Configura protezione frame di gestione 802.11w su WLC

Sommario

Introduzione

Questo documento descrive i dettagli relativi alla protezione del frame di gestione IEEE 802.11w e alla sua configurazione sul Cisco Wireless LAN Controller (WLC).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di Cisco WLC con codice 7.6 o versioni successive.

Componenti usati

Le informazioni di questo documento si basano sulla WLC 5508 con codice 7.6.

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

Lo standard 802.11w ha lo scopo di proteggere i frame di controllo e di gestione e una serie di solidi frame di gestione da attacchi di falsificazione e ripetizione. I tipi di frame protetti includono i frame Disassociazione, Deautenticazione e Azione efficace, quali:

- Gestione dello spettro
- QoS (Quality of Service)
- Simbolo matematico
- Misurazione radio
- Transizione Fast Basic Service Set (BSS)

802.11w non esegue la crittografia dei frame, ma protegge i frame di gestione. Essa garantisce che i messaggi provengano da fonti legittime. A tale scopo, è necessario aggiungere un elemento MIC (Message Integrity Check). Lo standard 802.11w ha introdotto una nuova chiave chiamata IGTK (Integrity Group Temporal Key), utilizzata per proteggere i frame di gestione affidabili per il broadcast/multicast. Questo valore viene derivato come parte del processo handshake con chiave a quattro vie utilizzato con Wireless Protected Access (WPA). Ciò rende dot1x/Pre-Shared Key (PSK) un requisito quando è necessario utilizzare 802.11w. Non può essere utilizzato con SSID (Service Set Identifier) open/webauth.

Quando Management Frame Protection viene negoziato, l'Access Point (AP) cripta i valori GTK e IGTK nel frame EAPOL-Key che viene consegnato nel messaggio 3 dell'handshake a 4 vie. Se in seguito l'access point modifica il GTK, invia il nuovo GTK e il nuovo IGTK al client con l'utilizzo dell'handshake con chiave di gruppo. Aggiunge un MIC calcolato con il tasto IGTK.

MMIE (Management MIC Information Element)

802.11w introduce un nuovo elemento di informazione chiamato elemento di informazione Management MIC. Il formato dell'intestazione è quello mostrato nell'immagine.

1	1	2	6	8
Element ID	Length	KeyID	IPN	MIC

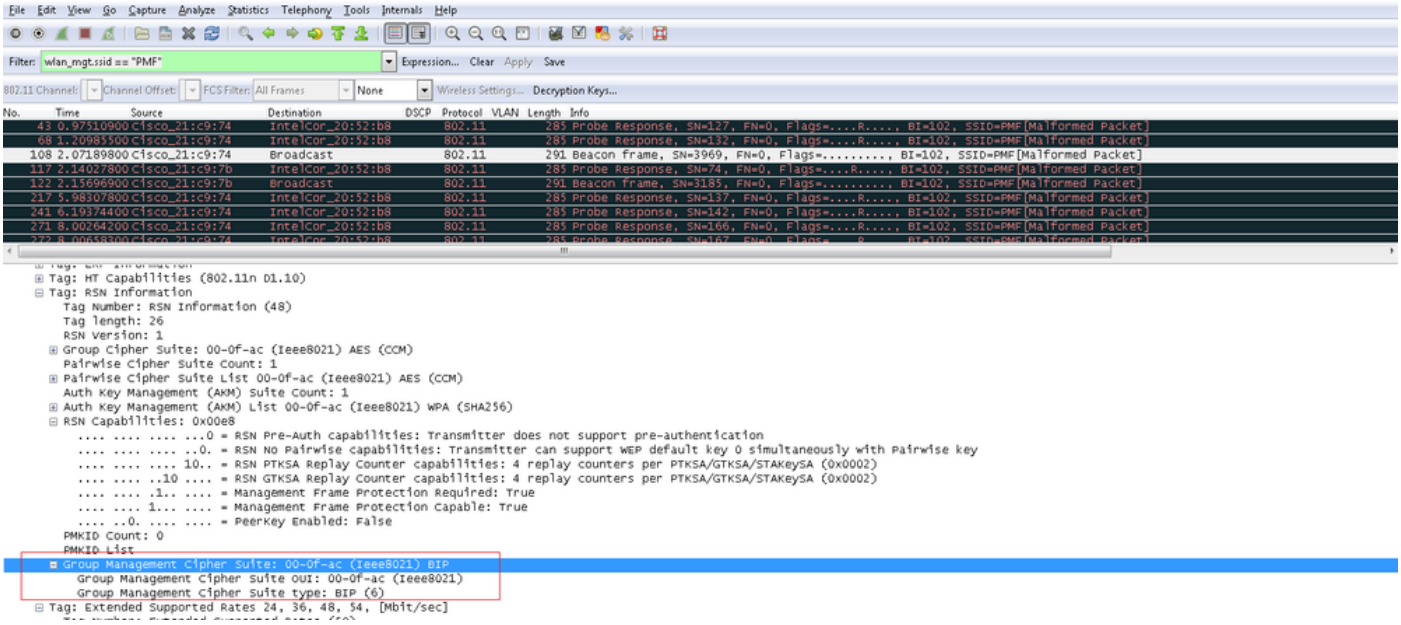
I principali settori che destano preoccupazione in questo caso sono l'ID elemento e il MIC. L'ID elemento per MMIE è 0x4c e serve come utile identificazione quando si analizzano le clip wireless.

Nota: MIC - Contiene il codice di integrità del messaggio calcolato nel frame di gestione. È importante notare che questo è aggiunto alla AP. Il client di destinazione ricalcola il MIC per il frame e lo confronta con quello inviato dall'access point. Se i valori sono diversi, il frame non valido viene rifiutato.

Modifiche a RSN IE

L'elemento RSN IE (Security Network Information Element) affidabile specifica i parametri di sicurezza supportati dall'access point. Lo standard 802.11w introduce un selettore di suite di cifratura per la gestione dei gruppi in RSN IE che contiene il selettore di suite di cifratura utilizzato

dall'access point per proteggere i frame di gestione affidabili di broadcast/multicast. Questo è il modo migliore per sapere se un punto di accesso utilizza lo standard 802.11w o meno. Questa condizione può essere verificata anche come mostrato nell'immagine.

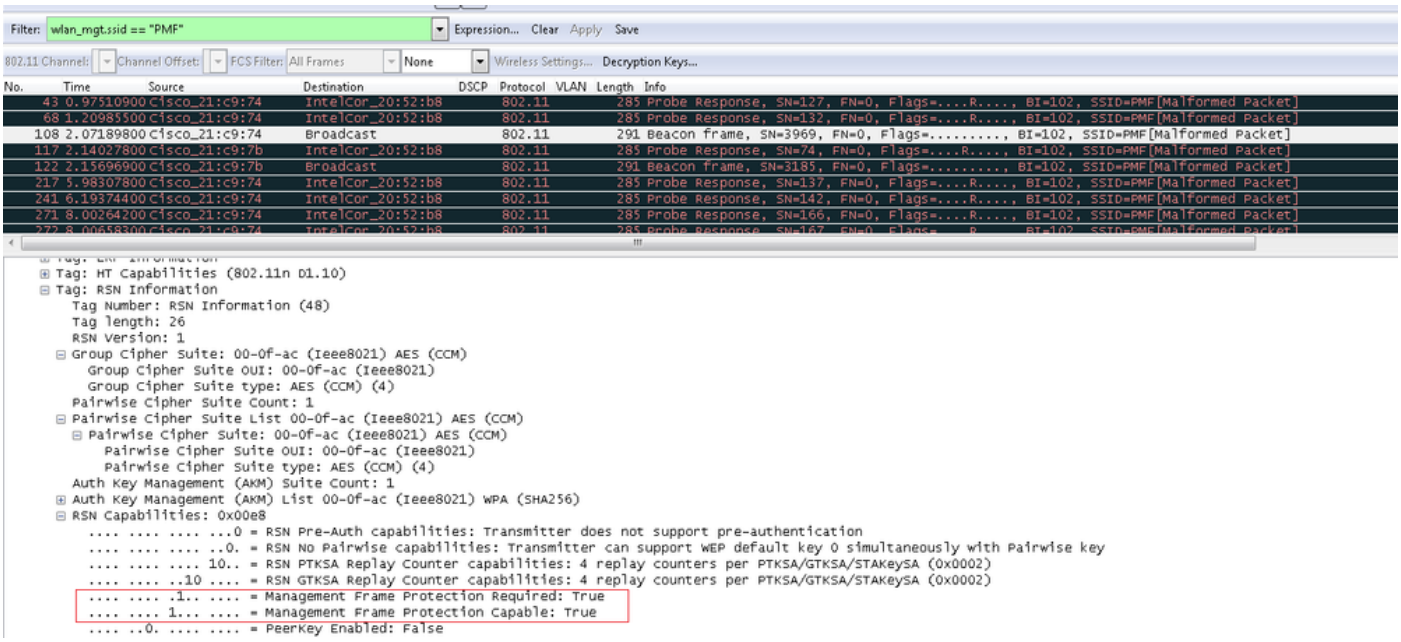


In questo campo è presente il campo group management cipher suite che indica che viene utilizzato 802.11w.

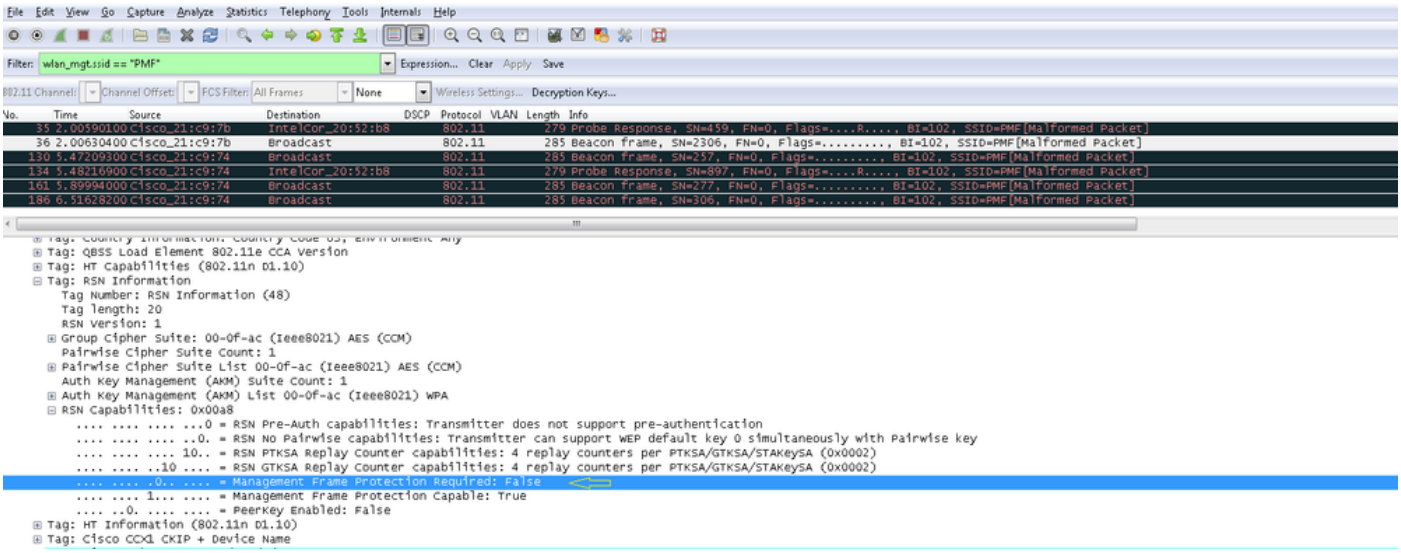
Sono state apportate modifiche anche nelle funzionalità RSN. I bit 6 e 7 vengono ora utilizzati per indicare parametri diversi per 802.11w.

- Bit 6: Management Frame Protection Required (MFPR) - Un STA imposta questo bit su 1 per annunciare che la protezione dei frame di gestione affidabili è obbligatoria.
- Bit 7: capacità di protezione del frame di gestione (MFPC) - Un STA imposta questo bit su 1 per annunciare che è abilitata la protezione dei frame di gestione affidabili. Quando l'access point imposta questa opzione, informa che supporta la protezione del frame di gestione.

Se si imposta la protezione del frame di gestione come richiesto nelle opzioni di configurazione, vengono impostati entrambi i bit 6 e 7. Come mostrato nell'immagine di acquisizione del pacchetto.



Tuttavia, se si imposta questa opzione su optional, viene impostato solo il bit 7, come mostrato nell'immagine.



Nota: il WLC aggiunge l'IE RSN modificato nelle risposte di associazione/riassociazione e l'AP aggiunge l'IE RSN modificato nei beacon e nelle risposte di richieste.

Vantaggi della protezione 802.11w Management Frame

- Protezione client

A tale scopo, è possibile aggiungere la protezione crittografica ai frame di disautenticazione e dissociazione. In questo modo si impedisce a un utente non autorizzato di lanciare un attacco Denial of Service (DOS) effettuando lo spoofing dell'indirizzo MAC degli utenti legittimi e inviando i frame di deautenticazione/dissociazione.

- Protezione AP

La protezione lato infrastruttura viene aggiunta con l'aggiunta di un meccanismo di protezione da ripristino della Security Association (SA), costituito da un tempo di ripristino dell'associazione e da una procedura SA-Query. Prima della versione 802.11w, se un access point ha ricevuto una richiesta di associazione o autenticazione da un client già associato, termina la connessione corrente e avvia una nuova connessione. Quando si utilizza la funzione MFP 802.11w, se la STA è associata e dispone di una protezione del frame di gestione negoziata, l'access point rifiuta la richiesta di associazione con codice di stato restituito 30 `Association request rejected temporarily; Try again later` al cliente.

Nella risposta associazione è incluso un elemento di informazioni sul tempo di ricomposizione dell'associazione che specifica un tempo di ricomposizione quando l'access point è pronto per accettare un'associazione con questo STA. In questo modo è possibile garantire che i client legittimi non vengano dissociati a causa di una richiesta di associazione falsificata.

Nota: il WLC (AireOS o 9800) ignora i frame di disassociazione o deautenticazione inviati dai client se non utilizzano 802.11w PMF. La voce client viene eliminata immediatamente alla ricezione di tale frame solo se il client utilizza PMF. In questo modo si evita la negazione del servizio da parte di dispositivi dannosi poiché non vi è sicurezza su tali frame senza PMF.

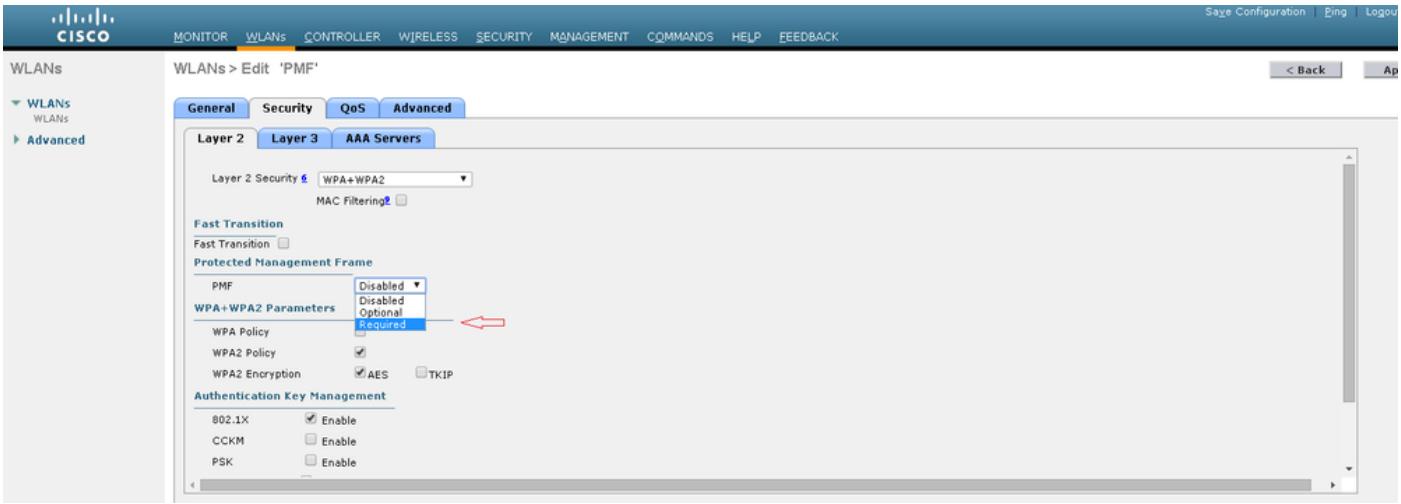
Requisiti per abilitare 802.11w

- 802.11w richiede che l'SSID sia configurato con dot1x o PSK.
- Lo standard 802.11w è supportato su tutti gli access point compatibili con 802.11n. Ciò significa che AP 1130 e 1240 non supportano 802.11w.
- 802.11w non è supportato sull'access point flexconnect e sul WLC 7510 nella versione 7.4. Il supporto è stato aggiunto dalla release 7.5.

Configurazione

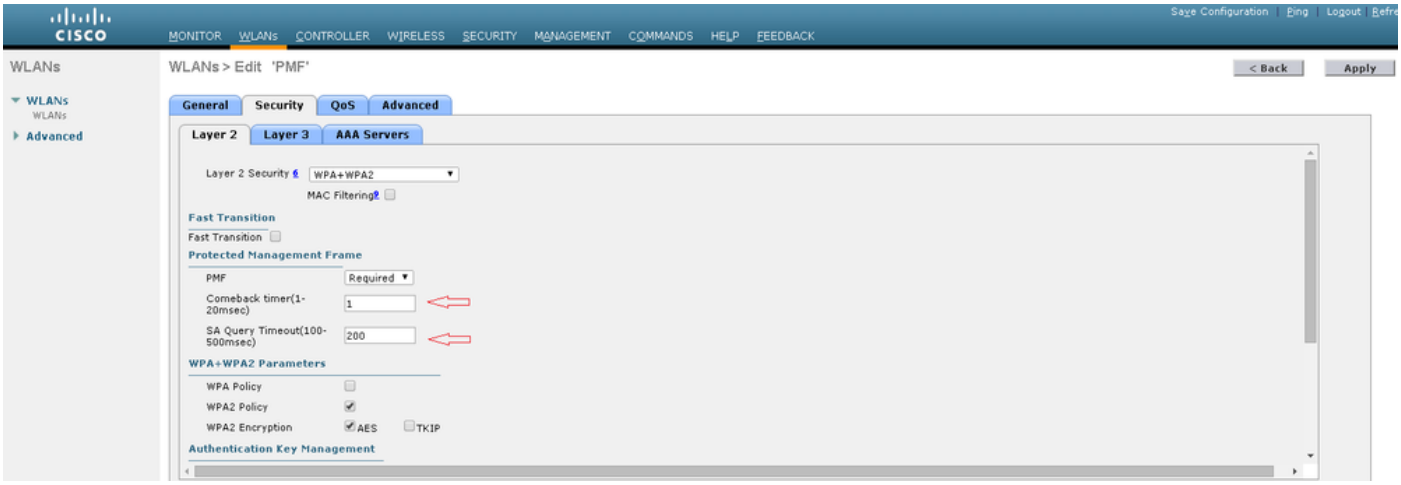
GUI

Passaggio 1. È necessario abilitare il frame di gestione protetto nell'SSID configurato con 802.1x/PSK. Sono disponibili tre opzioni, come illustrato nell'immagine.

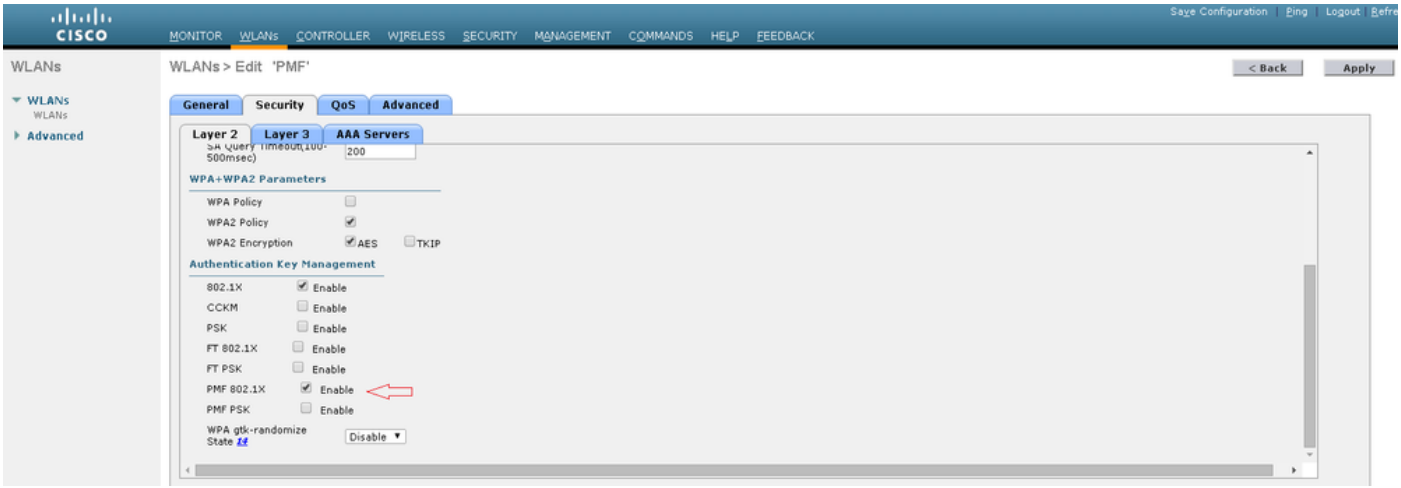


'Obbligatorio' specifica che un client che non supporta 802.11w non è autorizzato a connettersi. 'Facoltativo' specifica che anche i client che non supportano 802.11w possono connettersi.

Passaggio 2. È quindi necessario specificare il timer di ritorno e il timeout della query SA. Il timer di ritorno specifica il tempo di attesa che un client associato deve attendere prima che l'associazione possa essere riprovata quando viene prima negata con codice di stato 30. Il timeout della query SA specifica il tempo di attesa del WLC per una risposta dal client per il processo di query. Se il client non risponde, l'associazione viene eliminata dal controller. Questa operazione viene eseguita come mostrato nell'immagine.



Passaggio 3. È necessario abilitare 'PMF 802.1x' se si utilizza 802.1x come metodo di gestione delle chiavi di autenticazione. Se si utilizza PSK, è necessario selezionare la casella di controllo PMF PSK, come illustrato nell'immagine.



CLI

- Per abilitare o disabilitare la funzione 11w, eseguire il comando:

config wlan security wpa akm pmf 802.1x enable/disable

config wlan security wpa akm pmf psk enable/disable

- Per abilitare o disabilitare i frame di gestione protetti, eseguire il comando:

config wlan security pmf optional/required/disable

- Impostazioni tempo di ritorno associazione:

config wlan security pmf 11w-association-comeback

- Impostazioni timeout tentativi query SA:

config wlan security pmf saquery-retry-time

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

È possibile verificare la configurazione 802.11w. Controllare la configurazione WLAN:

```
(wlc)>show wlan 1
Wi-Fi Protected Access (WPA/WPA2)..... Enabled
<snip>
802.1x..... Enabled
PSK..... Disabled
CCKM..... Disabled
FT-1X(802.11r)..... Disabled
FT-PSK(802.11r)..... Disabled
PMF-1X(802.11w)..... Enabled
PMF-PSK(802.11w)..... Disabled
FT Reassociation Timeout..... 20
FT Over-The-DS mode..... Enabled
GTK Randomization..... Disabled
<snip>
PMF..... Required
PMF Association Comeback Time..... 1
PMF SA Query RetryTimeout..... 200
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

I seguenti comandi di debug sono disponibili per risolvere i problemi relativi a 802.11w sul WLC:

- **debug 11w-pmf events enable/disable**
- debug 11w-pmf keys enable/disable
- debug 11w-pmf all enable

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).