Firewall policies and NAT

Firewall policies are sets of rules used to control and monitor network traffic. These rules determine whether to allow or block traffic based on various criteria such as IP addresses, ports, protocols, and application types. Effective firewall policies ensure security, manage traffic flow, and prevent unauthorized access.

Firewall policies are a critical component of network security. They define the rules and conditions that dictate how traffic flows through a firewall, controlling what is allowed or denied based on predefined criteria. These policies protect the network from unauthorized access, prevent cyberattacks, and ensure efficient traffic management.

In Fortinet firewalls, such as FortiGate, policies are highly customizable, allowing administrators to filter traffic based on factors like source/destination IPs, protocols, ports, applications, and even user identity. Proper configuration of firewall policies ensures a secure, well-functioning network.

In today's interconnected world, networks are constantly exposed to potential threats from external and internal sources. Firewalls serve as the first line of defense, ensuring that only authorized traffic flows into or out of a network. This is achieved through **firewall policies**, which are rules that control how data packets are processed based on criteria such as source and destination IP addresses, ports, and protocols.

To complement this, **Network Address Translation (NAT)** plays a crucial role in managing IP address allocation and maintaining security. NAT allows private IP addresses within a local network to communicate with external networks, such as the internet, by translating them into a single public IP. This not only conserves public IP addresses but also hides internal network structures from external entities, adding an additional layer of protection.

Key Elements of Firewall Policies:

1. **Source and Destination**:
   - **Source IP/Network**: The originating IP address or subnet.
   - **Destination IP/Network**: The target IP address or subnet.
2. **Ports and Protocols**:
   - Specify allowed or blocked ports (e.g., 80 for HTTP, 443 for HTTPS).
   - Define protocols (e.g., TCP, UDP, ICMP).
3. **Actions**:
   - **Allow**: Permit traffic to pass.
   - **Deny**: Block traffic.
   - **Log**: Record details of the traffic without affecting flow.
4. **Application/Service Filtering**:
   - Policies can focus on specific applications (e.g., email, FTP).
   - Advanced firewalls (e.g., NGFW) include deep application-level inspections.
5. **User and Device Identification**:
   - Policies can target specific users, user groups, or devices.
6. **Time-Based Rules**:
   - Apply rules during specific times (e.g., office hours).
7. **Logging and Monitoring**:
   - Policies should include logging for auditing and troubleshooting.
8. **NAT Rules**:
   - Handle address translation for inbound or outbound traffic.

Common Types of Firewall Policies:

1. **Inbound Policies**:
   - Govern traffic entering the network from external sources.
   - Typically strict to protect against external threats.
2. **Outbound Policies**:
   - Manage traffic leaving the network.
   - Often more relaxed but still controlled to prevent data leaks or unauthorized communication.

3. **Zone-to-Zone Policies**:
   - Define rules between network zones (e.g., LAN to DMZ, LAN to WAN).

4. **VPN Policies**:
   - Secure communications between remote users or sites via encryption.

Best Practices for Configuring Firewall Policies:

1. **Follow the Principle of Least Privilege**:
   - Only allow traffic essential for business operations.
2. **Regular Updates**:
   - Review and update rules to reflect changes in the network.
3. **Log and Analyze Traffic**:
   - Monitor logs to identify patterns or potential threats.
4. **Implement Security Zones**:
   - Segment the network into zones (e.g., LAN, DMZ, WAN) and control traffic between them.
5. **Use Object Groups**:
   - Simplify management by grouping IPs, services, or users.
6. **Apply Stateful Inspection**:
   - Ensure the firewall tracks the state of active connections for dynamic rules.
7. **Test Policies**:
   - Use tools to validate that policies achieve the desired outcomes.
8. **Backup Configurations**:
   - Regularly back up policies to recover in case of configuration errors or device failure.

Key Elements of NAT:

1. **Private and Public IP Addressing:**
   - **Private IP Addresses:**
     - Assigned to devices within a local network (e.g., 192.168.x.x, 10.x.x.x).
     - Non-routable on the internet.
   - **Public IP Addresses:**
     - Globally unique addresses used for communication over the internet.
     - NAT translates private IPs into public IPs for internet access.
2. **NAT Types:**
   - **Source NAT (SNAT):**
     - Rewrites the source IP address of outgoing traffic from private to public.
     - Used for outbound internet access.

- **Destination NAT (DNAT):**
  - Rewrites the destination IP address of incoming traffic from public to private.
  - Enables external users to access internal resources like web servers.
- **Port Address Translation (PAT):**
  - A form of SNAT that allows multiple devices to share a single public IP by differentiating them using port numbers.
- **Static NAT:**
  - A one-to-one mapping between a specific private IP and a public IP.

3. NAT Table:

- Maintains a mapping of private and public IP addresses (and ports in the case of PAT).
- Ensures return traffic is routed correctly to the original device.

4. NAT Rules and Policies:

- Define which traffic is subject to NAT and how translation occurs.
- Configured based on:
  - Source IP/Port.
  - Destination IP/Port.
  - Network interfaces (e.g., LAN, WAN).

5. NAT Pools:

- A range of public IP addresses used for translation.
- Allows for scalability by dynamically assigning IPs to multiple devices.

6. Security Benefits:

- **IP Masking:**
  - Hides internal network structure from external entities.
- **Limited Exposure:**
- Only specific services and devices are exposed to the internet.

7. Scalability:

- Conserves public IP addresses by enabling multiple private IPs to share one public IP using PAT.

Types of NAT:

1. **Source NAT (SNAT):**
   - **Description:** SNAT modifies the source IP address of packets that are sent from an internal network to an external network (e.g., the internet).
   - **Usage:**
     - Primarily used for allowing devices within the private network to access the internet.
     - Often used in scenarios where multiple internal devices share a single public IP address.
     - Typically employed in conjunction with Port Address Translation (PAT) to handle multiple connections.
2. **Destination NAT (DNAT):**
   - **Description:** DNAT modifies the destination IP address of incoming packets from the internet (or external network) to the internal IP address.
   - **Usage:**
     - Commonly used to allow external users to access services hosted on an internal network (e.g., web servers, email servers).
     - Useful for setting up services like port forwarding where traffic from the internet is redirected to specific internal resources.
3. **Port Address Translation (PAT):**
   - **Description:** A form of Source NAT (SNAT), PAT allows multiple devices within a private network to share a single public IP address by differentiating them based on port numbers.
   - **Usage:**
     - Enables many internal devices to access the internet using a single public IP address.
     - Often referred to as "overloading" because it translates multiple internal private IPs to a single public IP.
4. **Static NAT:**
   - **Description:** Static NAT creates a one-to-one mapping between a specific private IP address and a public IP address.
   - **Usage:**
     - Used when you need a fixed external IP address to be mapped to an internal device.
     - Common for servers that must be reachable from the outside world (e.g., web servers, DNS servers).

5. Dynamic NAT:

- **Description:** Dynamic NAT translates private IP addresses to a public IP address from a pool of available public IPs.
- **Usage:**
  - Provides a dynamic mapping for internal devices to external addresses.
  - Used when the number of public IPs is less than the number of internal devices requiring access to the internet.

6. NAT Overload:

- **Description:** A method of performing NAT using PAT, where multiple internal IP addresses are mapped to a single public IP address using different port numbers.
- **Usage:**
  - Often used in home or small office networks to allow all devices to share a single public IP for internet access.
  - Commonly seen in consumer routers where many devices share one public IP for external communication.

Best Practices for Configuring NAT:

1. Use Port Address Translation (PAT) to Conserve IP Addresses:

- **Why**: PAT allows multiple devices within a private network to share a single public IP address, saving valuable public IPs.
- **Best Practice:** Use PAT whenever possible, especially in environments where public IP addresses are limited or costly. This is common for internet-bound traffic in both home and enterprise networks.

2. Avoid Overuse of Static NAT:

- **Why:** Static NAT creates a permanent one-to-one mapping between internal and external IP addresses, which may expose internal systems unnecessarily.
- **Best Practice**: Use static NAT only for services that must be publicly accessible, such as web servers or mail servers. Avoid using static NAT for general internet access or internal services that do not require external exposure.

3. Define NAT Rules Based on Security Policies:

- **Why:** NAT should not only manage IP translation but also ensure that only authorized traffic is allowed.
- **Best Practice:** Configure NAT rules that align with your organization's security policies. Use ACLs (Access Control Lists) in conjunction with NAT to restrict or permit traffic based on source/destination addresses, ports, and protocols.

4. Keep NAT Configurations Simple and Clear:

- **Why:** Complex or convoluted NAT rules can lead to misconfigurations, making it harder to troubleshoot and maintain.
- **Best Practice:** Use simple and organized NAT rules. Label each NAT rule clearly, avoid unnecessary complexity, and ensure that rules follow a logical order (e.g., source NAT first, then destination NAT). Regularly review and clean up unused rules.

5. Monitor and Log NAT Activity:

- **Why:** Monitoring NAT translations and logging activities helps in identifying potential issues and security threats.
- **Best Practice:** Enable logging for NAT translations to track traffic flow and detect anomalies. Use the logs to troubleshoot and optimize configurations, ensuring there are no unintended mappings or security vulnerabilities.

6. Consider Using Dynamic NAT for Large Networks:

- **Why:** Dynamic NAT allows for more flexibility than static NAT, providing a pool of public IPs to dynamically assign to private IPs.
- **Best Practice**: For larger networks or when more public IP addresses are available, use dynamic NAT to efficiently handle multiple devices accessing external networks. It reduces the need for fixed IP mappings while ensuring scalability.

7. Implement NAT at the Edge of Your Network:

- **Why:** NAT is typically applied at the edge of the network to isolate internal network structures and prevent direct exposure to the outside world.
- **Best Practice:** Place NAT devices (such as routers or firewalls) at the boundary between your internal network and the internet. This ensures that internal IP addresses remain hidden and that external communication is securely controlled.

8. Regularly Update and Review NAT Mappings:

- **Why:** Network configurations can change over time, leading to outdated NAT rules or IP mappings.
- **Best Practice**: Periodically review and update NAT mappings to reflect changes in your network architecture, IP addressing schemes, or public IP address allocations. Remove unused or unnecessary mappings to maintain an efficient and secure network.

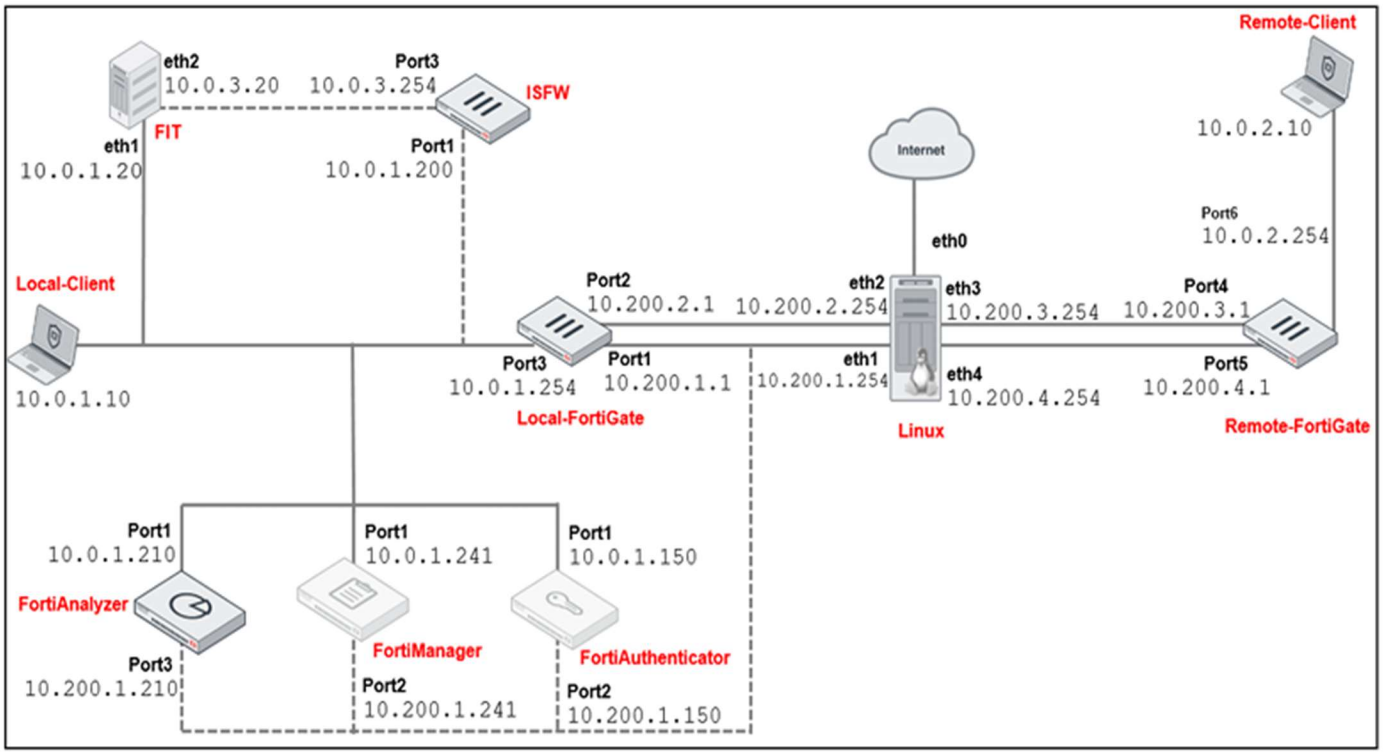
9. Implement Failover Mechanisms for NAT:

- **Why:** Network failure or downtime can disrupt NAT-based communications, particularly in high-availability environments.
- **Best Practice:** Implement redundancy and failover mechanisms to ensure that if one NAT device fails, another can take over seamlessly. This is crucial for mission-critical systems or businesses that require 24/7 availability.

10. Be Cautious with NAT in VPN Configurations:

- **Why:** NAT can sometimes interfere with VPN traffic, especially when IPs are being translated between networks.
- **Best Practice:** If using NAT with VPNs, ensure that NAT Traversal (NAT-T) is enabled, and test the configuration thoroughly. Avoid NAT on internal VPN traffic whenever possible, and configure the firewall or router to handle NAT correctly.

Network Topology:



Firewall Policy Configuration:

Step-by-Step Configuration:

1. **Login to FortiGate Web Interface:**
   - Open a web browser and enter the IP address of the FortiGate unit (e.g., https://<FortiGate_IP>).
   - Log in with the administrator credentials.
2. **Create an Address Object (Optional):**
   - Navigate to **Policy & Objects** > **Addresses**.
   - Click **Create New** to define network objects for internal and external addresses.
     - Example:
       - **Name:** Internal_Network
       - **Type:** Subnet
       - **Subnet/IP Range**: 192.168.1.0/24
3. **Configure Firewall Policy for Outbound (LAN to WAN) Traffic:**
   - Go to **Policy & Objects** > **IPv4 Policy**.
   - Click **Create New** to add a new firewall policy.
   - **Configure the following:**
     - **Name:** Allow_LAN_to_WAN
     - **Incoming Interface:** lan
     - **Outgoing Interface:** wan
     - **Source:** Internal_Network (or all for all internal IPs)
     - **Destination:** all
     - **Schedule:** always
     - **Service:** ALL
     - **Action:** Accept
     - **NAT:** Enable Source NAT (SNAT) to allow translation of internal IPs to public IP.
4. **Configure Firewall Policy for Inbound (WAN to LAN) Traffic:**
   - Go to **Policy & Objects** > **IPv4 Policy.**
   - Click **Create New** to add a new policy.
   - **Configure the following:**
     - **Name:** Allow_WAN_to_LAN
     - **Incoming Interface:** wan
     - **Outgoing Interface:** lan
     - **Source:** all
     - **Destination:** Internal_Server (Create an address object for the internal server if needed)
     - **Schedule:** always
     - **Service:** HTTP (or specific service you need)
     - **Action:** Accept
     - **NAT:** Disable NAT for inbound traffic.
5. **Apply and Save the policy.**

NAT Configuration:

Source NAT (SNAT) Configuration:

1. **Go to the Policy and Objects Menu:**
   - Navigate to Firewall Objects > NAT.
2. **Configure Source NAT (SNAT) for LAN to WAN:**
   - Select **Create New** and configure:
     - **Type:** SNAT
     - **Interface:** wan
     - **IP Pool:** Use Interface Address (if you want to use the public IP of the WAN interface)
     - **Enable Source NAT**: Enable.

Destination NAT (DNAT) Configuration:

1. **Go to Virtual IPs:**
   - Navigate to **Firewall Objects** > **Virtual IPs**.
2. **Create a Virtual IP for DNAT:**
   - Click **Create New** to create a virtual IP object.
   - Configure the following:
     - **Name:** Web_Server_VIP
     - **Interface:** wan
     - **External IP Address**: <Public_IP>
     - **Mapped IP Address:** 192.168.1.10 (Internal server IP)
     - **Port Forwarding**: Enable and define the specific service port (e.g., 80 for HTTP, 443 for HTTPS).
3. **Create a Firewall Policy for DNAT (Allowing External Access to Internal Server):**
   - Go to **Policy & Objects** > **IPv4 Policy**.
   - Click **Create New.**
   - **Configure the following:**
     - **Name:** Allow_WAN_to_Internal_Server
     - **Incoming Interface:** wan
     - **Outgoing Interface:** lan
     - **Source:** all
     - **Destination:** Web_Server_VIP
     - **Schedule:** always
     - **Service:** HTTP (or the appropriate service)
     - **Action:** Accept
     - **NAT:** Disable NAT for inbound traffic.
4. **Apply and Save the configuration.**

Verify Configuration:

After setting up the policies and NAT configurations, ensure everything is working properly:

- Test **outbound** traffic from the internal network to the internet to verify SNAT is working.
- Test **inbound** traffic to the internal server from the internet to ensure DNAT is configured correctly.
- Use **diag debug** commands on the FortiGate CLI to check real-time traffic flow and troubleshoot issues if necessary.

Example to monitor traffic:

```
diag debug enable
diag debug console timestamp enable
diag debug app ipsmonitor 255
```

In conclusion, the configuration of Firewall Policies and NAT (Network Address Translation) plays a critical role in securing and optimizing network traffic. By setting up proper firewall rules, we control the flow of traffic between different network zones, ensuring only authorized communication is allowed. Meanwhile, configuring NAT ensures that internal networks can securely interact with the external world, while also protecting internal resources from direct exposure.

For Firewall Policies, it is essential to align policies with security needs, ensure traffic flows are correctly filtered, and maintain strict control over which traffic is allowed to pass through the firewall. Similarly, for NAT, leveraging the appropriate types such as Source NAT (SNAT) and Destination NAT (DNAT) helps conserve IP addresses and direct traffic efficiently between internal and external networks.

By following the steps outlined in the configurations, and adhering to best practices, you ensure a robust and secure network environment. Always remember to test configurations thoroughly and review them periodically to maintain an optimized and secure network.