Ripristino e personalizzazione del dashboard di Secure Web Appliance

Sommario

- Introduzione
- Prerequisiti
  - Requisiti
  - Componenti usati
- Dashboard personale
  - Visualizzazione predefinita
  - Caratteristiche traffico proxy Web
  - Utilizzo risorse di sistema
  - Attività proxy Web totale
  - Riepilogo proxy Web
  - Riepilogo L4 Traffic Monitor
  - Transazioni sospette
  - Sintetico transazioni sospette
  - Categorie URL principali: Transazioni totali
  - Primi tipi di applicazione: Transazioni totali
  - Principali categorie di malware: Monitorato o bloccato
  - Utenti principali: Transazioni bloccate o avvisate
- Modifica intervallo di tempo
- Modifica set di dati
- Modifica struttura dashboard
- Ripristina dashboard predefinito
- Contenuto correlato

Introduzione

In questo documento viene descritto come personalizzare e ripristinare il dashboard Secure Web Appliance (SWA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso all'interfaccia grafica dell'SWA
- Accesso amministrativo all'SWA.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Dashboard personale

Per impostazione predefinita, la pagina iniziale SWA è My-Dashboard, ovvero la pagina visualizzata quando l'utente accede all'accessorio. Dashboard personale contiene due sezioni principali:

- Panoramica del sistema
- Intervallo

È possibile personalizzare varie proprietà di questi rapporti e statistiche, ad esempio:

- Tipo di dati
- Intervallo
- Posizione da visualizzare nella pagina
- Mostrare e nascondere set di dati

Visualizzazione predefinita

Per impostazione predefinita, i report e le statistiche in Dashboard personale sono:

- Panoramica del sistema
    - Panoramica > Caratteristiche del traffico del proxy Web
    - Panoramica > Utilizzo risorse di sistema

- Intervallo
    - Panoramica > Attività proxy Web totale
    - Panoramica > Riepilogo proxy Web
    - Panoramica > Riepilogo monitoraggio traffico layer 4 (L4)
    - Panoramica > Transazioni sospette
    - Panoramica > Sintetico transazioni sospette
    - Categorie URL principali: Transazioni totali
    - Primi tipi di applicazione: Transazioni totali
    - Principali categorie di malware: Monitorato o bloccato
    - Utenti principali: Transazioni bloccate o avvisate

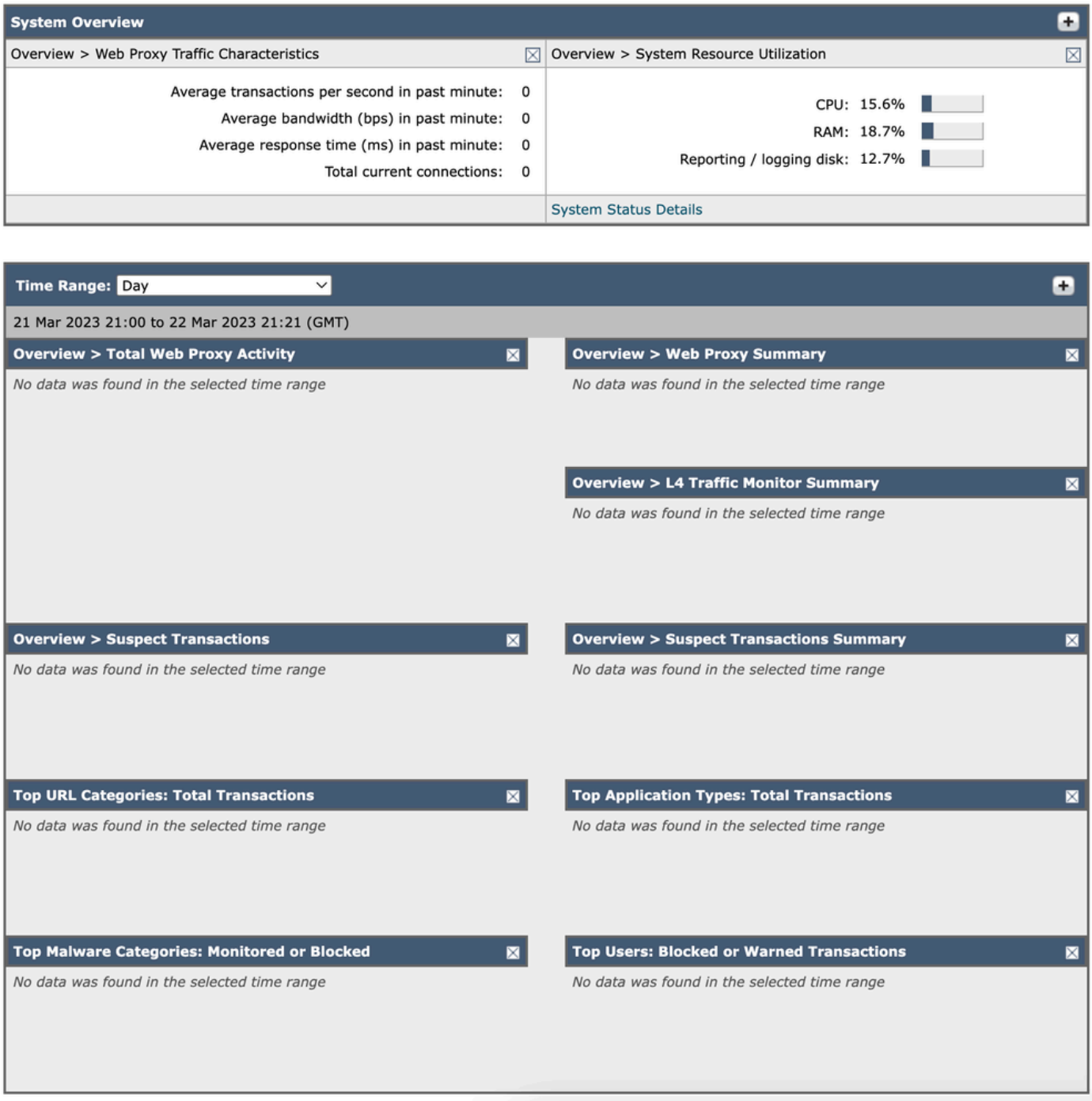


Immagine - Dashboard SWA

Caratteristiche traffico proxy Web

Le caratteristiche del traffico del proxy Web elencano le statistiche relative alla transazione:

Media transazioni al secondo nell'ultimo minuto: XX
Larghezza di banda media (bps) nell'ultimo minuto: XX
Tempo medio di risposta (ms) nell'ultimo minuto: XX
Totale connessioni correnti: XX

Utilizzo risorse di sistema

L'utilizzo delle risorse di sistema elenca il carico della CPU, la memoria RAM (Random Access Memory) e l'utilizzo del disco di report/log.

Fare clic su System Status Details (Dettagli stato sistema) per passare alla pagina System Status (Stato sistema).

Per controllare lo stato del sistema, utilizzare la pagina Reporting > Stato del sistema. In questa pagina vengono visualizzati lo stato corrente e la configurazione di Secure Web Appliance.)



Nota: Il valore di utilizzo della CPU visualizzato in questa pagina e il valore della CPU visualizzato nella pagina Stato sistema possono essere leggermente diversi perché vengono letti separatamente in momenti diversi.

Attività proxy Web totale

È possibile visualizzare l'attività del proxy Web segnalata dagli accessori Web protetti attualmente gestiti dall'accessorio di gestione della sicurezza.
In questa sezione vengono visualizzati in formato grafico il numero effettivo di transazioni e la data approssimativa in cui si è verificata l'attività.

È inoltre possibile visualizzare la percentuale di attività proxy Web sospetta o pulita, includendo il numero totale di transazioni.

Riepilogo proxy Web

Consente di visualizzare la percentuale di attività proxy Web sospetta o pulita.

Riepilogo L4 Traffic Monitor

È possibile visualizzare in formato grafico qualsiasi traffico L4 segnalato da Secure Web Appliance e attualmente gestito da Security Management Appliance.

Transazioni sospette

È possibile visualizzare in formato grafico le transazioni Web etichettate come sospette dall'amministratore.
In questa sezione vengono visualizzati, in formato grafico, il numero effettivo di transazioni e la data approssimativa in cui si è verificata l'attività.

Sintetico transazioni sospette

È inoltre possibile visualizzare la percentuale di transazioni sospette bloccate o avvisate.

È possibile visualizzare il tipo di transazioni rilevate e bloccate e il numero effettivo di volte in cui la transazione è stata bloccata.

Categorie URL principali: Transazioni totali

È possibile visualizzare le principali categorie URL visitate nel sito in formato grafico.

Primi tipi di applicazione: Transazioni totali

È possibile visualizzare in formato grafico i primi tipi di applicazione bloccati, che includono anche il nome del tipo di applicazione effettivo e il numero di volte in cui l'applicazione specifica è stata bloccata.

Principali categorie di malware: Monitorato o bloccato

È possibile visualizzare tutte le categorie di malware rilevate in formato grafico.

Utenti principali: Transazioni bloccate o avvisate

È possibile visualizzare in formato grafico gli utenti effettivi che hanno generato le transazioni

bloccate o avvisate. Gli utenti possono essere visualizzati per indirizzo IP o per nome utente.

Modifica intervallo di tempo

Per modificare la data dell'intervallo di tempo da Giorno a Ora, Settimana, 30 giorni, Ieri:

Passaggio 1: Scegli opzione (in alto a destra)

Passaggio 2: Scegliere Prestazioni.

Passaggio 3: Fare clic su Modifica preferenze.

Passaggio 4: Modificare Intervallo di tempo di reporting visualizzato (impostazione predefinita) in una delle opzioni disponibili.

Passaggio 5: Inviare. Non è necessario eseguire il commit delle modifiche.

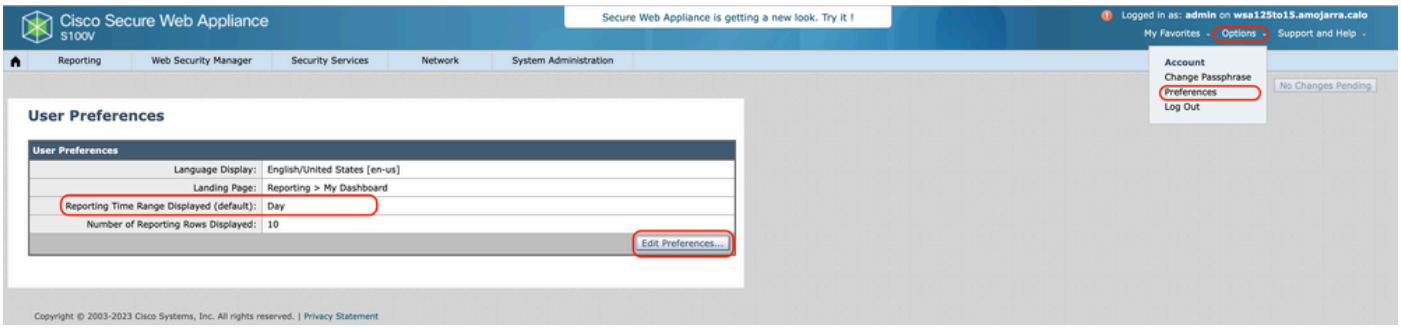


Immagine - Passi per modificare l'intervallo di tempo predefinito in My-Dashboard

Modifica set di dati

È possibile aggiungere e rimuovere set di dati e report nella pagina Dashboard personale. Utilizzare il segno più (+) per aggiungere altri report e il segno X in alto a destra di ogni report per rimuoverli.

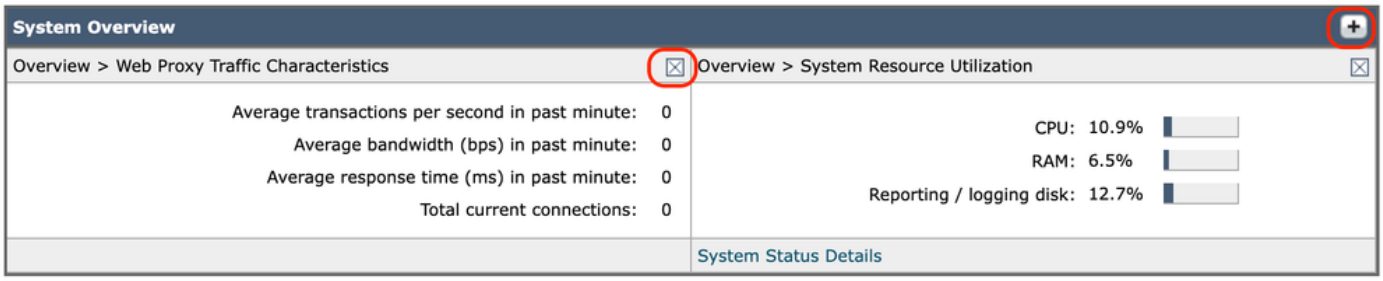


Immagine - Aggiungere e rimuovere report in Dashboard personale.

Attenzione: Le modifiche diventano effettive non appena vengono apportate. Non è necessario eseguire l'invio.

Modifica struttura dashboard

È possibile modificare l'ordine di ogni set di dati nella pagina My-Dashboard. Fare clic sulla barra multifunzione blu nella parte superiore di ogni report, quindi modificare la posizione del report.

Ripristina dashboard predefinito

Per ripristinare My-Dashboard al valore predefinito, modificare manualmente il file di configurazione eseguendo la procedura seguente:

Passaggio 1: Dalla GUI, selezionare System Administrations (Amministrazioni di sistema).

Passaggio 2: Selezionare File di configurazione.

Passaggio 3: Scaricare il file di configurazione più recente.

Nota: Selezionare Encrypt password (Crittografa password) nei file di configurazione.

Passaggio 4: modificare il file XML rimuovendo tutti gli elementi tra <user_reports> e </user_reports>.

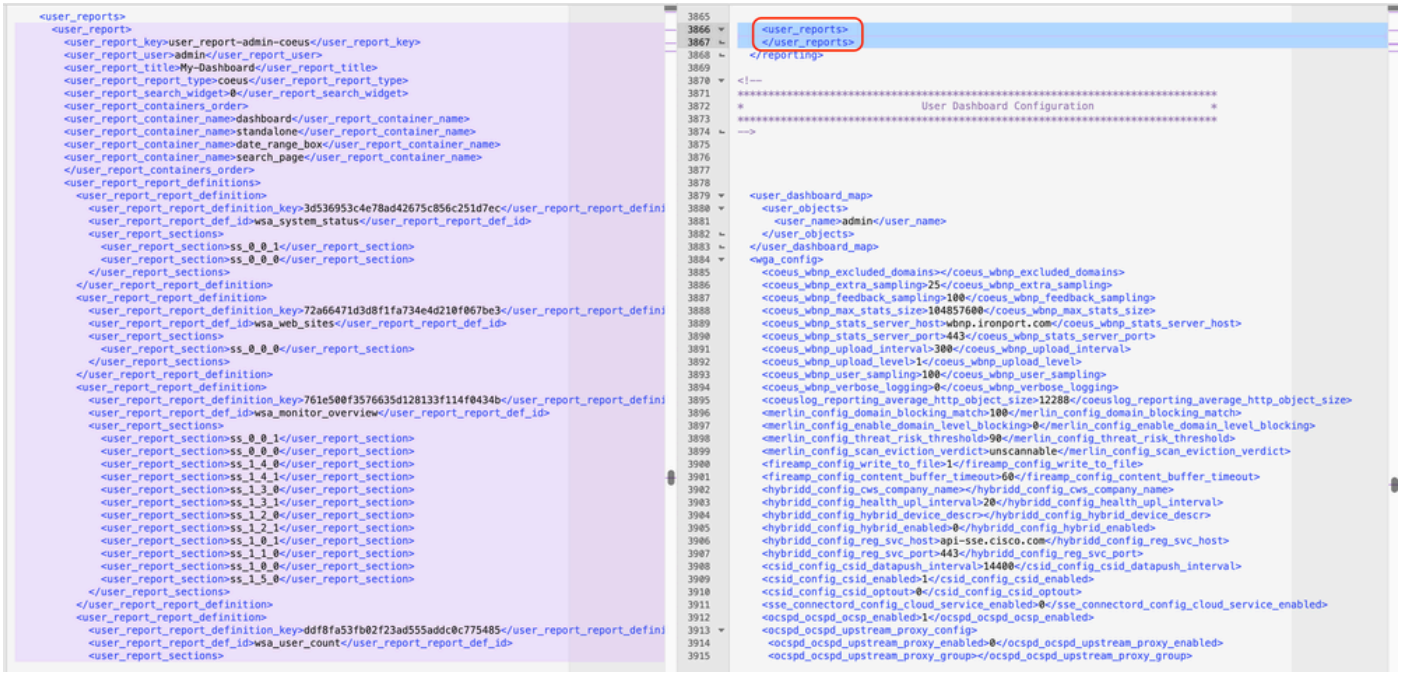


Immagine - File di configurazione di esempio con dashboard personalizzato (a destra) e file di configurazione predefinito (a sinistra).

Passaggio 5: Dalla pagina File di configurazione, nella sezione Carica configurazione, selezionare Carica un file di configurazione dal computer locale.

Passaggio 6: Caricare il file XML modificato.

Passaggio 7: Fare clic su Load and commit changes.

Contenuto correlato

Guida per l'utente di AsyncOS 14.5 for Cisco Secure Web Appliance - GD (General Deployment)

Supporto - Supporto e download Cisco - Documentazione, Strumenti, Richieste - Cisco

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).