Configurazione del timeout di connessione per il traffico specifico sull'appliance ASA con ASDM

Sommario

Introduzione

In questo documento viene descritto come configurare il timeout di connessione su ASA e ASDM per un protocollo applicativo specifico, ad esempio HTTP, HTTPS, FTP o altri protocolli. Il timeout di connessione è il periodo di inattività trascorso il quale un firewall o un dispositivo di rete termina una connessione inattiva per liberare risorse e migliorare la sicurezza. In anticipo, la prima domanda è: Quali sono i requisiti per questa configurazione? Se le applicazioni dispongono di impostazioni TCP keepalive appropriate, spesso non è necessario configurare il timeout di connessione su un firewall. Tuttavia, se le applicazioni non dispongono di impostazioni keepalive o configurazioni di timeout appropriate, in questo caso la configurazione del timeout di connessione su un firewall è fondamentale per la gestione delle risorse, il miglioramento della sicurezza, il miglioramento delle prestazioni di rete, la garanzia della conformità e l'ottimizzazione dell'esperienza utente.

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Access Control List (ACL)

- Criterio servizio
- Timeout connessione

Componenti usati

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

- ASA 9.17(1)
- ASDM 7.17(1)

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.

Valori predefiniti

Nota: timeout predefinito

Il timeout embrionale predefinito è 30 secondi.

Il timeout di inattività semichiuso predefinito è 10 minuti.

Il valore predefinito di dcd max_retries è 5.

Il valore predefinito di dcd retry_interval è 15 secondi.

Il timeout di inattività tcp predefinito è 1 ora.

Il timeout di inattività udp predefinito è di 2 minuti.

Il timeout di inattività icmp predefinito è 2 secondi.

Il timeout predefinito di inattività sip è 30 minuti.

Il timeout predefinito di inattività di sip_media è di 2 minuti.

Il timeout predefinito di esp e ha inattività è 30 secondi.

Per tutti gli altri protocolli, il timeout di inattività predefinito è di 2 minuti.

Per non impostare mai il timeout, immettere 0:0:0.

Configura timeout connessione

ASDM

Se un determinato traffico ha una tabella di connessione, ha un timeout di inattività specifico; ad esempio, in questo articolo viene modificato il timeout di connessione per il traffico DNS.

Di seguito sono elencate molte opzioni per configurare il timeout di connessione per il traffico specifico, in base al diagramma di rete del traffico:

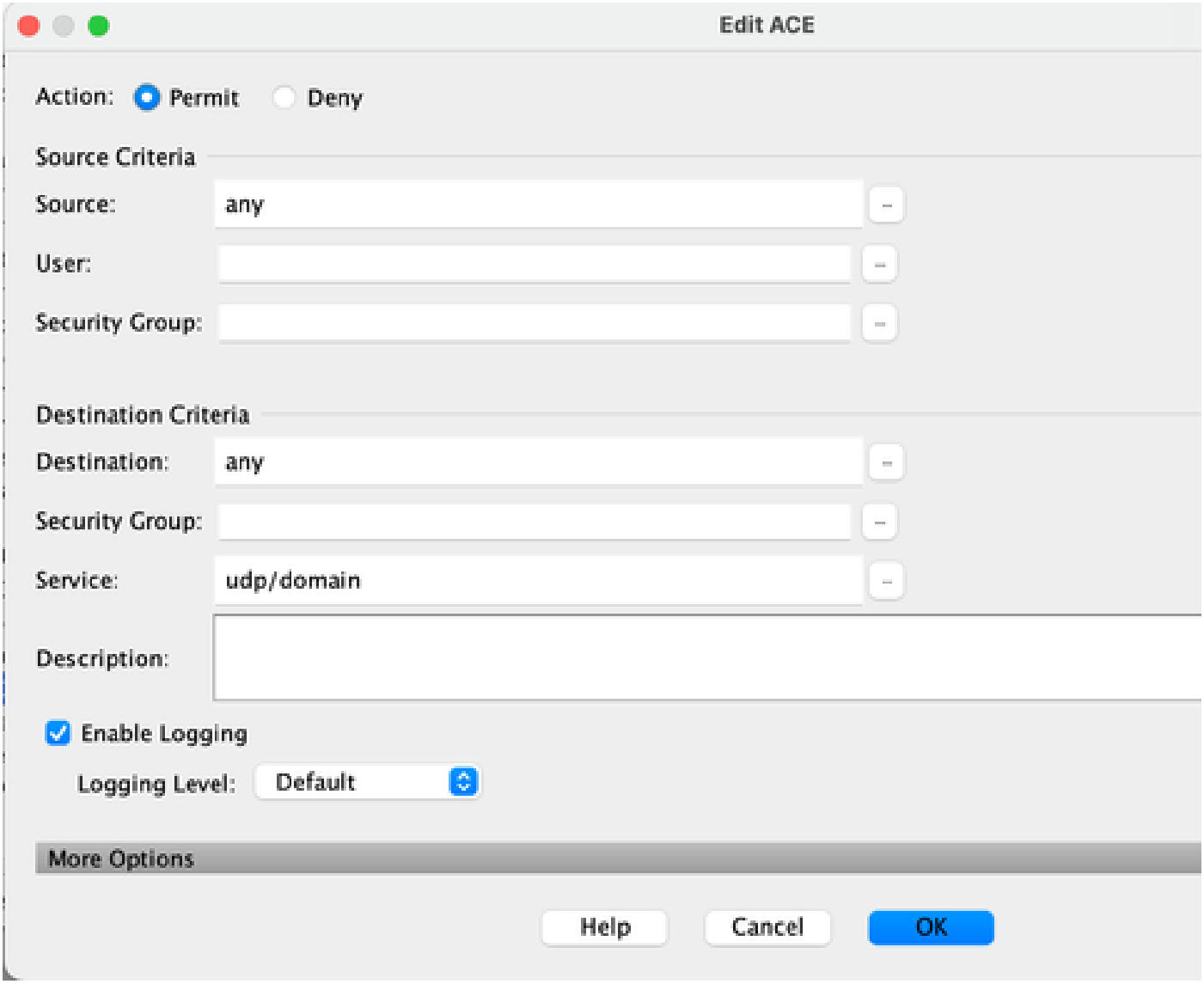
Client — [Interfaccia: MNG] Firewall [Interfaccia: OUT] — Server

È possibile assegnare un ACL all'interfaccia.

Passaggio 1: creazione di un ACL

È possibile assegnare origine, destinazione o servizio

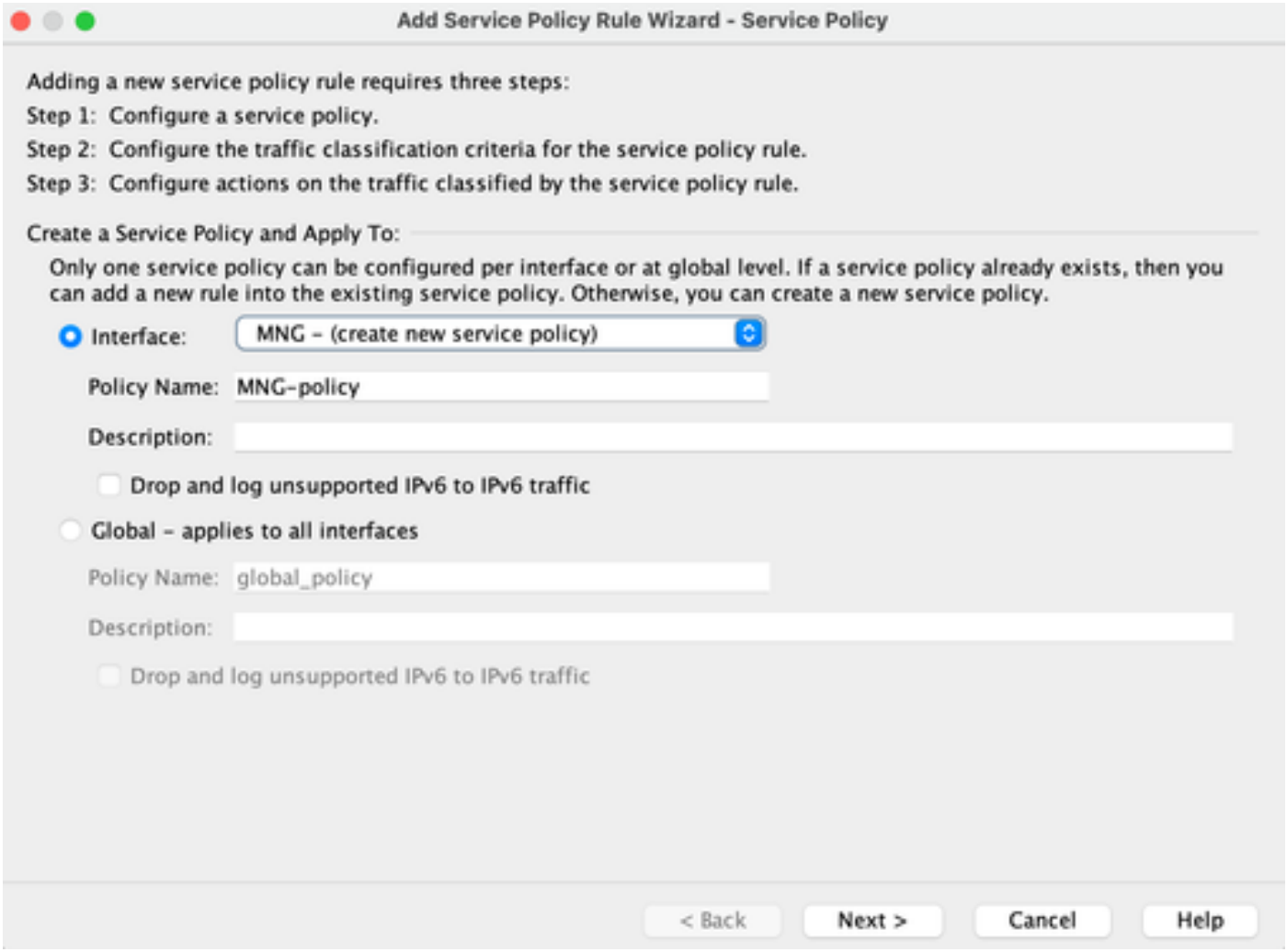
ASDM > Configurazione > Firewall > Avanzate > ACL Manager



Passaggio 2: Creare la regola dei criteri del servizio

È possibile saltare l'ultimo passaggio se si dispone già dell'ACL oppure assegnare uno di questi parametri (origine, destinazione o servizio) ai criteri del servizio per l'interfaccia.

ASDM > Configurazione > Firewall > Regole dei criteri di servizio

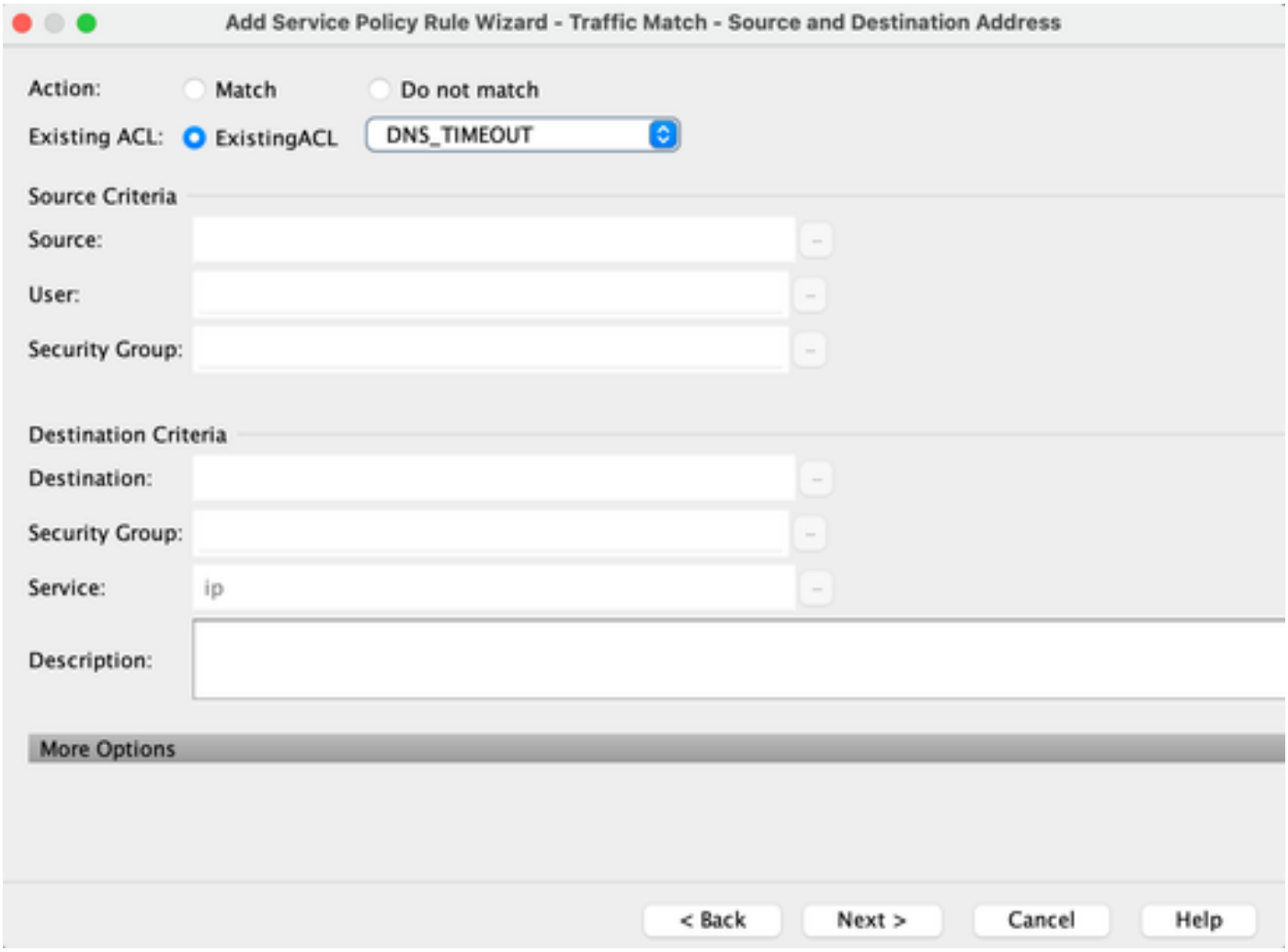


Fase 3. Creare la classe del traffico

È possibile scegliere l'indirizzo IP di origine e di destinazione (usa l'ACL)

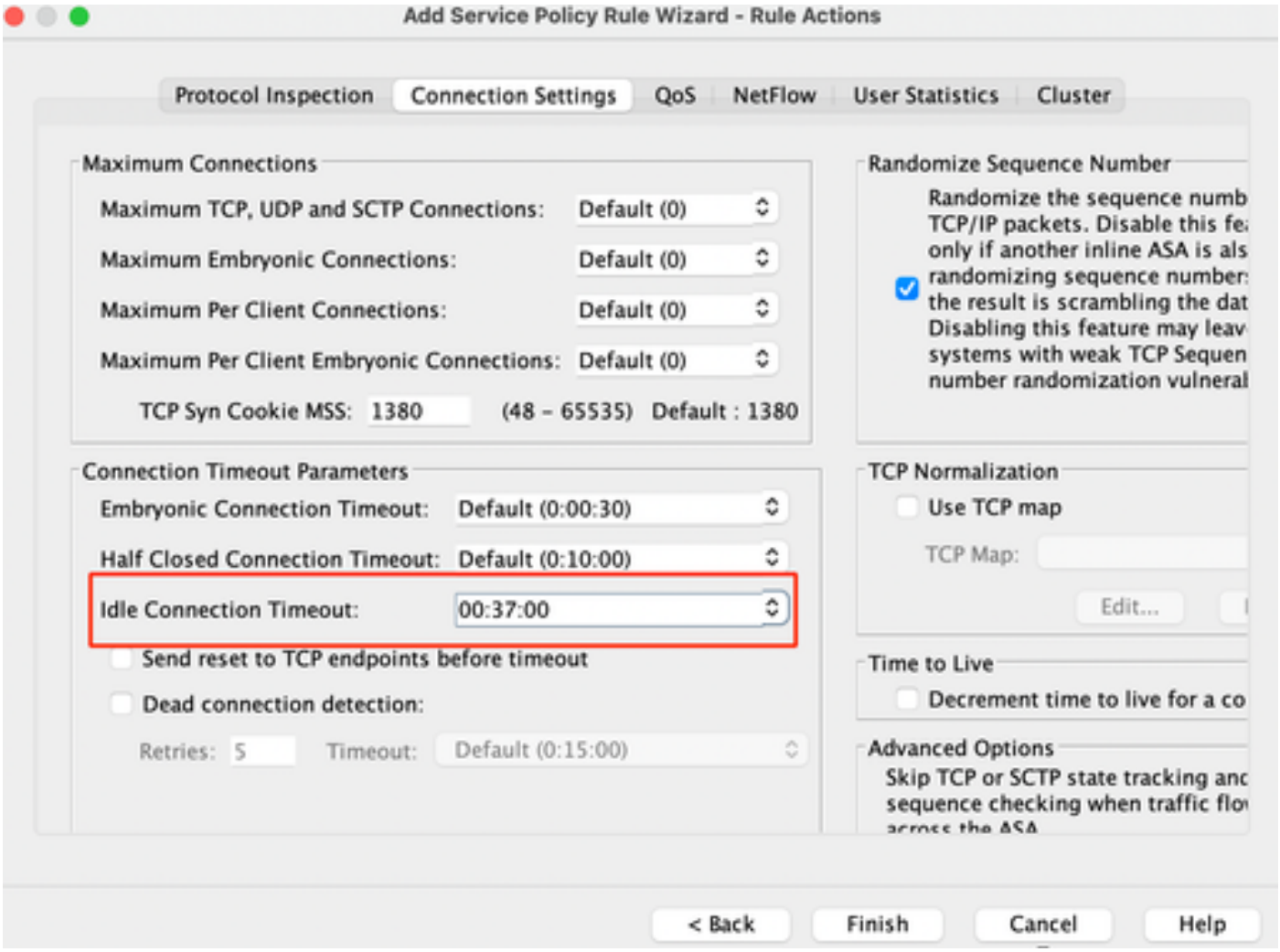
Passaggio 4: Assegnazione dell'ACL

In questo passaggio è possibile assegnare l'ACL esistente o selezionare condizioni di corrispondenza (origine, destinazione o servizio)



Passaggio 5: configurare il parametro Timeout di inattività

In base al formato valido HH:MM:SS configurare il timeout di inattività.



Cancella le connessioni per quel particolare traffico:

#clear conn addressImmettere un indirizzo IP o un intervallo di indirizzi IP #clear conn protocolImmettere questa parola chiave per cancellare solo le connessioni SCP/TCP/UDP

ASA CLI

È possibile configurare tutte queste impostazioni dalla CLI:

ACL: access-list DNS_TIMEOUT extended permette udp any any eq domain Mappa classi: class-map classe MNG match access-list DNS_TIMEOUT

Policy-map:

policy-map MNG-policy
classe MNG-class
imposta timeout connessione inattivo 0:37:00

Applicare la mappa dei criteri all'interfaccia:

service-policy MNG-policy interface

Verifica

Suggerimento: se eseguiamo questo comando, possiamo confermare il timeout della connessione del traffico DNS:

ASA CLI > modalità abilitazione > show conn long

Esempio: show conn long address 192.168.1.1

UDP MNG: 192.168.1.1/53 (192.168.1.1/53) OUT: 10.10.10.30/63327 (10.10.10.30/63327), flag -, idle 17s, uptime 17s, timeout 2m0s, byte 36

UDP MNG: 192.168.1.1/53 (192.168.1.1/53) OUT: 10.10.10.30/62558 (10.10.10.30/62558), flag -, idle 40s, uptime 40s, timeout 2m0s, byte 36

Quindi, dopo la configurazione, è possibile confermare la configurazione del timeout di inattività:

Esempio: show conn long address 192.168.1.1

UDP MNG: 192.168.1.1/53 (192.168.1.1/53) OUT: 10.10.10.30/63044 (10.10.10.30/63044), flag -, idle 8s, uptime 8s, timeout 37m0s, byte 37

UDP MNG: 192.168.1.1/53 (192.168.1.1/53) OUT: 10.10.10.30/63589 (10.10.10.30/63589), flag -, idle 5s, uptime 5s, timeout 37m0s, byte 41

Riferimenti

Che cosa sono le impostazioni di connessione

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).