WSA Upstream Proxy Health Check Issue After Network Disruption

Contents

Issue

After a prolonged network disruption, a Cisco Web Security Appliance (WSA) configured to use an upstream proxy specified by FQDN can fail to resume forwarding traffic to an upstream proxy and send traffic directly instead. This issue manifests when the WSA marks the upstream proxy as "dead" during the network outage, but fails to recognize when the upstream proxy becomes available again, even after network connectivity is restored.

The specific symptoms observed include:

- WSA configured with upstream proxy via FQDN and "Failure Handling = go Direct"
- Long-term network disruption affecting connectivity to both upstream proxy and the DNS server
- After network recovery, access logs show no DEFAULT_PARENT tags, indicating traffic continues to bypass the upstream proxy
- Issue occurs on one WSA appliance while another in the same environment operates normally

Environment

- Cisco Web Security Appliance (WSA) S-Series
- AsyncOS 14.5.2-011 (affected version)
- Hardware: S695
- Upstream Proxy Configured with FQDN Specification
- Failure Handling Configured as "go Direct"
- Network Environment with L2 Switch Infrastructure

Resolution

This issue is resolved by upgrading AsyncOS to a version that contains the fix for CSCwi13124. This bug has been fixed in these AsyncOS versions:

- AsyncOS 15.5.0-566
- AsyncOS 15.5.0-710

Temporary Workaround for Current Versions

For environments that cannot immediately upgrade, a temporary mitigation is available by adjusting the maximum idle timeout for checking unresponsive upstream proxies:

Step 1: Access the CLI and navigate to advanced proxy configuration:

```
cli -> advancedproxyconfig -> MISCELLANEOUS
```

Step 2: Modify the maximum idle timeout setting:

```
"Enter maximum idle timeout for checking unresponsive upstream proxy (in seconds)"
```

Step 3: Reduce the default maximum value (86400 seconds/24 hours) to a smaller value to decrease the time between health checks.

Immediate Recovery Method

If the issue is currently affecting traffic flow, the next command can immediately restore upstream proxy functionality:

Step 1: Access the diagnostic menu:

```
CLI > diagnostic > PROXY > kick
```

This restarts the proxy process and restores normal upstream proxy operations.

Validation and Testing Procedure

To test whether the issue is present or has been resolved after an upgrade, review these steps:

Step 1: Establish Baseline Monitoring

Monitor access logs and proxy logs to confirm WSA is sending traffic to the upstream proxy. Verify that traffic is reaching the upstream proxy side.

Step 2: Simulate Network Disruption

After confirming normal traffic flow to the upstream proxy, disconnect these connections:

- WSA to upstream proxy connection
- WSA to DNS server connection

Step 3: Monitor Failure Detection

Check proxy logs and system logs for these indicators:

- Proxy log can show upstream proxy as "... declared dead"
- System log can show "Critical: Reached maximum failures querying DNS server ..."

Step 4: Maintain Disrupted State

Without restarting the proxy process, maintain the disconnected state from **Step 2** and continue generating requests for approximately 10 hours.

Step 5: Restore Connectivity

After approximately 10 hours, restore the connections that were disconnected in Step 2.

Step 6: Monitor Recovery Behavior

After completing **Step 5**, monitor access logs and proxy logs without restarting the proxy process:

- In a fixed system: Traffic resumes flowing through the upstream proxy, and proxy logs show normal health status transitions
- In an affected system: Access logs show traffic continuing to bypass the upstream proxy, and proxy logs will not show "... was sick, now healthy" or "... was healthy, now sick" messages

Cause

The root cause of this issue is a logic flaw in the upstream proxy health-check mechanism. When WSA determines a configured upstream proxy is "dead" (unresponsive), it implements an exponential backoff algorithm that doubles the health-check interval after each failure. This interval can reach a maximum of 24 hours (86400 seconds).

This issue occurs when the upstream proxy becomes available again during one of these extended intervals. Even though the proxy has recovered and is responding normally, WSA will not perform a health check until the full configured time interval has elapsed. This can result in up to 24 hours of continued direct traffic routing instead of resuming upstream proxy usage.

This behavior affects WSA configurations where:

- Upstream proxy is specified by DNS hostname/FQDN (not IP address)
- Failure Handling is set to "go Direct"
- Extended network disruptions affect both upstream proxy and DNS server connectivity

Cisco bug ID: CSCwi13124

Related Content

- Cisco Technical Support & Downloads