Intermittent Traffic Disruptions Caused by IP SLA and Tracked Static Route Transitions on ASA/FTD

Contents

Issue

Network traffic can intermittently freeze, disconnect, or experience latency when an ASA/FTD tracked static route changes state because an IP SLA monitor skips probe operations and temporarily marks the preferred path as unavailable.

Environment

- Any Firepower hardware running ASA or FTD
- ASA software versions tested: 9.20(4)10 and 9.20(4)34
- Static routes configured with 'track' objects.
- IP SLA ICMP echo probes configured with:
- No. of packets = 3 probes per operation.
- Frequency = 5 second.
- Timeout = 5 second (Default - not modified by user)
- A backup route configured with a higher administrative distance
- Any application or network traffic using the tracked route

Resolution

Increase the IP SLA Frequency

Use this option when path monitoring and automatic route failover are required.
Configure the operation frequency to be greater than the operation timeout. For example, retain the default five-second timeout and increase the frequency to 10 seconds:

<#root>

```
configure terminal
sla monitor <sla-id>

 frequency 10


exit
write memory
```

Apply the same adjustment to any other SLA operation using the same timing pattern.

Note: Before making changes, confirm that the resulting failure-detection interval meets the network design requirements.

Verification

1. Confirm that the route remains stable. Verify that the operation frequency is greater than the timeout.

```
show route <destination>
```

2. Confirm the IP SLA configuration:

```
show sla monitor configuration
```

3. Review the IP SLA operational state:

```
show sla monitor operational-state
```

Check for:

- An **Operational state**: Active status.
- No continuing increase in **skipped** operations.

4. Check the track state:

```
show track <track-id>
```

The track must remain Up while the monitored gateway is reachable.

5. Test the affected traffic and applications, including:

- New connections.
- Existing sessions.
- TCP and UDP traffic, as applicable.
- Traffic to destinations using the monitored route.
- Applications that are sensitive to route changes or brief interruptions.

6. Monitor the environment during normal operation. Confirm that the preferred route does not repeatedly withdraw and reappear.

If the issue recurs, collect this data while the problem is active:

```
show sla monitor configuration
show sla monitor operational-state
show track
show route
show asp drop
show tech-support
```

Also collect packet captures for the IP SLA probes and the affected traffic.

Cause

The IP SLA operation frequency and timeout were both configured for five seconds. Under some conditions, the IP SLA scheduler considered the previous operation active when the next operation was scheduled.

Evidence included:

- A high number of skipped IP SLA operations.
- Packet captures showing successful probe replies, but approximately 10 second gaps between probe groups instead of the configured 5 second interval.
- No evidence of interface congestion, interface-buffer drops, or appliance resource exhaustion.
- Route changes occurring when the track object transitioned between Up and Down.

When the preferred track object transitioned to Down, the associated static route was withdrawn and traffic moved to the higher-distance route. When the track returned to Up, the preferred route was reinstalled. These route changes disrupted active traffic flows and could cause application timeouts, latency, freezes, or session disconnections.

The issue continued after reverting the ASA software, so the available evidence did not establish a software-version-specific regression.

Related Content

- Configure Static Route Tracking
- Configure ISP Failover with Default Routes Using IP SLA Tracking