Configura criteri di correlazione in FMC

Sommario

[Introduzione](#)

[Prerequisiti](#)

- [Requisiti](#)
- [Componenti usati](#)

[Premesse](#)

[Configurazione](#)

- [Configura regole di correlazione](#)
- [Configura avvisi](#)
- [Configura criterio di correlazione](#)

Introduzione

In questo documento viene descritta la procedura per configurare un criterio di correlazione per connettere eventi e rilevare anomalie nella rete.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti prodotti:

- Centro gestione firewall protetto (FMC)
- Secure Firewall Threat Defense (FTD)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Firepower Threat Defense per VMware versione 7.6.0

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.

Premesse

I criteri di correlazione vengono utilizzati per identificare le potenziali minacce alla sicurezza della

rete mediante la configurazione di diversi tipi di eventi e per la risoluzione dei problemi, gli avvisi condizionali e i criteri del traffico.

Configurazione

Configura regole di correlazione

Passaggio 1. Passare a Criteri > Correlazione e selezionare Gestione regole.

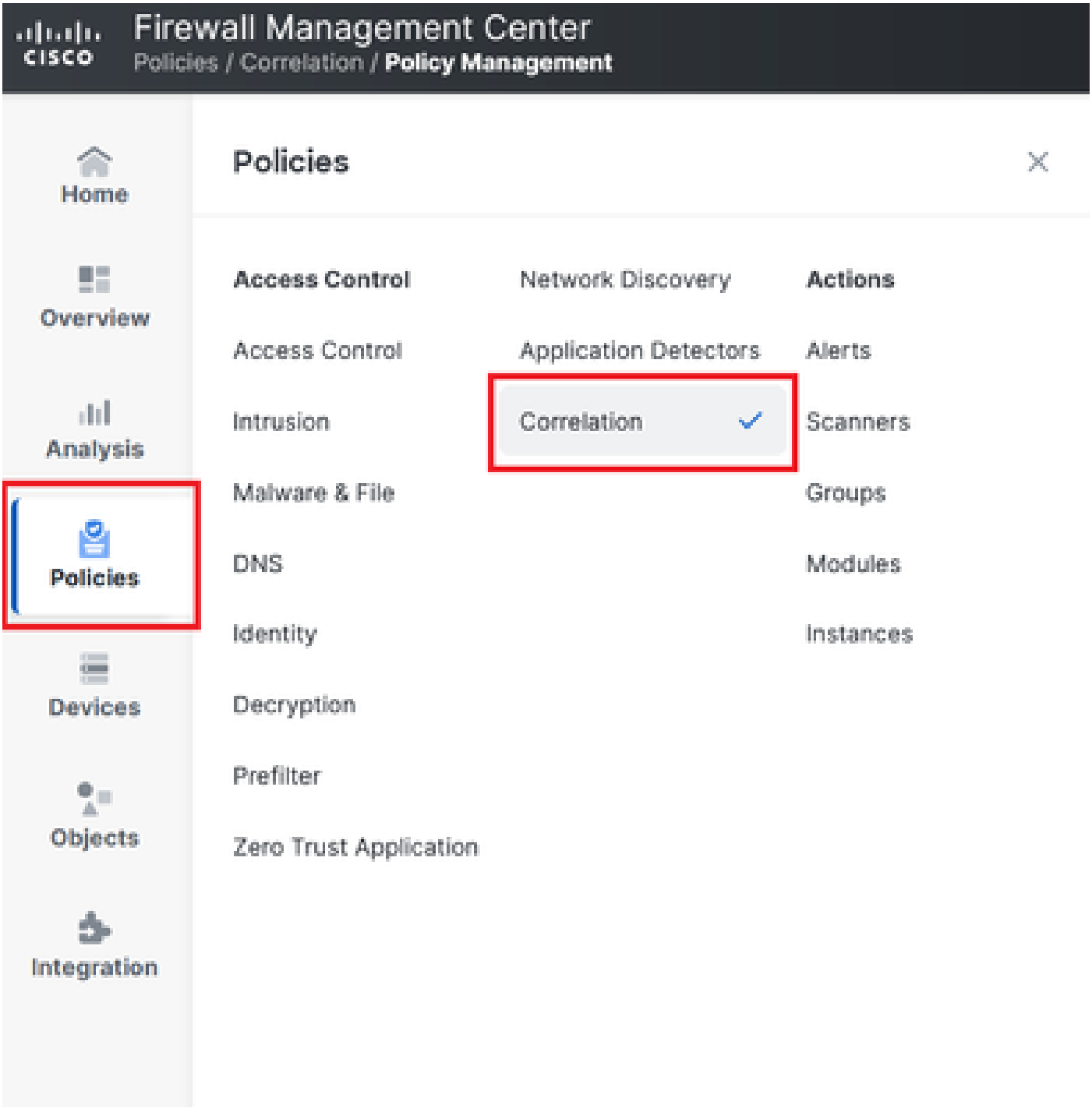


Immagine 1. Passa al menu Criteri di correlazione

Passaggio 2. Creare una nuova regola selezionando Crea regola.

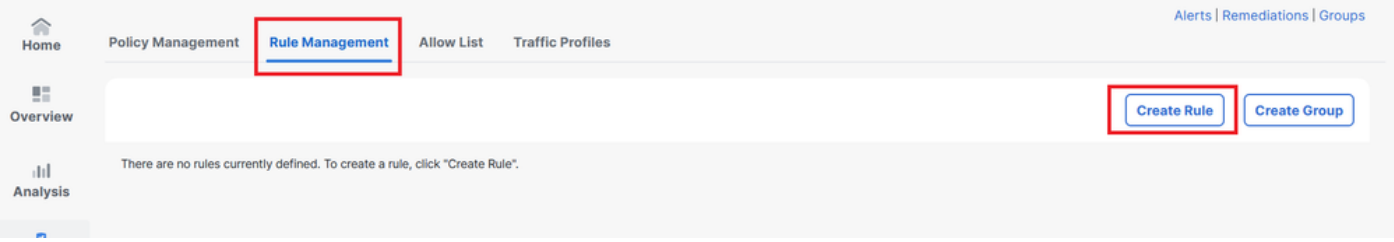


Immagine 2. Creazione di regole nel menu Gestione regole

Passaggio 3. Selezionare un tipo di evento e le condizioni che soddisfano la regola.

Se la regola contiene più condizioni, è necessario collegarle con l'operatore AND o OR.

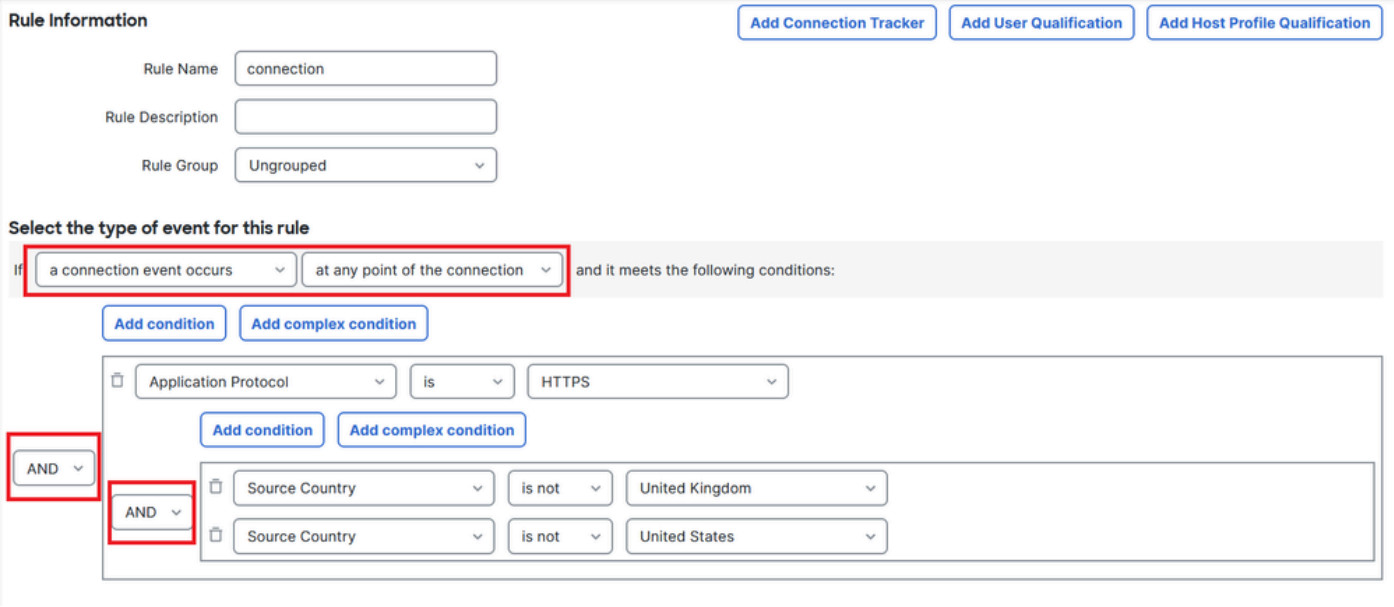


Immagine 3. Menu Creazione regola

Nota: le regole di correlazione non devono essere generiche. Se la regola viene costantemente attivata dal traffico normale, ciò può comportare l'utilizzo di CPU aggiuntiva e influire sulle prestazioni del CCP.

Configura avvisi

Passaggio 1. Passare a Criteri > Azioni > Avvisi.

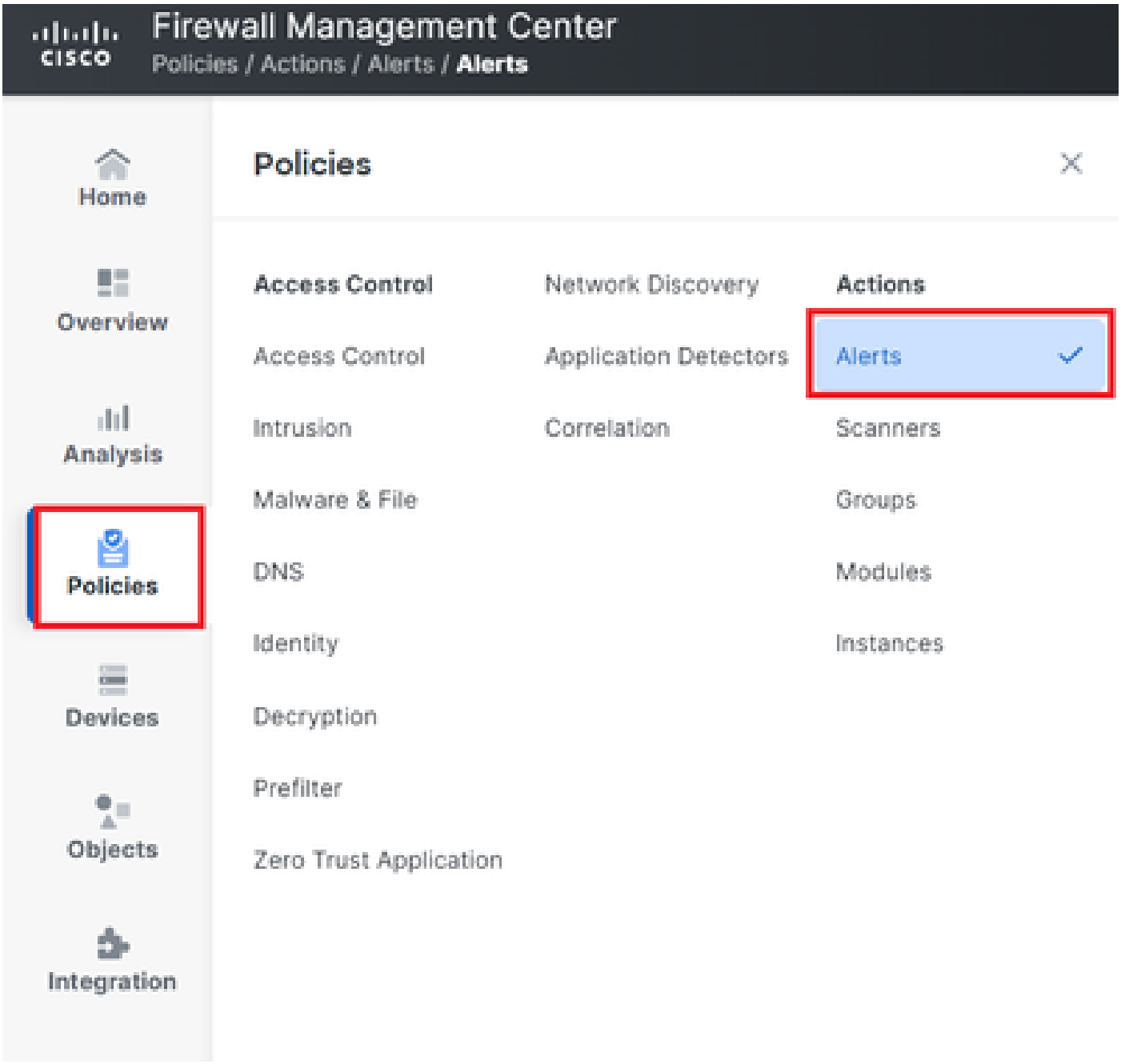


Immagine 4. Passa al menu Avvisi

Passaggio 2. Selezionare Create Alert (Crea avviso) e creare un avviso Syslog, SNMP o e-mail.

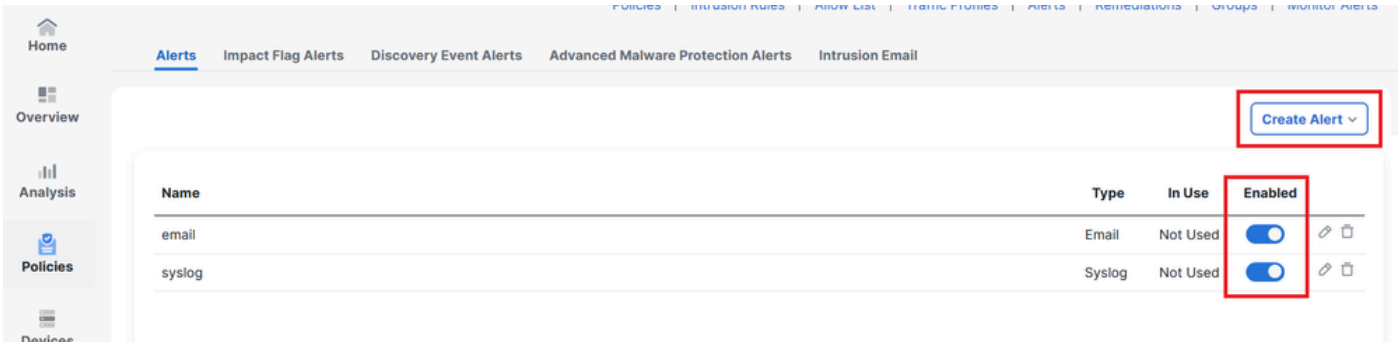
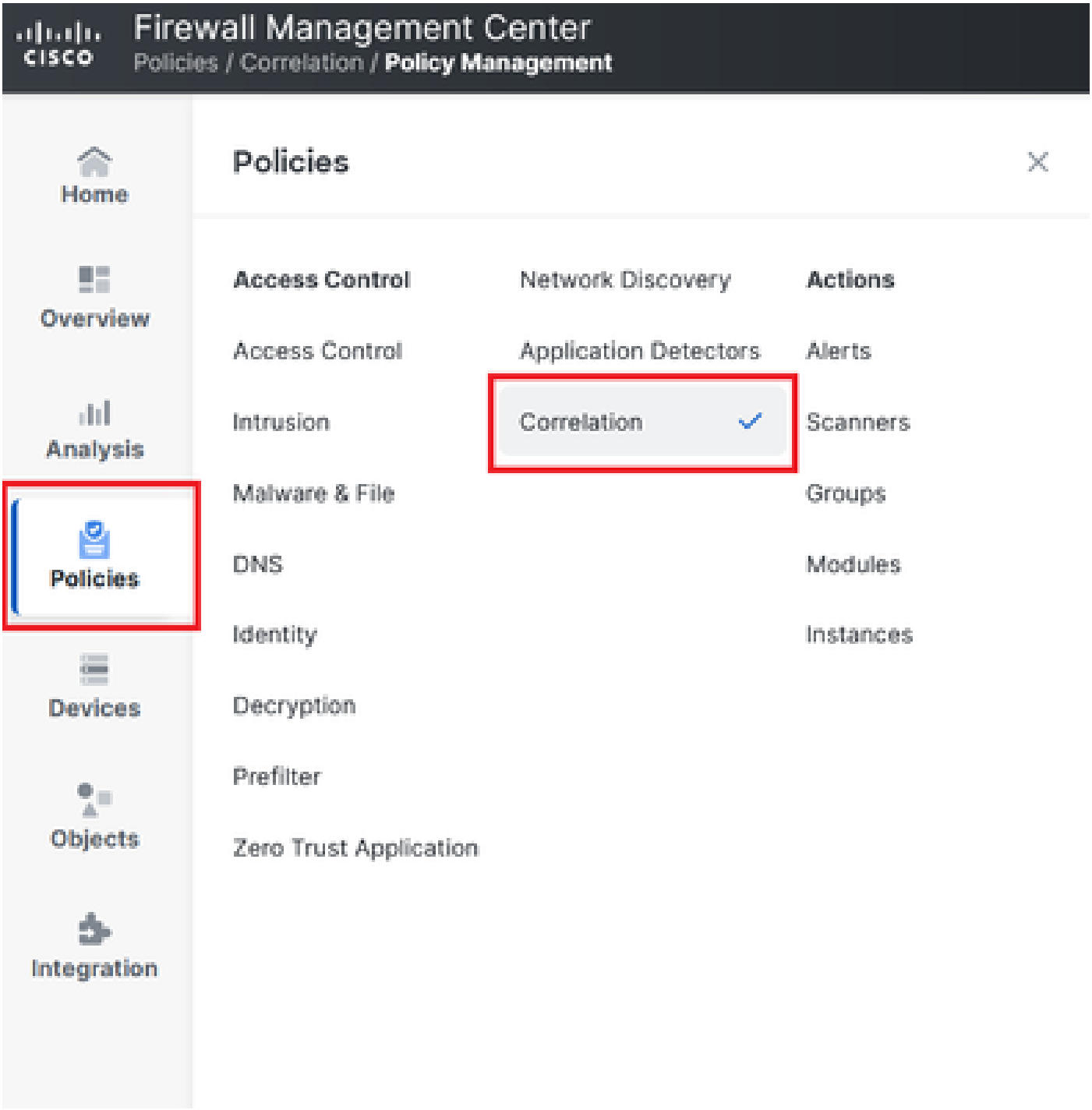


Immagine 5. Crea avviso

Passaggio 3. Verificare che l'avviso sia attivato.

Configura criterio di correlazione

Passaggio 1. Passare a Criteri > Correlazione.



Passa al menu Criteri di correlazione

Immagine 6. Passa al menu Criteri di correlazione

Passaggio 2. Crea un nuovo criterio di correlazione. Selezionare la priorità predefinita. Utilizzare Nessuno per utilizzare le priorità delle regole specifiche.

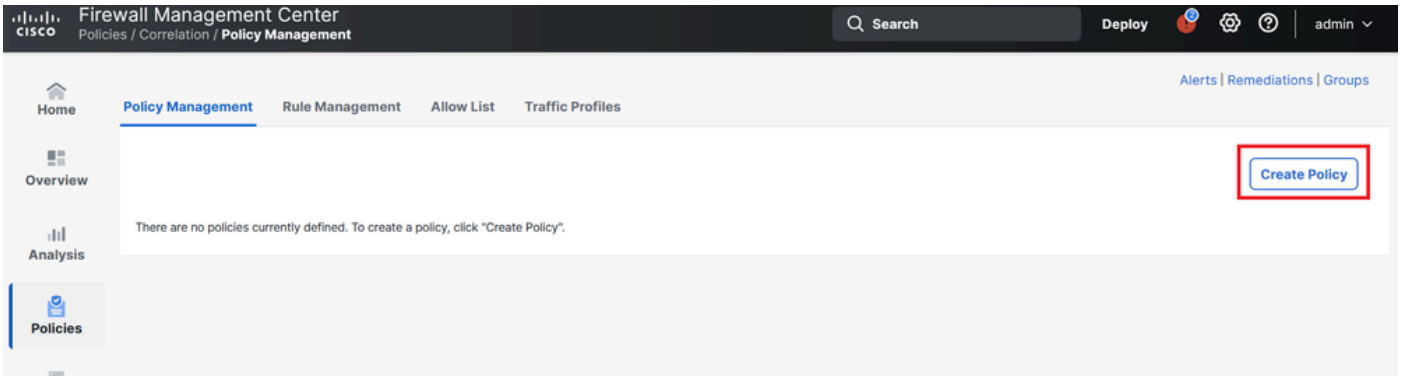


Immagine 7. Crea nuovo criterio di correlazione

Passaggio 3. Aggiungere regole al criterio selezionando Aggiungi regole.

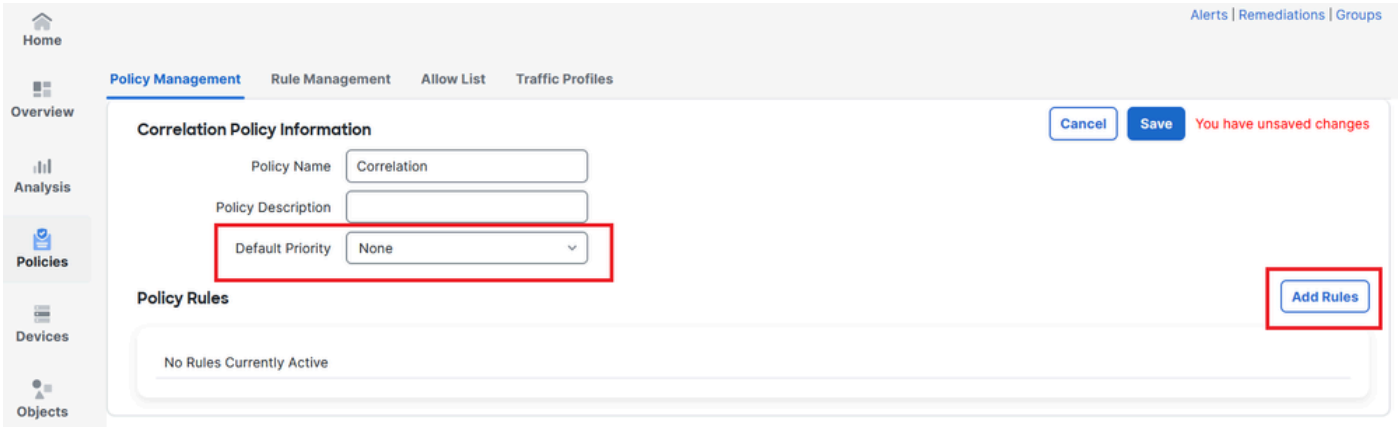


Immagine 8. Aggiungi regole e seleziona priorità per criterio di correlazione

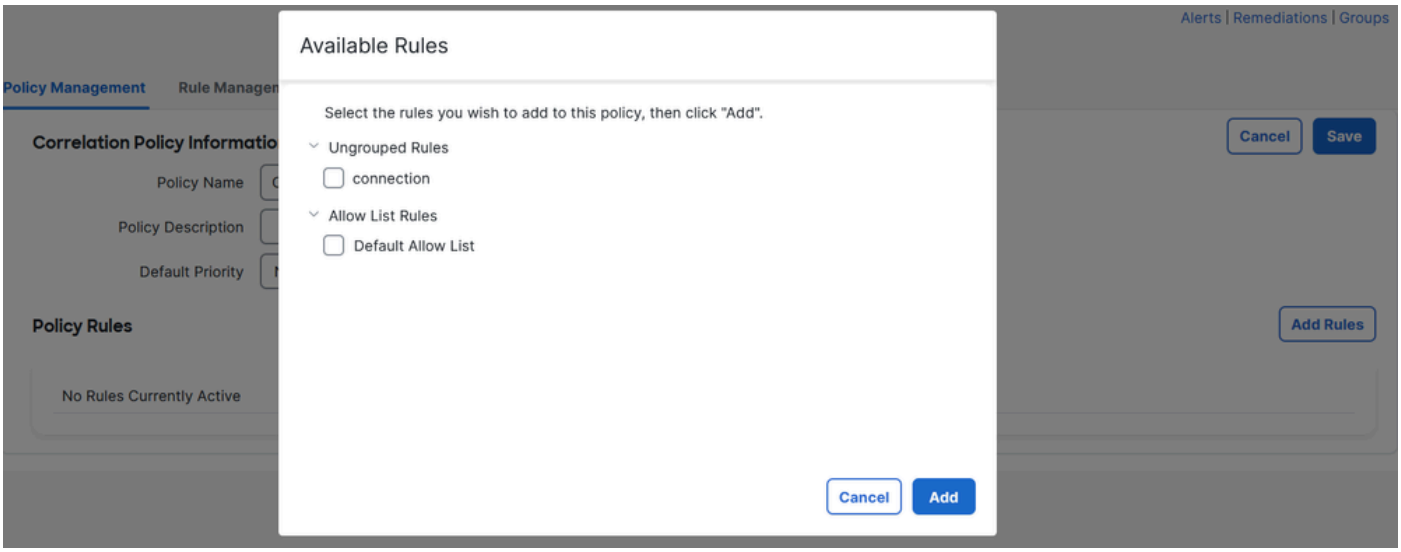


Immagine 9. Selezionare le regole da aggiungere al criterio di correlazione

Passaggio 4. Assegnare una risposta alla regola dagli alert creati, in modo che ogni volta che viene attivata, invii il tipo di alert selezionato.

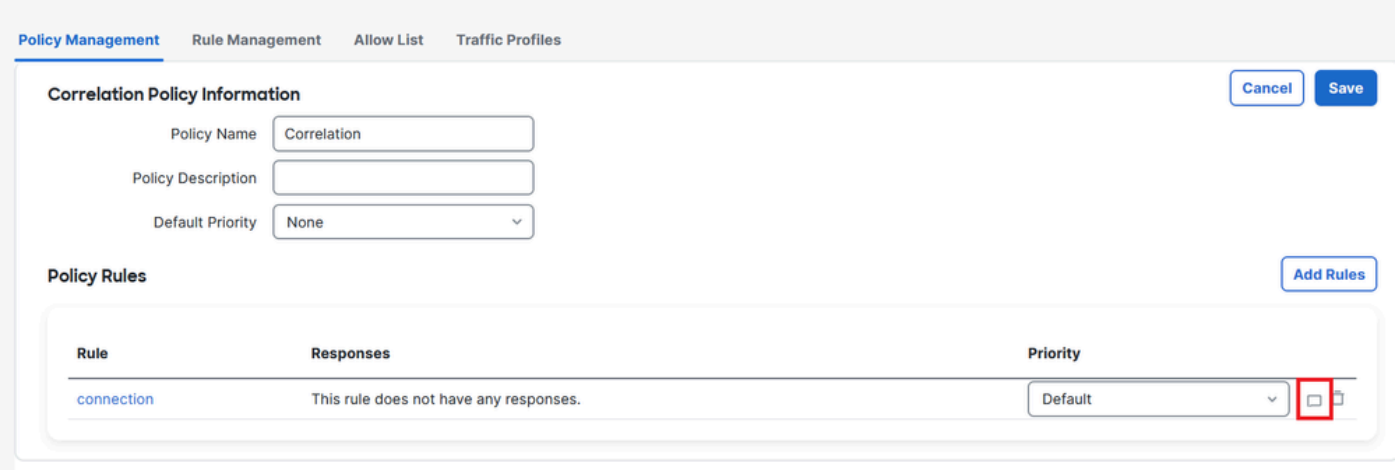


Immagine 10. Pulsante Aggiungi risposte

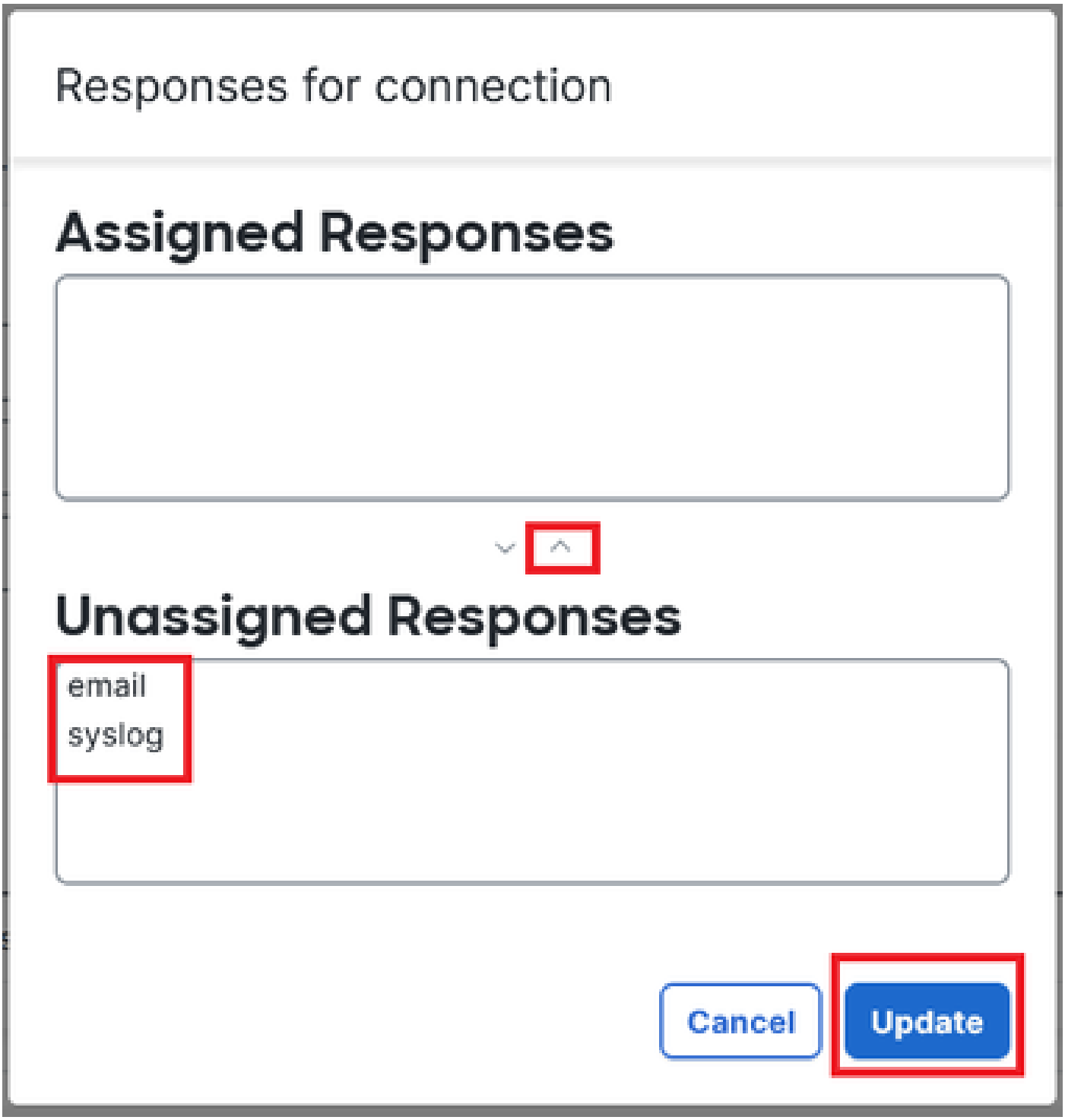


Immagine 11. Assegna risposte alla regola di correlazione

Passaggio 5. Salvare e abilitare i criteri di correlazione.

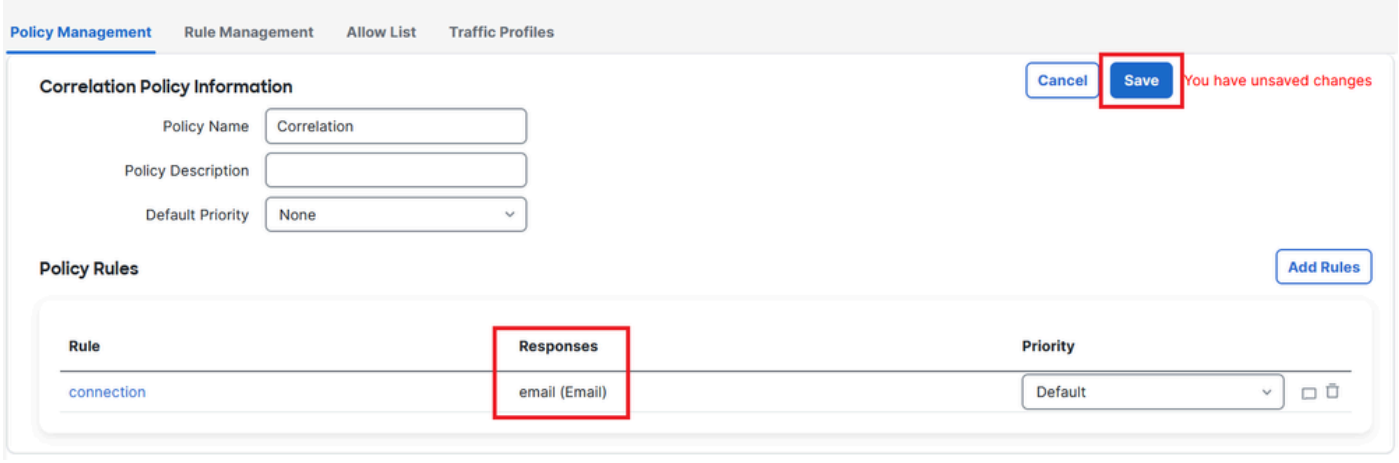


Immagine 12. Risposta aggiunta correttamente alla regola di correlazione

Immagine 13. Abilita criterio di correlazione

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).