

INFO813 Practical project documentation template (Engineering journal)

Stage Number 5

Student name: Raine Roberts

When doing practical work it is common practice and extremely useful to document the steps you took. This assists you make your learning more tangible and organize it. The more detail you can provide the better it is so that if ever you want to configure it in the future you have a personal record documented.

The project book gives the main implementation steps. However this documentation report requires you document what you did at each implementation step as you are doing the practical project. It is not advised to do this at the end otherwise you are likely to forget what you did. You can alter the format of this template as long it includes all the relevant information

Please write this in your own words as it is a record of your work. Copied material is not accepted.

Describe the Design of your project and justify your design. (100 words)

My project includes a Windows 10 client, a Windows Server 2022, a FortiGate firewall, and a TrueNAS server. The firewall performs Port Address Translation (PAT) to allow internal devices internet access, with rules to block specific sites and restrict protocols to HTTP, HTTPS, and DNS for security. Group policies set desktop wallpapers, restrict control and command prompts for non-administrative users, and enforce password policies. SSH access is enabled for secure firewall management, and static NAT forwards internet traffic to the Windows Server. The TrueNAS server provides user-specific datastores with weekly backups from the Windows Server, ensuring data integrity and security.

Describe the key features of one competing/alternative technology and compare it to the one implemented in the project (Pros and Cons). (200 words)

Comparison of FortiGate Firewall and Cisco ASA Firewall

Key Features of Cisco ASA Firewall:

Cisco ASA (Adaptive Security Appliance) is a robust network security solution offering advanced firewall capabilities, VPN support, and intrusion prevention. It integrates seamlessly with other Cisco products, providing a unified security approach. Cisco ASA supports application-layer filtering, secure remote access with SSL VPN, and detailed network monitoring through its Adaptive Security Device Manager (ASDM).

Comparison with FortiGate Firewall:

- **Ease of Use:**
FortiGate's intuitive web-based GUI and FortiOS simplify configuration and management. Cisco ASA, while powerful, has a steeper learning curve and relies on ASDM or CLI for configuration.
- **Features:**
FortiGate includes advanced features like web filtering, antivirus, and deep packet inspection

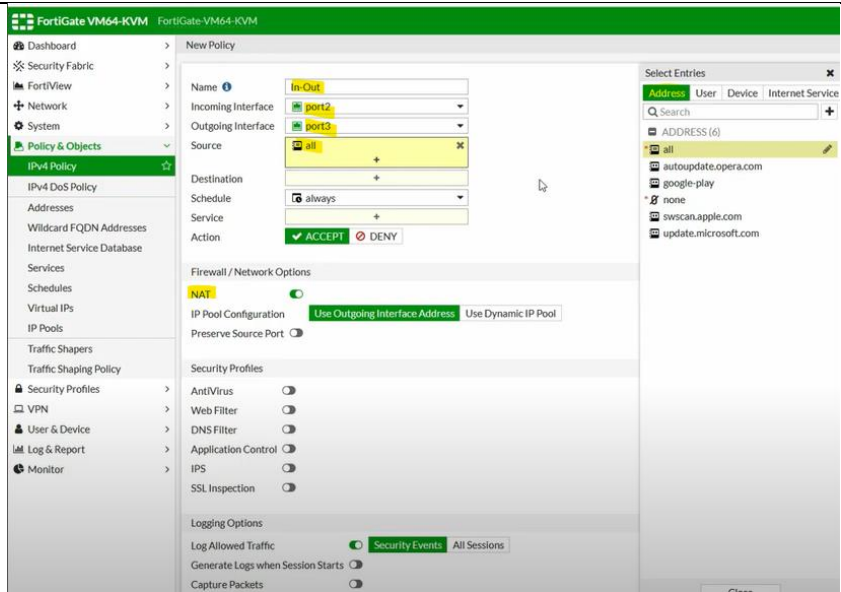
in its base offering. Cisco ASA requires additional licenses for similar features, making FortiGate more cost-effective.

- **Scalability:**
Cisco ASA excels in enterprise environments with high-performance hardware and seamless integration with other Cisco devices. FortiGate is versatile, catering to both small businesses and large organizations.
- **Cost:**
FortiGate is more affordable, offering a better value for small-to-medium businesses. Cisco ASA is costlier, focusing on large-scale deployments.

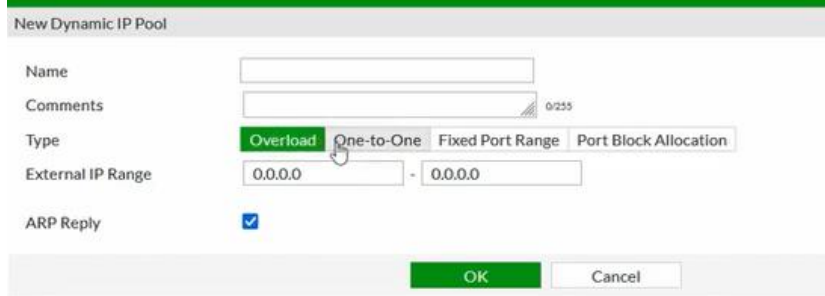
Conclusion:

FortiGate is ideal for organizations seeking comprehensive features at an affordable cost, while Cisco ASA suits enterprises prioritizing performance, scalability, and Cisco ecosystem integration.

Section summary	Implementation details at each step e.g. screenshots, written steps, value of settings, commands used, results, answers to questions etc where applicable.	Justification if needed
TASK 1	<ul style="list-style-type: none">• Configure your Fortigate Firewall to:<ul style="list-style-type: none">○ Perform Port Address Translation (PAT), this is like Network Address Translation (NAT), so internal devices e.g. Windows server and client can access the internet <p>Using the command line interface, we complete the commands below:</p> <p>TASK 1: Configure Port Address Translation (PAT) This ensures internal devices like the Windows Server and Windows client can access the internet using a single public IP.</p> <p>Steps:</p> <ol style="list-style-type: none">1. Log in to the Fortigate CLI or Web GUI.2. Create a NAT policy: <pre>arduino Copy code config firewall policy edit 1 set srcintf "internal" set dstintf "wan1" set srcaddr "all" set dstaddr "all" set action "accept" set nat enable set ippool enable end</pre>	



We can also use the Fortinet manager to easily complete this with the web gui. By setting a name, choosing the inside and outside interfaces and selecting the nat toggle. We can then press the overload toggle to configure nat overloading and turn NAT into PAT.



TASK 2

Implement firewall rules (Web Filter) to block certain sites.

Using the command line interface, we can use the commands below to complete web address filtering:

TASK 2: Implement Web Filtering to Block Certain Sites

Web filtering restricts access to specific URLs.

Steps:

1. Create a Web Filter Profile:
arduino
Copy code
config webfilter profile
edit "BlockCertainSites"
set block-url enable
config block-url

	<pre>edit 1 set url "example.com" next end end 2. Apply the Web Filter Profile to a Firewall Policy: arduino Copy code config firewall policy edit 2 set srcintf "internal" set dstintf "wan1" set srcaddr "all" set dstaddr "all" set action "accept" set service "ALL" set webfilter-profile "BlockCertainSites" end</pre>	
--	--	--



We can also use the previous Fortinet managerweb gui to add addresses to our filtering list.

TASK 3

Only allow specific protocols to be permitted from your internal organisation to the internet. Justify your design and test it to ensure it is working

TASK 3: Allow Specific Protocols to Access the Internet

This restricts internal traffic to only necessary protocols like HTTP, HTTPS, and DNS.

Steps:

1. Configure a firewall policy:
 - arduino
 - Copy code
 - config firewall policy
 - edit 3
 - set srcintf "internal"

	<pre> set dstintf "wan1" set srcaddr "all" set dstaddr "all" set action "accept" set service "HTTP" "HTTPS" "DNS" end </pre> <p>2. Justification:</p> <ul style="list-style-type: none"> ○ Only essential protocols are allowed to minimize attack surfaces and ensure business needs are met. ○ HTTP and HTTPS are necessary for web access; DNS for domain name resolution. 	
TASK 4	<p>Allow Secure Shell (SSH) access from internal devices to the firewall. You could use PuttyGen to generate keys and putty to connect from the windows client.</p> <p>🔗 Enable SSH Access:</p> <pre> arduino Copy code config system interface edit "port1" set allowaccess ping ssh end </pre> <p>🔗 Generate SSH Keys Using PuttyGen:</p> <ul style="list-style-type: none"> • Open PuttyGen and generate public/private key pairs. • Save the private key and copy the public key. <p>🔗 Add the Public Key to the Firewall:</p> <pre> arduino Copy code config system admin edit "admin" set ssh-public-key1 "ssh-rsa <Public_Key>" end </pre> <p>🔗 Test SSH Access:</p> <ul style="list-style-type: none"> • Use Putty to connect: <pre> kotlin Copy code ssh admin@<Firewall_IP> </pre>	
TASK 5	<p>Allow Port Forwarding (Static NAT) from the internet to your windows server.</p> <p>TASK 5: Configure Port Forwarding (Static NAT) This forwards traffic from the internet to the internal Windows Server.</p> <p>Steps:</p> <ol style="list-style-type: none"> 1. Create a Virtual IP (VIP): 	

	<pre> arduino Copy code config firewall vip edit "PortForwarding" set extip <Public_IP> set extintf "wan1" set mappedip <Internal_Server_IP> set portforward enable set extport 80 set mappedport 80 end </pre> <p>2. Create a Firewall Policy:</p> <pre> arduino Copy code config firewall policy edit 4 set srcintf "wan1" set dstintf "internal" set srcaddr "all" set dstaddr "PortForwarding" set action "accept" set service "HTTP" end </pre> <p>3. Test Port Forwarding:</p> <ul style="list-style-type: none"> From an external device, access <code>http://<Public_IP></code> and confirm it reaches the internal server.  <p>Create a virtual IP route</p>	
--	--	--

List the three most useful Internet resources that you used (provided by the tutor)

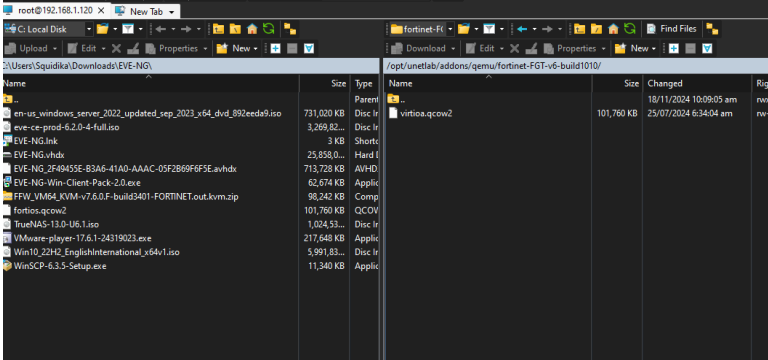
NAT
<ul style="list-style-type: none"> https://www.youtube.com/watch?v=5OhQNm2yc8U
Static NAT

<ul style="list-style-type: none"> • https://docs.fortinet.com/document/fortigate/6.4.5/administration-guide/898655/static-snat
SSH into Fortigate
<ul style="list-style-type: none"> • https://youtu.be/S5bM3hDvp5Q

List all (at least three) Internet resources that you found and used that were not provided by the tutor)

https://www.youtube.com/watch?v=03C1pBtlXVI
https://www.youtube.com/watch?v=vvAN5jxAGDo
https://www.youtube.com/watch?v=aigAlK7bOLA

Reflect on at least two significant problems you came across during the implementation of this section and the solution you found. Use at least five sentence to describe each problem and five sentences to describe each solution. Demonstrate your critical thinking and problem-solving abilities.

Problem	Solution
Firewall not starting	 <p>Renaming the firewall iso fixed the issue.</p>
Problem: The web filter overblocked, preventing all website access due to an unintended "BlockAll" category in the rule. This disrupted user access and testing.	Solution: I adjusted the web filter to block only specific URLs by unsetting the "BlockAll" category and testing the configuration: arduino Copy code config webfilter profile edit "BlockCertainSites" unset category-action end This resolved the issue, ensuring normal access while blocking targeted sites.