Configurazione dell'integrazione degli eventi FTD sicuri con Security Cloud Control tramite Secure Event Connector

Sommario

Introduzione

Questo documento descrive come configurare Cisco Secure FTD per inviare eventi di sicurezza al Security Cloud Control (SCC) utilizzando il Secure Event Connector (SEC).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Firewall Threat Defense (FTD)
- Interfaccia della riga di comando Linux (CLI)

Componenti usati

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

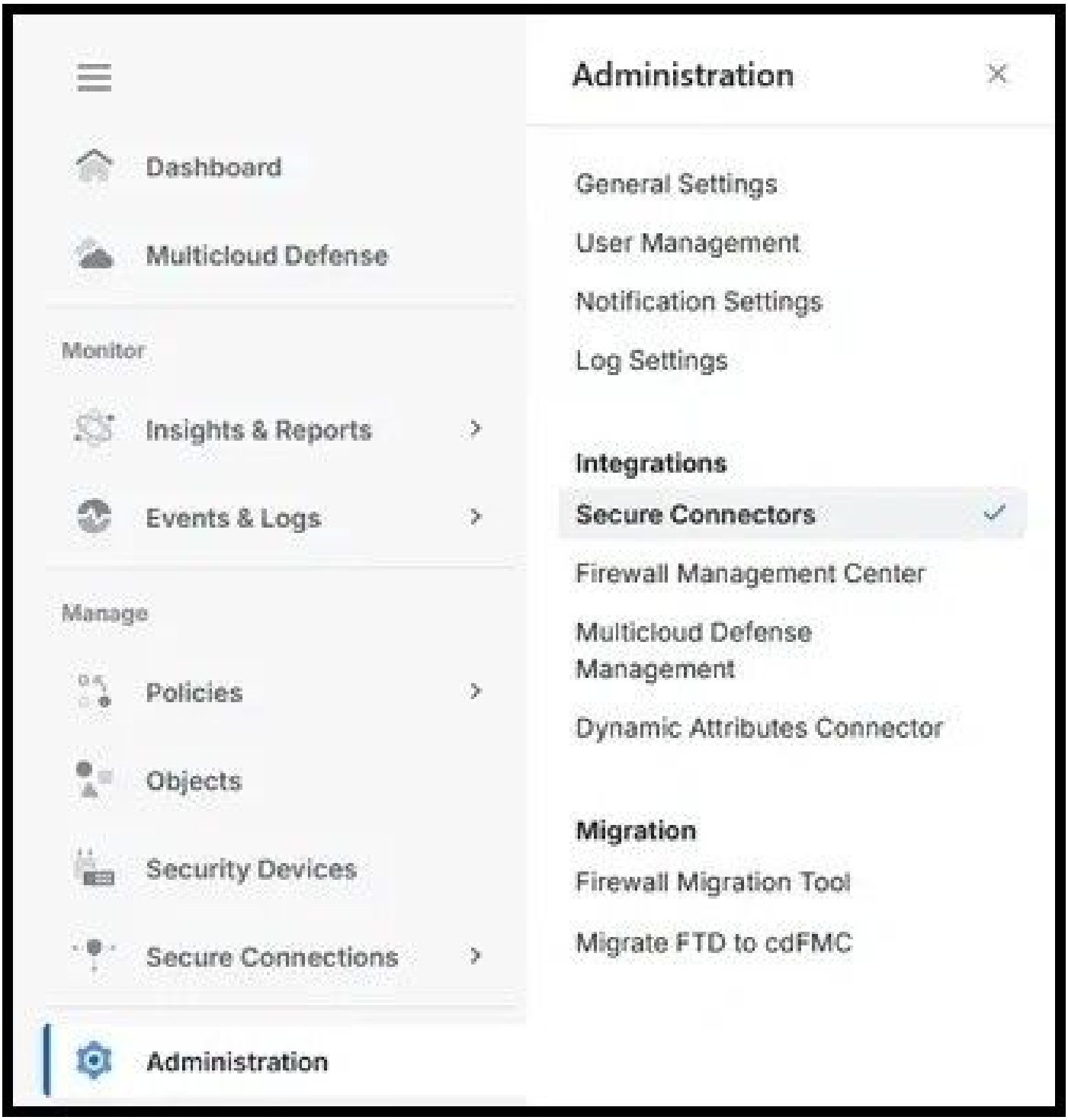
- Cisco Secure FTD 7.6
- Ubuntu Server versione 24.04

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.

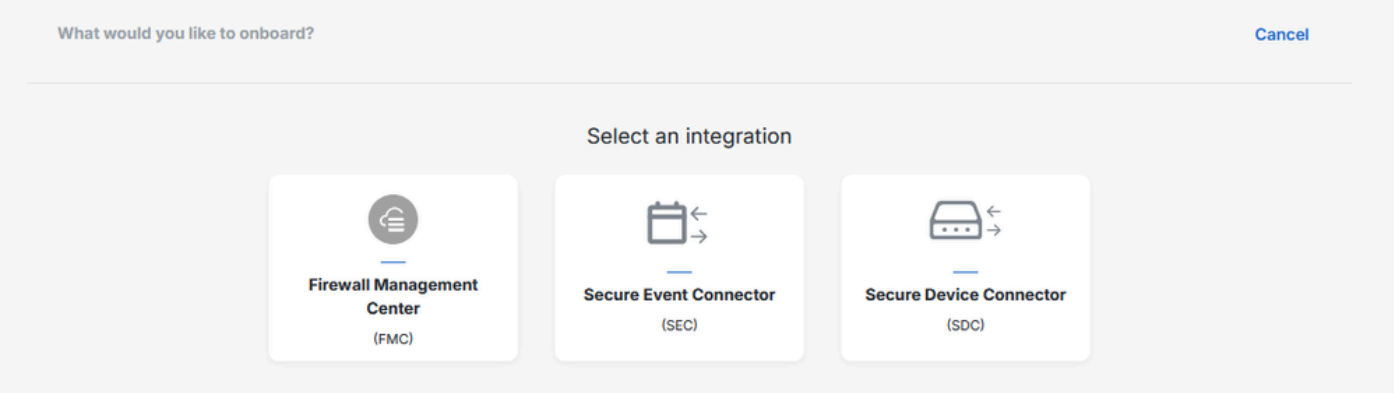
Configurazione

Passaggio 1. Accedere al portale del cloud SCC:

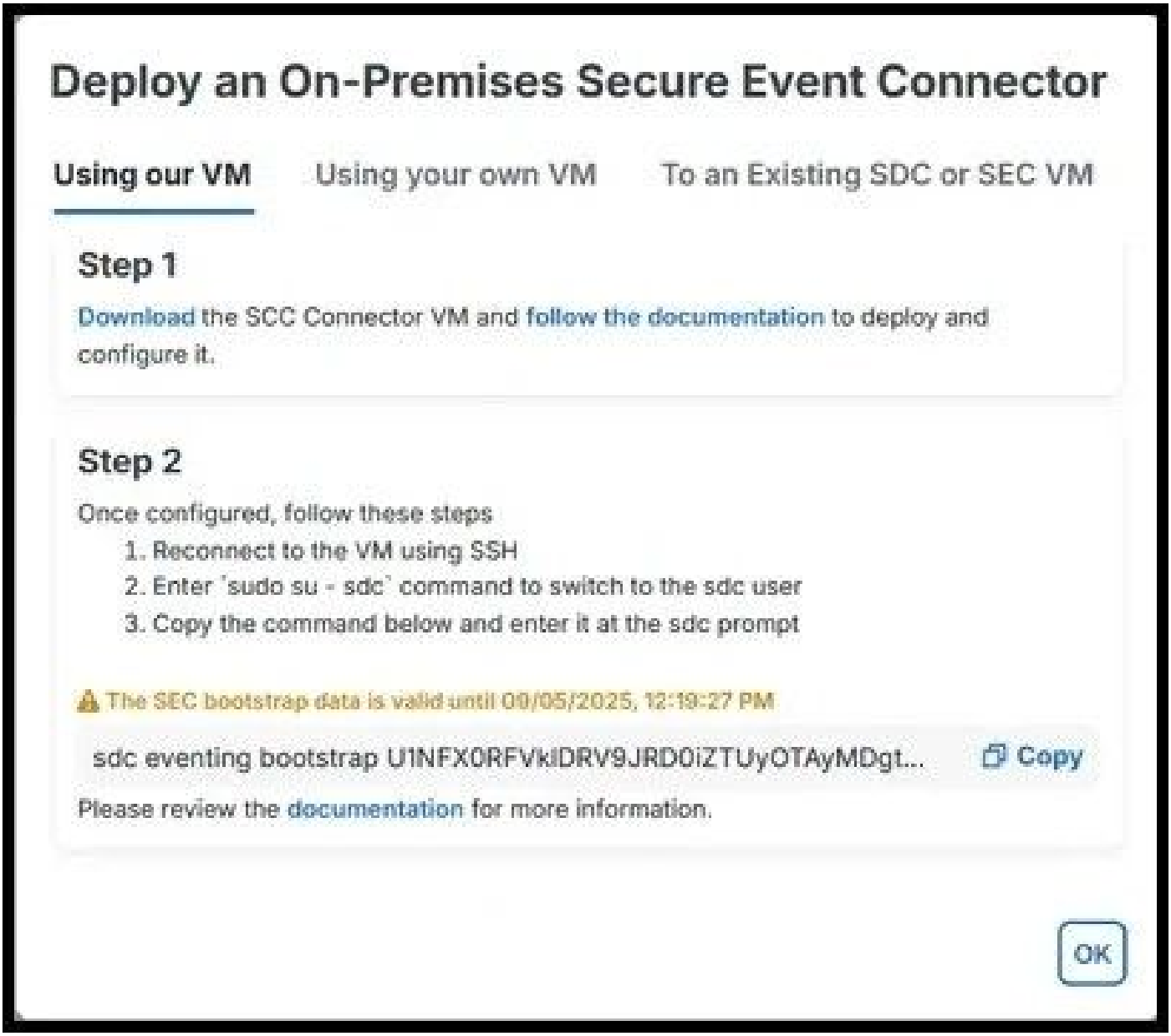
Passaggio 2. Dal menu a sinistra, scegliere Amministrazione e Secure Connectors:



Passaggio 3. Sul lato superiore destro, fare clic sull'icona più per incorporare un nuovo connettore e scegliere Secure Event Connector:



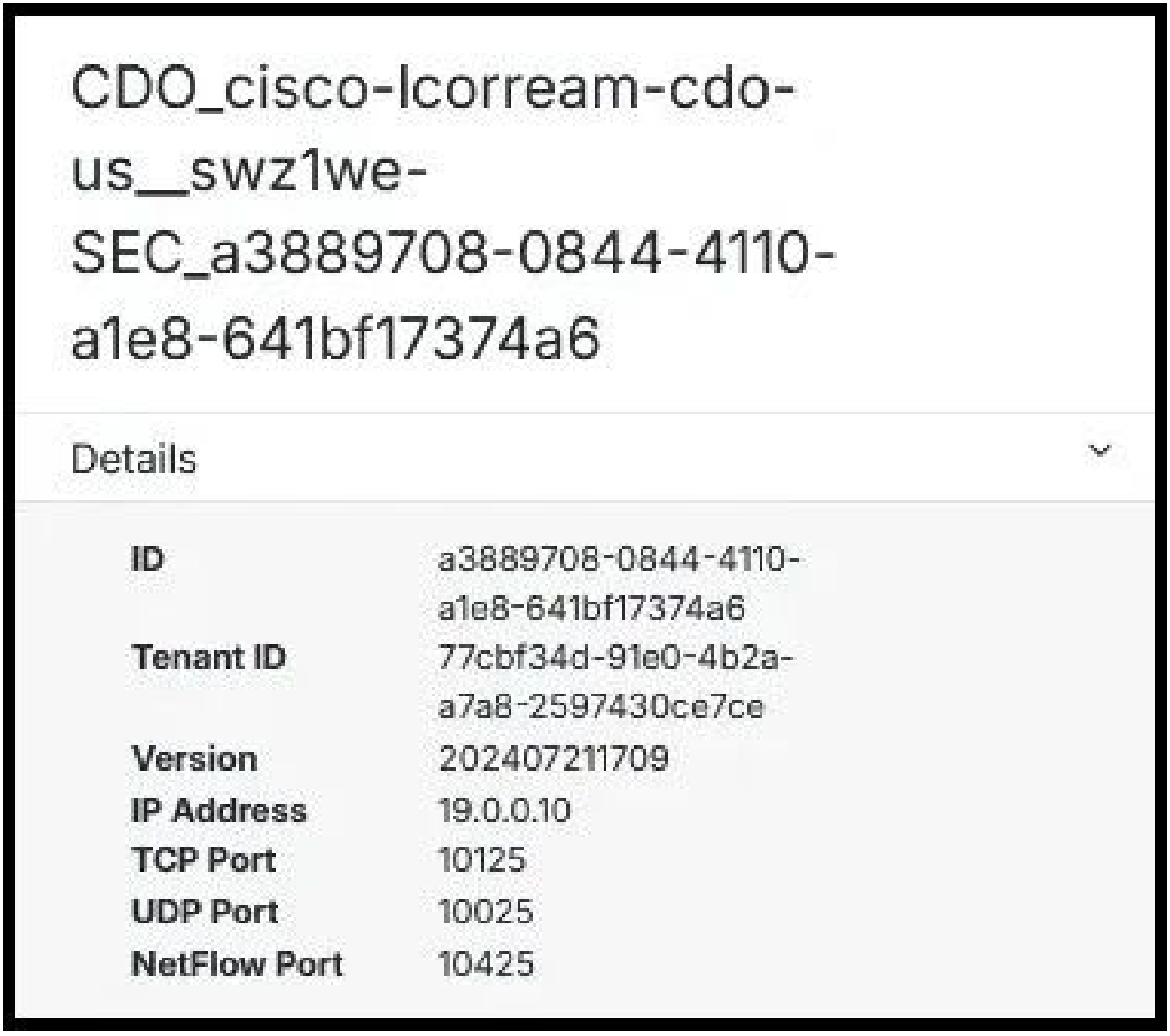
Passaggio 4. Utilizzare i passaggi per installare e avviare il connettore a seconda dell'opzione desiderata tra 'Utilizzo della VM', 'Utilizzo della VM personale' o 'A una VM SDC o SEC esistente':



Passaggio 5. Se il bootstrap viene eseguito correttamente, viene visualizzato un messaggio simile:

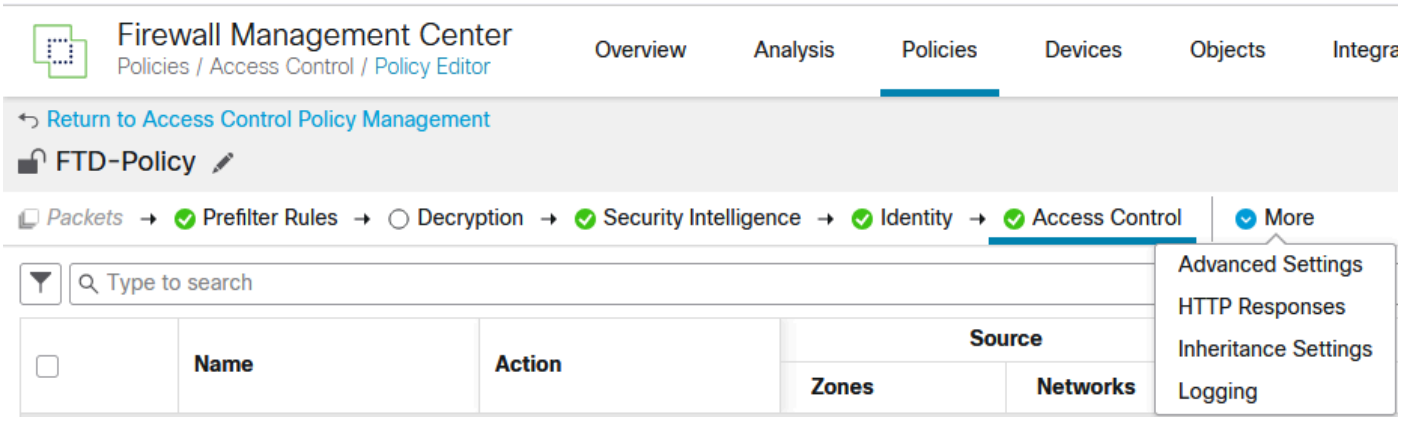
```
2025-06-09 05:41:56 [INFO] Bootstrap package processed successfully
2025-06-09 05:41:56 [INFO] Default AWS Region is us-west-2
2025-06-09 05:42:00 [INFO] Scanning for next available TCP port starting with 10125
2025-06-09 05:42:00 [INFO] TCP port found and set to 10125
2025-06-09 05:42:00 [INFO] Scanning for next available UDP port starting with 10025
2025-06-09 05:42:00 [INFO] UDP port found and set to 10025
2025-06-09 05:42:00 [INFO] Scanning for next available Netflow port starting with 10425
2025-06-09 05:42:00 [INFO] Netflow port found and set to 10425

WARNING! Your credentials are stored unencrypted in '/var/lib/sdc/.docker/config.json'.
Configure a credential helper to remove this warning. See
https://docs.docker.com/go/credential-store/

5a99d0351c1ae91cd790dcf18ee1d0594d37fcfaf5a1725473eeed042342a567
2025-06-09 05:42:06 [INFO] The SEC is up and running - You should be all set to go
2025-06-09 05:42:08 [INFO] Your SEC has been successfully bootstrapped! Please verify that everything is working within
the SCC UI, and thank you for being a customer
sdc@lcorream-sdc:~$
```

Passaggio 6. Dopo aver distribuito e avviato il connettore, le informazioni sulla porta sono visibili nel portale SCC:

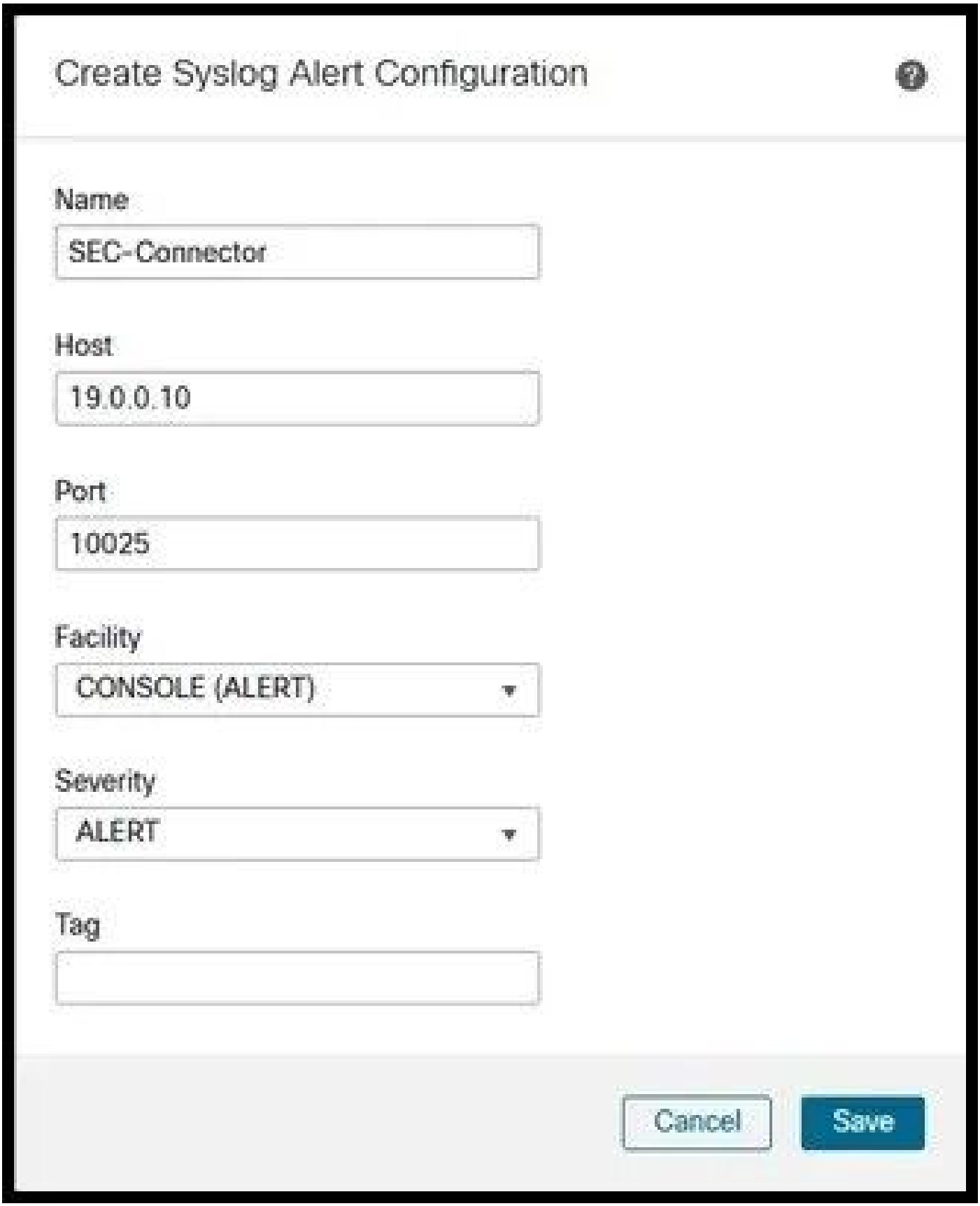


Passaggio 7. In Cisco Secure Firewall Management Center (FMC), passare a Policy e quindi a Controllo accesso. Scegliere il criterio corrispondente ai dispositivi da caricare.

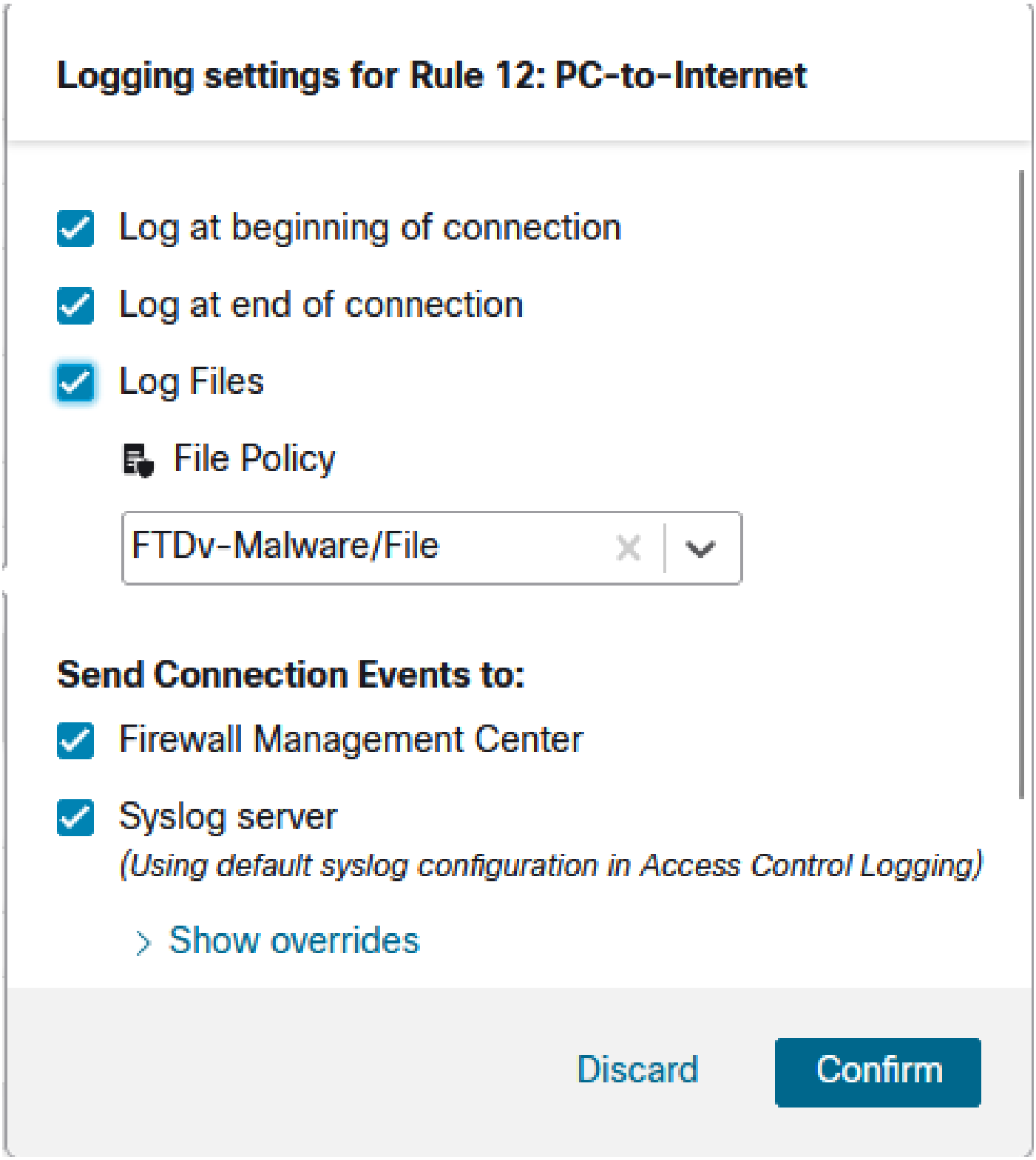
Passaggio 8. Scegliere Altro, quindi Log:



Passaggio 9. Abilitare l'opzione di avviso Invia utilizzando syslog specifico e aggiungere un nuovo avviso syslog. Utilizzare l'indirizzo IP (Internet Protocol) e le informazioni sulla porta ottenute dal connettore SEC nel portale SCC:



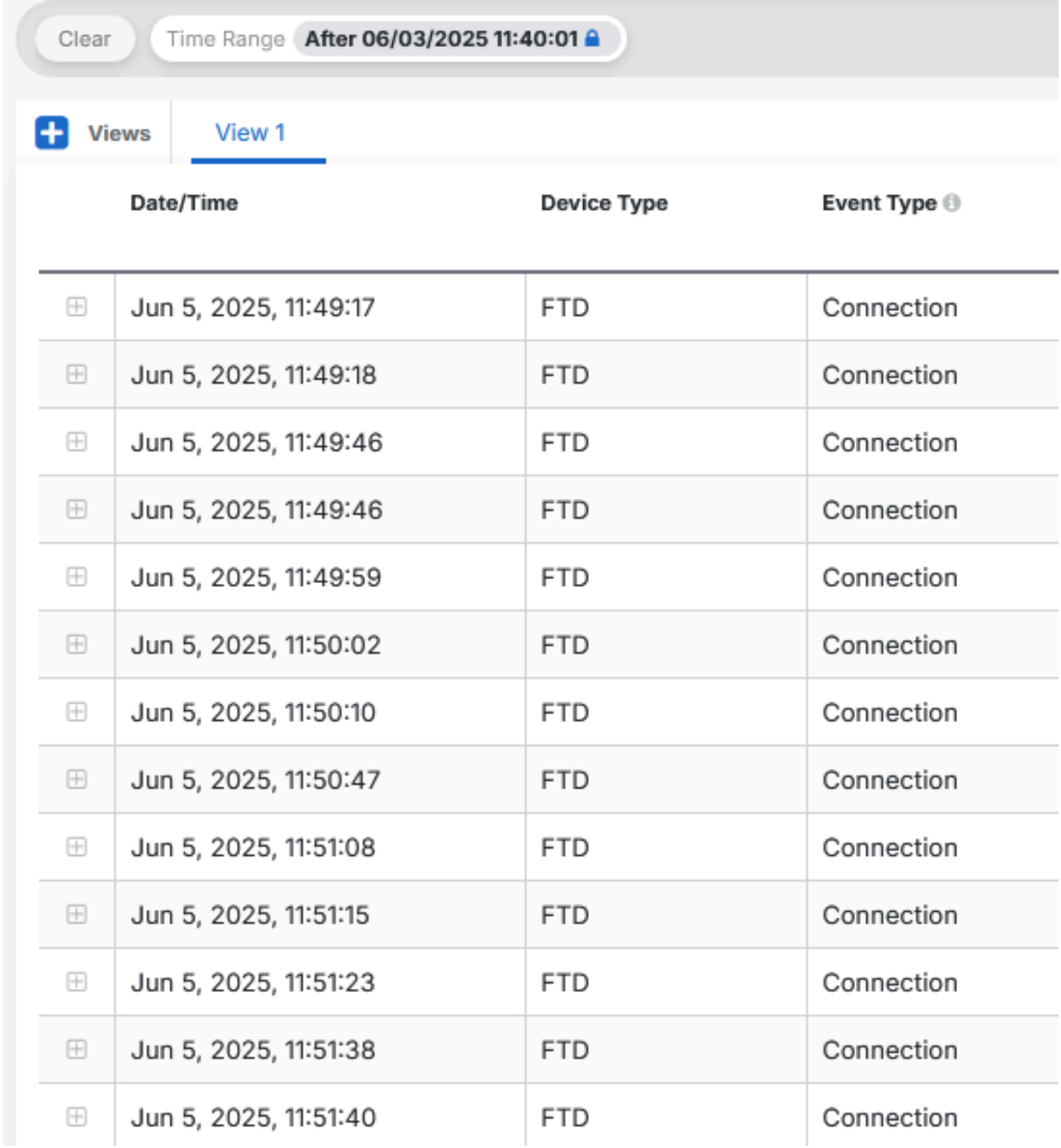
Passaggio 10. Di nuovo, in Access Control Policy, modificare le singole regole per inviare gli eventi al server Syslog:



Passaggio 11. Distribuire le modifiche apportate all'FTD in modo da consentire al firewall di avviare la registrazione degli eventi.

Verifica

Per verificare che le modifiche siano state eseguite correttamente e che la registrazione degli eventi sia in corso, passare a Eventi & registri e registrazione eventi nel portale SCC e confermare che gli eventi sono visibili:



Risoluzione dei problemi

Su FTD, eseguire un'acquisizione dei pacchetti sul dispositivo utilizzando l'interfaccia di gestione corrispondente al traffico che naviga fino al secondo per acquisire il traffico syslog:

```
> capture-traffic

Please choose domain to capture traffic from:
  0 - eth0
```

```
  1 - Global

Selection? 0

Warning: Blanket capture may cause high CPU usage and reduced throughput, use selective filtering to re
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: host 19.0.0.10 port 10025
Starting traffic capture, press ctrl + c to exit (Maximum 1,000,000 packets will be captured)
HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: can't parse filter expression: syntax error
Exiting.

> capture-traffic

Please choose domain to capture traffic from:
  0 - eth0
  1 - Global

Selection? 0

Warning: Blanket capture may cause high CPU usage and reduced throughput, use selective filtering to re
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: host 19.0.0.10 and port 10025
Starting traffic capture, press ctrl + c to exit (Maximum 1,000,000 packets will be captured)
HS_PACKET_BUFFER_SIZE is set to 4.
10:43:00.191655 IP firepower.56533 > 19.0.0.10.10025: UDP, length 876
10:43:01.195318 IP firepower.56533 > 19.0.0.10.10025: UDP, length 1192
10:43:03.206738 IP firepower.56533 > 19.0.0.10.10025: UDP, length 809
10:43:08.242948 IP firepower.56533 > 19.0.0.10.10025: UDP, length 1170
```

Dalla macchina virtuale SEC, verificare che la macchina virtuale disponga di connettività Internet. Eseguire il comando sdc troubleshoot per generare un pacchetto di risoluzione dei problemi che può essere usato per controllare il file lar.log per un'ulteriore diagnosi.

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).