Implementing U-turn NAT in Palo Alto Networks Firewalls: Resolving VPN Access Issues Due to IP Address Overlap

Shyamlal
Parul Institute of Technology, Parul
University, Vadodara, India
shyamaggarwal59@gmail.om

Abstract—This paper discusses the application of U-turn NAT in Palo Alto Networks firewalls, which would remedy access-related issues for VPN users trying to connect with DMZ servers that have overlapping IP addresses. It provides a practical way of dealing with a widespread networking problem in which source IPs from remote user's conflict with internal server addresses, causing connection failures

Keywords— U-Turn NAT, Palo Alto Networks, VPN, DMZ, IP Address Conflict, Network Security, Enterprise Networking

I. Introduction

As a standard part of corporate networks, virtual private networks (VPNs) are used for secure remote access to internal resources. As a result, there is considerable concern regarding conflicting situations where VPN users cannot access DMZ servers due to IP conflicts between the user's local network and the organization's internal server infrastructure. Such situations usually arise in case:

- Remote users have local networks using common private IP ranges.
- These IP ranges overlap with the organization's DMZ server addresses.

This researches the implementation of U-turn Network Address Translation (NAT) on the Palo Alto Networks firewall as one truly global solution to resolve the conflicts while striking an optimal balance between defensive security posture and network performance. U-turn NAT is emerging as an adequately strong medium for providing address translations in both directions, thus assuring prompt delivery of DMZ resources regardless of conflicts in the addressing format. [1].

II. Technical Analysis

2.1 Typical Scenario

Assume a case like this.

- VPN User Home Network: 192.168.1.0/24
- DMZ Server IP: 192.168.1.100
- VPN Pool: 10.10.0.0/24

In this case, access is failing when the VPN user tries to access the DMZ server, in return traffic, for the following reasons:

- The server sees the source as 192.168.1.x (the user's real IP)
- The server tries to respond to 192.168.1.x
- Return traffic never reaches the VPN user due to routing mix-up.

2.2 Solution Architecture

The U-turn NAT solution will keep the following features:

- It translates the source IP address of VPN users into an exclusive address space.
- It routes the return traffic through the firewall.
- However, the solution also applies NAT policies in both directions

III. Related Work

3.1 Several methods have been proposed to address overlapping IP addresses and VPN connectivity related problems.

- **IP Address Re-numbering**: One typical solution is to renumber either the home network of the client or the DMZ server network [2,5]. This measure, while very effective, is disruptive and requires time because it involves reconfiguration of many devices. This will not be permissible also in case IP addresses are inadequate in an environment.

- **Split tunneling with specific routes**: Split tunneling can be set up for directing DMZ servers' traffic through an open tunnel into the VPN [3]. This configuration would require some careful configuration of routing policies and can be rather elaborate under a huge network. In addition, this may not solve the case if a client attempts to access the server by using a public IP address.

- **DNS resolution manipulation**: Another form of circumvention involves having the DNS point to the server public IP from the internal clients regarding its private IP for purposes of routing [4]. This is in consideration of the possibility that managing the internal DNS servers would be an issue for most applications.

- **Policy-Based Routing**: Another suggested the use of Policy-Based Routing in resolving the conflicts. But their scheme works only for simple scenarios and does not scale well with multiple VPN user groups.[6]

- **NAT64 and Overlapping IPv4 with IPv6 Islands**: It is implemented in those where IPv6 is being installed along with existing networks of IPv4, where NAT64 ensures communications between hosts having IPv6 only and hosts having IPv4 only [7]. Although NAT64 configurations are complicated by the presence of overlapping IPv4 addresses, this requires a fair amount of address planning and formulation of translation policies. While this does not deal directly with overlay VPNs, it gives the wider landscape for so many NAT issues.

- **Zero Trust Network Access (ZTNA) and Overlapping IPs**: Architectures of ZTNA emphasize the capability of granting secure access to applications and resources based on user identity and device posture [8]. ZTNA solutions could use NAT or other kinds of address translation to solve overlapping IP address ranges. The integration of ZTNA with NAT solutions is a fast-expanding domain for research.

3.2 Identification of Shortcomings:

The solution as pointed out can be cumbersome with heavy setup, cause disruption, or may not apply in very limited circumstances. The need for a more straightforward and flexible approach, like U-Turn NAT for Palo Alto firewalls, was made evident here because it would avoid much of the configuration complexity and parameter changes of IP address renumbering.

3.3 Why Our Work is Better:

- Our scheme extends upon these previous ways but in a way to counter their shortcomings which include:
- Providing seamless bidirectional translation without any service interruption

- Enforcing a consistent security policy across all traffic
- Reduced configuration complexity through automated generation of rules
- Enterprise-wide scaling, but without compromising performance
- Complete elimination of service downtime or infrastructure changes.

IV. METHODOLOGY:

4.1 Block Diagram & Explationation

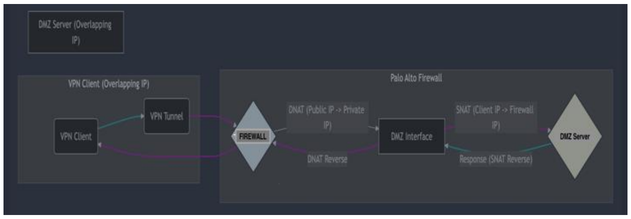

DMZ Server (Overlapping IP)
VPN Client (Overlapping IP)
VPN Client
VPN Tunnel
Palo Alto Firewall
FIREWALL
DNAT (Public IP -> Private IP)
DMZ Interface
SNAT (Client IP -> Firewall IP)
DMZ Server
DNAT Reverse
Response (SNAT Reverse)

Figure 1. U-Turn NAT Resolving IP Overlap

Explanation for the amended diagram and U-Turn NAT:

- **VPN Client**: The client connects through the tunnel.

- **Palo Alto Firewall (VPN Interface):** The traffic reaches the firewall on the VPN interface.

- **Combined DNAT and SNAT:** This is the important point. The firewall does DNAT from public IP to server's private IP and does SNAT from client's overlapping IP to firewall's own IP (more specifically, an IP address on the interface connected to DMZ). These operations are effectively being done in conjunction.

- **Firewall (DMZ Interface- Internal):** Within the diagram, this "node" does not relate to a separate physical interface. It is rather a logical representation of the firewall processing the traffic from a DMZ interface perspective while never truly leaving the firewall. The traffic is routed internally to the DMZ server.

- **DMZ Server:** The server will receive the traffic a "believing" it's coming from the firewall itself (thanks to the SNAT).

- **Reverse NATs:** The response from the server moves back to the firewall. Firewall implements the reverse NAT from SNAT to DNAT-back to revert to the original IP addresses.

- **Back to Client:** The response is sent back to the VPN client.

4.2 Algorithm

1. The client establishes a VPN connection to the DMZ server using its public IP address.

2. The traffic arrives at the Palo Alto firewall over the VPN tunnel

3. The Firewall checks the destination IP address, which matches the DMZ Server's public IP address.

4. Then, the Firewall verifies the source IP. It detects that the source IP belongs to the overlapping client's IP range.

5. The Firewall has U-Turn NAT:

   a) Destination NAT (DNAT): The Firewall translates the DMZ Server's public IP destination address into the private address of DMZ Server.
   b) Source NAT (SNAT): The Firewall translates the source IP address (the overlapping address for the VPN Client) to the firewall's IP on the DMZ network

6. The Firewall considers this traffic as forwarded to DMZ Server (Logical).

7. It is received by the DMZ Server as from that Firewall.

8. And to the Firewall, the DMZ Server replies.

9. The Firewall makes reverse NAT operations:

   a) Reverse SNAT: The Firewall translates the source IP address (its own IP) back to the original overlapping IP address for VPN Client.
   b) Reverse DNAT: The Firewall translates the destination IP address (its own IP, as DMZ server replied to it) back to the DMZ Server's public IP address.

10. Firewall back to the response VPN Client through the VPN tunnel.

11. The VPN Client receives the response, appearing to have communicated directly with the DMZ server using its public IP.

V. IMPLEMENTATION

5.1 Scenario:

- VPN Client: **192.168.1.10 (IP overlaps with the DMZ server's internal range)**
- DMZ Server Public IP: **20.20.0.1 (IP VPN clients use)**
- DMZ Server Private IP: **192.168.1.100 (server's actual internal IP)**
- Firewall DMZ Interface IP: **192.168.1.1 (The firewall's IP on the DMZ network)**

5.2 Configuration Steps:

1) **Create Address object:** creating address objects for your DMZ server and the overlapping client IP range can make your configuration more readable and manageable.

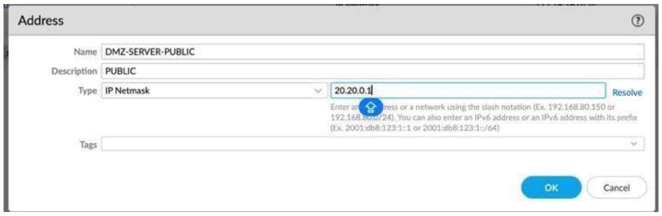

Address
Name: DMZ-SERVER-PUBLIC
Description: PUBLIC
Type: IP Netmask | 20.20.0.1
Enter an [illegible] ress or a network using the slash notation (Ex. 192.168.80.150 or 192.168.80.0/24). You can also enter an IPv6 address or an IPv6 address with its prefix (Ex. 2001:db8:123:1::1 or 2001:db8:123:1::/64)
Tags:

Figure 2. Create an address object for the DMZ server's public IP address

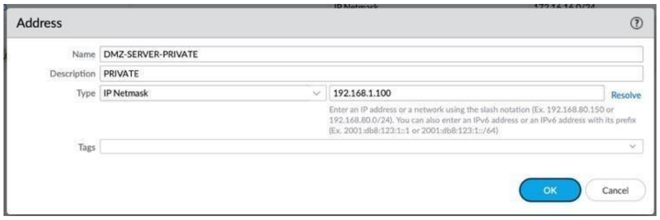

Address
Name: DMZ-SERVER-PRIVATE
Description: PRIVATE
Type: IP Netmask | 192.168.1.100
Enter an IP address or a network using the slash notation (Ex. 192.168.80.150 or 192.168.80.0/24). You can also enter an IPv6 address or an IPv6 address with its prefix (Ex. 2001:db8:123:1::1 or 2001:db8:123:1::/64)
Tags:

Figure 3. Create an address object for the DMZ server's private IP address

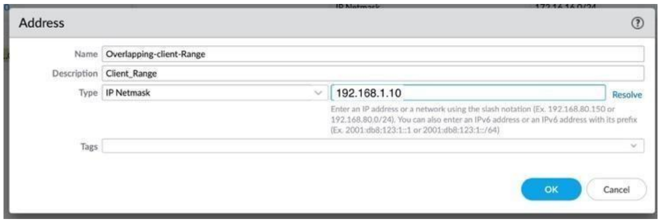

Address
Name: Overlapping-client-Range
Description: Client_Range
Type: IP Netmask | 192.168.1.10
Enter an IP address or a network using the slash notation (Ex. 192.168.80.150 or 192.168.80.0/24). You can also enter an IPv6 address or an IPv6 address with its prefix (Ex. 2001:db8:123:1::1 or 2001:db8:123:1::/64)
Tags:

Figure 4. Create an address object for the overlapping client IP range

2) **Configure Destination NAT (DNAT) Policy:** This policy translates the public IP address of the DMZ server to its private IP address when traffic originates from the overlapping IP range.

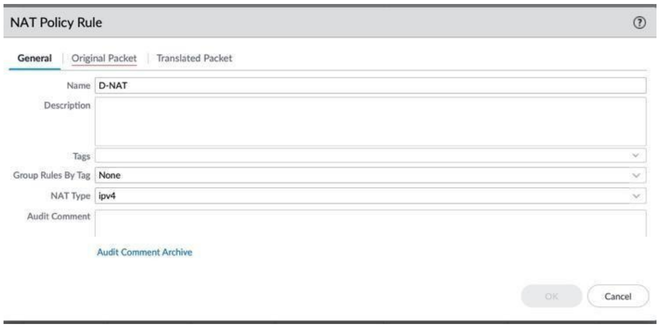

NAT Policy Rule
General | Original Packet | Translated Packet
Name: D-NAT
Description:
Tags:
Group Rules By Tag: None
NAT Type: ipv4
Audit Comment:

Figure 5. Create D-NAT Rule Name

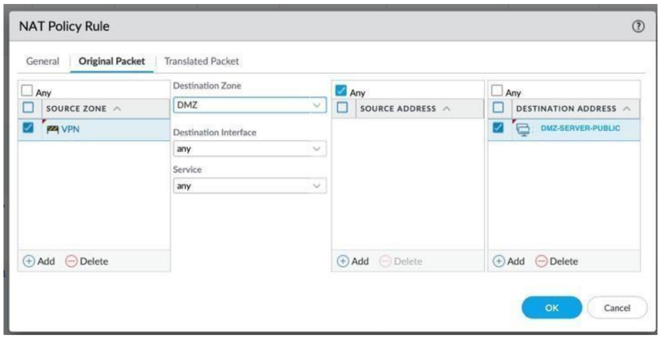

NAT Policy Rule
General | Original Packet | Translated Packet
□ Any
SOURCE ZONE
☑ VPN
Destination Zone: DMZ
Destination Interface: any
Service: any
☑ Any
SOURCE ADDRESS
□ Any
DESTINATION ADDRESS
☑ DMZ-SERVER-PUBLIC

Figure 6. Configure Original packets D-NAT

- Source Zone -> VPN Zone
- Destination Zone -> DMZ Zone
- Destination Address -> DMZ-SERVER-PUBLIC (20.20.0.1)

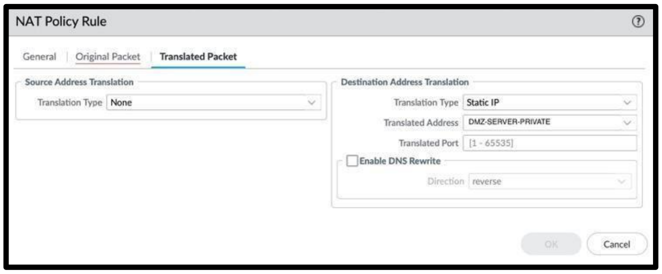

NAT Policy Rule
General | Original Packet | Translated Packet
Source Address Translation
Translation Type: None
Destination Address Translation
Translation Type: Static IP
Translated Address: DMZ-SERVER-PRIVATE
Translated Port: [1 - 65535]
□ Enable DNS Rewrite
Direction: reverse

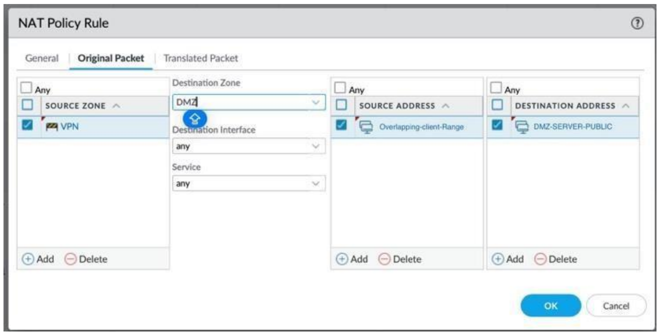
Figure 7. Configure Destination Address Translation

- Translation Packet – Destination Address Translation
- Translation Type –> Static IP
- Translation Address -> DMZ-SERVER-PRIVATE (192.168.1.100)

3) **Configure Source NAT (SNAT) Policy:** In *most* cases, we won't need a separate SNAT rule for U-Turn NAT. The DNAT rule often handles the necessary source NAT implicitly. However, in some more complex scenarios (e.g., if you have different routing tables or require more fine-grained control), we might need a separate SNAT rule. If we do need it:

➔ Create S-NAT RULE NAME
(Same as D-NAT Example)

➔ Configure Original Packet


NAT Policy Rule

General | Original Packet | Translated Packet

☐ Any	Destination Zone	☐ Any	☐ Any
☐ SOURCE ZONE	DMZ	☐ SOURCE ADDRESS	☐ DESTINATION ADDRESS
☑ VPN	Destination Interface: any Service: any	☑ Overlapping-client-Range	☑ DMZ-SERVER-PUBLIC

Figure 8. Configure Original packets of S-NAT

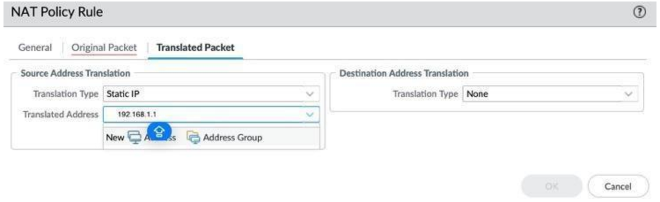
- Source Zone -> VPN Zone
- Destination Zone -> DMZ Zone
- Source Address -> Overlapping-client-Range

(192.168.1.10)

- Destination Address-> DMZ-SERVER-PUBLIC

(20.20.0.1)

→ Configure Translate Packets


NAT Policy Rule

General | Original Packet | Translated Packet

Source Address Translation
Translation Type: Static IP
Translated Address: 192.168.1.1

Destination Address Translation
Translation Type: None

Figure 9. Configure Source Address Translation

- Translated Packets -> Source Address Translation
- Translation Type -> Static IP
- Translated Address -> 192.168.1.1 (The firewall's IP on the DMZ network)

VI RESULTS

U-Turn NAT implementation on the Palo Alto Networks firewall turned out to be one of the most practical solutions for resolving VPN access issues arising due to overlapping IP address ranges between remote clients and DMZ servers.

After the configuration of U-Turn NAT policies, connectivity improved dramatically. VPN clients residing within the overlapping IP ranges were able to seamlessly connect to the DMZ server via its public IP address without experiencing any routing conflicts or connectivity errors.

VII CONCLUSION

The Implementation of U-Turn NAT on Palo Alto Networks firewalls provides organizations with a valuable solution when their VPN accesses fail, as a result of overlapping IP address ranges. This approach offers a practical, efficient, and user-friendly method for ensuring seamless remote access to critical network resources, ultimately contributing to improved productivity and service availability. The observed results strongly support the continued use of U-Turn NAT as a standard practice in network administration, particularly in environments where IP address overlaps are unavoidable or difficult to resolve through other means.

VIII FUTURE WORK

- Automation of U-Turn NAT configuration based on dynamic VPN IP address assignments.
- Integration with network monitoring tools will facilitate the tracking and reporting of U-Turn NAT usage.
- Checking the impact of U-Turn NAT on high-traffic networks.
- Investigating other Firewall vendors and compare the implementation of U-turn NAT

IX REFERENCES

[1] *Palo Alto Networks. (2024). "PAN-OS Administrator's Guide: NAT Configuration."*

[2] *Tanenbaum, A. S., & Wetherall, D. J. (2011).* Computer networks. *Pearson Education.*

[3] Kurose, J. F., & Ross, K. W. (2016). *Computer networking: A top-down approach*. Pearson.

[4] *Liu, J., & Nahrstedt, K. (2003). Providing end-to-end quality of service guarantees using differentiated services and dynamic packet state.* Proceedings 11th IEEE International Conference on Network Protocols (ICNP 2003), *128-137.*

[5] *Cisco Systems. (n.d.).* Configuring NAT. *Retrieved from Cisco Documentation. (Example of vendor documentation outlining NAT implementations, highlighting the complexities of IP renumbering alternatives)*

[6] *Zhang, H., et al., "Policy-Based Routing for VPN Access Control," International Conference on Network Security, 2022*

[7] *Boreham, M., & Wing, D. (2011).* Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers. *RFC 6146.*

[8] *Rose, S., Borchert, O., Mitchell, S., & Connolly, S. (2020).* Zero Trust Architecture. *NIST Special Publication 800-207*