# Guida alla risoluzione dei problemi GETVPN

## Sommario

# Introduzione

Questo documento presenta una metodologia strutturata di risoluzione dei problemi e strumenti utili per identificare e isolare i problemi relativi a Group Encrypted Transport VPN (GETVPN) e fornire possibili soluzioni.

# Prerequisiti

## Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- GETVPN
  [Guida ufficiale alla configurazione di GETVPN](#)
  [Guida ufficiale alla progettazione e implementazione di GETVPN](#)

- Utilizzo server Syslog

## Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

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.

# Metodologia di risoluzione dei problemi GETVPN

Come per la maggior parte delle procedure di risoluzione di problemi tecnologici complessi, la soluzione consiste nell'isolare il problema a una funzionalità, a un sottosistema o a un componente specifico. La soluzione GETVPN è costituita da diversi componenti, in particolare:

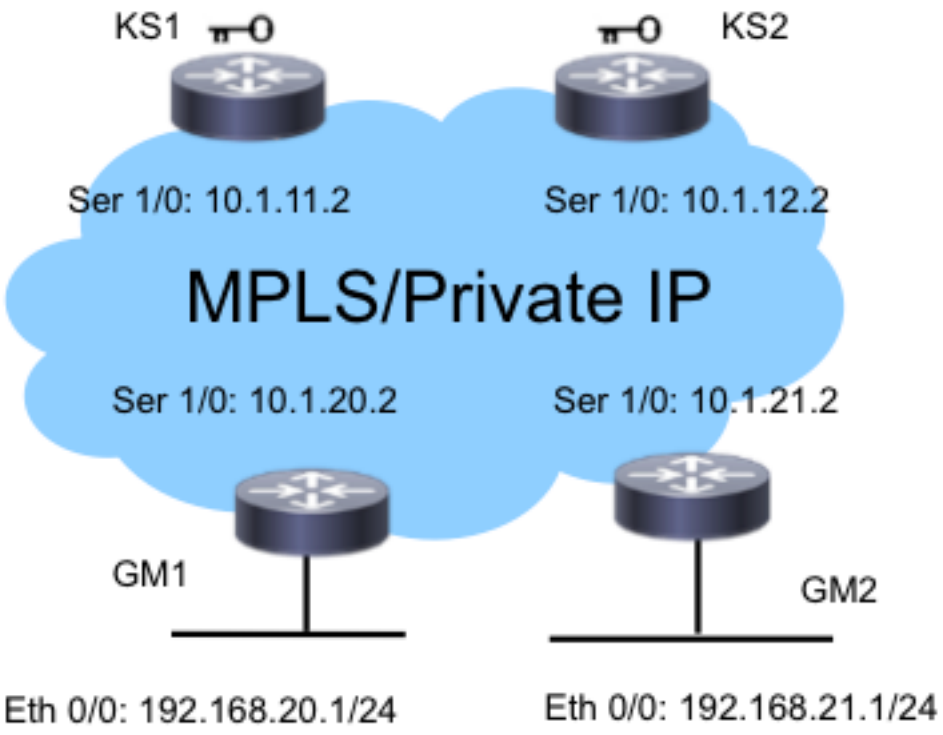
- IKE (Internet Key Exchange) - Utilizzato tra i Group Member (GM) e Key Server (KS) e tra i KS COOP (Cooperative Protocol) per autenticare e proteggere il Control Plane.
- Group Domain of Interpretation (GDOI) - Protocollo utilizzato per il KS per distribuire le chiavi del gruppo e fornire servizi chiave come la reimpostazione delle chiavi a tutti gli GM.
- COOP - Protocollo utilizzato per i KS per comunicare tra loro e fornire ridondanza.
- Conservazione intestazione: IPsec in modalità tunnel che mantiene l'intestazione del pacchetto dati originale per il recapito del traffico end-to-end.
- TBAR (Time Based Anti-Replay): meccanismo di rilevamento della riproduzione utilizzato in un ambiente con chiavi di gruppo.

Offre inoltre un'ampia gamma di strumenti di risoluzione dei problemi per semplificare il processo

di risoluzione. È importante capire quale di questi strumenti è disponibile e quando sono appropriati per ogni attività di risoluzione dei problemi. Quando si esegue la risoluzione dei problemi, è sempre consigliabile iniziare con i metodi meno intrusivi, in modo da evitare un impatto negativo sull'ambiente di produzione. La chiave per la risoluzione di questo problema strutturato è la capacità di suddividere il problema in un problema di controllo o di data plane. A tale scopo, è possibile seguire il protocollo o il flusso di dati e utilizzare i vari strumenti presentati qui per selezionarli.

## Topologia di riferimento

Questo schema di indirizzamento e topologia GETVPN viene utilizzato in tutto il resto di questo documento per la risoluzione dei problemi.




## Configurazioni di riferimento

- KS 1

```
crypto gdoi group G1
identity number 3333
server local
rekey authenmypubkeyrsa get
rekey transport unicast
sa ipsec 1
profile gdoi-p
match address ipv4ENCPOL
address ipv4 10.1.11.2
redundancy
local priority 10
peer address ipv4 10.1.12.2
```

- GM1

```
crypto gdoi group G1
identity number 3333
server address ipv4 10.1.11.2
server address ipv4 10.1.12.2
!
crypto map gm_map 10 gdoi
set group G1
!
interface Serial1/0
crypto map gm_map
```

**Nota:** Le configurazioni KS2 e GM2 non sono incluse qui per brevità.

## Terminologia

- **KS** - Server chiave
- **GM** - Membro del gruppo
- **COOP** - Protocollo di cooperazione
- **TBAR** - Funzione Time Based Anti-Replay
- **KEK** - Chiave di crittografia
- **TEK** - Chiave di crittografia del traffico

## Preparazione della funzione di registrazione e altre best practice

Prima di iniziare la risoluzione dei problemi, assicurarsi di aver preparato la funzione di registrazione come descritto di seguito. Di seguito sono elencate alcune procedure ottimali:

- Controllare la quantità di memoria disponibile sul router e configurare il **debug con buffer di registrazione** su un valore elevato (10 MB o più, se possibile).
- Disabilita la registrazione nei server console, monitor e syslog.
- Recuperare il contenuto del buffer di registrazione con il comando **show log** a intervalli regolari, da 20 minuti a un'ora, per evitare la perdita del log dovuta al riutilizzo del buffer.
- In ogni caso, immettere il comando **show tech** dagli oggetti GM e KS interessati e esaminare l'output del comando **show ip route** in modalità globale e in tutti gli eventuali VRF (Virtual Routing and Forwarding) interessati.
- Utilizzare il protocollo NTP (Network Time Protocol) per sincronizzare l'orologio tra tutti i dispositivi sottoposti a debug. Abilita timestamp in millisecondi (msec) per messaggi di debug e di registro:

```
service timestamps debug datetime msec
service timestamps log datetime msec
```

- Verificare che gli output del comando show abbiano un timestamp.

```
Router#terminal exec prompt timestamp
```

- Quando si raccolgono gli output del comando show per gli eventi del piano di controllo o i contatori del piano dati, si raccolgono sempre più iterazioni dello stesso output.

# Risoluzione dei problemi di GETVPN Control Plane

Control Plane indica tutti gli eventi del protocollo che hanno portato alla creazione della policy e della Security Association (SA) sull'oggetto GM in modo che siano pronti per crittografare e decrittografare il traffico del data plane. Alcuni dei checkpoint chiave nel control plane GETVPN sono:


## Procedure consigliate per il debug di Control Plane

Queste best practice per la risoluzione dei problemi non sono specifiche di GETVPN; si applicano a quasi tutte le operazioni di debug dei control plane. È fondamentale seguire queste procedure ottimali per garantire la risoluzione dei problemi più efficace:

- Disattivare la registrazione sulla console e usare il buffer di registrazione o il syslog per raccogliere i debug.
- Usare il protocollo NTP per sincronizzare gli orologi dei router su tutti i dispositivi sottoposti a debug.
- Abilita timestamp msec per i messaggi di debug e di registro:

```
service timestamp debug datetime msec
service timestamp log datetime msec
```

- Verificare che gli output del comando show dispongano di un timestamp per poter essere correlati all'output del comando debug:

```
terminal exec prompt timestamp
```

- Se possibile, utilizzare il debug condizionale in un ambiente di scalabilità.

## Strumenti di risoluzione dei problemi GETVPN Control Plane

### Comandi GETVPN Show

Come regola generale, questi sono gli output del comando da raccogliere per quasi tutti i problemi di GETVPN.

### KS

```
show crypto gdoi
show crypto gdoi ks coop
show crypto gdoi ks members
show crypto gdoi ks rekey
show crypto gdoi ks policy
```

### GM

```
show crypto eli
```

```
show crypto gdoi rekey sa
show crypto gdoi
show crypto gdoi gm
show crypto gdoi gm rekey
```

## Messaggi GETVPN Syslog

GETVPN fornisce un set esteso di messaggi syslog per eventi di protocollo e condizioni di errore significativi. Quando si esegue la risoluzione dei problemi GETVPN, il syslog deve essere sempre il primo punto in cui eseguire la ricerca.

### Messaggi di syslog KS comuni

| Messaggi syslog | Spiegazione |
|---|---|
| *COOP_CONFIG_MISMATCH* | La configurazione tra il server di chiave primaria e il server di chiave secondaria non corrisponde. |
| *COOP_KS_ELECTION* | Il server della chiave locale ha avviato il processo di selezione in un grupp |
| *COOP_KS_REACH* | Viene ripristinata la raggiungibilità tra i server delle chiavi cooperative configurati. |
| *COOP_KS_TRANS_TO_PRI* | Il server di chiave locale è passato a un ruolo primario da server secondar in un gruppo. |
| *COOP_KS_UNAUTH* | Un server remoto autorizzato ha tentato di contattare il server della chiave locale di un gruppo, il che potrebbe essere considerato un evento ostile. |
| *COOP_KS_UNREACH* | La raggiungibilità tra i server delle chiavi di cooperazione configurati viene persa e ciò potrebbe essere considerato un evento ostile. |
| *KS_GM_REVOKED* | Durante il protocollo di reimpostazione delle chiavi, un membro non autorizzato ha tentato di unirsi a un gruppo, il che potrebbe essere considerato un evento ostile. |
| *KS_SEND_MCAST_REKEY* | Invio della chiave multicast in corso. |
| *KS_SEND_UNICAST_REKEY* | Invio della chiave unicast in corso. |
| *KS_NON AUTORIZZATO* | Durante il protocollo di registrazione al GDOI, un membro non autorizzato tentato di unirsi a un gruppo, il che potrebbe essere considerato un evento ostile. |
| *INDIRIZZOIP_NON AUTORIZZATO* | La richiesta di registrazione è stata eliminata perché il dispositivo richieder non era autorizzato a partecipare al gruppo. |

### Messaggi di syslog GM comuni

| Messaggi syslog | Spiegazione |
|---|---|
| *GM_CLEAR_REGISTER* | Il comando **clear crypto gdoi** è stato eseguito dal membro del gruppo loc |
| *GM_CM_ATTACH* | Èstata associata una mappa crittografica per il membro del gruppo local |
| *GM_CM_DETACH* | Mappa crittografica scollegata per il membro del gruppo locale.& |
| *REGISTRA_RE_GM* | L'associazione di protezione IPsec creata per un gruppo potrebbe esser scaduta o cancellata. È necessario registrarsi nuovamente al server di chiave. |
| *GM_RECV_REKEY* | Ricevuta chiave. |
| *COMPL_REGS_GM* | Registrazione completata. |
| *GM_REKEY_TRANS_2_MULTI* | Il membro del gruppo è passato dall'utilizzo di un meccanismo di reimpostazione chiavi unicast all'utilizzo di un meccanismo multicast. |
| *GM_REKEY_TRANS_2_UNI* | Il membro del gruppo è passato dall'utilizzo di un meccanismo di reimpostazione delle chiavi multicast all'utilizzo di un meccanismo unica |
| *TEMPO_PSEUDO_GRANDE* | Un membro del gruppo ha ricevuto uno pseudotime con un valore che è |

| | |
|---|---|
| | gran parte diverso dal suo pseudotime. |
| *RIPRODUZIONE NON RIUSCITA* | Un membro del gruppo o un server di chiavi non ha superato un controll anti-replay. |

**Nota:** I messaggi evidenziati in rosso sono i messaggi più comuni o significativi visualizzati in un ambiente GETVPN.

### Debug globali di GDOI e crittografia

I debug GETVPN sono suddivisi in:

1. In primo luogo dal dispositivo su cui si sta eseguendo la risoluzione dei problemi.
```
F340.06.15-2900-18#debug cry gdoi ?
 all-features  All features in GDOI
 condition     GDOI Conditional Debugging
 gm            Group Member
 ks            Key Server
```
2. In base al tipo di problema che si sta risolvendo.
```
GM1#debug cry gdoi gm ?
 all-features    All Group Member features
 infrastructure  GM Infrastructure
 registration    GM messages related to registration
 rekey           GM messagese related to Re-Key
 replay          Anti Replay
```
3. Terzo livello di debug da abilitare. Nella versione 15.1(3)T e successive, tutti i debug delle funzionalità GDOI sono stati standardizzati per avere questi livelli di debug. Questa funzionalità è stata progettata per consentire la risoluzione dei problemi degli ambienti GETVPN su larga scala con granularità di debug sufficiente. Quando si esegue il debug di problemi GETVPN, è importante usare il livello di debug appropriato. Come regola generale, iniziare con il livello di debug più basso, ovvero il livello di errore, e aumentare la granularità del debug quando necessario.
```
GM1#debug cry gdoi gm all-features ?
 all-levels  All levels
 detail      Detail level
 error       Error level
 event       Event level
 packet      Packet level
 terse       Terse level
```

### Debug condizionale GDOI

In Cisco IOS® versione 15.1(3)T e successive, è stato aggiunto il debug condizionale GDOI per facilitare la risoluzione dei problemi di GETVPN in un ambiente su larga scala. Pertanto, tutti i debug ISAKMP (Internet Security Association and Key Management Protocol) e GDOI possono ora essere attivati con un filtro condizionale basato sull'indirizzo IP del gruppo o del peer. Per la maggior parte dei problemi GETVPN, è consigliabile abilitare i debug ISAKMP e GDOI con il filtro condizionale appropriato, poiché i debug GDOI mostrano solo le operazioni specifiche di GDOI. Per utilizzare i debug condizionali ISAKMP e GDOI, attenersi alla seguente procedura:

1. Impostare il filtro condizionale.
2. Abilitare ISAKMP e GDOI pertinenti come di consueto.

Ad esempio:

```
KS1# debug crypto gdoi condition peer add ipv4 10.1.20.2
% GDOI Debug Condition added.

KS1#
KS1# show crypto gdoi debug-condition
GDOI Conditional Filters:
Peer Address 10.1.20.2
Unmatched NOT set

KS1#debug crypto gdoi ks registration all-levels
GDOI Key Server Registration Debug level: (Packet, Detail, Event, Terse, Error)
```

> **Nota:** Con i debug condizionali ISAKMP e GDOI, per intercettare i messaggi di debug che potrebbero non contenere le informazioni del filtro condizionale, ad esempio l'indirizzo IP nel percorso di debug, è possibile abilitare il flag **unmatched**. Tuttavia, occorre procedere con cautela in quanto può produrre una grande quantità di informazioni di debug.

## Tracce eventi GDOI

Questo è stato aggiunto nella versione 15.1(3)T. Event Tracing offre funzionalità di trace leggero e sempre attivo per eventi ed errori GDOI significativi. È inoltre disponibile la traccia del percorso di uscita con il traceback abilitato per le condizioni di eccezione. Le tracce di eventi possono fornire più informazioni sulla cronologia degli eventi GETVPN rispetto ai syslog tradizionali.

Le tracce di eventi GDOI sono abilitate per impostazione predefinita e possono essere recuperate dal buffer di traccia con il comando **show monitor even-trace**.

```
GM1#show monitor event-trace gdoi ?
all Show all the traces in current buffer
back Show trace from this far back in the past
clock Show trace from a specific clock time/date
coop GDOI COOP Event Traces
exit GDOI Exit Traces
from-boot Show trace from this many seconds after booting
infra GDOI INFRA Event Traces
latest Show latest trace events since last display
merged Show entries in all event traces sorted by time
registration GDOI Registration event Traces
rekey GDOI Rekey event Traces

GM1#show monitor event-trace gdoi rekey all
*Nov 6 15:55:16.117: GDOI_REKEY_EVENT: ACK_SENT: From 10.1.12.2 to 10.1.13.2
with seq no 1 for the group G1
*Nov 6 15:55:16.117: GDOI_REKEY_EVENT: REKEY_RCVD: From 10.1.12.2 to 10.1.13.2
with seq no 1 for the group G1
*Nov 6 16:11:01.125: GDOI_REKEY_EVENT: ACK_SENT: From 10.1.12.2 to 10.1.13.2
with seq no 1 for the group G1
*Nov 6 16:11:01.125: GDOI_REKEY_EVENT: REKEY_RCVD: From 10.1.12.2 to 10.1.13.2
with seq no 1 for the group G1
```

La traccia del percorso di uscita fornisce informazioni dettagliate sul percorso di uscita, ovvero le eccezioni e le condizioni di errore, con l'opzione traceback abilitata per impostazione predefinita. I traceback possono quindi essere utilizzati per decodificare l'esatta sequenza di codice che ha determinato la condizione del percorso di uscita. Per recuperare i risultati di traccia dal buffer di traccia, usare l'opzione **detail**:

```
GM1#show monitor event-trace gdoi exit all detail
*Nov 6 15:15:25.611: NULL_VALUE_FOUND:Invalid GROUP Name
-Traceback= 0xCA51318z 0xCA1F4DBz 0xC9B2707z 0xCA1ED4Ez 0x97EB018z
0x97EA960z 0x97E8D62z 0x97F3706z 0x97F3361z 0xA02684Ez
*Nov 6 15:15:25.611: MAP_NOT_APPLIED_IN_ANY_INTERFACE:
-Traceback= 0xCA51318z 0xCA46718z 0xCA1EF79z 0x97EB018z 0x97EA960z
0x97E8D62z 0x97F3706z 0x97F3361z 0xA02684Ez 0xA01FD52z
*Nov 6 15:15:25.650: NULL_VALUE_FOUND:NULL Parameters passed idb or ipaddress
when idb ipaddress is changed
-Traceback= 0xCA51318z 0xCA22430z 0xA09A8DCz 0xA09D8F6z 0xA0F280Fz
0xBA1D1F4z 0xBA1CACCz 0xBA1C881z 0xBA1C5BBz 0xA0F494Az
```

La dimensione predefinita del buffer di traccia è di 512 voci e potrebbe non essere sufficiente se il problema è intermittente. Per aumentare le dimensioni predefinite della voce di traccia, è possibile modificare i parametri di configurazione della traccia eventi come illustrato di seguito:

```
GM1#show monitor event-trace gdoi rekey parameters
Trace has 512 entries
Stacktrace is disabled by default

GM1#
GM1#config t
Enter configuration commands, one per line. End with CNTL/Z.
GM1(config)#monitor event-trace gdoi rekey size ?
<1-1000000> Number of entries in trace
```

## Checkpoint del Control Plane GETVPN e problemi comuni

Di seguito sono riportati alcuni dei problemi comuni del control plane per GETVPN. Per ripetere, il Control Plane è definito come tutti i componenti della funzione GETVPN necessari per abilitare la crittografia e la decrittografia del dataplane sugli oggetti GM. Ad alto livello, ciò richiede la corretta registrazione di GM, i criteri di sicurezza e il download/installazione dell'ASA, nonché la successiva reimpostazione della chiave KEK/TEK.

### Impostazione COOP e creazione criteri

Per verificare che il servizio KS abbia creato correttamente il criterio di sicurezza e il codice KEK/TEK associato, immettere:

```
KS1#show crypto gdoi ks policy
Key Server Policy:
For group G1 (handle: 2147483650) server 10.1.11.2 (handle: 2147483650):

For group G1 (handle: 2147483650) server 10.1.12.2 (handle: 2147483651):

# of teks : 1 Seq num : 10
KEK POLICY (transport type : Unicast)
spi : 0x18864836BA888BCD1126671EEAFEB4C7
management alg : disabled encrypt alg : 3DES
crypto iv length : 8 key size : 24
orig life(sec): 1200 remaining life(sec): 528
sig hash algorithm : enabled sig key length : 162
sig size : 128
sig key name : key1

TEK POLICY (encaps : ENCAPS_TUNNEL)
spi : 0x91E3985A
access-list : ENCPOL
```

```
transform : esp-null esp-sha-hmac
alg key size : 0 sig key size : 20
orig life(sec) : 900 remaining life(sec) : 796
tek life(sec) : 2203 elapsed time(sec) : 1407
override life (sec): 0 antireplay window size: 4

Replay Value 442843.29 secs
```

Uno dei problemi più comuni dell'impostazione dei criteri KS è la presenza di criteri diversi configurati tra i KS primario e secondario. Questo può causare un comportamento imprevedibile di KS e questo errore verrà segnalato:

```
%GDOI-3-COOP_CONFIG_MISMATCH: WARNNING: replay method configuration between
Primary KS and Secondary KS are mismatched
```

Attualmente non esiste una sincronizzazione automatica della configurazione tra i KS primario e secondario, pertanto è necessario correggerli manualmente.

Poiché COOP è una configurazione critica (e quasi sempre obbligatoria) per GETVPN, è fondamentale verificare che COOP funzioni correttamente e che i ruoli COOP KS siano corretti:

```
KS1#show crypto gdoi ks coop
Crypto Gdoi Group Name :G1
Group handle: 2147483650, Local Key Server handle: 2147483650

Local Address: 10.1.11.2
Local Priority: 200
 Local KS Role: Primary   , Local KS Status: Alive
Local KS version: 1.0.4
Primary Timers:
Primary Refresh Policy Time: 20
Remaining Time: 10
Antireplay Sequence Number: 40

Peer Sessions:
Session 1:
Server handle: 2147483651
Peer Address: 10.1.12.2
Peer Version: 1.0.4
Peer Priority: 100
Peer KS Role: Secondary , Peer KS Status: Alive
Antireplay Sequence Number: 0

IKE status: Established
Counters:
Ann msgs sent: 31
Ann msgs sent with reply request: 2
Ann msgs recv: 64
Ann msgs recv with reply request: 1
Packet sent drops: 7
Packet Recv drops: 0
Total bytes sent: 20887
Total bytes recv: 40244
```

In una configurazione COOP funzionale, è necessario osservare questo flusso di protocollo:

### IKE Exchange > ANN con priorità COOP scambiate > COOP Election > ANN da KS primario a secondario (policy, database GM e chiavi)

Se COOP non funziona correttamente o se è presente una divisione COOP, ad esempio più KS

diventano il KS principale, è necessario raccogliere questi debug per la risoluzione dei problemi:

```
debug crypto isakmp
debug crypto gdoi ks coop all-levels
show crypto isakmp sa
show crypto gdoi ks coop
```

### Configurazione IKE

Per GETVPN è necessario uno scambio IKE riuscito per proteggere il canale di controllo per il successivo download dei criteri e delle associazioni di protezione. Al termine dello scambio IKE riuscito, viene creata un'associazione di sicurezza GDOI_REKEY.

Nelle versioni precedenti a Cisco IOS 15.4(1)T, il comando GDOI_REKEY può essere visualizzato con il comando **show crypto isakmp sa**:

```
GM1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
10.1.13.2 10.1.11.2 GDOI_REKEY        1075 ACTIVE
10.1.11.2 10.1.13.2 GDOI_IDLE         1074 ACTIVE

IPv6 Crypto ISAKMP SA

GM1#
```

In Cisco IOS versione 15.4(1)T e successive, questa sa GDOI_REKEY viene mostrata con il comando **show crypto gdoi rekey sa**:

```
GM1#show crypto gdoi rekey sa
GETVPN REKEY SA
dst             src             conn-id         status
10.1.13.2       10.1.11.2       1114            ACTIVE
```

> **Nota:** Una volta completato lo scambio IKE iniziale, i criteri e le chiavi successivi verranno **spostati** dal KS al GM utilizzando la SA GDOI_REKEY. Non viene quindi eseguita alcuna nuova chiave per l'associazione di sicurezza GDOI_IDLE alla scadenza; scompaiono quando scadono le loro vite. Tuttavia, affinché possa ricevere le chiavi di nuovo, sull'apparecchio GM deve sempre essere presente GDOI_REKEY SA.

Lo scambio IKE per GETVPN non è diverso da quello utilizzato nei tunnel IPsec point-to-point tradizionali, quindi il metodo di risoluzione dei problemi rimane lo stesso. Per risolvere i problemi di autenticazione IKE, è necessario raccogliere i seguenti debug:

```
debug crypto isakmp
debug crypto isakmp error
debug crypto isakmp detail (hidden command, if detailed isakmp exchange information
is needed)
debug crypto isakmp packet (hidden command, if packet level isakmp information is needed)
```

### Registrazione, download criteri e installazione SA

Una volta completata l'autenticazione IKE, GM si registra presso il KS. Quando il problema si verifica correttamente, è necessario visualizzare i seguenti messaggi di syslog:

```
%GDOI-5-GM_REKEY_TRANS_2_UNI: Group G1 transitioned to Unicast Rekey.
%GDOI-5-SA_KEK_UPDATED: SA KEK was updated
%GDOI-5-SA_TEK_UPDATED: SA TEK was updated
%GDOI-5-GM_REGS_COMPL: Registration to KS 10.1.12.2 complete for group G1 using
address 10.1.13.2
%GDOI-5-GM_INSTALL_POLICIES_SUCCESS: SUCCESS: Installation of Reg/Rekey policies
from KS 10.1.12.2 for group G1 & gm identity 10.1.13.2
```

Il criterio e le chiavi possono essere verificati con questo comando:

```
GM1#show crypto gdoi
GROUP INFORMATION

Group Name : G1
Group Identity : 3333
Crypto Path : ipv4
Key Management Path : ipv4
Rekeys received : 1
IPSec SA Direction : Both

Group Server list : 10.1.11.2
10.1.12.2

Group member : 10.1.13.2 vrf: None
Version : 1.0.4
Registration status : Registered
Registered with : 10.1.12.2
Re-registers in       : 139 sec
Succeeded registration: 1
Attempted registration: 1
Last rekey from : 10.1.11.2
Last rekey seq num : 0
Unicast rekey received: 1
Rekey ACKs sent : 1
Rekey Rcvd(hh:mm:ss)  : 00:05:20
allowable rekey cipher: any
allowable rekey hash : any
allowable transformtag: any ESP

Rekeys cumulative
Total received : 1
After latest register : 1
Rekey Acks sents : 1

ACL Downloaded From KS 10.1.11.2:
access-list deny icmp any any
access-list deny eigrp any any
access-list deny ip any 224.0.0.0 0.255.255.255
access-list deny ip 224.0.0.0 0.255.255.255 any
access-list deny udp any port = 848 any port = 848
access-list permit ip any any

KEK POLICY:
Rekey Transport Type : Unicast
Lifetime (secs) : 878
Encrypt Algorithm : 3DES
Key Size : 192
Sig Hash Algorithm : HMAC_AUTH_SHA
Sig Key Length (bits) : 1024
```

```
TEK POLICY for the current KS-Policy ACEs Downloaded:
Serial1/0:
IPsec SA:
spi: 0x8BF147EF(2347845615)
transform: esp-3des esp-sha-hmac
sa timing:remaining key lifetime (sec): (200)
Anti-Replay(Time Based) : 4 sec interval


GM1#
GM1#
GM1#show crypto ipsec sa

interface: Serial1/0
Crypto map tag: gm1map, local addr 10.1.13.2

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 0.0.0.0 port 848
PERMIT, flags={}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.1.13.2, remote crypto endpt.: 0.0.0.0
path mtu 1500, ip mtu 1500, ip mtu idb Serial1/0
current outbound spi: 0x0(0)
PFS (Y/N): N, DH group: none

local crypto endpt.: 10.1.13.2, remote crypto endpt.: 0.0.0.0
path mtu 1500, ip mtu 1500, ip mtu idb Serial1/0
current outbound spi: 0x8BF147EF(2347845615)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x8BF147EF(2347845615)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 1, flow_id: SW:1, sibling_flags 80000040, crypto map: gm1map
sa timing: remaining key lifetime (sec): (192)
Kilobyte Volume Rekey has been disabled
IV size: 8 bytes
replay detection support: Y replay window size: 4
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x8BF147EF(2347845615)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2, flow_id: SW:2, sibling_flags 80000040, crypto map: gm1map
sa timing: remaining key lifetime (sec): (192)
Kilobyte Volume Rekey has been disabled
IV size: 8 bytes
replay detection support: Y replay window size: 4
Status: ACTIVE(ACTIVE)
```

```
outbound ah sas:

outbound pcp sas:
GM1#
```

> **Nota:** Con GETVPN, le associazioni di protezione in entrata e in uscita utilizzano lo stesso SPI.

Con la registrazione di GETVPN e il tipo di installazione dei criteri, questi debug sono necessari per risolvere:

```
debug crypto isakmp (KS and GM)
debug crypto gdoi ks registration all-levels (KS)
debug crypto gdoi gm registration all-level (GM)
debug crypto engine (GM only)
show crypto eli detail (multiple iterations on GM)
```

> **Nota:** A seconda dei risultati, potrebbero essere necessari ulteriori debug.

Poiché la registrazione di GETVPN in genere avviene immediatamente dopo il ricaricamento di GM, questo script EEM può essere utile per raccogliere i seguenti debug:

```
event manager applet debug
event syslog pattern "RESTART"
action 1.0 cli command "enable"
action 2.0 cli command "debug crypto gdoi all all"
```

## Reimposta

Una volta che gli GM sono registrati sul KS e la rete GETVPN è configurata correttamente, il KS primario è responsabile dell'invio di messaggi di reimpostazione delle chiavi a tutti gli GM registrati su di esso. I messaggi di reimpostazione delle chiavi vengono utilizzati per sincronizzare tutte le policy, le chiavi e le pseudotipi sugli oggetti GM. I messaggi di reimpostazione chiavi possono essere inviati tramite un metodo unicast o multicast.

Questo messaggio syslog viene visualizzato sul KS quando si invia il messaggio di reimpostazione della chiave:

```
%GDOI-5-KS_SEND_UNICAST_REKEY: Sending Unicast Rekey for group G1 from address
10.1.11.2 with seq # 11
```

Sugli OGM, questo è il syslog che viene visto quando riceve la chiave di nuovo:

```
%GDOI-5-GM_RECV_REKEY: Received Rekey for group G1 from 10.1.11.2 to 10.1.20.2
with seq # 11
```

### Requisiti della coppia di chiavi RSA per la reimpostazione delle chiavi su KS

La funzionalità di reimpostazione delle chiavi richiede la presenza di chiavi RSA sul KS. Il KS fornisce la chiave pubblica della coppia di chiavi RSA al GM tramite questo canale sicuro durante la registrazione. Il KS firma quindi i messaggi GDOI inviati al GM con la chiave RSA privata nel payload GDOI SIG. L'amministratore delegato riceve i messaggi GDOI e usa la chiave RSA pubblica per verificare il messaggio. I messaggi tra KS e GM sono criptati con il KEK, che viene

distribuito anche al GM durante la registrazione. Al termine della registrazione, le successive chiavi vengono crittografate con la chiave KEK e firmate con la chiave RSA privata.

Se la chiave RSA non è presente sul KS durante la registrazione di un OGM, sul syslog viene visualizzato questo messaggio:

```
%GDOI-1-KS_NO_RSA_KEYS: RSA Key - get : Not found, Required for group G1
```

Quando i tasti non sono presenti sul KS, il GM si registra per la prima volta, ma la successiva rigenerazione non riesce dal KS. Alla fine le chiavi esistenti sul GM scadono e si registra nuovamente.

```
%GDOI-4-GM_RE_REGISTER: The IPSec SA created for group G1 may have expired/been
cleared, or didn't go through. Re-register to KS.
```

Poiché la coppia di chiavi RSA viene utilizzata per firmare i messaggi di rigenerazione della chiave, **DEVE** essere la stessa per tutti i KS primario e secondario. In questo modo, durante un guasto del KS primario, le richiavi inviate da un KS secondario (il nuovo KS primario) possono ancora essere convalidate correttamente dagli GM. Quando genera la coppia di chiavi RSA sul KS primario, la coppia di chiavi deve essere creata con l'opzione **exportable** in modo che possano essere esportate in tutti i KS secondari per soddisfare questo requisito.

#### Reimposta risoluzione dei problemi

L'errore di reimpostazione della chiave KEK/TEK è uno dei problemi più comuni di GETVPN riscontrati nelle installazioni dei clienti. Per risolvere i problemi relativi alla reimpostazione delle chiavi, seguire i passaggi descritti di seguito:

1. Le chiavi sono state inviate dal KS?

   Èpossibile verificare questa condizione tramite un'osservazione del messaggio syslog %GDOI-5-KS_SEND_UNICAST_REKEY o in modo più accurato tramite questo comando:

   ```
   KS1#show crypto gdoi ks rekey
   Group G1 (Unicast)
   Number of Rekeys sent               : 341
   Number of Rekeys retransmitted      : 0
   KEK rekey lifetime (sec) : 1200
   Remaining lifetime (sec) : 894
   Retransmit period : 10
   Number of retransmissions : 5
   IPSec SA 1 lifetime (sec) : 900
   Remaining lifetime (sec) : 405
   ```

   Il numero di chiavi ritrasmesse è indicativo dei pacchetti di conferma della chiave non ricevuti dal KS e pertanto di possibili problemi di chiave. Tenete presente che la reimpostazione della chiave GDOI utilizza UDP come meccanismo di trasporto inaffidabile, quindi ci si potrebbe aspettare qualche calo di reimpostazione della chiave a seconda dell'affidabilità della rete di trasporto sottostante, ma si dovrebbe sempre studiare una tendenza ad aumentare le ritrasmissioni della chiave.

   Si possono ottenere anche statistiche più dettagliate sulle chiavi rekey per GM. Si tratta in

genere del primo luogo in cui vengono ricercati potenziali problemi di reimpostazione delle chiavi.

```
KS1#show crypto gdoi ks members

Group Member Information :

Number of rekeys sent for group G1 : 346

Group Member ID : 10.1.14.2 GM Version: 1.0.4
Group ID : 3333
Group Name : G1
Key Server ID : 10.1.11.2
 Rekeys sent       : 346
Rekeys retries : 0
Rekey Acks Rcvd : 346
Rekey Acks missed : 0

Sent seq num : 2 1 2 1
Rcvd seq num : 2 1 2 1

Group Member ID : 10.1.13.2 GM Version: 1.0.4
Group ID : 3333
Group Name : G1
Key Server ID : 10.1.12.2
 Rekeys sent       : 340
Rekeys retries : 0
Rekey Acks Rcvd : 340
Rekey Acks missed : 0

Sent seq num : 2 1 2 1
Rcvd seq num : 2 1 2 1
```

2. I pacchetti di reimpostazione delle chiavi sono stati recapitati nella rete dell'infrastruttura sottostante?

   Si consiglia di seguire la risoluzione dei problemi IP standard lungo il percorso di inoltro della chiave di nuova generazione per essere certi che i pacchetti della chiave di nuova generazione non vengano scartati nella rete di transito tra KS e GM. Alcuni strumenti comuni di risoluzione dei problemi utilizzati qui sono gli Access Control Lists (ACL) di input/output, Netflow e l'acquisizione dei pacchetti nella rete di transito.

3. I pacchetti di reimpostazione delle chiavi hanno raggiunto il processo GDOI per l'elaborazione della reimpostazione delle chiavi?

   Controllare le statistiche di reimpostazione chiavi GM:

```
GM1#show crypto gdoi gm rekey
Group G1 (Unicast)
Number of Rekeys received (cumulative) : 340
Number of Rekeys received after registration : 340
Number of Rekey Acks sent : 340
```

4. Il pacchetto di conferma della reimpostazione della chiave è stato restituito al servizio KS?

   Seguire i passaggi da 1 a 3 per rintracciare il pacchetto di conferma della chiave di ripristino

dal GM al KS.

#### Reimpostazione chiavi multicast

La rigenerazione della chiave multicast è diversa dalla rigenerazione della chiave unicast per questi aspetti:

- Poiché il multicast viene utilizzato per trasportare questi pacchetti di reimpostazione delle chiavi dal KS agli GM, il KS non deve replicare i pacchetti di reimpostazione delle chiavi. Il servizio KS invia solo una copia del pacchetto di rigenerazione delle chiavi, che vengono replicate nella rete abilitata per il multicast.
- Non esiste un meccanismo di riconoscimento per la chiave multicast, quindi se un GM non ricevesse il pacchetto di rigenerazione delle chiavi, il KS non ne sarebbe a conoscenza e non rimuoverebbe mai un GM dal suo database GM. E siccome non c'è conferma, il servizio KS trasmette sempre nuovamente i pacchetti di rekey in base alla configurazione di rekey transmission.

Il problema più comune della reimpostazione della chiave multicast si verifica quando la reimpostazione della chiave non viene ricevuta sul server GM. Le possibili cause potrebbero essere diverse, ad esempio:

- Problema di consegna dei pacchetti all'interno dell'infrastruttura di routing multicast
- Routing multicast end non abilitato nella rete

Il primo passaggio per risolvere un problema relativo alla reimpostazione della chiave multicast consiste nel verificare se la reimpostazione della chiave funziona quando si passa dal metodo multicast a quello unicast.

Dopo aver identificato che il problema è specifico della chiave multicast, verificare che KS invii la nuova chiave all'indirizzo multicast specificato.

```
%GDOI-5-KS_SEND_MCAST_REKEY: Sending Multicast Rekey for group G1 from address
10.1.11.2 to 226.1.1.1 with seq # 6
```

Verificare la connettività multicast tra KS e GM con una richiesta ICMP (Internet Control Message Protocol) all'indirizzo multicast. Tutti gli OGM che fanno parte del gruppo multicast devono rispondere al ping. Verificare che ICMP sia escluso dai criteri di crittografia KS per il test.

```
KS1#ping 226.1.1.1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 226.1.1.1, timeout is 2 seconds:

Reply to request 0 from 10.1.21.2, 44 ms
```

Se il test ping multicast ha esito negativo, è necessario eseguire la risoluzione dei problemi multicast, che non rientra nell'ambito di questo documento.

### Controllo relè piano di controllo

#### Sintomo

Quando i clienti aggiornano il proprio GM a una nuova versione di Cisco IOS, potrebbero

riscontrare errori di reimpostazione chiavi KEK con questo messaggio osservato nel syslog:

```
%GDOI-3-GDOI_REKEY_SEQ_FAILURE: Failed to process rekey seq # 1 in seq payload for
group G1, last seq # 11
%GDOI-3-GDOI_REKEY_FAILURE: Processing of REKEY payloads failed on GM 10.1.13.2 in the group G1,
with peer at 10.1.11.2
%CRYPTO-6-IKMP_MODE_FAILURE: Processing of GDOI mode failed with peer at 10.1.11.2
```

Questo comportamento è causato da un problema di interoperabilità introdotto con il controllo anti-replay aggiunto per i messaggi del control plane. In particolare, un KS che esegue il codice precedente reimposterà il numero di sequenza di reimpostazione chiavi KEK su 1, e questo verrà scartato dal GM che esegue il nuovo codice quando lo interpreta come un pacchetto di reimpostazione chiavi riprodotto. Per ulteriori informazioni, vedere l'ID bug Cisco CSCta05809 (GETVPN: GETVPN control-plane sensibile alla riproduzione) e GETVPN Configuration Restrictions.

#### Sfondo

Con GETVPN, i messaggi del Control Plane possono trasportare informazioni sensibili al tempo per fornire il servizio di controllo anti-replay basato sul tempo. Pertanto, questi messaggi richiedono la protezione anti-replay per garantire la precisione del tempo. Questi messaggi sono:

- **Reimposta messaggi** da KS a GM
- **Messaggi di annuncio COOP** tra KS

Nell'ambito di questa implementazione della protezione anti-replay, sono stati aggiunti controlli del numero di sequenza per proteggere i messaggi riprodotti, oltre a un controllo pseudotime quando TBAR è abilitato.

## Soluzione

Per risolvere questo problema, sia la versione GM che la versione KS devono essere aggiornate alle versioni Cisco IOS dopo la funzione di controllo della ripetizione sul piano di controllo. Con il nuovo codice Cisco IOS, KS non reimposta il numero di sequenza su 1 per una chiave di nuovo KEK, ma continua a utilizzare il numero di sequenza corrente e reimposta solo il numero di sequenza per le chiavi di nuovo TEK.

Queste versioni di Cisco IOS dispongono delle funzionalità di controllo della riproduzione:

- 12.4(15)T10
- 12.4(22)T3
- 12.4(24)T2
- 15.0(1)M e versioni successive

#### Altri problemi correlati alla ripetizione

- Errore COOP a causa di un errore nel controllo della riproduzione dei messaggi ANN (ID bug Cisco CSCtc52655)

#### Errori di riesecuzione del piano di controllo di debug

Per altri errori di ripetizione del piano di controllo, raccogliere queste informazioni e assicurarsi che

i tempi siano sincronizzati tra KS e GM.

- Syslog da GM e KS
- Debug ISAKMP
- Debug GDOI (rekey e replay) da KS e GM

## Problemi di frammentazione dei pacchetti Control Plane

Con GETVPN, la frammentazione dei pacchetti del Control Plane è un problema comune e può manifestarsi in uno di questi due scenari quando i pacchetti del Control Plane sono così grandi da richiedere la frammentazione IP:

- Pacchetti di annuncio GETVPN COOP
- Ottieni pacchetti di reimpostazione chiavi VPN

### Pacchetti annuncio COOP

I pacchetti COOP Announcement contengono le informazioni del database GM e possono quindi crescere in modo significativo in un'installazione GETVPN di grandi dimensioni. In base all'esperienza passata, una rete GETVPN composta da oltre 1500 GM produrrà pacchetti di annuncio superiori a 18024 byte, ovvero le dimensioni predefinite del buffer di Cisco IOS. In questo caso, il KS non riesce ad allocare un buffer abbastanza grande da trasmettere i pacchetti ANN con questo errore:

```
%SYS-2-GETBUF: Bad getbuffer, bytes= 18872 -Process= "Crypto IKMP", ipl= 0, pid= 183
```

Per risolvere questo problema, si consiglia di eseguire il tuning del buffer:

```
buffers huge permanent 10
buffers huge size 65535
```

#### Reimposta chiavi pacchetti

I pacchetti di rigenerazione delle chiavi GETVPN possono inoltre superare le dimensioni tipiche di 1500 MTU (Maximum Transition Unit) IP quando i criteri di crittografia sono grandi, ad esempio un criterio costituito da più di 8 righe di voci di controllo di accesso (ACE, Access Control Entries) nell'ACL di crittografia.

#### Problema di frammentazione e identificazione

In entrambi gli scenari precedenti, per il corretto funzionamento della chiave COOP o GDOI, GETVPN deve essere in grado di trasmettere e ricevere correttamente i pacchetti UDP frammentati. La frammentazione IP può essere un problema in alcuni ambienti di rete. Ad esempio, una rete costituita da un piano di inoltro ECMP (Equal Cost Multi Path) e alcuni dispositivi del piano di inoltro richiedono il riassemblaggio virtuale dei pacchetti IP frammentati, ad esempio il riassemblaggio della frammentazione virtuale (VFR).

Per identificare il problema, controllare gli errori di riassemblaggio sul dispositivo dove si sospetta che i pacchetti UDP 848 frammentati non vengano ricevuti correttamente:

```
KS1#show ip traffic | section Frags
```

```
Frags: 10 reassembled, 3 timeouts, 0 couldn't reassemble
0 fragmented, 0 fragments, 0 couldn't fragment
```

Se i timeout di riassemblaggio continuano ad aumentare, usare il comando **debug ip error** per verificare se il rilascio fa parte del flusso del pacchetto rekey/COOP. Dopo la conferma, si consiglia di eseguire la normale procedura di risoluzione dei problemi di inoltro IP per isolare l'esatto dispositivo sul piano di inoltro che potrebbe aver perso i pacchetti. Di seguito sono riportati alcuni strumenti utilizzati comunemente:

- Acquisizione pacchetti
- Statistiche inoltro traffico
- Statistiche delle funzionalità di sicurezza (firewall, IPS)
- Statistiche VFR

#### Problemi di interoperabilità GDOI

Nel corso degli anni sono stati riscontrati diversi problemi di interoperabilità con GETVPN ed è fondamentale notare le versioni di Cisco IOS tra KS e GM e tra gli KS per i problemi di interoperabilità.

Altri problemi noti di interoperabilità GETVPN sono:

- Controllo relè piano di controllo
- Modifica comportamento reimpostazione chiave GETVPN
- ID bug Cisco CSCub42920 (GETVPN: KS non riesce a convalidare l'hash nella rekey ACK (da versioni precedenti di GM)
- ID bug Cisco CSCuw48400 (GetVPN GM non è in grado di registrare o reimpostare la chiave sui bug - sig-hash > SHA-1 predefinito)
- ID bug Cisco CSCvg19281 ( più arresti anomali di GETVPN GM dopo la migrazione a una nuova coppia di KS ; se una versione GM è precedente alla 3.16 e KS viene aggiornato da un codice precedente alla 3.16 o successiva, il problema può verificarsi)

##### Procedura di aggiornamento GETVPN IOS

Questa procedura di aggiornamento del codice Cisco IOS deve essere seguita quando è necessario eseguire un aggiornamento del codice Cisco IOS in un ambiente GETVPN:

1. Aggiornare prima un KS secondario e attendere il completamento della scelta di COOP KS.
2. Ripetere il punto 1 per tutti i KS secondari.
3. Aggiornare il KS primario.
4. Aggiornare gli oggetti GM.

## Risoluzione dei problemi di GETVPN Data Plane

Rispetto ai problemi del Control Plane, i problemi del Data Plane GETVPN sono problemi in cui il GM ha la policy e le chiavi per eseguire la crittografia e la decrittografia del dataplane, ma per qualche motivo il flusso di traffico end-to-end non funziona. La maggior parte dei problemi relativi al dataplane per GETVPN si riferisce all'inoltro IPsec generico e non è specifica di GETVPN. Pertanto, la maggior parte dell'approccio di risoluzione dei problemi qui descritto si applica anche ai problemi generici delle corsie dati IPsec.

Con i problemi di crittografia (tunnel basati su gruppo o a coppie), è importante risolvere il problema e isolarlo in una determinata parte del percorso dati. In particolare, l'approccio alla risoluzione dei problemi descritto di seguito ha lo scopo di aiutare l'utente a rispondere alle seguenti domande:

- Quale dispositivo è il responsabile della crittografia del router o della decrittografia del router?
- In che direzione sta avvenendo il problema - in entrata o in uscita?

## Strumenti di risoluzione dei problemi GETVPN Data Plane

La risoluzione dei problemi del dataplane IPsec è molto diversa da quella del Control Plane. Con il dataplane, in genere non sono presenti debug che è possibile eseguire o almeno eseguire in modo sicuro in un ambiente di produzione. La risoluzione dei problemi si basa quindi in gran parte su contatori e statistiche del traffico diversi che possono aiutare a tracciare il pacchetto lungo un percorso di inoltro. L'idea è quella di sviluppare una serie di checkpoint che aiutino ad isolare dove i pacchetti potrebbero essere scartati, come mostrato di seguito:


Di seguito sono riportati alcuni strumenti di debug del piano dati:

- Elenchi di accesso
- Accounting IP Precedence
- NetFlow
- Contatori interfaccia
- Contatori crittografia
- Contatori globali e per singola funzione di eliminazione IP Cisco Express Forwarding (CEF)
- EPC (Embedded Packet Capture)
- Debug del piano dati (debug di pacchetti IP e CEF)

I checkpoint nel datapath dell'immagine precedente possono essere convalidati con questi strumenti:

### Crittografia di GM

- Interfaccia LAN in ingresso
  - ACL di input
  - NetFlow in ingresso
  - Embedded Packet Capture
  - Input precedence accounting

- Motore di crittografia
  - **show crypto ipsec sa**
  - **mostra dettagli sa crypto ipsec**
  - **mostra statistiche dell'acceleratore del motore crittografico**

- Esci dall'interfaccia WAN
    Netflow in uscita
    Embedded Packet Capture
    Accounting priorità output

### Decrittografia di GM

- Interfaccia WAN in ingresso
    ACL di input
    NetFlow in ingresso
    Embedded Packet Capture
    Input precedence accounting

- Motore di crittografia
    **show crypto ipsec sa**
    **mostra dettagli sa crypto ipsec**
    **mostra statistiche dell'acceleratore del motore crittografico**

- Interfaccia LAN in uscita
    Netflow in uscita
    Acquisizione dei pacchetti integrata

Il percorso di ritorno segue lo stesso flusso di traffico. Nelle sezioni seguenti vengono illustrati alcuni esempi di questi strumenti per le corsie dati.

### Contatori crittografia/decrittografia

I contatori di crittografia/decrittografia su un router sono basati su un flusso IPsec. Sfortunatamente, questo non funziona bene con GETVPN, poiché GETVPN in genere distribuisce una policy di crittografia "allow ip any" (permetti qualsiasi) che crittografa tutto. Quindi, se il problema si verifica solo per alcuni dei flussi e non per tutti, l'uso di questi contatori può risultare difficoltoso per valutare correttamente se i pacchetti sono crittografati o decriptati quando c'è abbastanza traffico in background che funziona.

```
GM1#show crypto ipsec sa | in encrypt|decrypt
#pkts encaps: 100, #pkts encrypt: 100, #pkts digest: 100
#pkts decaps: 100, #pkts decrypt: 100, #pkts verify: 100
```

### NetFlow

Netflow può essere usato per monitorare sia il traffico in entrata che in uscita su entrambi gli GM. Nota con il GETVPN **allow ip qualsiasi** criterio, il traffico crittografato verrà aggregato e non fornirà le informazioni per flusso. Le informazioni per flusso dovranno quindi essere raccolte con il contrassegno di precedenza DSCP/DSCP descritto più avanti.

In questo esempio, il netflow per un ping di 100 conteggi da un host dietro GM1 a un host dietro GM2 viene mostrato nei vari checkpoint.

### Crittografia di GM

Configurazione NetFlow:

```
interface Ethernet0/0
description LAN
ip address 192.168.13.1 255.255.255.0
ip flow ingress
ip pim sparse-dense-mode
!
interface Serial1/0
description WAN interface
ip address 10.1.13.2 255.255.255.252
ip flow egress
ip pim sparse-dense-mode
crypto map gm1map
```

Uscita NetFlow:

```
GM1#show ip cache flow | be SrcIf
SrcIf SrcIPaddress DstIf DstIPaddress Pr SrcP DstP Pkts
Et0/0 192.168.13.2 Se1/0* 192.168.14.2 32 8DE1 6523   100
Et0/0 192.168.13.2 Se1/0 192.168.14.2 01 0000 0800   100
GM1#
```

> **Nota:** Nell'output precedente, * indica il traffico in uscita. La prima riga mostra il traffico crittografato in uscita (con protocollo 0x32 = ESP) dall'interfaccia WAN e la seconda riga il traffico ICMP in entrata che colpisce l'interfaccia LAN.

### Decrittografia di GM

Configurazione:

```
interface Ethernet0/0
description LAN interface
ip address 192.168.14.1 255.255.255.0
ip flow egress
ip pim sparse-dense-mode
!
interface Serial1/0
description WAN interface
ip address 10.1.14.2 255.255.255.252
ip flow ingress
ip pim sparse-dense-mode
crypto map gm1map
```

Uscita NetFlow:

```
GM2#show ip cache flow | be SrcIf
SrcIf SrcIPaddress DstIf DstIPaddress Pr SrcP DstP Pkts
Se1/0 192.168.13.2 Et0/0 192.168.14.2 32 8DE1 6523   100
Se1/0 192.168.13.2 Et0/0* 192.168.14.2 01 0000 0800   100
GM2#
```

### Contrassegno di precedenza DSCP/IP

Il problema con la risoluzione dei problemi di crittografia è che una volta crittografato il pacchetto, si perde la visibilità nel payload, che è la funzione della crittografia, e questo rende difficile tracciare il pacchetto per un particolare flusso IP. Per risolvere questo problema, è possibile procedere in due modi:

- Utilizzare ESP-NULL come trasformazione IPSec. IPsec esegue ancora l'incapsulamento ESP, ma non viene applicata alcuna crittografia al payload, in modo che siano visibili in un'acquisizione pacchetto.
- Contrassegnare un flusso IP con un DSCP (Differentiated Services Code Point)/contrassegno di precedenza univoco in base alle relative caratteristiche L3/L4.

ESP-NULL richiede modifiche su entrambi gli endpoint del tunnel e spesso non è consentito in base ai criteri di sicurezza del cliente. Pertanto, Cisco in genere consiglia di utilizzare invece il contrassegno di precedenza/DSCP.

#### Grafico di riferimento DSCP/Precedence

| ToS (hex) | ToS(Decimale) | Precedenza IP | DSCP | Binario |
|---|---|---|---|---|
| 0xE0 | 224 | 7 Controllo della rete | 56 CS7 | 11100000 |
| 0xC0 | 192 | 6 Controllo Internetwork | 48 CS6 | 11000000 |
| 0xB8 | 184 | 5 Critiche | 46 EF | 10111000 |
| 0xA0 | 160 | | 40 CS5 | 10100000 |
| 0x88 | 136 | 4 Flash Override | 34 AF41 | 10001000 |
| 0x80 | 128 | | 32 CS4 | 10000000 |
| 0x68 | 104 | 3 Flash | 26 AF31 | 01101000 |
| 0x60 | 96 | | 24 CS3 | 01100000 |
| 0x48 | 72 | 2 Immediato | 18 AF21 | 01001000 |
| 0x40 | 64 | | 16 CS2 | 01000000 |
| 0x20 | 32 | 1 Priorità | 8 CS1 | 00100000 |
| 0x00 | 0 | 0 Routine | 0 Dflt | 00000000 |

#### Contrassegna pacchetti con DSCP/Precedenza

Questi metodi sono in genere utilizzati per contrassegnare i pacchetti con le marcature DSCP/Precedence specifiche.

### PBR

```
interface Ethernet1/0
ip policy route-map mark
!
access-list 150 permit ip host 172.16.1.2 host 172.16.254.2
!
route-map mark permit 10
match ip address 150
set ip precedence flash-override
```

### MQC

```
class-map match-all my_flow
match access-group 150
!
policy-map marking
class my_flow
set ip precedence 4
!
interface Ethernet1/0
service-policy input marking
```

### Ping router

```
GM1-host#ping ip
Target IP address: 192.168.14.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface:
Type of service [0]: 136
...
<snip>
```

> **Nota:** È sempre consigliabile monitorare il flusso del traffico normale e il profilo DSCP/precedenza prima di applicare il contrassegno in modo che il flusso del traffico contrassegnato sia univoco.

#### Monitora pacchetti contrassegnati

### Accounting IP Precedence

```
interface Ethernet0/0
ip address 192.168.1.2 255.255.255.0
ip accounting precedence input
```

```
middle_router#show interface precedence
Ethernet0/0
Input
Precedence 4: 100 packets, 17400 bytes
```

### ACL interfaccia

```
middle_router#show access-list 144
Extended IP access list 144
10 permit ip any any precedence routine
20 permit ip any any precedence priority
30 permit ip any any precedence immediate
40 permit ip any any precedence flash
50 permit ip any any precedence flash-override (100 matches)
60 permit ip any any precedence critical
70 permit ip any any precedence internet (1 match)
80 permit ip any any precedence network
```

### Embedded Packet Capture

L'EPC (Embedded Packet Capture) è uno strumento utile per acquisire i pacchetti a livello di interfaccia e identificare se un pacchetto ha raggiunto un dispositivo specifico. L'EPC è adatto al traffico in formato testo non crittografato, ma può rappresentare un problema quando i pacchetti acquisiti vengono crittografati. Pertanto, per rendere più efficace la risoluzione dei problemi, è necessario utilizzare insieme all'EPC tecniche quali il contrassegno di precedenza/DSCP descritto in precedenza o altri caratteri IP, come la lunghezza del pacchetto IP.

### Cisco IOS-XE Packet Trace

Questa funzionalità è utile per tracciare il percorso di inoltro delle funzionalità su tutte le piattaforme che eseguono Cisco IOS-XE, ad esempio CSR1000v, ASR1000 e ISR4451-X.

## Problemi comuni di GETVPN Data Plane

La risoluzione dei problemi del dataplane IPsec per GETVPN non è per lo più diversa dalla risoluzione dei tradizionali problemi del dataplane IPsec point-to-point, con due eccezioni dovute a queste proprietà univoche del dataplane di GETVPN.

### Errore Anti-Replay Basato Su Tempo

In una rete GETVPN, gli errori TBAR possono spesso essere difficili da risolvere perché non sono più presenti tunnel a coppie. Per risolvere i problemi relativi agli errori di GETVPN TBAR, procedere come segue:

1. Identificare il pacchetto che viene scartato a causa di un errore TBAR e successivamente identificare l'algoritmo di crittografia.

   Nelle versioni precedenti alla 15.3(2)T, il syslog degli errori TBAR non aveva stampato l'indirizzo di origine del pacchetto in errore, rendendo molto difficile identificare il pacchetto in errore. Questa funzionalità è stata notevolmente migliorata nella versione 15.3(2)T e successive, dove Cisco IOS stampa quanto segue:

   ```
   %CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed
   connection id=13, sequence number=1

   %GDOI-4-TIMEBASED_REPLAY_FAILED: An anti replay check has failed in group G1:
   my_pseudotime = 620051.84 secs, peer_pseudotime = 619767.09 secs, replay_window =
   4 (sec), src_ip = 192.168.13.2, dst_ip = 192.168.14.2
   ```

   In questa versione è stata implementata anche una cronologia TBAR:

   ```
   GM2#show crypto gdoi gm replay
   Anti-replay Information For Group G1:
   Timebased Replay:
   Replay Value : 621388.66 secs
   Input Packets : 0 Output Packets : 0
   Input Error Packets : 2 Output Error Packets : 0
   Time Sync Error : 0 Max time delta : 0.00 secs


   TBAR Error History (sampled at 10pak/min):
   19:29:32.081 EST Wed Nov 13 2013: src=192.168.13.2; my_pst=620051.84 secs;
   peer_pst=619767.09 secs; win=4
   ```

   **Nota:** I miglioramenti menzionati precedentemente sono stati implementati in Cisco IOS-XE dall'ID bug Cisco CSCun49335 e in Cisco IOS dall'ID bug Cisco CSCub91811.
   Per le versioni Cisco IOS in cui questa funzionalità non è disponibile, è possibile fornire queste informazioni anche **nei dettagli di riproduzione GDM di debug crypto**, sebbene questo debug stamperà le informazioni TBAR per tutto il traffico (non solo per i pacchetti scartati a causa di errori TBAR), quindi potrebbe non essere possibile eseguirlo in un ambiente di

produzione.

```
GDOI:GM REPLAY:DET:(0):my_pseudotime is 621602.30 (secs), peer_pseudotime is 621561.14
(secs), replay_window is 4 (secs), src_addr = 192.168.14.2, dest_addr = 192.168.13.2
```

2. Una volta identificata l'origine del pacchetto, dovrebbe essere possibile trovare il file GM crittografato. Quindi, lo pseudotimestamp su entrambi gli GM di crittografia e decrittografia deve essere monitorato per ogni potenziale deriva pseudotime. Il modo migliore per farlo sarebbe quello di sincronizzare sia gli GM che il KS con l'NTP e raccogliere periodicamente le informazioni pseudotime con un orologio di sistema di riferimento su tutti loro al fine di determinare se il problema è causato da sfasamento di clock sugli GM.

GM1

```
GM1#show crypto gdoi gm replay
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *21:06:26.469 EST Wed Nov 13 2013

Anti-replay Information For Group G1:
Timebased Replay:
Replay Value             : 625866.26 secs
Input Packets : 0 Output Packets : 0
Input Error Packets : 0 Output Error Packets : 0
Time Sync Error : 0 Max time delta : 0.00 secs
```

GM2

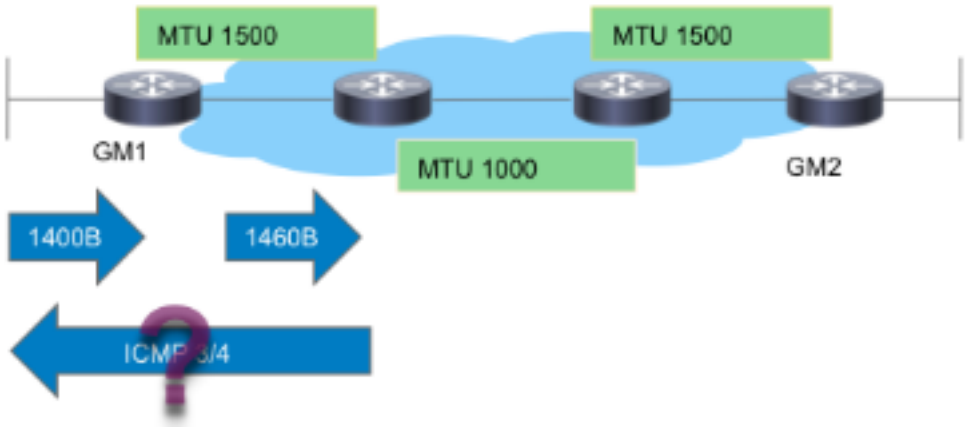
```
GM2#show crypto gdoi gm replay
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *21:06:26.743 EST Wed Nov 13 2013

Anti-replay Information For Group G1:
Timebased Replay:
Replay Value             : 625866.51 secs
Input Packets : 4 Output Packets : 4
Input Error Packets : 2 Output Error Packets : 0
Time Sync Error : 0 Max time delta : 0.00 secs
```

Nell'esempio precedente, se lo pseudotime (come indicato da Replay Value) è significativamente diverso tra gli oggetti GM quando le uscite vengono catturate con lo stesso tempo di riferimento, il problema può essere attribuito all'inclinazione dell'orologio.

> **Nota:** Sulla piattaforma Cisco Aggregated Services Router serie 1000, a causa dell'architettura della piattaforma, il datapath sul Quantum Flow Processor (QFP) in realtà si riferisce all'orologio a parete per contare i tick pseudotimi. Ciò ha creato problemi con TBAR quando l'ora dell'orologio a parete cambia a causa della sincronizzazione NTP. Questo problema è documentato con l'ID bug Cisco CSCum37911.

#### Conservazione delle intestazioni PMTUD e GETVPN

Con GETVPN, il rilevamento della MTU del percorso (PMTUD) non funziona tra gli oggetti GM in crittografia e decrittografia, mentre i pacchetti di grandi dimensioni con bit "non frammentare" (DF, Don't Fragment) impostato possono rimanere bloccati. Il problema è dovuto alla conservazione dell'intestazione GETVPN, in cui gli indirizzi di origine/destinazione dei dati vengono mantenuti nell'intestazione di incapsulamento ESP. Questa è l'immagine:




Come mostrato nell'immagine, il PMTUD si interrompe con GETVPN con questo flusso:

1. Un grande pacchetto di dati arriva sul GM1 di crittografia.
2. Il pacchetto ESP post-crittografia viene inoltrato fuori da GM1 e consegnato alla destinazione.
3. Se esiste un collegamento in transito con MTU IP di 1400 byte, il pacchetto ESP viene scartato e un messaggio ICMP 3/4 troppo grande viene inviato all'origine del pacchetto, che è l'origine del pacchetto dati.
4. Il pacchetto ICMP3/4 viene scartato perché l'ICMP non è escluso dai criteri di crittografia GETVPN, oppure viene scartato dall'host finale perché non sa nulla del pacchetto ESP (payload non autenticato).

In breve, la funzionalità PMTUD non funziona con GETVPN oggi. Per risolvere questo problema, Cisco consiglia la seguente procedura:

1. Implementare il protocollo "ip tcp adjust-mss" per ridurre le dimensioni del segmento del pacchetto TCP in modo da supportare il sovraccarico di crittografia e la MTU del percorso minimo nella rete di transito.
2. Per evitare la funzionalità PMTUD, annullare il bit DF nel pacchetto dati in arrivo sul file GM crittografato.

### Problemi generici del dataplane IPsec

La maggior parte delle procedure per la risoluzione dei problemi dei dataplane IPsec è analoga alla risoluzione dei problemi dei tunnel IPsec point-to-point tradizionali. Uno dei problemi più comuni è %CRYPTO-4-RECVD_PKT_MAC_ERR. Per ulteriori informazioni sulla risoluzione dei problemi, vedere il messaggio di errore Syslog "%CRYPTO-4-RECVD_PKT_MAC_ERR:" con la risoluzione dei problemi del tunnel Ping Loss Over IPsec.

### Problemi noti

Questo messaggio può essere generato quando si riceve un pacchetto IPsec che non corrisponde a un SPI nel SADB. Vedere l'ID bug Cisco CSCtd47420 - GETVPN - CRYPTO-4-RECVD_PKT_NOT_IPSEC segnalato per il flusso del pacchetto non corrispondente. Un esempio è:

```
%CRYPTO-4-RECVD_PKT_NOT_IPSEC: Rec'd packet not an IPSEC packet. (ip)
```

```
vrf/dest_addr= /192.168.14.2, src_addr= 192.168.13.2, prot= 50
```

Il messaggio dovrebbe essere %CRYPTO-4-RECVD_PKT_INV_SPI, che è ciò che viene segnalato per IPsec tradizionale e su alcune piattaforme hardware come ASR. Il problema cosmetico è stato risolto dall'ID bug Cisco CSCup80547: Errore nella segnalazione di CRYPTO-4-RECVD_PKT_NOT_IPSEC per ESP pak.

> **Nota:** Questi messaggi possono a volte essere visualizzati a causa di un altro bug GETVPN CSCup3471: GETVPN GM interrompe la decrittografia del traffico dopo la reimpostazione della chiave TEK.

In questo caso, il server GM non può decrittografare il traffico GETVPN, anche se dispone di un'associazione di protezione IPsec valida nel database SADB (associazione di protezione da reimpostare). Il problema scompare non appena l'associazione di protezione scade e viene rimossa dall'SADB. Questo problema causa un'interruzione significativa, in quanto la chiave TEK viene eseguita in anticipo. Ad esempio, l'interruzione può essere di 22 minuti nel caso di una durata TEK di 7200 secondi. Per informazioni sulla condizione esatta da soddisfare per rilevare il bug, consultare la descrizione del bug.

# Risoluzione dei problemi di GETVPN sulle piattaforme con Cisco IOS-XE

## Comandi per la risoluzione dei problemi

Le piattaforme che eseguono Cisco IOS-XE hanno implementazioni specifiche e spesso richiedono il debug specifico della piattaforma per i problemi GETVPN. Di seguito è riportato un elenco di comandi utilizzati in genere per risolvere i problemi di GETVPN su queste piattaforme:

**show crypto eli all**

**mostra statistiche criteri ipsec software della piattaforma**

**show platform software ipsec fp active inventory**

**show platform hardware qfp active feature ipsec spd all**

**mostra eliminazione statistiche attive qfp hardware piattaforma**

**show platform hardware qfp active feature ipsec data drop clear**

**show crypto ipsec sa**

**show crypto gdoi**

**show crypto ipsec internal**

**debug crypto ipsec**

**errore debug crypto ipsec**

**debug stati ipsec di crittografia**

**debug crypto ipsec message**

**debug crypto ipsec hw-req**

**dettagli infra debug crypto gdoi gm**

**dettagli della richiave gm di debug crypto**

### Problemi comuni di ASR1000

#### Errore di installazione del criterio IPSec (nuova registrazione continua)

Èpossibile che un ASR1000 GM continui a registrarsi sul server chiavi se il motore di crittografia non supporta la policy o l'algoritmo IPsec ricevuto. Ad esempio, sulle piattaforme ASR basate su Nitrox (come ASR1002), le policy Suite-B o SHA2 non sono supportate e questo può causare i sintomi di una nuova registrazione continua.

## Problemi comuni di migrazione/aggiornamento

### Limitazione barra ASR1000

Sulla piattaforma ASR1000, la correzione dell'ID bug Cisco CSCum37911 ha introdotto un limite su questa piattaforma dove non è supportato il tempo TBAR inferiore a 20 secondi. Vedere Restrizioni per GETVPN su IOS-XE.

Questo bug è stato aperto per eliminare la restrizione, l'ID bug Cisco CSCuq25476 - ASR1k deve supportare una dimensione della finestra GETVPN TBAR inferiore a 20 secondi.

**Update:** Questa restrizione è stata successivamente eliminata con la correzione per il bug Cisco con ID CSCur57558 e non è più una limitazione nel codice XE3.10.5, XE3.13.2 e versioni successive.

Inoltre, per un dispositivo GM in esecuzione su piattaforme Cisco IOS-XE (ASR1k o ISR4k), si consiglia vivamente di eseguire una versione con la correzione per questo problema se TBAR è abilitato; ID bug Cisco CSCut91647 - GETVPN su IOS-XE: GM rifiuta erroneamente i pacchetti a causa di un errore TBAR.

### Problema di classificazione ISR4x00

Èstata rilevata una regressione nella piattaforma ISR4x00 in cui i criteri di negazione vengono ignorati. Per i dettagli, vedere l'ID bug Cisco CSCut14355 - GETVPN - ISR4300 GM ignora la policy di negazione.

## Informazioni correlate

- Group Encrypted Transport VPN (GET VPN) - Cisco Systems
- Documentazione e supporto tecnico – Cisco Systems