

SECURITY | REV 2.0 | REVIEWED 2026-10-10

NAT, zones & session troubleshooting

01 / Quick reference and concepts

Track the original and translated tuples and avoid the common destination-NAT address-versus-zone mistake.

PAN-OS 11.2 policy concepts and IOS XE inspection examples. Juniper SRX flow/NAT is outside the EX/MX command scope of this library.



Document both tuples and zones. A NAT translation changes addressing; it does not by itself authorize the application.

Item	Record	Why it matters
Original flow	Source / destination / ports	Rule match and original identity
Translated flow	Source / destination / ports	Server and return-path observations
NAT rule	Ordered first matching rule	Shadowed rules may never apply
Security rule	Addresses plus effective zones	Permission is a separate decision
Return path	Route back to translated source	Asymmetry can bypass session state

What to understand first

- Source NAT changes the source identity; destination NAT changes the destination. Port translation can change the transport tuple as well. Write the protocol and both ports, not just an IP pair.
- For PAN-OS destination NAT, NAT-rule destination-zone matching follows the original destination route lookup. Security policy uses original addresses with post-NAT zones.
- A first-match ordered NAT policy can select an unexpected earlier rule. Examine the actual session and applied translation instead of relying only on configuration intent.
- Existing sessions, policy-based forwarding and routing context can affect observations. A new controlled attempt gives clearer evidence after a reviewed change.

SECURITY | REV 2.0 | REVIEWED 2026-10-10

NAT, zones & session troubleshooting

02 / Commands and worked example

Replace documentation addresses, example interfaces and every <PLACEHOLDER>. Check command help for your model/release and routing context. Examples are documentation-reviewed, not executed on customer equipment.

PAN-OS

Read-only operational

```
show session all filter source 198.51.100.10 destination 203.0.113.20
show session id <SESSION_ID>
```

Inspect: Read original and translated flows, rule, zones, application and byte counters; select the correct vsys.

Cisco IOS XE

Read-only EXEC

```
show ip nat translations
show ip nat statistics
show ip route 192.0.2.20
```

Inspect: Compare translation entries and counters with intended interfaces and the server route. NAT feature support varies.

Illustrative inbound destination NAT

Illustrative teaching example, not captured device output.

```
Original:  198.51.100.10 -> 203.0.113.20:443
Translated: 198.51.100.10 -> 192.0.2.20:443
Original destination zone: untrust
Server destination zone:  dmz
```

- In this simplified PAN-OS example, the NAT rule matches the original destination route zone; the security rule targets dmz with the original destination address.
- Server replies must follow a path that permits the firewall to apply the session translation. The documentation addresses are not deployment values.

SECURITY | REV 2.0 | REVIEWED 2026-10-10

NAT, zones & session troubleshooting

03 / Troubleshooting and acceptance

1. Capture the original tuple, time and ingress zone of one failing attempt.
2. Identify the first matching NAT rule and inspect the resulting session translation.
3. Check security policy with original addresses and the effective destination zone.
4. Verify server reachability and return routing for the translated source.
5. Compare both flow directions and new-session logs after the approved correction.

Common mistakes

- Assuming NAT implies an allow rule.
- Using the private server address where a PAN-OS security rule requires the original destination.
- Clearing all production sessions to test a single changed flow.

Acceptance checks

- The intended rule and translation match a fresh session.
- Forward and reverse counters move for the real application.
- Adjacent applications and intended denies remain correct.

Primary references

[PAN-OS destination NAT example](#)[PAN-OS NAT rules](#)[PAN-OS session interpretation](#)[Cisco IOS XE NAT monitoring](#)

Original Wolex diagrams, scenarios and troubleshooting sequences. Vendor names identify platform scope; no affiliation is implied.

[Read the full web guide and supporting references](#)[Deployment and migration help](#) | [Network security review from Wolex](#)