Sicheres Web-Appliance-Dashboard wiederherstellen und anpassen

Inhalt

- Einleitung
- Voraussetzungen
  - Anforderungen
  - Verwendete Komponenten
- Mein Dashboard
  - Standardansicht
  - Merkmale des Webproxy-Datenverkehrs
  - Auslastung der Systemressourcen
  - Webproxy-Aktivität gesamt
  - Webproxy-Zusammenfassung
  - Zusammenfassung der L4-Datenverkehrsüberwachung
  - Verdächtige Transaktionen
  - Zusammenfassung der verdächtigen Transaktionen
  - Häufigste URL-Kategorien: Transaktionen gesamt
  - Wichtigste Anwendungstypen: Transaktionen gesamt
  - Häufigste Malwarekategorien: Überwacht oder gesperrt
  - Top-Benutzer: Gesperrte oder mit Warnung versehene Transaktionen
- Zeitbereich ändern
- Datensätze ändern
- Dashboard-Design ändern
- Mein Dashboard auf die Standardeinstellungen zurücksetzen
- Verwandte Inhalte

Einleitung

In diesem Dokument werden die Schritte zum Anpassen und Wiederherstellen des Secure Web Appliance (SWA)-Dashboards beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Zugriff auf die grafische Benutzeroberfläche (GUI) von SWA
- Administrator-Zugriff auf die SWA

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Mein Dashboard

Standardmäßig ist die SWA-Landing Page My-Dashboard. Diese Seite wird angezeigt, wenn sich der Benutzer bei der Appliance anmeldet. Mein Dashboard umfasst zwei Hauptabschnitte:

- Systemübersicht
- Zeitbereich

Sie können verschiedene Eigenschaften dieser Statistiken und Berichte anpassen, z. B.:

- Datentyp
- Zeitbereich
- Auf der Seite anzuzeigende Position
- Datensätze anzeigen und ausblenden

Standardansicht

Standardmäßig sind die Berichte und Statistiken in My-Dashboard:

- Systemübersicht
  - Übersicht > Eigenschaften des Webproxy-Datenverkehrs
  - Übersicht > Auslastung der Systemressourcen
- Zeitbereich

- Übersicht > Webproxy-Aktivität gesamt
- Übersicht > Webproxy-Zusammenfassung
- Überblick > Layer 4 (L4) Traffic Monitor-Zusammenfassung
- Übersicht > Verdächtige Transaktionen
- Übersicht > Übersicht über verdächtige Transaktionen
- Häufigste URL-Kategorien: Transaktionen gesamt
- Wichtigste Anwendungstypen: Transaktionen gesamt
- Häufigste Malwarekategorien: Überwacht oder gesperrt
- Top-Benutzer: Gesperrte oder mit Warnung versehene Transaktionen



Bild - SWA-Dashboard

Merkmale des Webproxy-Datenverkehrs

Webproxy-Datenverkehrsmerkmale listet Statistiken über die Transaktion auf:

Durchschnittliche Transaktionen pro Sekunde in der letzten Minute: XX
Durchschnittliche Bandbreite (bit/s) in der letzten Minute: XX
Durchschnittliche Reaktionszeit (ms) in der letzten Minute: XX
Aktuelle Verbindungen gesamt: XX

Auslastung der Systemressourcen

Die Systemressourcennutzung listet die aktuelle Gesamtlast der zentralen Verarbeitungseinheit (CPU), den Arbeitsspeicher mit wahlfreiem Zugriff (RAM) und die Auslastung der Berichts-/Protokollfestplatten auf.

Klicken Sie auf System Status Details (Systemstatusdetails), um zur Seite System Status (Systemstatus) zu wechseln.

(Verwenden Sie die Seite Reporting > System Status (Berichte > Systemstatus), um den Systemstatus zu überwachen. Auf dieser Seite werden der aktuelle Status und die Konfiguration der sicheren Web-Appliance angezeigt.)



Anmerkung: Der CPU-Auslastungswert auf dieser Seite und der CPU-Wert auf der Seite "Systemstatus" können sich leicht unterscheiden, da sie zu unterschiedlichen Zeitpunkten separat gelesen werden.

Webproxy-Aktivität gesamt

Sie können die Webproxy-Aktivität anzeigen, die von den sicheren Webanwendungen gemeldet wird, die derzeit von der Sicherheitsverwaltungs-Appliance verwaltet werden.
In diesem Abschnitt werden die tatsächliche Anzahl der Transaktionen und das ungefähre Datum angezeigt, an dem die Aktivität im grafischen Format durchgeführt wurde.

Sie können auch den Prozentsatz der verdächtigen Web-Proxy-Aktivitäten oder die Aktivität "Sauberer Proxy" anzeigen, einschließlich der Gesamtanzahl der Transaktionen.

Webproxy-Zusammenfassung

Ermöglicht Ihnen, den Prozentsatz der Webproxy-Aktivität anzuzeigen, die verdächtig oder unschädlich ist.

Zusammenfassung der L4-Datenverkehrsüberwachung

Sie können jeden L4-Datenverkehr, der von den derzeit von der Security Management Appliance verwalteten sicheren Web-Appliances gemeldet wird, im grafischen Format anzeigen.

Verdächtige Transaktionen

Sie können die Webtransaktionen, die vom Administrator als verdächtig gekennzeichnet wurden, in einem grafischen Format anzeigen.
Dieser Abschnitt zeigt die tatsächliche Anzahl der Transaktionen und das ungefähre Datum, an dem die Aktivität stattgefunden hat, im grafischen Format an.

Zusammenfassung der verdächtigen Transaktionen

Sie können auch den Prozentsatz der gesperrten oder mit Warnung versehenen Transaktionen anzeigen, die verdächtig sind.

Sie können die Art der erkannten und gesperrten Transaktionen sowie die tatsächliche Anzahl der gesperrten Transaktionen anzeigen.

Häufigste URL-Kategorien: Transaktionen gesamt

Sie können die wichtigsten URL-Kategorien, die auf der Website besucht werden, in einem grafischen Format anzeigen.

Wichtigste Anwendungstypen: Transaktionen gesamt

Sie können die wichtigsten blockierten Anwendungstypen im grafischen Format anzeigen. Dazu gehören auch der Name des Anwendungstyps und die Anzahl der Blockierungen für die jeweilige Anwendung.

Häufigste Malwarekategorien: Überwacht oder gesperrt

Sie können alle erkannten Malware-Kategorien im grafischen Format anzeigen.

Top-Benutzer: Gesperrte oder mit Warnung versehene Transaktionen

Sie können die tatsächlichen Benutzer, die die gesperrten oder mit Warnung versehenen Transaktionen generiert haben, im grafischen Format anzeigen. Benutzer können nach IP-Adresse oder Benutzername angezeigt werden.

Zeitbereich ändern

So ändern Sie den Zeitraum von "Tag" bis "Stunde", "Woche", "30 Tage" oder "Gestern":

Schritt 1: Option auswählen (oben rechts)

Phase 2: Wählen Sie Leistung aus.

Schritt 3: Klicken Sie auf Voreinstellungen bearbeiten.

Schritt 4: Ändern Sie den angezeigten Berichtszeitbereich (Standard) in eine der verfügbaren Optionen.

Schritt 5: Senden. Die Änderungen müssen nicht bestätigt werden.

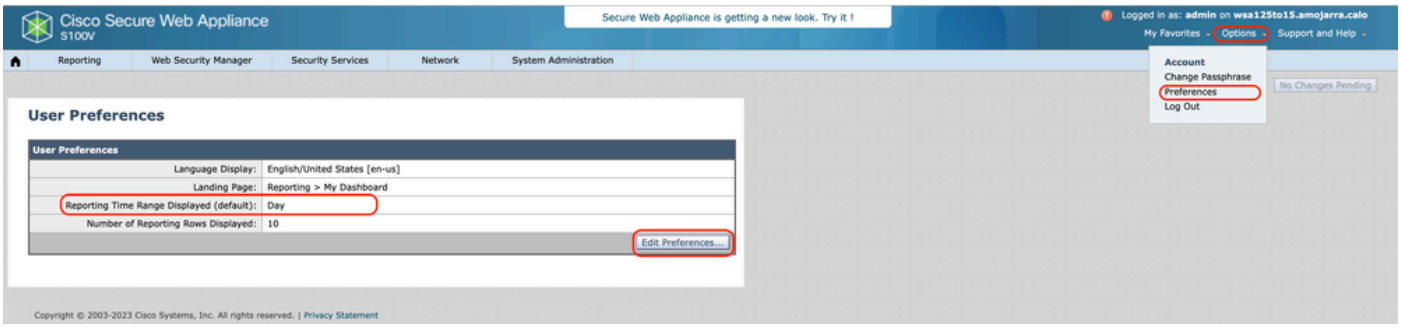


Bild - Schritte zum Bearbeiten des Standardzeitbereichs in My-Dashboard

Datensätze ändern

Sie können Datensätze und Berichte auf der Seite Mein Dashboard hinzufügen und entfernen. Verwenden Sie das Pluszeichen (+), um weitere Berichte hinzuzufügen, und verwenden Sie X-Zeichen oben rechts neben jedem Bericht, um diese zu entfernen.

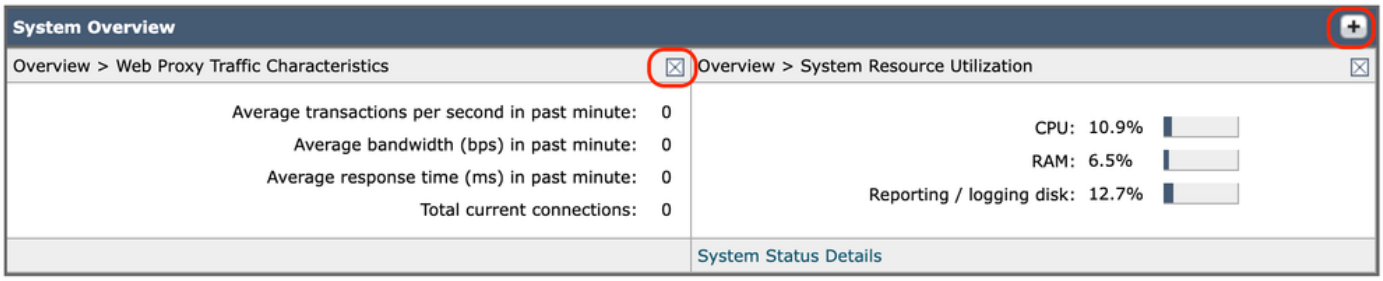


Bild - Hinzufügen und Entfernen von Berichten in My-Dashboard.

Vorsicht: Änderungen werden wirksam, sobald Sie sie ändern. Die Einsendung ist nicht erforderlich.

Dashboard-Design ändern

Sie können die Reihenfolge der einzelnen Datensätze auf der Seite Mein Dashboard ändern. Klicken Sie auf das blaue Band am oberen Rand der einzelnen Berichte, und ändern Sie dann den Ort für den Bericht.

Mein Dashboard auf die Standardeinstellungen zurücksetzen

Um My-Dashboard auf den Standardwert zurückzusetzen, bearbeiten Sie die Konfigurationsdatei manuell mit den folgenden Schritten:

Schritt 1: Navigieren Sie in der GUI zu Systemadministrationen.

Phase 2: Wählen Sie Konfigurationsdatei aus.

Schritt 3: Laden Sie die neueste Konfigurationsdatei herunter.

Anmerkung: Wählen Sie in den Konfigurationsdateien die Option Kennwörter verschlüsseln aus.

Schritt 4: Ändern Sie die XML-Datei, indem Sie alle Elemente zwischen <user_reports> und </user_reports> entfernen.

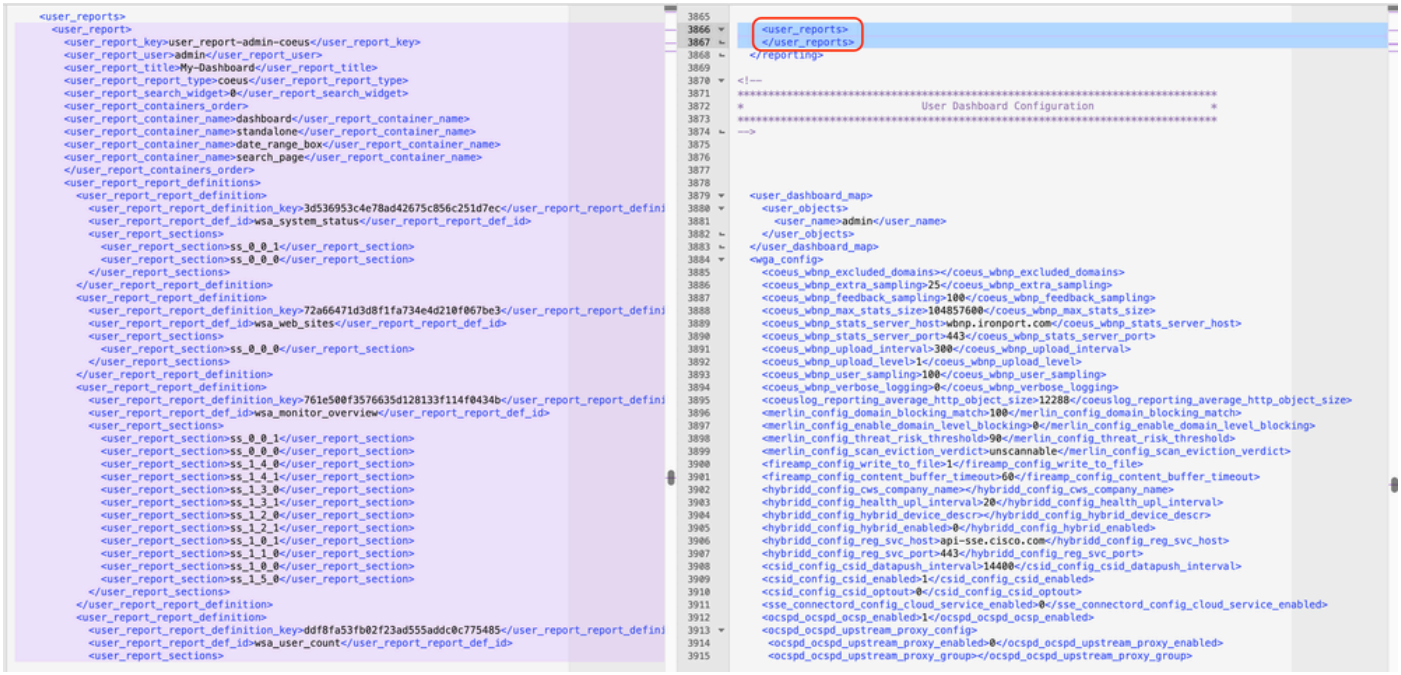


Image - Beispiel-Konfigurationsdateien mit benutzerdefiniertem Dashboard (rechts) und Standardkonfigurationsdatei (links).

Schritt 5: Wählen Sie auf der Seite Konfigurationsdatei im Abschnitt Konfiguration laden die Option Konfigurationsdatei vom lokalen Computer laden aus.

Schritt 6: Laden Sie die geänderte XML-Datei hoch.

Schritt 7: Klicken Sie auf Laden und bestätigen Sie die Änderungen.

Verwandte Inhalte

[Benutzerhandbuch für AsyncOS 14.5 für Cisco Secure Web Appliance - GD (Allgemeine Bereitstellung)]

[Support - Cisco Support und Downloads - Dokumentation, Tools, Tickets - 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.