Risoluzione dei problemi ACI L3Out - PcTag1 subnet a connessione diretta

Sommario

Introduzione

Questo documento descrive uno scenario in cui il traffico proveniente da una subnet L3Out con connessione diretta e senza la corretta configurazione nell'EPG esterno può causare perdite di contratto.

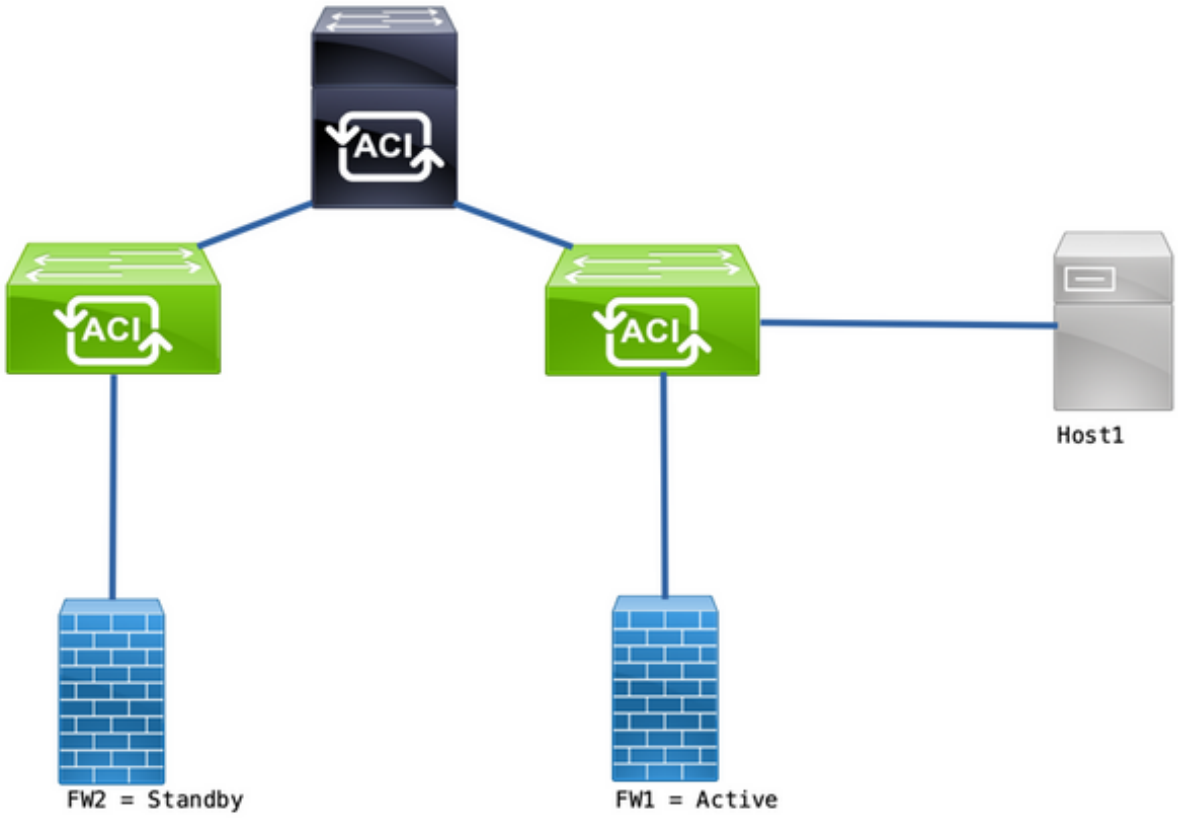
Premesse

La sezione "**Un'eccezione per una subnet a connessione diretta con 0.0.0.0/0**" del white paper ACI L3out richiama questo comportamento in relazione a pcTag 1:

"...per impostazione predefinita, alle subnet collegate direttamente viene assegnato il tag pcTag 1, un tag pcTag speciale che consente di ignorare un contratto. In questo modo le comunicazioni del protocollo di routing vengono consentite in modo implicito in uno scenario con corner case. Tuttavia... questo può causare problemi di sicurezza. Questo comportamento viene spiegato in dettaglio con l'ID bug Cisco CSCuz12913 , che introduce anche una configurazione di soluzione:"

Scenario

Topologia e configurazione



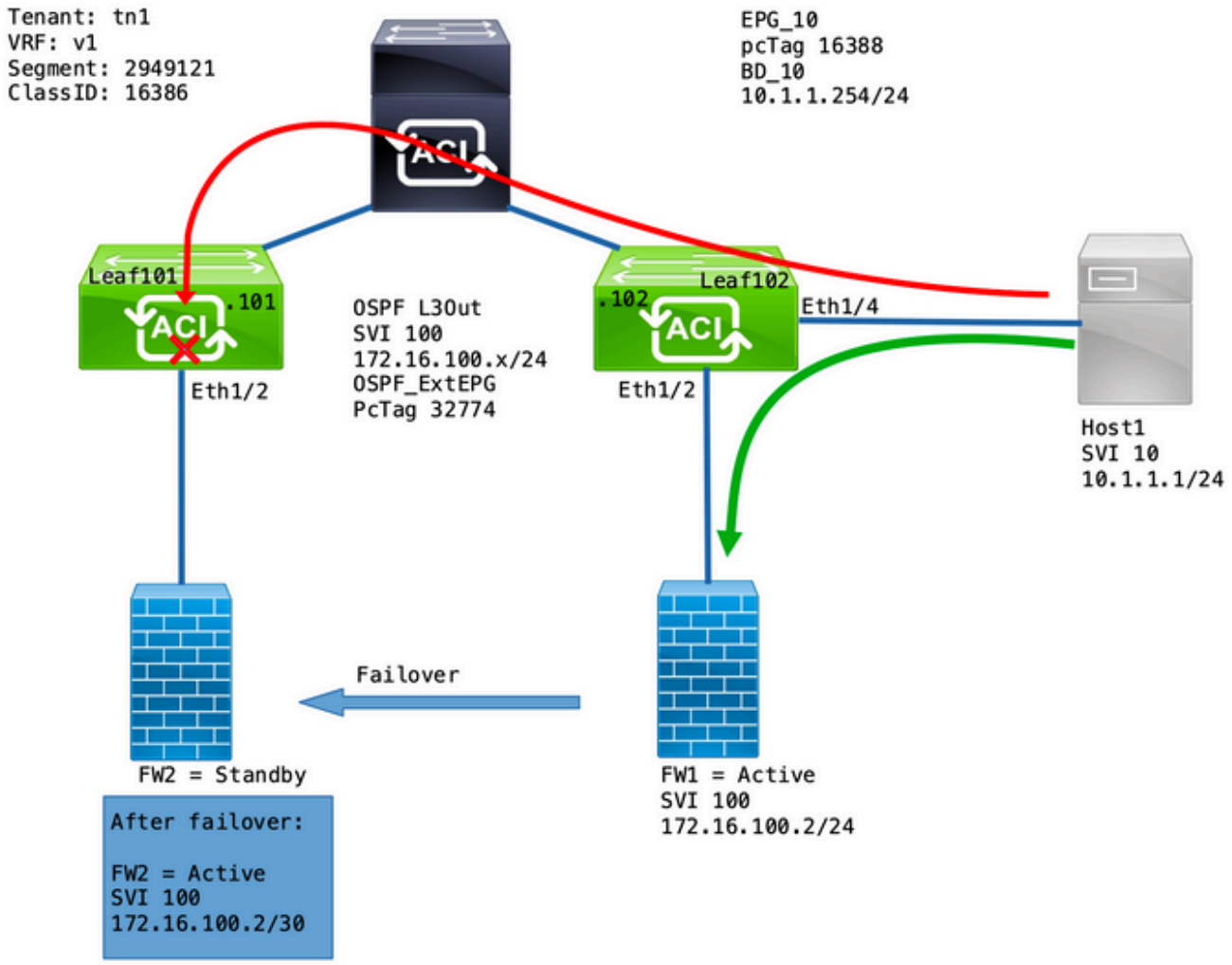
Topologia

- I firewall (FW) sono configurati con Network Address Translation (NAT).
- Tutto il traffico inviato all'infrastruttura ACI proviene dall'IP del firmware che forma l'adiacenza OSPF con ACI.
- L'EPG esterno dispone di una rete 0.0.0.0/0 configurata con **subnet esterne per l'EPG esterno**.
- Esiste un contratto per la comunicazione tra l'EPG interno e l'EPG esterno.

Problema osservato

Se il dispositivo attivo è FW1, il traffico funziona come previsto. Non si osservano gocce.

Dopo il failover dei servizi firewall su FW2, la connettività viene interrotta - 10.1.1.1 e 172.16.100.2 non sono più in grado di comunicare.



Problema di approfondimento

Un'acquisizione ELAM su Leaf101 ci consente di verificare se il traffico dall'host 1 al FW2 viene interrotto.

Sono state utilizzate le seguenti opzioni ELAM:

```
leaf101# vsh_lc
module-1# debug platform internal roc elam asic 0
module-1(DBG-elam-insel6)# trigger reset
module-1(DBG-elam)# trigger init in-select 14 out-select 1
module-1(DBG-elam-insel14)# set inner ipv4 src_ip 10.1.1.1 dst_ip 172.16.100.2
module-1(DBG-elam-insel14)# start
module-1(DBG-elam-insel14)# status
```

Quando viene attivato, l'e-report consente di visualizzare i risultati della ricerca:

```
<snip>
================================================================================================================
================================================
Captured Packet
================================================================================================================
================================================
<snip>
```

```
------------------------------------------------------------------------------------------------
------------------------------------------------
Inner L3 Header
------------------------------------------------------------------------------------------------
------------------------------------------------
L3 Type : IPv4
DSCP : 0
Don't Fragment Bit : 0x0
TTL : 254
IP Protocol Number : ICMP
Destination IP                : 172.16.100.2   <<<----
Source IP                     : 10.1.1.1   <<<----
<snip>
================================================================================================
================================================
Contract Lookup ( FPC )
================================================================================================
================================================

------------------------------------------------------------------------------------------------
------------------------------------------------
Contract Lookup Key
------------------------------------------------------------------------------------------------
------------------------------------------------
IP Protocol : ICMP( 0x1 )
L4 Src Port : 2048( 0x800 )
L4 Dst Port : 52579( 0xCD63 )
sclass (src pcTag)                      : 16388( 0x4004 )   <<<----
dclass (dst pcTag)                      : 16386( 0x4002 )   <<<----
<snip>

------------------------------------------------------------------------------------------------
------------------------------------------------
Contract Result
------------------------------------------------------------------------------------------------
------------------------------------------------
Contract Drop                           : yes   <<<----
Contract Logging : yes
Contract Applied : no
Contract Hit : yes
Contract Aclqos Stats Index : 81824
( show sys int aclqos zoning-rules | grep -B 9 "Idx: 81824" )
```

In questo rapporto viene mostrato che il flusso è contratto eliminato insieme ai seguenti dettagli:

- SCLASS è 16388, che è il pcTag di EPG_10.
- DCLASS è 16386, ovvero il tag pcTag del VRF v1.

Convalidare quindi le regole di zoning per il VRF:

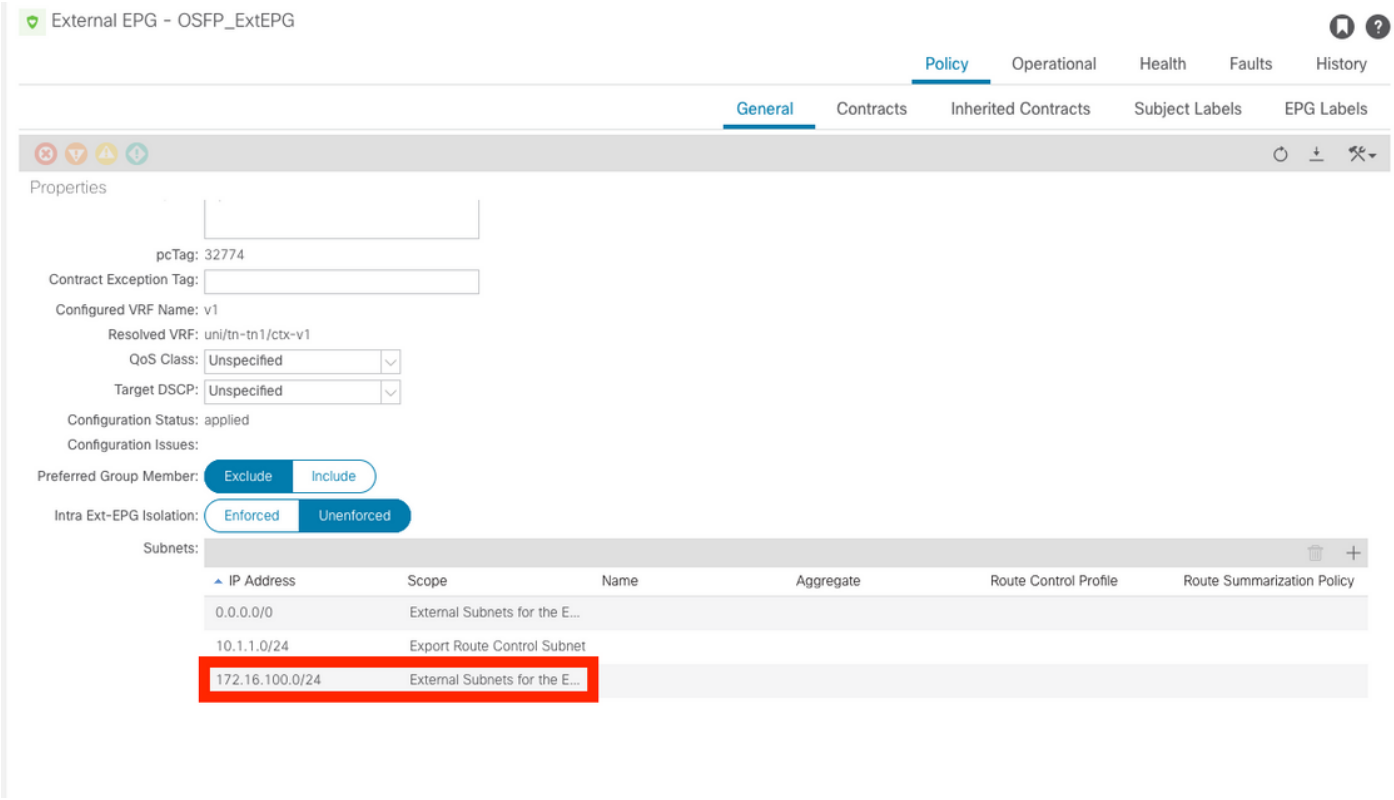
```
leaf102# show zoning-rule scope 2949121
+---------+--------+--------+----------+---------+---------+---------+-----------------+-------
---+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |   Dir   |  operSt |  Scope  |       Name      |
Action  |       Priority       |
+---------+--------+--------+----------+---------+---------+---------+-----------------+-------
---+----------------------+
|   4131  |   0    |   15   | implicit | uni-dir | enabled | 2949121 |                 |
deny,log | any_vrf_any_deny(22) |
|   4130  |   0    |   0    | implarp  | uni-dir | enabled | 2949121 |                 |
permit  |  any_any_filter(17)  |
|   4129  |   0    |   0    | implicit | uni-dir | enabled | 2949121 |                 |
deny,log |   any_any_any(21)    |
```

```
|   4132  |   0    | 49155  | implicit | uni-dir | enabled | 2949121 |                 |
permit  |   any_dest_any(16)   |
|   4112  | 16386  | 16388  | default  | uni-dir | enabled | 2949121 | tn1:EPG-to-L3Out |
permit  |    src_dst_any(9)    |
|   4133  | 16388  |   15   | default  | uni-dir | enabled | 2949121 | tn1:EPG-to-L3Out |
permit  |    src_dst_any(9)    |
+---------+--------+--------+----------+---------+---------+---------+-----------------+-------
---+----------------------+
```

Esiste un contratto per la comunicazione da EPG_10 (16388) alle reti dietro OSPF L3Out (0.0.0.0/0 = 15). Tuttavia, il traffico proveniente da 172.16.100.2 è contrassegnato con il tag pcTag (16386) del VRF v1.

Soluzione

Aggiungere la subnet connessa direttamente dell'uscita L3 sotto OSPF Ext_EPG.



Questa aggiunta ha due effetti:

1. Il traffico proveniente dalla subnet a connessione diretta è contrassegnato con OSPF_ExtEPG pcTag (32774)
2. Vengono aggiunte regole per consentire il flusso da e verso EPG_10 e OSPF_ExtEPG

```
leaf102# show zoning-rule scope 2949121
+---------+--------+--------+----------+----------------+---------+---------+-----------------
+----------+----------------------+ | Rule ID | SrcEPG | DstEPG | FilterID | Dir | operSt |
Scope | Name | Action | Priority | +---------+--------+--------+----------+----------------+----
-----+---------+------------------+----------+----------------------+ | 4131 | 0 | 15 | implicit
| uni-dir | enabled | 2949121 | | deny,log | any_vrf_any_deny(22) | | 4130 | 0 | 0 | implarp |
uni-dir | enabled | 2949121 | | permit | any_any_filter(17) | | 4129 | 0 | 0 | implicit | uni-
dir | enabled | 2949121 | | deny,log | any_any_any(21) | | 4132 | 0 | 49155 | implicit | uni-dir
| enabled | 2949121 | | permit | any_dest_any(16) | | 4112 | 16386 | 16388 | default | uni-dir |
enabled | 2949121 | tn1:EPG-to-L3Out | permit | src_dst_any(9) | | 4133 | 16388 | 15 | default |
```

```
uni-dir | enabled | 2949121 | tn1:EPG-to-L3Out | permit | src_dst_any(9) | |   4134  | 16388  |
32774  | default  |     bi-dir     | enabled | 2949121 | tn1:EPG-to-L3Out |  permit  |
src_dst_any(9)    |  <<<----
|   4135  | 32774  | 16388  | default  | uni-dir-ignore | enabled | 2949121 | tn1:EPG-to-L3Out |
permit  |    src_dst_any(9)    |  <<<----
+---------+--------+--------+----------+----------------+---------+---------+-----------------
+----------+----------------------+
```

Spiegazione

Il motivo per cui funziona quando il firmware e l'host sono connessi alla stessa foglia (senza l'aggiunta della subnet L3Out) è che le subnet connesse direttamente utilizzano un pcTag speciale di 1 che ignora tutti i contratti. In questo modo le comunicazioni del protocollo di routing vengono consentite in modo implicito in uno scenario con corner case.

Con questi trigger possiamo catturare un flusso di traffico da 172.16.100.2 a 10.1.1.1 mentre su Leaf102:

```
leaf102# vsh_lc
module-1# debug platform internal roc elam asic 0
module-1(DBG-elam)# trigger reset
module-1(DBG-elam)# trigger init in-select 6 out-select 1
module-1(DBG-elam-insel6)# set outer ipv4 src_ip 172.16.100.2 dst_ip 10.1.1.1
module-1(DBG-elam-insel6)# start
module-1(DBG-elam-insel6)# status
 ELAM STATUS
===========
Asic 0 Slice 0 Status Triggered
```

In questo rapporto vengono visualizzati i risultati della ricerca:

```
module-1(DBG-elam-insel6)# ereport
Python available. Continue ELAM decode with LC Pkg
 ELAM REPORT
================================================================================================
================================================
                                                                  Captured Packet
================================================================================================
================================================

------------------------------------------------------------------------------------------------
------------------------------------------------
Outer L3 Header
------------------------------------------------------------------------------------------------
------------------------------------------------
L3 Type                       : IPv4
IP Version                    : 4
DSCP                          : 0
IP Packet Length              : 84 ( = IP header(28 bytes) + IP payload )
Don't Fragment Bit            : not set
TTL                           : 255
IP Protocol Number            : ICMP
IP CheckSum                   : 32320( 0x7E40 )
Destination IP                : 10.1.1.1      <<<----
Source IP                     : 172.16.100.2  <<<----
```

```
================================================================================================
=====================================================
                                                                  Contract Lookup ( FPC )
================================================================================================
=====================================================

------------------------------------------------------------------------------------------------
-----------------------------------------------------
Contract Lookup Key
------------------------------------------------------------------------------------------------
-----------------------------------------------------
IP Protocol                           : ICMP( 0x1 )
L4 Src Port                           : 0( 0x0 )
L4 Dst Port                           : 19821( 0x4D6D )
sclass (src pcTag)                    : 1( 0x1 )           <<<----
dclass (dst pcTag)                    : 16388( 0x4004 )    <<<----
src pcTag is from local table         : yes
derived from a local table on this node by the lookup of src IP or MAC
Unknown Unicast / Flood Packet        : no
If yes, Contract is not applied here because it is flooded

------------------------------------------------------------------------------------------------
-----------------------------------------------------
Contract Result
------------------------------------------------------------------------------------------------
-----------------------------------------------------
Contract Drop                         : no  <<<----
Contract Logging                      : no
Contract Applied                      : no  <<<----
Contract Hit                          : yes
Contract Aclqos Stats Index           : 81903
```

Per convalidare il flusso di reso:

```
module-1(DBG-elam-insel6)# trigger reset
module-1(DBG-elam)# trigger init in-select 6 out-select 1
module-1(DBG-elam-insel6)# set outer ipv4 src_ip 10.1.1.1 dst_ip 172.16.100.2
module-1(DBG-elam-insel6)# start
module-1(DBG-elam-insel6)# status
 ELAM STATUS
===========
Asic 0 Slice 0 Status Triggered
```

Risultati della ricerca del flusso di ritorno:

```
module-1(DBG-elam-insel6)# ereport
Python available. Continue ELAM decode with LC Pkg
 ELAM REPORT
================================================================================================
=====================================================
                                                                Captured Packet
================================================================================================
=====================================================
------------------------------------------------------------------------------------------------
-----------------------------------------------------
Outer L3 Header
------------------------------------------------------------------------------------------------
-----------------------------------------------------
L3 Type                     : IPv4
```

```
IP Version                    : 4
DSCP                          : 0
IP Packet Length              : 84 ( = IP header(28 bytes) + IP payload )
Don't Fragment Bit            : not set
TTL                           : 255
IP Protocol Number            : ICMP
IP CheckSum                   : 32198( 0x7DC6 )
Destination IP                : 172.16.100.2  <<<----
Source IP                     : 10.1.1.1      <<<----

================================================================================================
=====================================================
                                                                Contract Lookup ( FPC )
================================================================================================
=====================================================

------------------------------------------------------------------------------------------------
-----------------------------------------------------
Contract Lookup Key
------------------------------------------------------------------------------------------------
-----------------------------------------------------
IP Protocol                           : ICMP( 0x1 )
L4 Src Port                           : 2048( 0x800 )
L4 Dst Port                           : 18134( 0x46D6 )
sclass (src pcTag)                    : 16388( 0x4004 ) <<<----
dclass (dst pcTag)                    : 1( 0x1 )        <<<----
src pcTag is from local table         : yes
derived from a local table on this node by the lookup of src IP or MAC
Unknown Unicast / Flood Packet        : no
If yes, Contract is not applied here because it is flooded

------------------------------------------------------------------------------------------------
-----------------------------------------------------
Contract Result
------------------------------------------------------------------------------------------------
-----------------------------------------------------
Contract Drop                         : no    <<<----
Contract Logging                      : no
Contract Applied                      : no    <<<----
Contract Hit                          : yes
Contract Aclqos Stats Index           : 81903
```

La tabella seguente riepiloga il comportamento previsto sugli switch Gen2:

Scenario	Direzionalità	Eliminazione contratto	Nessuna eliminazi contratto
Su tutta la stessa foglia Applicazione delle policy VRF: Entrambi	Da X a L3Out		X
	Da L3a X		X
Su 2 nodi foglia Applicazione delle policy VRF: In ingresso	Da X a L3Out	X	
	Da L3a X		X
Su 2 nodi foglia Applicazione delle policy VRF: In uscita	Da X a L3Out		X
	Da L3a X		X

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).