select this if a sub network of computers is to be covered by the object and enter the sub network address**
* **IP address - Select this if a single host is to be covered by the object and enter the IP address of the host**
* **IP range - Select this if more than one host is to be covered by the object and enter the IP address range of the hosts**
* **Click 'Add'. The new object will be added to the list.**

**The object will be available for selection for specifying source or destination while creating a firewall rule, by starting to type the first few letters of the object name.**

****

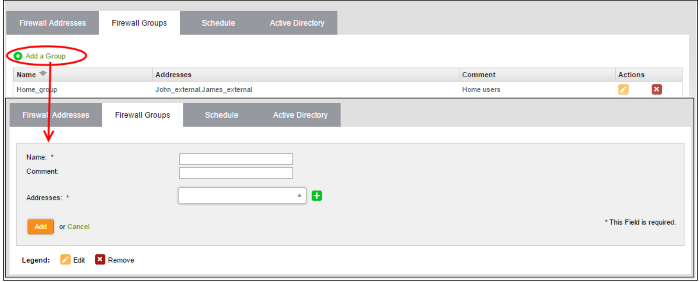
**Firewall Groups**

**The firewall object group can be created in two ways:**

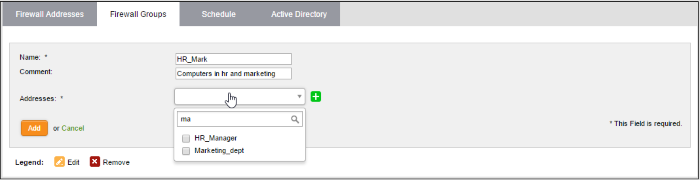
* **From the 'Add a Group' pane by defining a name for the group and the member objects to be included in the group. See**[**section below**](https://help.comodo.com/topic-451-1-938-12953-.html#add_firewall_object_group)**for more details.**
* **Importing users from Active Directory. See 'Active Directory' for more information.**

**To create a new object group**

* **Open the 'Firewall Groups' interface by clicking the 'Firewall Groups' tab under 'Firewall' > 'Objects'**
* **Click the 'Add a group' at the top left**

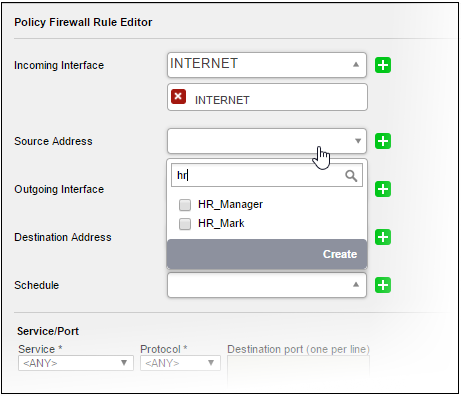


* **Enter the parameters for the new group as shown below:**
* **Name - Specify a name for the group (15 characters max).**
* **Comment - Enter a short description of the group.**
* **Addresses - Enter the names of the objects separated by comma, for inclusion in the group. Typing the first few letters of the name of an object will show the matching objects as a drop-down to select from.**



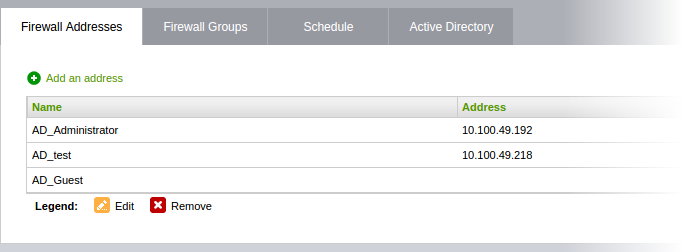
* **Click 'Add'. The new object will be added to the list.**

**The group will be available for selection for specifying source or destination while creating a firewall rule, by starting to type the first few letters of the group name.**



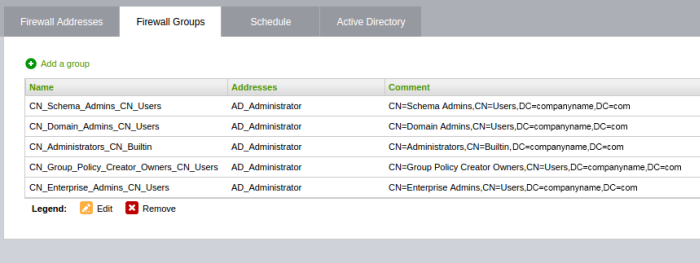
**Adding User to Firewall Objects**

* **Click the Domain name to expand the tree structure of the active directory.**
* **Locate the user by expanding the parents.**
* **Click 'Add User' to add the user to Firewall Objects**.

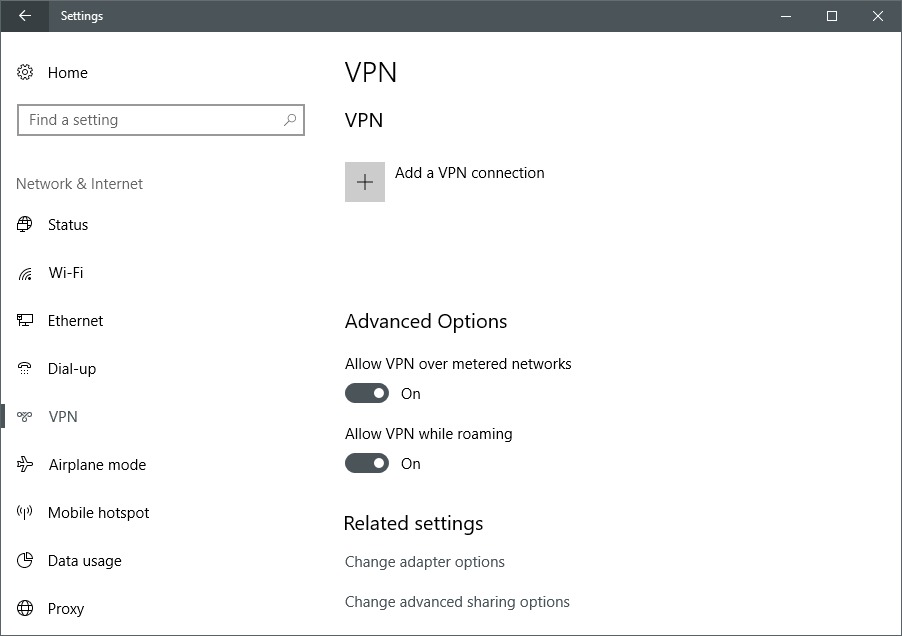


**Adding User Groups to Firewall Objects**

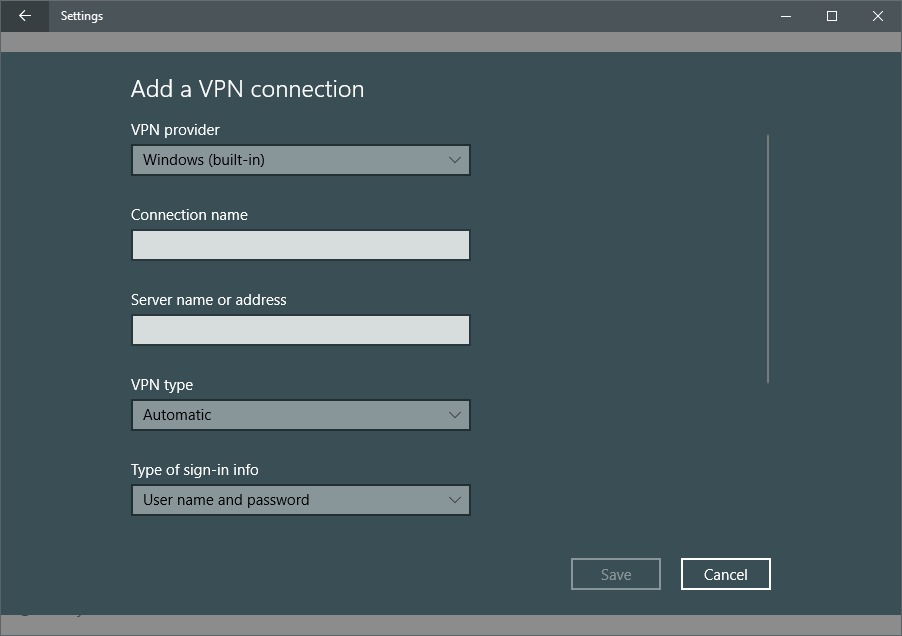
* **Click the Domain name to expand the tree structure of the active directory.**
* **Locate the user group by expanding the parents.**
* **Click 'Add Group' to add the user group to Firewall Object Groups**.



* How to configure VPN   
  **Step 1**The top choice should be Change virtual private networks (VPN). Alternatively, open the Settings app and go to Network & Internet > VPN.



**Step 2**At the top of the VPN screen in the Settings app, click Add a VPN connection.



**Part B**

Students are required to create step by step procedure for installation and configuration of server. They need to create technical manual for configuration of following:

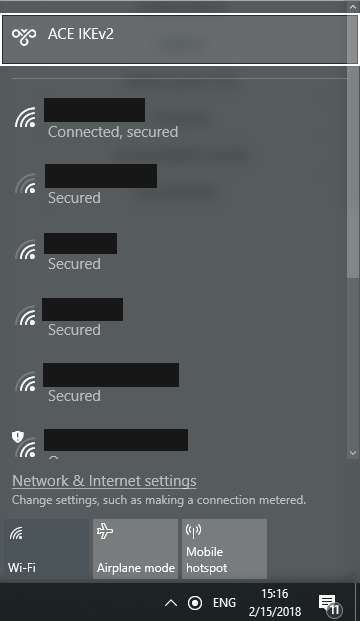
**Step 3**In the screen that appears, enter the details for your VPN connection. Under “VPN provider” click on the drop-down menu, and select Windows (built-in). This will also change “VPN type” to Automatic, and “Type of sign-in info” to User name and password.

**Step 4** Next fill out the “Connection name” and “Server name or address.” These vary based on your VPN provider—whether a third-party service or an employer. For this example, we’re using [Acevpn](https://www.acevpn.com/), a clientless VPN service that supports various connection types such as IKEv2, L2TP, and PPTP.

**Step 5** Scroll down this screen and you’ll see a spot to enter your username and password for the VPN—again provided by your VPN service. Once the information is entered, click Save, and close the Settings app.

**Step 6**Click the Wi-Fi icon in the system tray on your taskbar, and select your newly created VPN connection, which should be right at the top of the list. It should automatically start to connect, and if all goes well the connection process should happen relatively quickly.

The above process works for the easier VPN connection types such as PPTP and L2TP, but if you want to use IKEv2 that requires installing a[root certificate](https://support.dnsimple.com/articles/what-is-ssl-root-certificate/) from your VPN provider. Keep in mind that not every service supports IKEv2 so using this method depends greatly on your VPN service provider or employer.



* How to configure Firewall

**Type firewall and click on the Windows Firewall with Advanced Security icon**

**Open your firewall, you will see the firewall overview, this shows what the current settings are for each profile (Domain, Private and Public).**

**To check your Inbound or Outbound rules select either one from the left hand pane.**

* **Open the Server Manager from the task bar.**
* **Click the Tools menu and select Windows Firewall with Advanced Security.**
* **Select Inbound Rules under Windows Firewall with Advanced Security on the left side of the management console.**
* **From the right side click New Rule.**
* **Select Port and then Next.**
* **Select TCP and enter 8080 into the Specific local ports input box. Click Next.**
* **Select allow the connection and click next.**
* **For the “When does this rule apply” question, select one (or all =default) of the radio-buttons depending on your environment and click Next.**
* How to configure VPN
* **Open control panel**
* **Click on Network and Sharing**
* **Using the left pane, click the change adapter settings link**
* **In Network Connections open the file menu pressing the alt key, and select the new incoming Connection option**
* **Check the users you want to VPN access to your computer, and click the next button Alternatively, you can click the Add someone button to create a new VPN user:**
* **Check the Through the Internet option.**
* **Click the Next button.**
* **In the networking software page, select Internet Protocol Version 4 (TCP/IPv4) option.**
* **Click the Properties button.**
* **Check the Allow callers to access my local area network option.**
* **Under “IP address assignment,” click Specify IP addresses, and specify the number of clients allowed to access using a VPN connection. (You will do this by specifying an IP address range, and it’s recommended that you use high-order range of IP addresses to help avoid conflicts in the network with the IPs distributed by your router.)**
* **Click the OK button.**
* **Click the Allow access button.**
* **Click the Close button to complete setting up the VPN server on Windows 10.**

**Part C**

**All students are required to submit their project in written document. The document must include:**

1. Identify, list and discuss threats to enterprise security

## Phishing

**Phishing emails are a common way hackers gain access to enterprise systems or trick business leaders into fraudulently wiring money, Hill said. "Big companies are hard to attack, so hackers have to attack you, the individuals," Hill said. "It's where the vulnerabilities are. People click on links."**

## CEO spoofing

**CEO spoofing is a similar concept to phishing, but with a twist: It tricks users via an email, instead of a link. It can occur like this: Using social media, a cybercriminal can see when a CEO is at a conference. Then, he or she can send an email that appears to be from the CEO to the CFO, saying "I'm here in China, we need to make an acquisition immediately, please transfer me $1 million."**

## Insider threats

**Insider threats are a major cybersecurity concern for enterprises that are often overlooked, Hill said. Employees may resign or be terminated, and create a backdoor for themselves, or take data with them to a competing company.**

## ****Zeus malware****

**In 2010, more than**[**100 people were arrested**](http://www.bbc.com/news/world-us-canada-11457611)**in a major cyber crime ring after using phishing emails to infect computers of small businesses and individuals in the US with Zeus, a type of malware used to steal banking information by man-in-the-browser keystroke logging and form grabbing. Zeus allows criminals to access users' online passwords and bank account details and transfer money out.**

## Internet of Things (IoT) vulnerabilities

**"Everything today is connected," Hill said, which can make our work and personal lives easier, but also opens up a number of new security concerns.**

**This is especially the case for businesses such as connected public utilities, Hill said. Remote access to these systems can be convenient for solving problems in off-hours, but also creates security vulnerabilities. For example, in Blaine, MN, the IoT-controlled water system was shut down twice in two months this year, leading to school closures and a city recommendation to boil water before drinking it.**

## Ransomware

**Ransomware attacks have exploded in number in the past year,**[**research shows**](https://www.techrepublic.com/article/report-ransomware-attacks-grew-600-in-2016-costing-businesses-1b/)**. "Ransomware is a huge threat, where perpetrators will come in, access your network via a phishing scam or other means, and then encrypt all of your data, leaving you virtually helpless unless you pay the fee or keep current backup**

1. What sort of security measures we must take to protect our enterprise.

**Establish strong passwords**

### Put up a strong firewall

### Install antivirus protection

### Update your programs regularly

### Backup regularly

### Monitor diligently

### Be careful with email, IM, and surfing the web

### Educate your employees

1. Identify available security options for those threats

**Establish strong passwords  
Implementing strong passwords is the easiest thing you can do to strengthen your security.**

[**According to Microsoft**](https://www.microsoft.com/protect/fraud/passwords/create.aspx)**, you should definitely avoid using:**

* **any personal data (such as your birthdate)**
* **common words spelled backwards**
* **sequences of characters or numbers, or those that are close together on the keyboard**

### Put up a strong firewall

**In order to have a properly protected network, 'firewalls are a must,**

**A firewall protects your network by controlling internet traffic coming into and flowing out of your business. They're pretty standard across the board.**

### Install antivirus protection

**Antivirus and anti-malware software are essentials in your arsenal of online security weapons, as well.**

**'They're the last line of defence' should an unwanted attack get through to your network,**

### Update your programs regularly

**Making sure your computer is 'properly patched and updated' is a necessary step towards being fully protected; there's little point in installing all this great software if you're not going to maintain it right.**

**'Your security applications are only as good as their most recent update While applications are not 100 per cent fool-proof, it is important to regularly update these tools to help keep your users safe.'**

**Frequently updating your programs keeps you up-to-date on any recent issues or holes that programmers have fixed.**

### Backup regularly

**Scheduling regular backups to an external hard drive, or in the cloud, is a painless way to ensure that all your data is stored safely.**

**The general rule of thumb for backups: servers should have a complete backup weekly, and incremental backups every night; personal computers should also be backed up completely every week, but you can do incremental backups every few days if you like.**

**Getting your data compromised is a painful experience -- having it all backed up so you don't completely lose it will make it much less so.**

### Monitor diligently

**One good monitoring tool is data-leakage prevention software, which is set up at key network touchpoints to look for specific information coming out of your internal network. It can be configured to look for credit card numbers, pieces of code, or any bits of information relevant to your business that would indicate a breach.**

**If you don't monitor things 'it's a waste of time and a waste of resources.' And you won't know that you've been compromised until it's far too late.**

### Educate your employees

**Teaching your employees about safe online habits and proactive defence is crucial.**

**'Educating them about what they are doing and why it is dangerous is a more effective strategy than expecting your IT security staff to constantly react to end users' bad decisions**

1. Design and implement security perimeters to security options  
   **Border Routers  
   They direct traffic into, out of, and within our networks. The border router is the last router you control before an untrusted network such as the internet. Because all of an organization’s internet traffic comes through this router, it often functions as a network’s first and last line of defence through initial and final filtering.  
     
   Firewalls  
   A firewall is a chokepoint device that has a set of rules specifying what traffic it will allow or deny to pass through it. A firewall typically picks up where the border router leaves off and makes a much more accurate pass at filtering traffic.**

**Intrusion Detection Systems  
An IDS is similar to a burglar alarm system for your network that is used to detect and alert on malicious events, and they might perform statistical and anomaly analysis. When IDS sensors places at strategic points in your network. IDS sensors watch for predefines signatures of malicious events, and they might perform statistical and anomaly analysis. When IDS sensors detect suspicious events, they can alert in several different ways, including email, paging, or simply logging the occurrence. IDS sensors can usually report to a central database that collects their information to view the network from multiple points.**

**APA reference list.**

[**https://support.rackspace.com/how-to/best-practices-for-firewall-rules-configuration/**](https://support.rackspace.com/how-to/best-practices-for-firewall-rules-configuration/)

[**https://help.comodo.com/topic-451-1-938-12953-.html**](https://help.comodo.com/topic-451-1-938-12953-.html)

[**https://www.pcworld.com/article/210562/how-set-up-vpn-in-windows.html**](https://www.pcworld.com/article/210562/how-set-up-vpn-in-windows.html)

[**https://www.esecurityplanet.com/network-security/vpn-virtual-private-network.html**](https://www.esecurityplanet.com/network-security/vpn-virtual-private-network.html)