

Esempio di configurazione del filtro URL su un sistema FireSIGHT

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Richiesta della licenza del filtro URL](#)

[Requisito porta](#)

[Componenti usati](#)

[Configurazione](#)

[Abilitazione del filtro URL su FireSIGHT Management Center](#)

[Applicazione della licenza del filtro URL a un dispositivo gestito](#)

[Esclusione di un sito specifico dalla categoria URL bloccati](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare il filtro URL sul sistema FireSIGHT. La funzionalità di filtro URL di FireSIGHT Management Center consente di scrivere una condizione in una regola di controllo dell'accesso per determinare il traffico che attraversa una rete in base alle richieste di URL non crittografati da parte degli host monitorati.

Prerequisiti

Requisiti

In questo documento vengono descritti alcuni requisiti specifici per la licenza del filtro URL e per la porta.

Richiesta della licenza del filtro URL

Un centro di gestione FireSIGHT richiede una licenza per il filtro URL per contattare periodicamente il cloud per un aggiornamento delle informazioni URL. È possibile aggiungere condizioni URL basate sulla categoria e sulla reputazione per accedere alle regole di controllo senza una licenza per il filtro URL; tuttavia, per applicare la policy di controllo dell'accesso, è necessario prima aggiungere una licenza di filtro URL al centro di gestione FireSIGHT e quindi abilitarla sui dispositivi interessati dalla policy.

Se una licenza del filtro URL scade, le regole di controllo dell'accesso con condizioni di URL basate sulla categoria e sulla reputazione cessano di filtrare gli URL e il centro di gestione FireSIGHT non contatta più il servizio cloud. Senza una licenza per il filtro URL, è possibile

impostare singoli URL o gruppi di URL in modo da consentire o bloccare, ma non è possibile usare la categoria dell'URL o i dati sulla reputazione per filtrare il traffico di rete.

Requisito porta

Un sistema FireSIGHT utilizza le porte 443/HTTPS e 80/HTTP per comunicare con il servizio cloud. La porta 443/HTTPS deve essere aperta bidirezionalmente e l'accesso in entrata alla porta 80/HTTP deve essere consentito sul centro di gestione FireSIGHT.

Componenti usati

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

- Appliance FirePOWER: Serie 7000, serie 8000
- Appliance virtuale Next-Generation Intrusion Prevention System (NGIPS)
- Adaptive Security Appliance (ASA) FirePOWER
- Software Sourcefire versione 5.2 o successive

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.

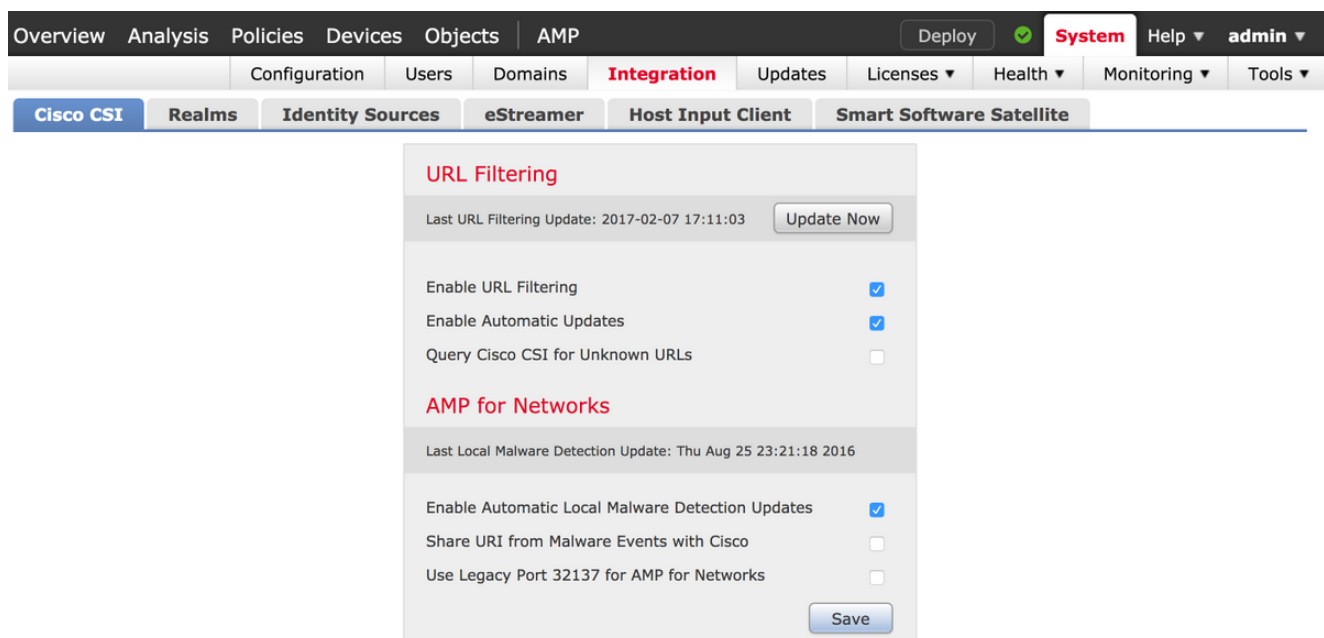
Configurazione

Abilitazione del filtro URL su FireSIGHT Management Center

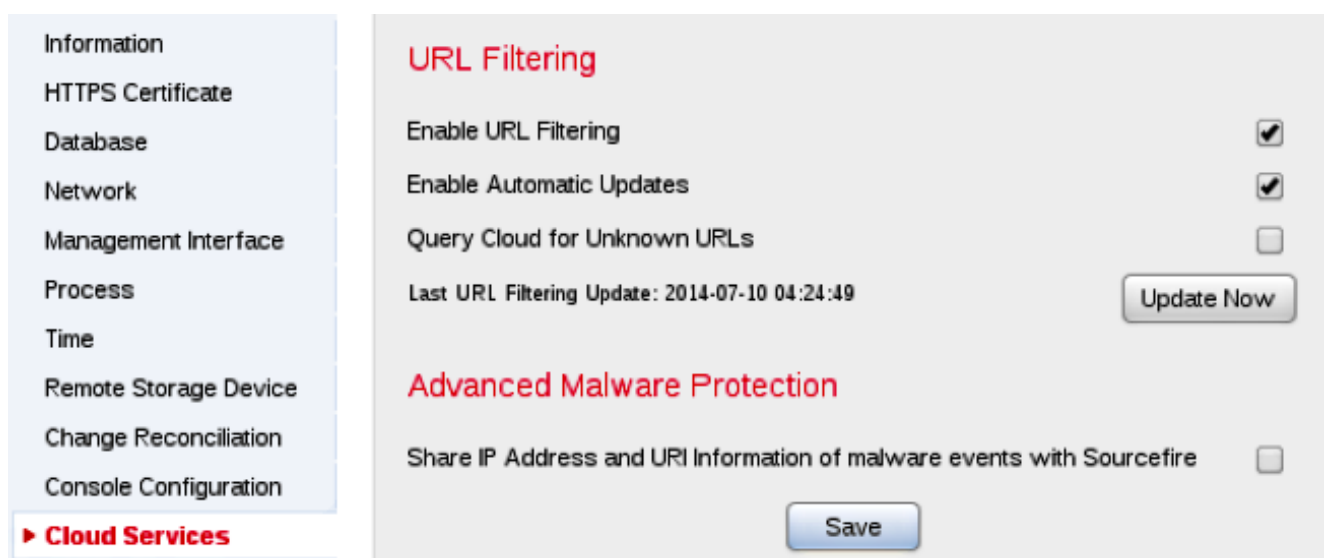
Per abilitare il filtro URL, procedere come segue:

1. Accedere all'interfaccia utente Web di FireSIGHT Management Center.
2. La navigazione è diversa in base alla versione del software in uso:

Nella versione 6.1.x, scegliere **Sistema > Integrazione > Cisco CSI**.



Nella versione 5.x, scegliere **Sistema > Locale > Configurazione**. Scegliere **Servizi cloud**.



3. Per abilitare il filtro URL, selezionare la casella di controllo **Abilita filtro URL**.
4. Se lo si desidera, selezionare la casella di controllo **Abilita aggiornamenti automatici** per abilitare gli aggiornamenti automatici. Questa opzione consente al sistema di contattare regolarmente il servizio cloud per ottenere aggiornamenti dei dati URL nei set di dati locali dell'accessorio.

Nota: Sebbene il servizio cloud in genere aggiorni i propri dati una volta al giorno, se si abilitano gli aggiornamenti automatici, il centro di gestione FireSIGHT deve controllare ogni 30 minuti per assicurarsi che le informazioni siano sempre aggiornate. Sebbene gli aggiornamenti giornalieri siano in genere di piccole dimensioni, se sono trascorsi più di cinque giorni dall'ultimo aggiornamento, il download dei nuovi dati del filtro URL potrebbe richiedere fino a 20 minuti. Una volta scaricati gli aggiornamenti, l'esecuzione dell'aggiornamento stesso potrebbe richiedere fino a 30 minuti.

5. Facoltativamente, selezionare la casella di controllo **Query su cloud per URL sconosciuti** per ottenere URL sconosciuti. Questa opzione consente al sistema di eseguire una query sul cloud Sourcefire quando un utente della rete monitorata tenta di individuare un URL non

presente nel set di dati locale. Se il cloud non conosce la categoria o la reputazione di un URL, o se il FireSIGHT Management Center non è in grado di contattare il cloud, l'URL non corrisponde alle regole di controllo dell'accesso con le condizioni dell'URL basate sulla categoria o sulla reputazione.

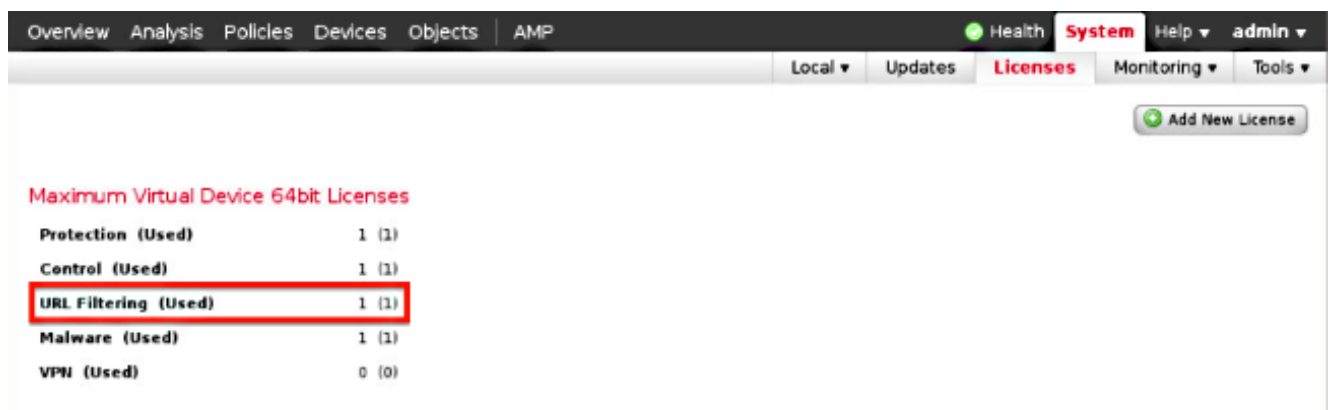
Nota: Non è possibile assegnare categorie o reputazione agli URL manualmente. Disabilitare questa opzione se non si desidera che gli URL non classificati vengano catalogati dal cloud Sourcefire, ad esempio per motivi di privacy.

6. Fare clic su **Salva**. Le impostazioni del filtro URL sono state salvate.

Nota: In base alla durata dell'ultima abilitazione del filtro URL o, se è la prima volta che il filtro URL è stato abilitato, un centro di gestione FireSIGHT recupera i dati del filtro URL dal servizio cloud.

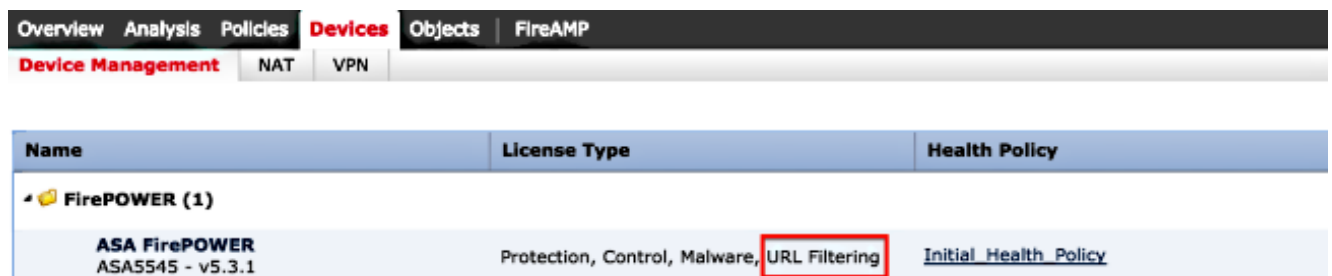
Applicazione della licenza del filtro URL a un dispositivo gestito

1. Verificare che la licenza del filtro URL sia installata sul centro di gestione FireSIGHT. Per un elenco delle licenze, andare alla pagina **Sistema > Licenze**.



Maximum Virtual Device 64bit Licenses	
Protection (Used)	1 (1)
Control (Used)	1 (1)
URL Filtering (Used)	1 (1)
Malware (Used)	1 (1)
VPN (Used)	0 (0)

2. Andare alla pagina **Dispositivi > Gestione dispositivi** e verificare se la licenza del filtro URL è applicata al dispositivo di monitoraggio del traffico.

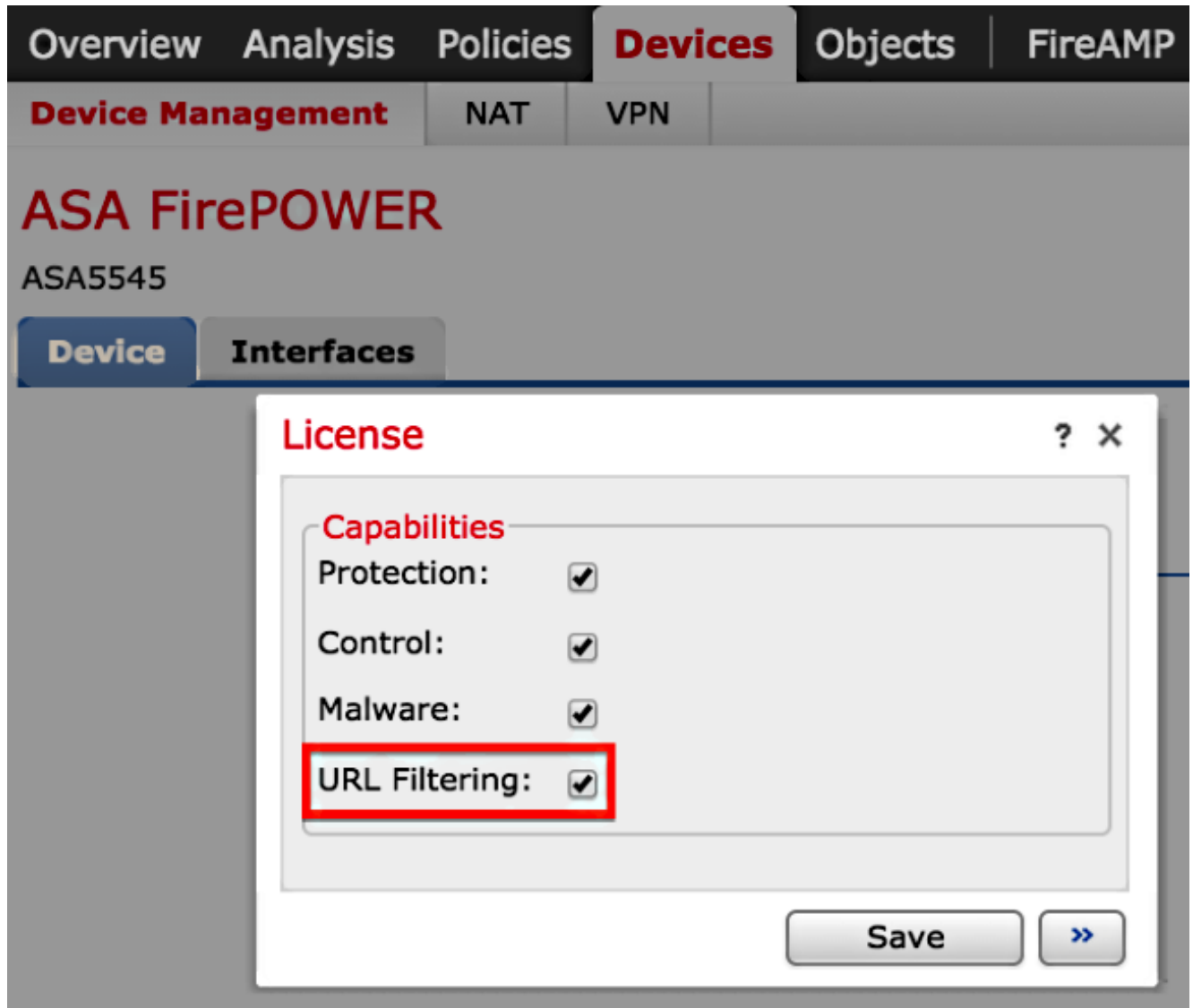


Name	License Type	Health Policy
FirePOWER (1)		
ASA FirePOWER ASA5545 - v5.3.1	Protection, Control, Malware, URL Filtering	Initial Health Policy

3. Se la licenza del filtro URL non è applicata a un dispositivo, fare clic sull'icona a forma di **matita** per modificare le impostazioni. L'icona si trova accanto al nome del dispositivo.



4. È possibile abilitare la licenza del filtro URL su un dispositivo dalla scheda **Dispositivi**.



5. Dopo aver attivato una licenza e aver salvato le modifiche, è necessario fare clic su **Apply Changes** (Applica modifiche) per applicare la licenza sul dispositivo gestito.

 **You have unapplied changes**



Esclusione di un sito specifico dalla categoria URL bloccati

FireSIGHT Management Center non consente di avere una classificazione locale degli URL che sostituiscono la classificazione di categoria predefinita fornita da Sourcefire. Per eseguire questa operazione, è necessario utilizzare un criterio di controllo dell'accesso. Nelle istruzioni che seguono viene descritto come utilizzare un oggetto URL in una regola di controllo di accesso per escludere un sito specifico da una categoria di blocco.

1. Andare alla pagina **Oggetti > Gestione oggetti**.
2. **Scegliere Oggetti singoli** per URL e fare clic sul pulsante **Aggiungi URL**. Viene visualizzata la

finestra Oggetti URL.

URL Objects

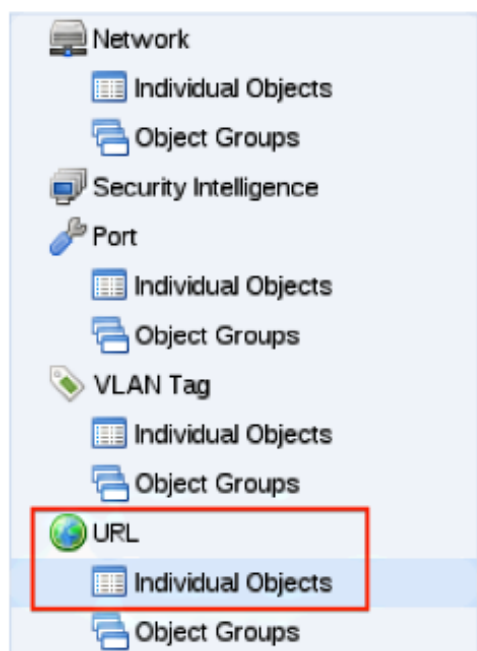


Name:

URL:

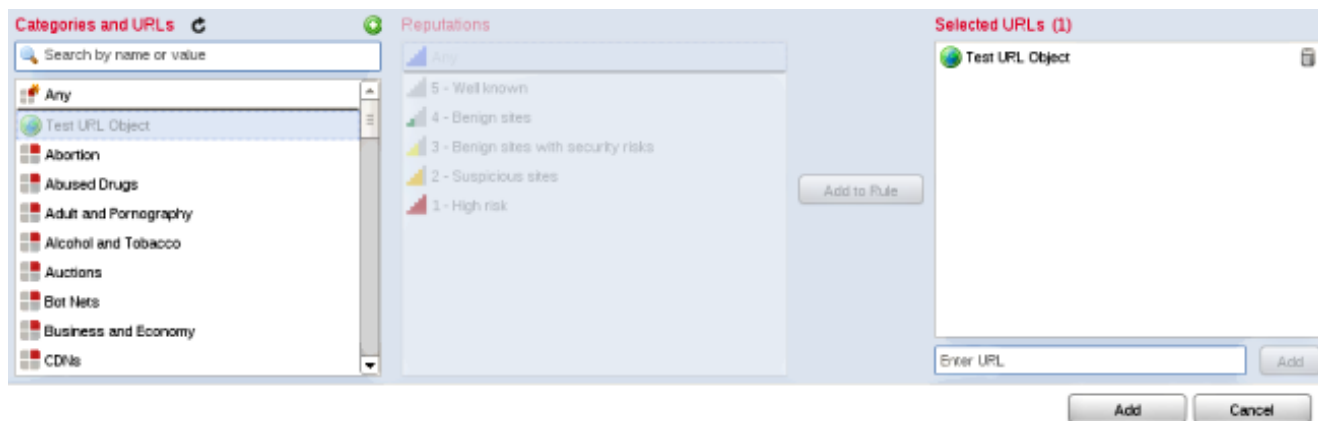
Overview Analysis Policies Devices **Objects** FireAMP

Object Management



Name	Value
Test URL Object	http://www.cisco.com

3. Dopo aver salvato le modifiche, scegliere **Criteri > Controllo di accesso** e fare clic sull'icona a forma di **matita** per modificare il criterio di controllo di accesso.
4. Fare clic su **Aggiungi regola**.
5. Aggiungere l'oggetto URL alla regola con l'azione **Consenti** e posizionarlo sopra la regola Categoria URL, in modo che la relativa azione della regola venga valutata per prima.



6. Dopo aver aggiunto la regola, fare clic su **Salva e applica**. Le nuove modifiche vengono salvate e i criteri di controllo dell'accesso vengono applicati agli accessori gestiti.

Verifica

Per informazioni sulla verifica o la risoluzione dei problemi, fare riferimento all'articolo **Risoluzione dei problemi relativi al filtro URL sul sistema FireSIGHT** collegato nella sezione Informazioni correlate.

Risoluzione dei problemi

Per informazioni sulla verifica o la risoluzione dei problemi, consultare **Risoluzione dei problemi relativi al filtro URL sul sistema FireSIGHT** nella sezione Informazioni correlate.

Informazioni correlate

- [Risoluzione dei problemi relativi al filtro URL sul sistema FireSIGHT](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

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).