Statusüberprüfung des WSA-Upstream-Proxys nach Netzwerkunterbrechung

Inhalt

Problem

Nach einer längeren Netzwerkunterbrechung kann eine Cisco Web Security Appliance (WSA), die für die Verwendung eines durch FQDN angegebenen Upstream-Proxys konfiguriert ist, die Weiterleitung des Datenverkehrs an einen Upstream-Proxy nicht fortsetzen und den Datenverkehr stattdessen direkt senden. Dieses Problem tritt auf, wenn die WSA den Upstream-Proxy während des Netzwerkausfalls als "ausgefallen" markiert, jedoch nicht erkennt, wann der Upstream-Proxy wieder verfügbar ist, selbst wenn die Netzwerkverbindung wiederhergestellt ist.

Zu den beobachteten spezifischen Symptomen gehören:

- WSA mit Upstream-Proxy über FQDN und "Failure Handling = go Direct" konfiguriert
- Langfristige Netzwerkunterbrechung mit Auswirkungen auf die Verbindung zum Upstream-Proxy und zum DNS-Server
- Nach der Netzwerkwiederherstellung werden in den Zugriffsprotokollen keine DEFAULT_PARENT-Tags angezeigt, was darauf hinweist, dass der Datenverkehr weiterhin den Upstreamproxy umgeht
- Das Problem tritt auf einer WSA-Appliance auf, während eine andere in derselben Umgebung normal funktioniert.

Umwelt

- Cisco Web Security Appliance (WSA) der S-Serie
- AsyncOS 14.5.2-011 (betroffene Version)
- Hardware: S695

- Mit FQDN-Spezifikation konfigurierter Upstream-Proxy
- Fehlerbehandlung, konfiguriert als "Direkt gehen"
- Netzwerkumgebung mit L2-Switch-Infrastruktur

Auflösung

Dieses Problem wird durch ein Upgrade von AsyncOS auf eine Version behoben, die das Fix für CSCwi13124 enthält. Dieser Fehler wurde in den folgenden AsyncOS-Versionen behoben:

- AsyncOS 15.5.0-566
- AsyncOS 15.5.0-710

Temporäre Problemumgehung für aktuelle Versionen

Für Umgebungen, die nicht sofort aktualisiert werden können, ist eine temporäre Reduzierung verfügbar, indem der maximale Timeout bei Inaktivität für das Überprüfen nicht reagierender Upstreamproxys angepasst wird:

Schritt 1: Rufen Sie die CLI auf, und navigieren Sie zur erweiterten Proxy-Konfiguration:

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

Phase 2: Ändern Sie die Einstellung für die maximale Leerlaufzeitüberschreitung:

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

Schritt 3: Reduzieren Sie den voreingestellten Maximalwert (86400 Sekunden/24 Stunden) auf einen kleineren Wert, um die Zeit zwischen Integritätsprüfungen zu verkürzen.

Sofortige Wiederherstellungsmethode

Wenn das Problem derzeit den Datenverkehrsfluss beeinträchtigt, kann der nächste Befehl die Upstream-Proxy-Funktionalität sofort wiederherstellen:

Schritt 1: Rufen Sie das Diagnosemenü auf:

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

Dadurch wird der Proxy-Prozess neu gestartet und der normale Upstream-Proxy-Betrieb wiederhergestellt.

Validierungs- und Testverfahren

So testen Sie, ob das Problem vorhanden ist oder nach einem Upgrade behoben wurde:

Schritt 1: Einrichtung einer Baseline-Überwachung

Überwachen Sie Zugriffsprotokolle und Proxyprotokolle, um zu bestätigen, dass die WSA Datenverkehr an den Upstream-Proxy sendet. Überprüfen Sie, ob der Datenverkehr die Upstream-Proxyseite erreicht.

Phase 2: Simulieren von Netzwerkunterbrechungen

Trennen Sie nach der Bestätigung des normalen Datenverkehrsflusses zum Upstream-Proxy die folgenden Verbindungen:

- WSA an Upstream-Proxyverbindung
- Verbindung zwischen WSA und DNS-Server

Schritt 3: Erkennung von Überwachungsfehlern

Überprüfen Sie die Proxyprotokolle und Systemprotokolle auf folgende Indikatoren:

- Proxyprotokoll kann Upstreamproxy als "... deklariert tot" anzeigen
- Systemprotokoll kann "Kritisch: Maximale Anzahl an Fehlern beim Abfragen des DNS-Servers erreicht..."

Schritt 4: Unterbrechungsstatus beibehalten

Behalten Sie ohne Neustart des Proxyprozesses den getrennten Status von Schritt 2 bei, und fahren Sie mit der Generierung von Anforderungen für ca. 10 Stunden fort.

Schritt 5: Verbindung wiederherstellen

Stellen Sie nach ca. 10 Stunden die Verbindungen wieder her, die in Schritt 2 getrennt wurden.

Schritt 6: Überwachen des Wiederherstellungsverhaltens

Nach Abschluss von Schritt 5 überwachen Sie Zugriffsprotokolle und Proxyprotokolle, ohne den Proxyprozess neu zu starten:

- In einem festen System: Der Datenverkehr fließt wieder über den Upstream-Proxy, und die Proxyprotokolle zeigen normale Statusübergänge an
- Bei einem betroffenen System: Zugriffsprotokolle zeigen an, dass der Datenverkehr weiterhin den Upstream-Proxy umgeht, und die Proxyprotokolle zeigen keine Meldungen wie "... was sick, now health" oder "... was health, now sick" an.

Ursache

Die Ursache dieses Problems ist ein logischer Fehler im Upstream-Proxy-Health-Check-Mechanismus. Wenn die WSA feststellt, dass ein konfigurierter Upstreamproxy "inaktiv" ist (nicht reagiert), implementiert sie einen exponentiellen Backoff-Algorithmus, der das Integritätsprüfungsintervall nach jedem Fehler verdoppelt. Dieses Intervall kann maximal 24 Stunden (86400 Sekunden) betragen.

Dieses Problem tritt auf, wenn der Upstreamproxy während eines dieser erweiterten Intervalle wieder verfügbar wird. Obwohl der Proxy wiederhergestellt wurde und normal reagiert, führt die WSA erst nach Ablauf des vollständig konfigurierten Zeitintervalls eine Integritätsprüfung durch. Dies kann zu bis zu 24 Stunden Weiterleitung des direkten Datenverkehrs führen, anstatt die Nutzung des Upstream-Proxys fortzusetzen.

Dieses Verhalten wirkt sich auf WSA-Konfigurationen aus, bei denen:

- Der Upstream-Proxy wird über den DNS-Hostnamen/FQDN (nicht über die IP-Adresse) angegeben.
- Fehlerbehandlung ist auf "Direkt gehen" gesetzt
- Erweiterte Netzwerkunterbrechungen wirken sich sowohl auf die Verbindung mit dem Upstream-Proxy als auch mit dem DNS-Server aus.

Cisco Bug-ID: CSCwi13124

Verwandte Inhalte

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.