Palo Alto Policy

When Do You Need NAT?

You only need NAT if your networks require address translation to communicate properly. This typically happens in scenarios like: ✅ Internet Access (Outbound NAT) → If internal devices need to reach the internet using a public IP.
✅ Inbound NAT (Port Forwarding) → If external devices need access to internal services.
✅ Overlapping Subnets → If two networks use the same subnet and require translation to avoid conflicts.
✅ Different Security Zones Without Direct Routing → If traffic between zones needs NAT due to firewall policies.

Do You Need NAT in Your Setup?

Traffic Flow	Directly Routable?	Needs NAT?
Site A (10.1.0.0/24) → Site B (10.2.0.0/24)	✅ Routed via VPN	❌ No NAT
VLAN 20 (10.2.20.0/24) → VLAN 100 (10.2.100.0/24)	✅ Routed via Palo Alto	❌ No NAT
Site B → Internet (Outbound)	❌ Needs public IP	✅ Yes (Outbound NAT)
Internet → DMZ (Inbound from public services)	❌ Needs public IP translation	✅ Yes (Inbound NAT)

When You Don't Need NAT

- **Internal VLANs (20, 100) communicate directly via routing → No NAT needed.**
- **Site A and Site B communicate via IPSec VPN → No NAT needed.**
- **Devices in Site B already have direct routing between VLANs → No NAT needed.**

NAT is NOT Needed for Directly Routed Networks

- **Your Splunk components (Search Heads, Indexers, Heavy Forwarder, etc.) are on directly routable subnets (VLAN 20 and VLAN 100).**
- **Since these VLANs are already connected via routing and security policies on your Palo Alto firewall, NAT is unnecessary.**
- **If they can already ping and exchange data, NAT will actually break things by modifying the source IPs.**

When Would NAT Be Needed for Splunk?

The only cases where NAT would be needed for Splunk communication are:

1. **If Splunk instances are on overlapping subnets**
   - **Example: If Site A had `10.2.20.0/24` as well, then NAT would be needed to avoid IP conflicts.**
   - ✅ **NOT your case.**
2. **If Splunk instances were trying to communicate across the internet**
   - **If an external Splunk instance (outside your network) needed access, you'd need NAT.**
   - ✅ **NOT your case.**
3. **If firewall rules were misconfigured, forcing NAT to "fix" them**
   - **If the firewall was accidentally blocking communication, NAT might be suggested as a workaround.**
   - ✅ **You already have firewall rules allowing Splunk communication, so this is NOT necessary.**

Scenario	Needs NAT?	Why?
Internal VLANs (100 ↔ 20) communicating	❌ No	Firewall routes traffic naturally.
VLANs talking to the internet	✅ Yes	Outbound NAT required.
Overlapping subnets (e.g., two 10.2.20.0/24 networks)	✅ Yes	To avoid conflicts.
External access to DMZ services (e.g., Security Onion Web UI from the internet)	✅ Yes	Inbound NAT required.

Communication List (Splunk & Security Onion)

Source	Destination	Purpose	Port
Heavy Forwarder (VLAN 100 - DMZ)	Indexers (VLAN 20 - Tools)	Log Forwarding	9997 (TCP)
Indexers (VLAN 20 - Tools)	Cluster Manager (VLAN 20 - Tools)	Cluster Coordination	8089 (TCP)
Indexers (VLAN 20 - Tools)	Other Indexers (VLAN 20 - Tools)	Data Replication	9887 (TCP)
Search Heads (VLAN 20 - Tools)	Indexers (VLAN 20 - Tools)	Search Queries	8089 (TCP)
Search Heads (VLAN 20 - Tools)	Deployer (VLAN 20 - Tools)	Config Management	8089 (TCP)
User Workstations (VLAN 20 - Tools / Site A - Users)	Search Heads (VLAN 20 - Tools)	Splunk Web UI Access	8000 (TCP)
Security Onion Heavy Nodes (VLAN 100 - DMZ)	Security Onion Search Head Manager (VLAN 20 - Tools)	Log forwarding & search queries	9200 (TCP), 5601 (TCP)
Security Onion Heavy Nodes (VLAN 100 - DMZ)	Splunk Heavy Forwarder (VLAN 100 - DMZ)	Log forwarding to Splunk	9997 (TCP)
Security Onion Search Head Manager (VLAN 20 - Tools)	Security Onion Heavy Nodes (VLAN 100 - DMZ)	Querying & data retrieval	443 (TCP), 22 (TCP - SSH Admin Access)
User Workstations (VLAN 20 - Tools / Site A - Users)	Security Onion Search Head Manager (VLAN 20 - Tools)	Web access to Kibana	443 (TCP)

🔷 Splunk Security Policies

Source Zone	Destination Zone	Source IP	Destination IP	Purpose	Port
DMZ (ethernet1/4 - 10.2.100.1)	Interior (ethernet1/3 - 10.2.20.1)	Splunk Heavy Forwarder	Splunk Indexers	Splunk Data Transfer	9997 (TCP)
Interior (ethernet1/3 - 10.2.20.1)	Interior (ethernet1/3 - 10.2.20.1)	Splunk Indexers	Splunk Indexers	Index Replicatio n	9887 (TCP)
Interior (ethernet1/3 - 10.2.20.1)	Interior (ethernet1/3 - 10.2.20.1)	Splunk Search Heads	Splunk Indexers	Search Queries	8089 (TCP)
Interior (ethernet1/3 - 10.2.20.1)	Interior (ethernet1/3 - 10.2.20.1)	Splunk Search Heads	Splunk Deployer	Config Sync	8089 (TCP)
Interior (Site A - ethernet1/2 - 10.1.0.0/24)	Interior (Site B - ethernet1/3 - 10.2.20.1)	Any	Splunk Search Heads	Splunk Web UI Access	8000 (TCP)

🔷 Security Onion (SecO) Security Policies

Source Zone	Destination Zone	Source IP	Destination IP	Purpose	Port
DMZ (ethernet1/4 - 10.2.100.1)	Interior (ethernet1/3 - 10.2.20.1)	Security Onion Heavy Nodes	Security Onion Search Head Manager	Log Forwardin g	9200 (TCP), 5601 (TCP)
DMZ (ethernet1/4 - 10.2.100.1)	DMZ (ethernet1/4 - 10.2.100.1)	Security Onion Heavy Nodes	Splunk Heavy Forwarder	Log Forwardin g to Splunk	9997 (TCP)
Interior (ethernet1/3 - 10.2.20.1)	DMZ (ethernet1/4 - 10.2.100.1)	Security Onion Search Head Manager	Security Onion Heavy Nodes	Querying & Admin	443 (TCP), 22 (TCP - SSH Access)
Interior (Site A - ethernet1/2 - 10.1.0.0/24)	Interior (Site B - ethernet1/3 - 10.2.20.1)	Any	Security Onion Search Head Manager	Kibana Web UI Access	443 (TCP)

BL24 Basic Routing Table

Destination Network	Next Hop	Interface	Purpose
10.2.20.0/24 (Tools)	Directly Connected	ethernet1/3	Ensures local VLAN 20 traffic reaches the firewall
10.2.100.0/24 (DMZ)	Directly Connected	ethernet1/4	Ensures local VLAN 100 traffic reaches the firewall
10.1.0.0/24 (504 Network)	VPN Tunnel Interface	tunnel.1	Routes traffic from Site B to Site A over IPSec VPN
0.0.0.0/0 (Internet)	ISP Gateway (137.0.0.X)	ethernet1/2 (WAN)	Allows external internet access