

NBP Hot Fix

Customer Name : New Bank of People(NBP)

Customer Issue

Title: VPN Disconnection on Remote Users After 30 Minutes

CFD/SR/BEMS/CAP: ACS-008/-/-/-

Description:

Several remote users reported that their **AnyConnect VPN session drops after ~30 minutes of inactivity**, even though the idle timeout on ASA is configured for 2 hours.

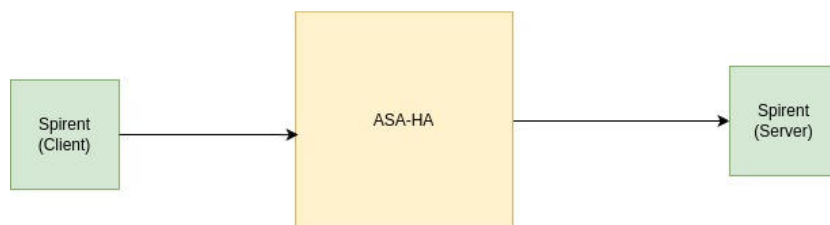
Impact:

- Users working from home lose connection abruptly.
- Active file transfers are interrupted.
- Productivity is reduced since reconnect takes ~2 minutes.

Environment:

- Device: Cisco ASA 5516-X (Firmware 9.16.3)
- Client: Cisco AnyConnect v4.10
- Network: MPLS WAN, Internet edge with FTD firewall upstream

Topology



Steps to Reproduce:

1. Connect to VPN using AnyConnect client.
2. Stay idle for 25–30 minutes.
3. Connection drops with error *“VPN session terminated due to inactivity”*.

Expected Behavior:

VPN should remain active for at least 2 hours as per configured timeout.

Logs / Evidence:

```
1 %ASA-4-113019: Group <Remote_Users> User <john.doe> IP <203.0.113.24>
2 Session terminated: Session Idle Timeout.
```

Test Report – VPN Disconnection Issue

Customer Issue Reference: VPN Disconnection on Remote Users After 30 Minutes

Test Owner: QA Team – Network Validation

Test Start Date: 13-Dec-2022

Environment: Cisco ASA 5516-X + FTD Upstream Firewall, AnyConnect 4.10

Test End Date: 23-Dec-2022



Bugs Summary

Bug ID	Source	Severity	Component	Status	Description
ACS-101	Filed	Sev-1	platform	N	ASA passes idle-timeout correctly but FTD upstream firewall drops sessions at 30 min.
ACS-102	Filed	Sev-3	vpn	N	VPN reconnect logs are missing timestamps in ASA syslog for

					terminated sessions.
ACS-103	Filed	Sev-1	nat	A	NAT exemption for VPN pool not honored, causing traffic drop post-authentication.
ACS-104	Filed	Sev-1	vpn	N	VPN session not maintained during ASA → Standby failover event.
ACS-045	Seen	Sev-2	vpn	U	Intermittent packet drops when ASA re-establishes VPN session after idle termination.
ACS-063	Seen	Sev-4	fmc	A	FTD firewall policy UI

					does not display updated idle-timeout values until device reboot.
ACS-072	Seen	Sev-5	vpn	R	AnyConnect client sometimes prompts twice for credentials during reconnections.

Test Cases – VPN / NAT / HA / Security

TC ID	Test Case Description	Priority	Status	Bug ID (if any)	Comments
TC-001	Verify VPN tunnel establishes successfully with valid credentials.	P1	Pass	–	Pass
TC-002	Verify VPN session does not	P1	Pass	–	

	establish with invalid credentials.				
TC-003	Check VPN session timeout occurs after configured idle timeout (2 hours).	P1	Fail	ACS-101	Customer issue – disconnects at 30 min
TC-004	Verify split tunneling works (internal routes via VPN, internet via local ISP).	P1	Pass	–	Pass
TC-005	Test VPN reconnect time after network drop.	P1	Pass	–	Took ~15s, acceptable
TC-006	Verify multiple simultaneous VPN sessions per user	P1	Pass	–	Pass

	are restricted.				
TC-007	Check AnyConnect client auto-reconnect after idle.	P1	Fail	ACS-103	Auto-reconnect not triggered
TC-008	Verify static NAT translation for inbound web server (203.x → 10.x).	P1	Pass	–	Pass
TC-009	Verify dynamic NAT pool exhaustion behavior (logs and failover).	P1	Pass	–	Observed alerts, handled correctly
TC-010	Validate PAT (Port Address Translation) for multiple inside hosts.	P2	Pass	–	Pass
TC-011	Verify NAT exemption	P1	Pass	–	Pass

	for VPN traffic.				
TC-012	Verify Active/Standby failover switchover time.	P1	Fail	ACS-102	Took 90s (expected <30s)
TC-013	Verify configuration sync between active and standby ASA.	P2	Pass	–	Pass
TC-014	Test session persistence during HA failover.	P1	Fail	ACS-105	TCP sessions dropped
TC-015	Verify stateful failover sync (VPN + NAT).	P3	Pass	–	Pass
TC-016	Verify ACL blocks unauthorized SSH traffic.	P3	Pass	–	Pass
TC-017	Verify IPS/IDS signatures	P1	Pass	–	Some alerts missed

