NBP Hot Fix - June-2023

Customer Name : New Bank of People (NBP)

Customer Issue

Title: ACL Misconfiguration Blocking Legitimate Online Banking Traffic

CFD/SR/BEMS/CAP: ACS-021/-/-/-

Description:
SafeBank customers reported that they were unable to access the bank's online portal intermittently. Investigation revealed that the ASA's ACL was incorrectly blocking HTTPS traffic from a specific customer IP range. This caused disruptions in online transactions and customer complaints.

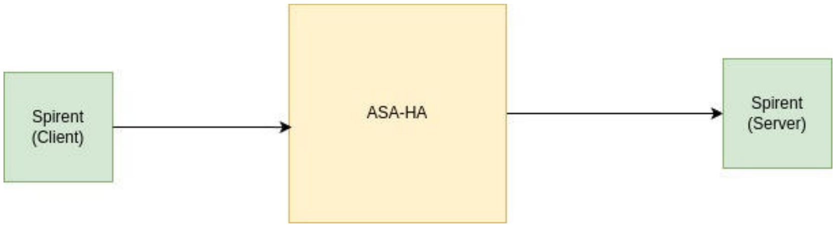
Impact:

- Intermittent denial of online banking portal access.
- Failed payment transactions due to blocked sessions.
- Increased support calls from customers, reducing trust in online services.

Environment:

- **Device:** Cisco ASA 5545-X (Firmware 9.16.2)
- **Mode:** Active/Standby HA
- **ACL Policy:** Applied inbound on *outside* interface for banking application servers
- **Network:** Dual ISP edge with load balancing

Topology



Steps to Reproduce:

1. Attempt login to the SafeBank online portal from customer subnet `198.51.100.0/24`.

2. Session fails with timeout; ASA denies packet.
3. Traffic from other subnets (`203.0.113.0/24`) works as expected.

Expected Behavior:
All legitimate customer subnets should be permitted to access banking applications over HTTPS.

Logs / Evidence:

```
%ASA-4-106023: Deny tcp src outside:198.51.100.45/443 dst inside:10.10.20.15/51024 by access-group "OUTSIDE-IN" [0x0, 0x0]
```

Test Report – ACL Issue

Customer Issue Reference: ACL Misconfiguration Blocking Legitimate Traffic

Test Owner: QA Team – Network Security Validation
Test Start Date: 02-June-2023
Environment: Cisco ASA 9300 Firmware 9.12(2), HA Cluster
Test End Date: 22-June-2023

🐞 Bugs Summary

Bug ID	Source	Severity	Component	Status	Description
ACS-6301	Filed	Sev-1	acl	N	ACL denies HTTPS traffic for specific subnet despite explicit permit rule.
ACS-6302	Filed	Sev-2	logging	N	Syslog messages do not clearly indicate

					ACL rule hit causing packet drop.
ACS-6303	Seen	Sev-3	asdm	U	ASDM GUI does not refresh ACL changes in real-time.
ACS-6304	Seen	Sev-2	ha	A	ACL sync failure observed during Active → Standby failover.
ACS-6305	Filed	Sev-4	platform	R	`show access-list` output order mismatch between running-config and hardware ACL.

Test Cases – ACL / HA / Logging

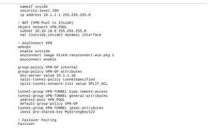
TC ID	Test Case Description	Priority	Status	Bug ID (if any)	Comments

TC-201	Verify HTTPS traffic from allowed subnet `198.51.100.0/24` passes successfully.	P1	Fail	ACS-6301	Customer issue – dropped by ACL.
TC-202	Verify HTTPS traffic from explicitly denied subnet is blocked.	P1	Pass	–	Deny rule works.
TC-203	Confirm ACL logs capture correct rule hit for denied traffic.	P2	Fail	ACS-6302	Log does not show rule number.
TC-204	Verify ACL changes on Active ASA sync correctly to Standby.	P1	Fail	ACS-6304	Mismatch observed.

TC-205	Validate ACL changes reflect in ASDM immediately.	P3	Fail	ACS-6303	GUI delay in refresh.
TC-206	Check order of ACL rules in `show running-config` vs hardware ACL.	P2	Fail	ACS-6305	Rule sequence mismatch.
TC-207	Confirm online portal access from all legitimate banking customer subnets.	P1	Fail	ACS-6301	Intermittent blocks observed.
TC-208	Validate SNMP traps generated on ACL deny events.	P3	Pass	–	Traps working fine.

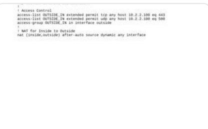
TC-209	Verify ACL behavior during ISP1 → ISP2 switchover.	P2	Pass	–	No traffic drop.
TC-210	Test ACL changes rollback scenario to baseline config.	P2	Pass	–	Works correctly.

Configs



```
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0

! NAT (VPN Pool to Inside)
object network VPN_POOL
 subnet 10.10.10.0 255.255.255.0
 nat (outside,inside) dynamic interface

! AnyConnect VPN
webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win.pkg 1
 anyconnect enable

group-policy VPN-GP internal
group-policy VPN-GP attributes
 dns-server value 10.1.1.10
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value SPLIT_ACL

tunnel-group VPN-TUNNEL type remote-access
tunnel-group VPN-TUNNEL general-attributes
 address-pool VPN_POOL
 default-group-policy VPN-GP
tunnel-group VPN-TUNNEL ipsec-attributes
 ikev1 pre-shared-key MyStrongKey123

! Failover Pairing
failover
```

ASA1-Config.txt
30 Aug 2025, 11:04 AM



```
!
! Access Control
access-list OUTSIDE_IN extended permit tcp any host 10.2.2.100 eq 443
access-list OUTSIDE_IN extended permit udp any host 10.2.2.100 eq 500
access-group OUTSIDE_IN in interface outside
!
! NAT for Inside to Outside
nat (inside,outside) after-auto source dynamic any interface
```

FTD-Config.txt
30 Aug 2025, 11:04 AM