Risoluzione dei problemi comuni relativi alla VPN IPsec di L2L e Remote Access

Sommario

Introduzione

In questo documento vengono fornite le soluzioni più comuni ai problemi della VPN IPsec.

Premesse

Le soluzioni descritte qui provengono direttamente dalle richieste di assistenza risolte dal supporto tecnico Cisco.

Molte di queste soluzioni vengono implementate prima della risoluzione dettagliata dei problemi di una connessione VPN IPsec.

In questo documento viene fornito un riepilogo delle procedure comuni da eseguire prima di iniziare a risolvere i problemi relativi a una connessione.

Sebbene gli esempi di configurazione riportati in questo documento siano destinati all'utilizzo su router e appliance di sicurezza, quasi tutti questi concetti sono validi anche per VPN 3000.

Per una descrizione dei comandi di debug comuni utilizzati per risolvere i problemi relativi a IPsec sul software Cisco IOS® e sul server, consultare il documento sulla risoluzione dei problemi relativi alla sicurezza IP - Comprensione e uso dei comandi di debug.

Nota: l'ASA non passa il traffico multicast sui tunnel VPN IPsec.

Avviso: molte delle soluzioni presentate in questo documento possono causare la perdita temporanea di tutta la connettività VPN IPsec su un dispositivo.

È consigliabile implementare queste soluzioni con cautela e in conformità con i criteri di controllo

delle modifiche.

Prerequisiti

Requisiti

Cisco consiglia di conoscere la configurazione della VPN IPsec sui seguenti dispositivi Cisco:

- Cisco ASA serie 5500 Security Appliance
- Router Cisco IOS®

Componenti usati

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

- Cisco ASA serie 5500 Security Appliance
- Cisco IOS®

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.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

La configurazione della VPN IPsec non funziona

Problema

Una soluzione VPN IPsec configurata o modificata di recente non funziona.

Una configurazione VPN IPsec corrente non funziona più.

Soluzioni

In questa sezione vengono illustrate le soluzioni ai problemi più comuni delle VPN IPsec.

Anche se non sono elencate in un ordine particolare, queste soluzioni possono essere utilizzate come un elenco di controllo di elementi da verificare o provare prima di intraprendere un risanamento approfondito.

Tutte queste soluzioni provengono direttamente dalle richieste di assistenza TAC e hanno risolto numerosi problemi.

- Abilita NAT-Traversal (problema VPN RSA n. 1)
- Verifica corretta della connettività
- Abilita ISAKMP
- Abilita/Disabilita PFS
- Cancella associazioni di sicurezza precedenti o esistenti (tunnel)
- Verifica della durata ISAKMP
- Attivare o disattivare i pacchetti keepalive ISAKMP
- Reimmettere o recuperare chiavi già condivise
- Chiave già condivisa non corrispondente
- Rimuovere e riapplicare le mappe crittografiche
- Verificare che i comandi sysopt siano presenti (solo ASA).
- Verifica dell'identità ISAKMP
- Verifica timeout di inattività/sessione
- Verificare che gli ACL siano corretti e associati alla mappa crittografica
- Verifica delle policy ISAKMP
- Verifica della correttezza del routing
- Verificare che Transform-Set sia corretto
- Verifica dei numeri di sequenza e del nome della mappa crittografica
- Verificare che l'indirizzo IP del peer sia corretto
- Verifica dei nomi dei gruppi di tunnel e dei gruppi
- Disabilita XAUTH per peer L2L
- Pool VPN in esaurimento
- Problemi di latenza per il traffico dei client VPN

Nota: per problemi di spazio, alcuni comandi di queste sezioni sono stati riportati su una seconda riga.

Abilita NAT-Traversal (problema VPN RSA n. 1)

NAT-Traversal (o NAT-T) consente al traffico VPN di passare attraverso dispositivi NAT o PAT, ad esempio un router Linksys SOHO.

Se NAT-T non è abilitato, gli utenti del client VPN spesso sembrano connettersi all'appliance ASA senza problemi, ma non sono in grado di accedere alla rete interna dietro l'appliance di sicurezza.

Se non si abilita NAT-T nel dispositivo NAT/PAT, è possibile ricevere il messaggio di errore **`PAT (Translation Creation Failed) per il protocollo 50 src inside:10.0.1.26 dst outside:10.9.69.4`**nell'appliance ASA.

Analogamente, se non è possibile eseguire l'accesso simultaneo dallo stesso indirizzo IP, **`la connessione VPN sicura viene terminata localmente dal client. Motivo 412: il peer remoto non risponde più.`** Viene visualizzato il messaggio di errore.

Per risolvere il problema, abilitare NAT-T nel dispositivo VPN headend.

Nota: con il software Cisco IOS® versione 12.2(13)T e successive, NAT-T è abilitato per impostazione predefinita in Cisco IOS®.

Di seguito viene riportato il comando per abilitare NAT-T su un'appliance di sicurezza Cisco. Il valore venti (20) di questo esempio corrisponde al tempo keepalive (predefinito).

ASA

<#root>

securityappliance(config)#

crypto isakmp nat-traversal 20

Anche i client devono essere modificati per poter funzionare.

In Cisco VPN Client, passare a Voci di connessione e fare clic su Modifica. Viene visualizzata una nuova finestra in cui è necessario scegliere la scheda Trasporto.

In questa scheda, fare clic su Enable Transparent Tunneling e sul pulsante di opzione IPSec over UDP (NAT / PAT). Quindi fate clic su Salva (Save) e verificate la connessione.

È importante consentire la configurazione di UDP 4500 per le porte NAT-T, UDP 500 ed ESP tramite la configurazione di un ACL, in quanto l'ASA funziona come dispositivo NAT.

Per ulteriori informazioni sulla configurazione degli ACL nell'appliance ASA, consultare il documento sulla configurazione del tunnel IPsec attraverso un firewall con NAT.

Verifica corretta della connettività

Idealmente, la connettività VPN viene testata dai dispositivi dietro i dispositivi endpoint che eseguono la crittografia, ma molti utenti testano la connettività VPN con il comando ping sui dispositivi che eseguono la crittografia.

Anche se in genere il ping ha questo scopo, è importante sorgente il ping dall'interfaccia corretta.

Se l'origine del ping non è corretta, è possibile che la connessione VPN non sia riuscita quando funziona davvero. Questo è un esempio:

ACL crittografico del router A

```
access-list 110 permit ip 192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255
```

ACL crittografico del router B

```
access-list 110 permit ip 192.168.200.0 0.0.0.255 192.168.100.0 0.0.0.255
```

In questo caso, il ping deve essere inviato dalla rete interna dietro uno dei router. Infatti gli ACL crittografici sono configurati solo per crittografare il traffico con questi indirizzi di origine.

Le assegnazioni originate dalle interfacce esterne di uno dei router non sono crittografate. Utilizzare le opzioni estese del comando ping in modalità di esecuzione privilegiata per originare un ping dall'interfaccia interna di un router:

<#root>

```
routerA#
ping
Protocol [ip]:
Target IP address: 192.168.200.10
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.100.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds:
```

```
Packet sent with a source address of 192.168.100.1

!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = ½/4 ms
```

Si supponga che i router descritti in questo diagramma siano stati sostituiti da appliance di sicurezza ASA. Il theping utilizzato per verificare la connettività può anche essere originato dall'interfaccia interna con la parola chiave insidekeyword:

```
<#root>

securityappliance#

ping inside 192.168.200.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Si consiglia di non utilizzare il comando ping sull'interfaccia interna di un'appliance di sicurezza.

Se l'interfaccia interna deve essere indirizzata al ping, è necessario abilitare l'accesso management all'interfaccia, altrimenti l'accessorio non risponderà.

```
<#root>

securityappliance(config)#

management-access inside
```

Quando si verifica un problema di connettività, anche la fase uno (1) della VPN non funziona.

Sull'appliance ASA, se la connettività non riesce, l'output dell'associazione di sicurezza è simile a questo esempio, il che indica una possibile configurazione peer crittografica e/o una configurazione della proposta ISAKMP errata:

```
<#root>

Router#

show crypto isakmp sa


1   IKE Peer: XX.XX.XX.XX
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_WAIT_MSG2
```

Lo stato può essere compreso tra MM_WAIT_MSG2 e MM_WAIT_MSG5, che indica un errore dello scambio di stato interessato in modalità principale (MM).

L'output dell'associazione di sicurezza crittografica quando la fase 1 è attiva è simile a questo esempio:

<#root>

```
Router#

show crypto isakmp sa


1   IKE Peer: XX.XX.XX.XX
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
```

Abilita ISAKMP

Se non vi sono indicazioni sul funzionamento di un tunnel VPN IPsec, è possibile che ISAKMP non sia stato abilitato. Accertarsi di aver abilitato ISAKMP sui dispositivi.

Utilizzare uno dei seguenti comandi per abilitare ISAKMP sui dispositivi:

Cisco IOS®

<#root>

```
router(config)#

crypto isakmp enable
```

Cisco ASA (sostituire all'esterno dell'interfaccia desiderata)

<#root>

```
securityappliance(config)#

crypto isakmp enable outside
```

Questo errore si può verificare anche quando si abilita il protocollo ISAKMP sull'interfaccia esterna:

```
UDP: ERROR - socket <unknown> 62465 in used
ERROR: IkeReceiverInit, unable to bind to port
```

L'errore può essere causato dal fatto che il client dietro l'ASA ottiene il PAT sulla porta udp 500 prima che l'isakmp possa essere abilitato sull'interfaccia. Una volta che la traduzione PAT è stata rimossa (deselezionata xlate), l'isakmp può essere abilitato.

Verificare che i numeri di porta UDP 500 e 4500 siano riservati per la negoziazione delle connessioni ISAKMP con il peer.

Quando ISAKMP non è abilitato sull'interfaccia, il client VPN visualizza un messaggio di errore simile al seguente:

```
Secure VPN connection terminated locally by client.
Reason 412: The remote peer is no longer responding
```

Per risolvere questo errore, abilitare il protocollo ISAKMP sull'interfaccia crittografica del gateway VPN.

Abilita/Disabilita PFS

Nelle negoziazioni IPSec, PFS (Perfect Forward Secrecy) garantisce che ogni nuova chiave di crittografia non sia correlata a nessuna chiave precedente.

Abilitare o disabilitare il protocollo PFS su entrambi i peer del tunnel; in caso contrario, il tunnel IPsec LAN-LAN (L2L) non viene stabilito nel router ASA/Cisco IOS®.

Perfect Forward Secrecy (PFS) è proprietario di Cisco e non è supportato sui dispositivi di terze parti.

ASA:

PFS è disattivato per impostazione predefinita. Per abilitare PFS, utilizzare il comando pfscon la parola chiave enable in modalità di configurazione Criteri di gruppo. Per disabilitare PFS, immettere la parola chiave disable.

<#root>

```
hostname(config-group-policy)#
```

pfs {enable | disable}

Per rimuovere l'attributo PFS dalla configurazione, immettere la forma no di questo comando.

Un criterio di gruppo può ereditare un valore per PFS da un altro criterio. Immettere la forma no di questo comando per impedire il trasferimento di un valore.

<#root>

hostname(config-group-policy)#

no pfs

Router Cisco IOS®:

Per specificare che IPsec deve richiedere PFS quando vengono richieste nuove associazioni di sicurezza per questa voce della mappa crittografica, utilizzare il comando set pfsnella modalità di configurazione della mappa crittografica.

Per specificare che IPSec richiede PFS quando riceve richieste per nuove associazioni di protezione, utilizzare il comando set pfsin modalità di configurazione mappa crittografica.

Per specificare che IPsec non deve richiedere PFS, utilizzare la forma no di questo comando. Per impostazione predefinita, PFS non è richiesto. Se con questo comando non si specifica alcun gruppo, per impostazione predefinita verrà utilizzato gruppo1.

```
set pfs [group1 | group2]
no set pfs
```

Per il comando set pfs:

- group1 —Specifica che IPSec deve utilizzare il gruppo di moduli primari Diffie-Hellman a 768 bit quando viene eseguito il nuovo scambio Diffie-Hellman.
- group2 - Specifica che IPSec deve utilizzare il gruppo di moduli primari Diffie-Hellman a 1024 bit quando viene eseguito il nuovo scambio Diffie-Hellman.

Esempio:

<#root>

```
Router(config)#crypto map map 10 ipsec-isakmp
Router(config-crypto-map)#
```

set pfs group2

Cancella associazioni di sicurezza precedenti o correnti (tunnel)

Se viene visualizzato questo messaggio di errore sul router Cisco IOS®, l'appliance ASA è scaduta o è stata cancellata.

Il dispositivo terminale del tunnel remoto non è a conoscenza del fatto che utilizza l'associazione

di protezione scaduta per inviare un pacchetto (non un pacchetto di istituzione dell'associazione di protezione).

Quando viene stabilita una nuova SA, la comunicazione riprende, quindi viene avviato il traffico interessante attraverso il tunnel per creare una nuova SA e ristabilire il tunnel.

<#root>

```
%CRYPTO-4-IKMP_NO_SA: IKE message from x.x.x.x  has no SA
```

Se si cancellano le associazioni di sicurezza (SA) ISAKMP (Fase I) e IPsec (Fase II), è la soluzione più semplice e spesso la migliore per risolvere i problemi della VPN IPsec.

Se si cancellano le associazioni di protezione, è spesso possibile risolvere un'ampia varietà di messaggi di errore e comportamenti anomali senza dover risolvere i problemi.

Anche se questa tecnica può essere facilmente utilizzata in qualsiasi situazione, è quasi sempre necessario cancellare le associazioni di protezione dopo la modifica o l'aggiunta a una configurazione VPN IPsec corrente.

Inoltre, mentre è possibile cancellare solo specifiche associazioni di protezione, la soluzione più vantaggiosa è quella di cancellare le associazioni di protezione a livello globale sul dispositivo.

Dopo aver cancellato le associazioni di sicurezza, può essere necessario inviare il traffico attraverso il tunnel per ristabilirle.

Avviso: se non si specificano le associazioni di protezione da cancellare, i comandi elencati possono cancellare tutte le associazioni di protezione presenti nel dispositivo. Procedere con cautela se sono in uso altri tunnel VPN IPsec.

1. Visualizzare le associazioni di sicurezza prima di cancellarle

    a. Cisco Cisco IOS®

    <#root>

    ```
    router#

    show crypto isakmp sa

    router#

    show crypto ipsec sa
    ```

    b. Appliance di sicurezza Cisco ASA

    <#root>

```
securityappliance#
show crypto isakmp sa
securityappliance#
show crypto ipsec sa
```

2. Cancellare le associazioni di protezione. Ogni comando può essere immesso come indicato in grassetto o con le opzioni visualizzate.

    a. Cisco IOS®

        a. ISAKMP (fase I)

```
<#root>
router#
clear crypto isakmp
 ?
  <0 - 32766>  connection id of SA
  <cr>
```

        b. IPsec (fase II)

```
<#root>
router#
clear crypto sa
 ?
  counters  Reset the SA counters
  map       Clear all SAs for a given crypto map
  peer      Clear all SAs for a given crypto peer
  spi       Clear SA by SPI
  <cr>
```

    b. Appliance di sicurezza Cisco ASA

        a. ISAKMP (fase I)

```
<#root>
securityappliance#
clear crypto isakmp sa
```

b. IPsec (fase II)

<#root>

```
security appliance#

clear crypto ipsec sa

 ?

  counters  Clear IPsec SA counters
  entry     Clear IPsec SAs by entry
  map       Clear IPsec SAs by map
  peer      Clear IPsec SA by peer
  <cr>
```

Verifica della durata ISAKMP

Se gli utenti vengono disconnessi di frequente attraverso il tunnel L2L, il problema può essere dovuto alla durata inferiore configurata in ISAKMP SA.

Se si verifica una discrepanza durante la durata di ISAKMP, è possibile ricevere il messaggio di errore%ASA-5-713092: Group = x.x.x.x, IP = x.x.x.x, Errore durante il tentativo di reimpostazione della chiave di fase 1 a causa di un messaggio di errore di collisione in /ASA.

L'impostazione predefinita è 86.400 secondi o 24 ore. In generale, una durata più breve garantisce negoziazioni ISAKMP più sicure (fino a un punto), ma, con durate più brevi, l'appliance di sicurezza imposta le future associazioni di protezione IPSec più rapidamente.

Una corrispondenza viene creata quando entrambi i criteri dei due peer contengono gli stessi valori di crittografia, hash, autenticazione e parametro Diffie-Hellman e quando il criterio del peer remoto specifica una durata inferiore o uguale alla durata del criterio confrontato.

Se le durate non sono identiche, viene utilizzata la durata più breve, derivata dalla regola del peer remoto. Se non viene trovata una corrispondenza accettabile, IKE rifiuta la negoziazione e l'associazione di protezione IKE non viene stabilita.

Specificare la durata dell'associazione di protezione. In questo esempio viene impostata una durata di 4 ore (1400 secondi). L'impostazione predefinita è 86400 secondi (24 ore).

ASA

<#root>

```
hostname(config)#

isakmp policy 2 lifetime  14400
```

Router Cisco IOS®

<#root>

R2(config)#

crypto isakmp policy 10

R2(config-isakmp)#

lifetime 86400

Se viene superata la durata massima configurata, viene visualizzato questo messaggio di errore quando la connessione VPN viene terminata:

Connessione VPN sicura terminata localmente dal client. Motivo 426: durata massima configurata superata.

Per risolvere questo messaggio di errore, impostare elifetimevalue su zero (0) per impostare la durata di un'associazione di protezione IKE su infinito. La VPN è sempre connessa e non termina.

hostname(config)#isakmp policy 2 lifetime 0

Per risolvere il problema, è inoltre possibile disabilitare re-xauth nei criteri di gruppo.

Attivare o disattivare i pacchetti keepalive ISAKMP

Configurando i pacchetti keepalive ISAKMP, contribuisce a prevenire la perdita sporadica di connessioni LAN a LAN o VPN ad accesso remoto, inclusi i client VPN, i tunnel e i tunnel scartati dopo un periodo di inattività.

Questa funzionalità consente all'endpoint del tunnel di monitorare la presenza continua di un peer remoto e segnalare la propria presenza a tale peer.

Se il peer non risponde, l'endpoint rimuove la connessione.

Affinché i pacchetti keepalive ISAKMP funzionino, entrambi gli endpoint VPN devono supportarli.

Configurare i pacchetti keepalive ISAKMP in Cisco IOS® con questo comando:

<#root>

router(config)#

crypto isakmp keepalive 15

Utilizzare questi comandi per configurare i pacchetti keepalive ISAKMP sulle appliance di sicurezza ASA:

Cisco ASA per il gruppo di tunnel denominato10.165.205.222

```
<#root>

securityappliance(config)#

tunnel-group 10.165.205.222
   ipsec-attributes


securityappliance(config-tunnel-ipsec)#

isakmp keepalive
   threshold 15 retry 10
```

In alcune situazioni, è necessario disabilitare questa funzione per risolvere il problema, ad esempio se il client VPN è protetto da un firewall che impedisce i pacchetti DPD.

Cisco ASA, per il gruppo di tunnel con nome 10.165.205.222

Disabilita l'elaborazione keepalive IKE, abilitata per impostazione predefinita.

```
<#root>

securityappliance(config)#

tunnel-group 10.165.205.222
   ipsec-attributes


securityappliance(config-tunnel-ipsec)#

isakmp keepalive


disable
```

Disabilitare Keepalive per Cisco VPN Client 4.x

Passare a%System Root% > Programmi > Cisco Systems > VPN Client > Profili sul PC client in cui si è verificato il problema per disabilitare IKE keepalive e modificare il file PCF, se applicabile, per la connessione.

Modificare la proprietà ForceKeepAlives=0(impostazione predefinita) in ForceKeepAlives=1.

I pacchetti keepalive sono di proprietà di Cisco e non sono supportati da dispositivi di terze parti.

Reimmettere o recuperare chiavi già condivise

In molti casi, quando un tunnel VPN IPsec non funziona, è possibile che sia presente un semplice errore tipografico. Ad esempio, sull'appliance di sicurezza, le chiavi già condivise diventano nascoste una volta immesse.

Questo tipo di offuscamento rende impossibile determinare se una chiave non è corretta. Accertarsi di aver immesso correttamente eventuali chiavi già condivise su ciascun endpoint VPN.

Immettere nuovamente una chiave per assicurarsi che sia corretta. Si tratta di una soluzione semplice che consente di evitare una risoluzione approfondita dei problemi.

In VPN ad accesso remoto, verificare che il nome del gruppo valido e la chiave già condivisa siano stati immessi nel client VPN di Cisco.

È possibile risolvere questo errore se il nome del gruppo o la chiave già condivisa non corrispondono tra il client VPN e il dispositivo headend.

```
 1 12:41:51.900 02/18/06 Sev=Warning/3 IKE/0xE3000056
 The received HASH payload cannot be verified
 2 12:41:51.900 02/18/06 Sev=Warning/2 IKE/0xE300007D
Hash verification failed
3      14:37:50.562  10/05/06  Sev=Warning/2 IKE/0xE3000099
Failed to authenticate peer (Navigator:904)
4      14:37:50.593  10/05/06  Sev=Warning/2 IKE/0xE30000A5
Unexpected SW error occurred while processing Aggressive Mode
negotiator:(Navigator:2202)
5      14:44:15.937  10/05/06  Sev=Warning/2 IKE/0xA3000067
Received Unexpected InitialContact Notify (PLMgrNotify:888)
6      14:44:36.578  10/05/06  Sev=Warning/3 IKE/0xE3000056
The received HASH payload cannot be verified
7      14:44:36.593  10/05/06  Sev=Warning/2 IKE/0xE300007D
Hash verification failed... possibly be configured with invalid group password.
8      14:44:36.609  10/05/06  Sev=Warning/2 IKE/0xE3000099
Failed to authenticate peer (Navigator:904)
9      14:44:36.640  10/05/06  Sev=Warning/2 IKE/0xE30000A5
Unexpected SW error occurred while processing Aggressive Mode
negotiator:(Navigator:2202)
```

Avviso: se si rimuovono i comandi relativi alla crittografia, è probabile che si interrompa uno o tutti i tunnel VPN. Utilizzare questi comandi con cautela e consultare i criteri di controllo delle modifiche dell'organizzazione prima di rimuovere i comandi relativi alla crittografia.

Utilizzare questi comandi per rimuovere e immettere nuovamente il keysecretkeypre-condiviso per il peer10.0.0.1o il groupvpngroupin Cisco IOS®:

Cisco VPN da LAN a LAN

<#root>

```
router(config)#

no crypto isakmp key secretkey
   address 10.0.0.1

router(config)#

crypto isakmp key secretkey
   address 10.0.0.1
```

Cisco Remote Access VPN

<#root>

```
router(config)#

crypto isakmp client configuration
   group vpngroup

router(config-isakmp-group)#

no key secretkey

router(config-isakmp-group)#

key secretkey
```

Utilizzare questi comandi per rimuovere e immettere nuovamente il keysecretkeypre-condiviso per peer10.0.0.1su appliance di sicurezza /ASA:

Cisco 6.x

<#root>

```
(config)#

no isakmp key secretkey address 10.0.0.1

(config)#

isakmp key secretkey address 10.0.0.1
```

Cisco /ASA 7.x e versioni successive

<#root>

```
securityappliance(config)#

tunnel-group 10.0.0.1
   ipsec-attributes

securityappliance(config-tunnel-ipsec)#

no ikev1 pre-shared-key
```

```
securityappliance(config-tunnel-ipsec)#
ikev1


pre-shared-key
   secretkey
```

Chiave già condivisa non corrispondente

L'avvio del tunnel VPN viene disconnesso. Questo problema si verifica a causa di una mancata corrispondenza della chiave già condivisa durante le negoziazioni della fase I.

Il messaggio MM_WAIT_MSG_6nel comando show crypto isakmp sacommand indica una chiave già condivisa non corrispondente, come mostrato nell'esempio:

<#root>

```
ASA#
show crypto isakmp sa


Active SA: 1
Rekey SA: 0 (A tunnel reports 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1         IKE Peer: 10.7.13.20
             Type : L2L                                Role : initiator
             Rekey : no                                State :
MM_WAIT_MSG_6
```

Per risolvere il problema, reimmettere la chiave già condivisa in entrambi gli accessori. La chiave già condivisa deve essere univoca e deve corrispondere. Per ulteriori informazioni, vedere Reimmettere o recuperare le chiavi già condivise.

Rimuovere e riapplicare le mappe crittografiche

Quando si cancellano le associazioni di sicurezza e questo non risolve un problema della VPN IPsec, rimuovere e riapplicare la mappa crittografica appropriata per risolvere una vasta gamma di problemi, tra cui gocce intermittenti del tunnel VPN e problemi di alcuni siti VPN.

Avviso: se si rimuove una mappa crittografica da un'interfaccia, in questo modo vengono eliminati tutti i tunnel IPsec associati a tale mappa crittografica. Procedere con cautela con questi passaggi e considerare i criteri di controllo delle modifiche dell'organizzazione prima di procedere.

Utilizzare questi comandi per rimuovere e sostituire una mappa crittografica in Cisco IOS®:

Iniziare con la rimozione della mappa crittografica dall'interfaccia. Utilizzare la forma no del

comando crypto map.

<#root>

```
router(config-if)#
no crypto map mymap
```

Continuare a utilizzare la forma per rimuovere un'intera mappa crittografica.

<#root>

```
router(config)#
no crypto map mymap 10
```

Sostituire la mappa crittografica sull'interfaccia Ethernet0/0 per il peer10.0.0.1. Nell'esempio viene mostrata la configurazione minima richiesta per la mappa crittografica:

<#root>

```
router(config)#
crypto map mymap 10 ipsec-isakmp
router(config-crypto-map)#
match address 101
router(config-crypto-map)#
set transform-set mySET
router(config-crypto-map)#
set peer 10.0.0.1
router(config-crypto-map)#
exit
router(config)#
interface ethernet0/0
router(config-if)#
crypto map mymap
```

Utilizzare questi comandi per rimuovere e sostituire una mappa crittografica sull'appliance ASA:

Iniziare con la rimozione della mappa crittografica dall'interfaccia. Utilizzare la forma no del comando crypto map.

<#root>

```
securityappliance(config)#

no crypto map mymap interface outside
```

Continuare a utilizzare la maschera per rimuovere gli altri comandi della mappa crittografica.

<#root>

```
securityappliance(config)#

no crypto map mymap 10 match
   address 101

securityappliance(config)#

no crypto map mymap set
   transform-set mySET

securityappliance(config)#

no crypto map mymap set
   peer 10.0.0.1
```

Sostituire la mappa crittografica per il peer10.0.0.1. Nell'esempio viene mostrata la configurazione minima richiesta per la mappa crittografica:

<#root>

```
securityappliance(config)#

crypto map mymap 10 ipsec-isakmp

securityappliance(config)#

crypto map mymap 10
   match address 101

securityappliance(config)#

crypto map mymap 10 set
   transform-set mySET

securityappliance(config)#

crypto map mymap 10 set
   peer 10.0.0.1

securityappliance(config)#

crypto map mymap interface outside
```

La rimozione e la riapplicazione della mappa crittografica risolvono il problema di connettività se

l'indirizzo IP dell'headend è stato modificato.

Verificare che i comandi sysopt siano presenti (solo ASA)

Il comando commandssyspot connection allow-ipsecandsysopt connection allow-vpnallow permette ai pacchetti provenienti da un tunnel IPsec e dai relativi payload di ignorare gli ACL di interfaccia sull'appliance di sicurezza.

I tunnel IPsec terminati sull'appliance di sicurezza potrebbero non riuscire se uno di questi comandi non è abilitato.

Nel software Security Appliance versione 7.0 e precedenti, il comando syspot appropriato per questa situazione è anyspot connection allow-ipsec.

Nel software Security Appliance versione 7.1(1) e successive, il comando di sistema relativo a questa situazione è anyspot connection allow-vpn.

Nella versione 6.x, questa funzionalità è disattivata per impostazione predefinita. Con /ASA 7.0(1) e versioni successive, questa funzionalità è attivata per impostazione predefinita. Utilizzare i seguenti comandi show per determinare se il comando pertinente sysoptè abilitato sul dispositivo:

Cisco ASA

<#root>

```
securityappliance#
```

show running-config all sysopt

```
no sysopt connection timewait
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
```

sysopt connection permit-vpn

```
!--- sysopt connection permit-vpn is enabled !--- This device is running 7.2(2)
```

Utilizzare questi comandi per abilitare il comando rectsysoptper il dispositivo:

Cisco ASA

<#root>

```
securityappliance(config)#
```

sysopt connection permit-vpn

Se non si desidera utilizzare il comando sysost connection, autorizzare in modo esplicito il traffico interessante richiesto dall'origine alla destinazione.

Ad esempio, dalla LAN remota a locale del dispositivo remoto e dalla "porta UDP 500" per l'interfaccia esterna del dispositivo remoto all'interfaccia esterna del dispositivo locale, nell'ACL esterno.

Verifica dell'identità ISAKMP

Se il tunnel VPN IPSec non è riuscito nella negoziazione IKE, l'errore può essere dovuto all'errore o all'impossibilità del peer di riconoscere l'identità del peer.

Quando due peer utilizzano IKE per stabilire le associazioni di sicurezza IPSec, ogni peer invia la propria identità ISAKMP al peer remoto.

e invia il proprio indirizzo IP o nome host a seconda di come è stata impostata l'identità ISAKMP di ciascuno di essi.

Per impostazione predefinita, l'identità ISAKMP dell'unità firewall è impostata sull'indirizzo IP.

Come regola generale, impostare l'appliance di sicurezza e le identità dei peer allo stesso modo per evitare un errore di negoziazione IKE.

Per impostare l'ID Fase 2 da inviare al peer, utilizzare il comando isakmp identity in modalità di configurazione globale.

```
crypto isakmp identity address

!--- If the RA or L2L (site-to-site) VPN tunnels connect !--- with pre-shared key as authentication typ
```

O

```
crypto isakmp identity auto

!--- If the RA or L2L (site-to-site) VPN tunnels connect !--- with ISAKMP negotiation by connection typ
```

O

```
crypto isakmp identity hostname

!--- Uses the fully-qualified domain name of !--- the host exchange ISAKMP identity information (defaul
```

Il tunnel VPN non viene attivato dopo un passaggio della configurazione da all'ASA con lo strumento di migrazione della configurazione ASA. I seguenti messaggi vengono visualizzati nel log:

[IKEv1]: Gruppo = x.x.x.x, IP = x.x.x.x, Trovata voce di tabella peer non aggiornata. Rimozione in corso...

[IKEv1]: gruppo = x.x.x, IP = x.x.x.x, rimozione del peer dalla tabella dei correlatori non riuscita. Nessuna corrispondenza.

[IKEv1]: Gruppo = x.x.x.x, IP = x.x.x.x, costrutto_ipsec_delete(): Nessun SPI per identificare SA fase 2.

[IKEv1]: gruppo = x.x.x, IP = x.x.x.x, rimozione del peer dalla tabella dei correlatori non riuscita. Nessuna corrispondenza.

Verifica timeout di inattività/sessione

Se il timeout di inattività è impostato su 30 minuti (impostazione predefinita), il tunnel viene scartato dopo 30 minuti di traffico non transitabile.

Il client VPN si disconnette dopo 30 minuti indipendentemente dal parametro del timeout di inattività e rileva `l'`errore **`PEER_DELETE-IKE_DELETE`**_UNSPECIFIED.

Configurare idle timeoutandsession timeoutasnone per fare in modo che il tunnel si fermi sempre, e che il tunnel non venga mai scartato anche quando si usano dispositivi di terze parti.

ASA

Immettere il comando pn-idle-timeout in modalità di configurazione criteri di gruppo o in modalità di configurazione nome utente per configurare il periodo di timeout utente:

<#root>

```
hostname(config)#
group-policy DfltGrpPolicy attributes
hostname(config-group-policy)#
vpn-idle-timeout none
```

Configurare un periodo di tempo massimo per le connessioni VPN con il comando vpn-session-timeout in modalità di configurazione criteri di gruppo o in modalità di configurazione nome utente:

<#root>

```
hostname(config)#
```

group-policy DfltGrpPolicy attributes

hostname(config-group-policy)#

vpn-session-timeout none

Se è stato configurato tunnel-all, non è necessario configurare il timeout di inattività perché, anche se si configura il timeout di inattività della VPN, non funziona perché tutto il traffico attraversa il tunnel (poiché è configurato tunnel all).

Pertanto, il traffico interessante (o anche il traffico generato dal PC) è interessante e non consente l'attivazione del timeout di inattività.

Router Cisco IOS®

Per configurare il timer di inattività della SA IPsec, usare il comando crypto ipsec security-association idle-timein modalità di configurazione globale o in modalità di configurazione della mappa crittografica.

Per impostazione predefinita, i timer di inattività delle SA IPsec sono disabilitati.

<#root>

crypto ipsec security-association idle-time

seconds

Il tempo viene misurato in secondi, in cui il timer di inattività consente a un peer inattivo di mantenere un'associazione di protezione. I valori validi per l'argomento secondi sono compresi tra 60 e 86400.

Verificare che gli ACL siano corretti e associati alla mappa crittografica

In una configurazione VPN IPsec tipica vengono utilizzati due elenchi degli accessi. Un elenco degli accessi viene usato per esentare il traffico destinato al tunnel VPN dal processo NAT.

Il secondo elenco degli accessi definisce il traffico da crittografare, includendo un ACL crittografico in una configurazione da LAN a LAN o un ACL con tunnel diviso in una configurazione di accesso remoto.

Quando gli ACL non sono configurati correttamente o sono mancati, il traffico potrebbe fluire in una direzione attraverso il tunnel VPN, o non essere inviato attraverso il tunnel.

Verificare di aver associato l'ACL crittografico con la mappa crittografica con il comando crypto map match address in modalità di configurazione globale.

Accertarsi di aver configurato tutti gli elenchi degli accessi necessari per completare la configurazione della VPN IPsec e che tali elenchi degli accessi definiscano il traffico corretto.

Questo elenco contiene elementi semplici da controllare quando si sospetta che un ACL sia la causa del problema con la VPN IPsec.

Verificare che l'esenzione NAT e gli ACL di crittografia specifichino il traffico corretto.

Se si hanno più tunnel VPN e più ACL crittografici, verificare che tali ACL non si sovrappongano.

Verificare che il dispositivo sia configurato per l'utilizzo dell'ACL di esenzione NAT. Su un router, ciò significa che si utilizza therroute-mapcommand.

Sull'appliance ASA, questo significa che si usa il comando at (0). Per le configurazioni LAN-to-LAN e di accesso remoto è necessario un ACL di esenzione NAT.

In questo caso, un router Cisco IOS® è configurato in modo da esentare il traffico inviato tra le versioni 192.168.100.0 /24e 192.168.200.0 /24o192.168.1.0 /24da NAT. Il traffico destinato a qualsiasi altro luogo è soggetto a sovraccarico NAT:

```
access-list 110 deny ip 192.168.100.0 0.0.0.255
   192.168.200.0 0.0.0.255
access-list 110 deny ip 192.168.100.0 0.0.0.255
   192.168.1.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255 any

route-map nonat permit 10
  match ip address 110

ip nat inside source route-map nonat interface FastEthernet0/0 overload
```

Gli ACL di esenzione NAT funzionano solo con l'indirizzo IP o le reti IP, come negli esempi menzionati (access-list noNAT), e devono essere identici agli ACL delle mappe crittografiche.

Gli ACL di esenzione NAT non funzionano con i numeri di porta (ad esempio, 23, 25,...).

In un ambiente VOIP, in cui le chiamate vocali tra le reti vengono comunicate tramite VPN, le chiamate vocali non funzionano se gli ACL NAT 0 non sono configurati correttamente.

Prima di risolvere il problema, si consiglia di controllare lo stato della connettività VPN, in quanto il problema potrebbe essere causato da una configurazione errata di ACL con esenzione NAT.

È possibile visualizzare il messaggio di errore come mostrato in caso di configurazione errata negli ACL di esenzione NAT (nat 0).

```
%ASA-3-305005: No translation group found for
udp src Outside:x.x.x.x/p dst Inside:y.y.y.y/p
```

Esempio non corretto:

<#root>

```
access-list noNAT extended permit ip 192.168.100.0
   255.255.255.0 192.168.200.0 255.255.255.0
```

eq 25

Se l'esenzione NAT (nat 0) non funziona, provare a rimuoverla ed eseguire il comando NAT 0affinché funzioni.

Verificare che gli ACL non siano arretrati e che siano del tipo corretto.

Gli ACL di esenzione Crypto e NAT per le configurazioni da LAN a LAN devono essere scritti dal punto di vista del dispositivo su cui è configurato l'ACL.

Ciò significa che gli ACL devono essere sincronizzati. Nell'esempio, viene impostato un tunnel da LAN a LAN tra le versioni 192.168.100.0 /24e 192.168.200.0 /24.

ACL crittografico del router A

```
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.200.0 0.0.0.255
```

ACL crittografico del router B

```
access-list 110 permit ip 192.168.200.0 0.0.0.255
   192.168.100.0 0.0.0.255
```

Anche se non viene illustrato qui, lo stesso concetto si applica alle appliance di sicurezza ASA.

Nell'ASA, gli ACL con tunnel suddivisi per le configurazioni di accesso remoto devono fornire elenchi degli accessi standard che autorizzino il traffico sulla rete a cui i client VPN devono accedere.

I router Cisco IOS® possono usare ACL estesi per lo split-tunnel. Nell'elenco degli accessi estesi, usare 'any' all'origine nell'ACL del tunnel suddiviso equivale a disabilitare lo split tunnel.

Usare solo le reti di origine nell'ACL esteso per il tunnel suddiviso.

Esempio corretto:

<#root>

access-list 140 permit ip

```
10.1.0.0 0.0.255.255

 10.18.0.0 0.0.255.255
```

Esempio non corretto:

```
<#root>

access-list 140 permit ip

any

 10.18.0.0 0.0.255.255
```

Cisco IOS®

```
<#root>

router(config)#

access-list 10 permit ip 192.168.100.0

router(config)#

crypto isakmp client configuration group MYGROUP

router(config-isakmp-group)#

acl 10
```

Cisco ASA

```
<#root>

securityappliance(config)#

access-list 10 standard
   permit 192.168.100.0 255.255.255.0

securityappliance(config)#

group-policy MYPOLICY internal

securityappliance(config)#

group-policy MYPOLICY attributes

securityappliance(config-group-policy)#

split-tunnel-policy
   tunnelspecified

securityappliance(config-group-policy)#

split-tunnel-network-list
```

```
   value 10
```

Configurazione dell'esenzione NAT in ASA versione 8.3 per il tunnel VPN da sito a sito:

È necessario stabilire una VPN da sito a sito tra HOASA e BOASA con entrambe le appliance ASA versione 8.3. La configurazione di esenzione NAT su HOASA è simile alla seguente:

```
object network obj-local
subnet 192.168.100.0 255.255.255.0
object network obj-remote
subnet 192.168.200.0 255.255.255.0
nat (inside,outside) 1 source static obj-local obj-local destination static obj-remote objremote
```

Verifica delle policy ISAKMP

Se il tunnel IPsec non è attivo, verificare che i criteri ISAKMP corrispondano ai peer remoti. Questo criterio ISAKMP è applicabile sia alla VPN IPsec da sito a sito (L2L) che alla VPN IPsec di accesso remoto.

Se i client VPN Cisco o la VPN da sito a sito non sono in grado di stabilire il tunnel con il dispositivo remoto, verificare che i due peer contengano gli stessi valori di crittografia, hash, autenticazione e parametro Diffie-Hellman.

Verificare quando il criterio peer remoto specifica una durata inferiore o uguale alla durata del criterio inviato dall'iniziatore.

Se le durate non sono identiche, l'appliance di sicurezza utilizza la durata più breve. Se non esiste una corrispondenza accettabile, ISAKMP rifiuta la negoziazione e l'associazione di protezione non viene stabilita.

```
"Error: Unable to remove Peer TblEntry, Removing peer from peer table
failed, no match!"
```

Di seguito è riportato il messaggio dettagliato del registro:

```
4|Mar 24 2010 10:21:50|713903: IP = X.X.X.X, Error: Unable to remove PeerTblEntry
3|Mar 24 2010 10:21:50|713902: IP = X.X.X.X, Removing peer from peer table failed,
no match!
3|Mar 24 2010 10:21:50|713048: IP = X.X.X.X, Error processing payload: Payload ID: 1
4|Mar 24 2010 10:21:49|713903: IP = X.X.X.X, Information Exchange processing failed
5|Mar 24 2010 10:21:49|713904: IP = X.X.X.X, Received an un-encrypted
NO_PROPOSAL_CHOSEN notify message, drop
```

Questo messaggio viene in genere visualizzato a causa di una mancata corrispondenza delle policy ISAKMP o di un'istruzione NAT 0 mancante.

Viene inoltre visualizzato il messaggio seguente:

```
Error Message    %ASA-6-713219: Queueing KEY-ACQUIRE messages to be processed when
P1 SA is complete.
```

Questo messaggio indica che i messaggi della fase 2 sono nella coda dopo il completamento della fase 1. Questo messaggio di errore è dovuto a uno dei motivi seguenti:

- Mancata corrispondenza nella fase su uno dei peer
- ACL blocca i peer dal completamento della fase 1

Questo messaggio viene in genere visualizzato dopo **che la rimozione del peer dalla tabella peer non è riuscita.** Messaggio di errore **no match!**.

Se il client VPN Cisco non è in grado di connettere il dispositivo headend, il problema può essere la mancata corrispondenza della policy ISAKMP. Il dispositivo headend deve corrispondere a una delle proposte IKE del client VPN Cisco.

Per il criterio ISAKMP e l'insieme di trasformazioni IPsec usato sull'appliance ASA, il client VPN Cisco non può usare un criterio con una combinazione di DES e SHA.

Se si utilizza DES, è necessario utilizzare MD5 per l'algoritmo hash oppure le altre combinazioni, 3DES con SHA e 3DES con MD5.

Verifica della correttezza del routing

Verificare che i dispositivi di crittografia, come i router e le appliance di sicurezza ASA, dispongano delle informazioni di routing corrette per inviare il traffico sul tunnel VPN.

Se dietro il dispositivo gateway sono presenti altri router, verificare che sappiano come raggiungere il tunnel e quali reti sono dall'altro lato.

Un componente chiave del routing in una distribuzione VPN è l'Reverse Route Injection (RRI).

RRI posiziona le voci dinamiche per le reti remote o i client VPN nella tabella di routing di un gateway VPN.

Queste route sono utili al dispositivo su cui sono installate e ad altri dispositivi nella rete, in quanto le route installate da RRI possono essere ridistribuite tramite un protocollo di routing, ad esempio EIGRP o OSPF.

In una configurazione da LAN a LAN, è importante che ciascun endpoint disponga di una o più route alle reti per le quali si prevede di crittografare il traffico.

Nell'esempio, il router A deve avere i percorsi alle reti dietro il router B fino a 10.89.129.2. Il router B deve avere un percorso simile a 192.168.100.0 /24:

Il primo modo per accertarsi che ciascun router conosca i percorsi appropriati è configurare i percorsi statici per ciascuna rete di destinazione. Ad esempio, per il router A è possibile configurare le seguenti istruzioni di routing:

```
ip route 0.0.0.0 0.0.0.0 172.22.1.1
ip route 192.168.200.0 255.255.255.0 10.89.129.2
ip route 192.168.210.0 255.255.255.0 10.89.129.2
ip route 192.168.220.0 255.255.255.0 10.89.129.2
ip route 192.168.230.0 255.255.255.0 10.89.129.2
```

Se il router A è stato sostituito con un'ASA, la configurazione può essere simile alla seguente:

```
route outside 0.0.0.0 0.0.0.0 172.22.1.1
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
```

Se dietro ciascun endpoint esiste un numero elevato di reti, diventa difficile gestire la configurazione delle route statiche.

Si consiglia invece di utilizzare Reverse Route Injection, come descritto. RRI posiziona nelle route della tabella di routing per tutte le reti remote elencate nell'ACL crittografico.

Ad esempio, l'ACL crittografico e la mappa crittografica del router A possono avere questo aspetto:

<#root>

```
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.200.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.210.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.220.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.230.0 0.0.0.255

crypto map myMAP 10 ipsec-isakmp
 set peer 10.89.129.2

reverse-route

 set transform-set mySET
 match address 110
```

Se il router A è stato sostituito da un'appliance ASA, la configurazione può essere simile alla seguente:

<#root>

```
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.200.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.210.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.220.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.230.0 255.255.255.0

crypto map myMAP 10 match address cryptoACL
crypto map myMAP 10 set peer 10.89.129.2
crypto map myMAP 10 set transform-set mySET
```

crypto map mymap 10 set reverse-route

In una configurazione di Accesso remoto, le modifiche di routing non sono sempre necessarie.

Tuttavia, se dietro il router gateway VPN o l'appliance di sicurezza sono presenti altri router, questi router devono imparare in qualche modo il percorso ai client VPN.

Nell'esempio, si supponga che ai client VPN vengano assegnati indirizzi compresi nell'intervallo 10.0.0.0 /24quando si connettono.

Se tra il gateway e gli altri router non è in uso alcun protocollo di routing, è possibile usare le route statiche sui router come il router 2:

```
ip route 10.0.0.0 255.255.255.0 192.168.100.1
```

Se tra il gateway e altri router è in uso un protocollo di routing, ad esempio EIGRP o OSPF, si consiglia di utilizzare il comando Reverse Route Injection come descritto.

RRI aggiunge automaticamente le route per il client VPN alla tabella di routing del gateway. Queste route possono quindi essere distribuite agli altri router della rete.

Router Cisco IOS®:

<#root>

```
crypto dynamic-map dynMAP 10
 set transform-set mySET
```

reverse-route

```
crypto map myMAP 60000 ipsec-isakmp dynamic dynMAP
```

Cisco ASA Security Appliance:

<#root>

```
crypto dynamic-map dynMAP 10 set transform-set mySET
```

crypto dynamic-map dynMAP 10 set reverse-route

```
crypto map myMAP 60000 ipsec-isakmp dynamic dynMAP
```

Il problema di routing si verifica se il pool di indirizzi IP assegnati ai client VPN si sovrappone alle reti interne del dispositivo headend. Per ulteriori informazioni, fare riferimento alla sezione Sovrapposizione di reti private .

Verificare che Transform-Set sia corretto

Verificare che gli algoritmi di crittografia IPSec e hash utilizzati dalla trasformazione impostata su entrambe le estremità siano gli stessi.

Per ulteriori informazioni, consultare la sezione relativa ai comandi nella guida alla configurazione di Cisco Security Appliance.

Per il criterio ISAKMP e l'insieme di trasformazioni IPsec usato sull'appliance ASA, il client VPN Cisco non può usare un criterio con una combinazione di DES e SHA.

Se si utilizza DES, è necessario utilizzare MD5 per l'algoritmo hash oppure le altre combinazioni, 3DES con SHA e 3DES con MD5.

Verificare i numeri di sequenza e il nome della mappa crittografica, nonché controllare che la mappa crittografica venga applicata nell'interfaccia corretta in cui il tunnel IPsec inizia/termina

Se i peer statici e dinamici sono configurati sulla stessa mappa crittografica, l'ordine delle voci della mappa crittografica è molto importante.

Il numero di sequenza della voce della mappa crittografica dinamica deve essere maggiore di tutte le altre voci della mappa crittografica statica.

Se le voci statiche sono numerate più in alto rispetto alla voce dinamica, le connessioni con questi peer hanno esito negativo e viene visualizzato il messaggio Debug (Debug) come mostrato di seguito.

```
IKEv1]: Group = x.x.x.x, IP = x.x.x.x, QM FSM error (P2 struct &0x49ba5a0, mess id 0xcd600011)!
[IKEv1]: Group = x.x.x.x, IP = x.x.x.x, Removing peer from correlator table failed, no match!
```

È consentita una sola mappa crittografica dinamica per ciascuna interfaccia dell'appliance di sicurezza.

Di seguito è riportato un esempio di mappa crittografica correttamente numerata contenente una voce statica e una voce dinamica. Si noti che la voce dinamica ha il numero di sequenza più alto e che è stata lasciata spazio sufficiente per aggiungere altre voci statiche:

<#root>

```
crypto dynamic-map cisco 20 set transform-set myset
crypto map mymap 10 match address 100
crypto map mymap 10 set peer 172.16.77.10
crypto map mymap 10 set transform-set myset
crypto map mymap interface outside
```

crypto map mymap 60000 ipsec-isakmp dynamic ciscothe

I nomi delle mappe crittografiche distinguono tra maiuscole e minuscole.

Questo messaggio di errore può essere visualizzato anche quando la sequenza man di crittografia dinamica non è corretta, il che provoca l'accesso del peer alla mappa crittografica errata.

La causa è anche un elenco degli accessi crittografati non corrispondente che definisce il traffico interessante:**%ASA-3-713042: l'iniziatore IKE non è in grado di trovare il criterio:**

In uno scenario in cui più tunnel VPN devono essere terminati nella stessa interfaccia, creare la mappa crittografica con lo stesso nome (è consentita una sola mappa crittografica per interfaccia) ma con un numero di sequenza diverso.

Ciò vale sia per il router sia per l'ASA.

Analogamente, fare riferimento a ASA: Add a New Tunnel or Remote Access to an Existing L2L VPN - Cisco per ulteriori informazioni sulla configurazione della mappa crittografica per lo scenario L2L e la VPN ad accesso remoto.

Verificare che l'indirizzo IP del peer sia corretto

Creare e gestire il database dei record specifici della connessione per IPSec.

Per una configurazione VPN IPsec da LAN a LAN (L2L) di un'appliance di sicurezza ASA, specificare il <nome>del gruppo di tunnel come indirizzo IP peer remoto (estremità tunnel remota) nel comando tunnel-group <nome> digitare ipsec-l2.

L'indirizzo IP del peer deve corrispondere al nome del gruppo di tunnel e ai comandi set address della mappa crittografica.

Durante la configurazione della VPN con ASDM, il nome del gruppo di tunnel è stato generato automaticamente con l'indirizzo IP del peer corretto.

Se l'indirizzo IP del peer non è configurato correttamente, i registri possono contenere questo messaggio, che può essere risolto mediante la corretta configurazione dell'indirizzo IP del peer.

```
[IKEv1]: Group = DefaultL2LGroup, IP = x.x.x.x,
ERROR, had problems decrypting packet, probably due to mismatched pre-shared key. Aborting
```

Quando l'indirizzo IP del peer non è stato configurato correttamente sulla configurazione crittografica ASA, l'ASA non è in grado di stabilire il tunnel VPN e si blocca solo nella fase MM_WAIT_MSG4.

Per risolvere il problema, correggere l'indirizzo IP del peer nella configurazione.

Di seguito è riportato l'output del comando show crypto isakmp sacommand quando il tunnel VPN si blocca nello stato MM_WAIT_MSG4.

<#root>

```
hostname#
```

show crypto isakmp sa

```
1   IKE Peer: XX.XX.XX.XX
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_WAIT_MSG4
```

Verifica dei nomi dei gruppi di tunnel e dei gruppi

```
%ASA-3-713206: Tunnel Rejected: Conflicting protocols specified by
tunnel-group and group-policy
```

Il messaggio viene visualizzato quando un tunnel viene eliminato perché il tunnel consentito specificato in Criteri di gruppo è diverso da quello consentito nella configurazione del gruppo di tunnel.

<#root>

```
group-policy hf_group_policy attributes
  vpn-tunnel-protocol l2tp-ipsec

username hfremote attributes
```

```
  vpn-tunnel-protocol l2tp-ipsec
```

Both lines read:

```
  vpn-tunnel-protocol ipsec l2tp-ipsec
```

Abilitare IPSec in Criteri di gruppo predefiniti per i protocolli già esistenti in Criteri di gruppo predefiniti.

```
group-policy DfltGrpPolicy attributes
   vpn-tunnel-protocol L2TP-IPSec IPSec webvpn
```

Disabilita XAUTH per peer L2L

Se un tunnel LAN-LAN e un tunnel VPN ad accesso remoto sono configurati sulla stessa mappa crittografica, il peer LAN-LAN richiede le informazioni XAUTH e il tunnel LAN-LAN non riesce con "CONF_XAUTH" nell'output del comando show crypto isakmp sacommand.

Di seguito è riportato un esempio dell'output dell'associazione di protezione:

<#root>

```
Router#
```

show crypto isakmp sa

```
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id  slot  status
X.X.X.X         Y.Y.Y.Y         CONF_XAUTH       10223    0   ACTIVE
X.X.X.X         Z.Z.Z.Z         CONF_XAUTH       10197    0   ACTIVE
```

questo problema si verifica solo con Cisco IOS®, mentre l'appliance ASA non è interessata dal problema perché usa gruppi di tunnel.

Utilizzare theno-xauthkeyword quando si immette la chiave isakmp, in modo che il dispositivo non richieda al peer le informazioni XAUTH (nome utente e password).

Questa parola chiave disabilita XAUTH per i peer IPsec statici. Immettere un comando simile a questo sul dispositivo con VPN L2L e RA configurate sulla stessa mappa crittografica:

<#root>

```
router(config)#
```

crypto isakmp key cisco123 address
**   172.22.1.164 no-xauth**

Nello scenario in cui l'ASA agisce come server Easy VPN, il client Easy VPN non è in grado di connettersi all'headend a causa del problema di Xauth.

Per risolvere il problema, disabilitare l'autenticazione dell'utente nell'appliance ASA come mostrato:

```
<#root>

ASA(config)#

tunnel-group example-group type ipsec-ra

ASA(config)#

tunnel-group example-group ipsec-attributes

ASA(config-tunnel-ipsec)#

isakmp ikev1-user-authentication none
```

Per ulteriori informazioni sul comando ikev1-user-authentication dell'isakmp, consultare la sezione Varie di questo documento.

Pool VPN in esaurimento

Quando l'intervallo di indirizzi IP assegnato al pool VPN non è sufficiente, è possibile estendere la disponibilità degli indirizzi IP in due modi:

1. Rimuovere l'intervallo esistente e definire il nuovo intervallo. Di seguito è riportato un esempio:

   ```
   <#root>

   CiscoASA(config)#

   no ip local pool testvpnpool 10.76.41.1-10.76.41.254

   CiscoASA(config)#

   ip local pool testvpnpool 10.76.41.1-10.76.42.254
   ```

2. Quando si aggiungono subnet non contigue al pool VPN, è possibile definire due pool VPN separati e quindi specificarli in ordine in "attributi del gruppo di tunnel ". Di seguito è riportato un esempio:

   ```
   <#root>

   CiscoASA(config)#
   ```

```
ip local pool testvpnpoolAB 10.76.41.1-10.76.42.254
CiscoASA(config)#
ip local pool testvpnpoolCD 10.76.45.1-10.76.45.254
CiscoASA(config)#
tunnel-group test type remote-access
CiscoASA(config)#
tunnel-group test general-attributes
CiscoASA(config-tunnel-general)#
address-pool (inside) testvpnpoolAB testvpnpoolCD
CiscoASA(config-tunnel-general)#
exit
```

L'ordine in cui si specificano i pool è molto importante perché l'ASA alloca gli indirizzi da questi pool nell'ordine in cui i pool vengono visualizzati in questo comando.

Le impostazioni dei pool di indirizzi nel comando address-pool dei criteri di gruppo sostituiscono sempre le impostazioni del pool locale nel comando tunnel-group address-pool.

Problemi di latenza per il traffico dei client VPN

In caso di problemi di latenza su una connessione VPN, verificare queste condizioni per risolvere il problema:

1. Verificare se il valore MSS del pacchetto può essere ulteriormente ridotto.
2. Se si utilizza IPsec/tcp anziché IPsec/udp, configurare preserve-vpn-flow.
3. Ricaricare Cisco ASA.

I client VPN non sono in grado di connettersi con l'ASA

Problema

I client VPN Cisco non sono in grado di eseguire l'autenticazione quando X-auth viene utilizzato con il server Radius.

Soluzione

Il problema può essere che lo xauth scade. Per risolvere il problema, aumentare il valore di timeout per il server AAA.

Ad esempio:

<#root>

```
Hostname(config)#
aaa-server test protocol radius

hostname(config-aaa-server-group)#
aaa-server test host 10.2.3.4

hostname(config-aaa-server-host)#
timeout 10
```

Problema

I client VPN Cisco non sono in grado di eseguire l'autenticazione quando X-auth viene utilizzato con il server Radius.

Soluzione

Inizialmente, verificare che l'autenticazione funzioni correttamente. Per risolvere il problema, verificare prima l'autenticazione con il database locale sull'appliance ASA.

```
tunnel-group tggroup general-attributes
              authentication-server-group none
              authentication-server-group LOCAL
        exit
```

Se questa operazione funziona correttamente, il problema è relativo alla configurazione del server Radius.

Verificare la connettività del server Radius dall'appliance ASA. Se il ping funziona senza problemi, controllare la configurazione relativa a Radius sull'appliance ASA e la configurazione del database sul server Radius.

È possibile utilizzare il comando debug radius per risolvere i problemi relativi al raggio. Per l'output del comando sampledebug radiusoutput, consultare questo output di esempio.

Prima di usare il comando debugsull'appliance ASA, consultare questa documentazione:messaggio di avviso.

Il client VPN interrompe frequentemente la connessione al primo tentativo o "Connessione VPN di sicurezza terminata dal peer". Motivo 433." o "Connessione VPN sicura terminata dal peer.

Motivo 433: (motivo non specificato dal peer)"

Problema

Gli utenti di client VPN Cisco ricevono questo errore quando tentano la connessione con il dispositivo VPN headend.

Il client VPN interrompe frequentemente la connessione al primo tentativo

Connessione VPN di sicurezza terminata dal peer. 433.

Connessione VPN sicura terminata dal peer. Motivo 433: (motivo non specificato dal peer)

Tentativo di assegnare un indirizzo IP di rete o di trasmissione, rimozione (x.x.x.x) dal pool

Soluzione 1

Il problema può essere dovuto all'assegnazione del pool IP tramite ASA, server Radius, server DHCP o server Radius che funge da server DHCP.

Per verificare che la netmask e gli indirizzi IP siano corretti, usare il comando debug crypto. Verificare inoltre che il pool non includa l'indirizzo di rete e l'indirizzo di broadcast.

I server Radius devono essere in grado di assegnare gli indirizzi IP corretti ai client.

Soluzione 2

Questo problema si verifica anche a causa di un errore di autenticazione estesa. Per risolvere il problema, controllare il server AAA.

Controllare la password di autenticazione del server sul server e sul client. Per risolvere il problema, ricaricare il server AAA.

Soluzione 3

Per risolvere questo problema, è inoltre possibile disabilitare la funzione di rilevamento delle minacce.

In alcuni casi, quando sono presenti più ritrasmissioni per diverse associazioni di sicurezza (SA) incomplete, l'ASA con la funzione di rilevamento delle minacce abilitata ritiene che si sia verificato un attacco di scansione e le porte VPN sono contrassegnate come il responsabile principale.

Provare a disabilitare la funzione di rilevamento delle minacce in quanto potrebbe causare un notevole sovraccarico sull'elaborazione dell'appliance ASA. Per disabilitare il rilevamento delle minacce, usare questi comandi:

```
no threat-detection basic-threat
```

```
no threat-detection scanning-threat shun
no threat-detection statistics
no threat-detection rate
```

Questa opzione può essere utilizzata come soluzione per verificare se il problema è stato risolto.

Verificare che la disabilitazione del rilevamento delle minacce sull'appliance Cisco ASA comprometta effettivamente diverse funzionalità di sicurezza, come la riduzione dei tentativi di scansione, DoS con SPI non valido, pacchetti che non superano il controllo delle applicazioni e sessioni incomplete.

Soluzione 4

Questo problema si verifica anche quando un set di trasformazioni non è configurato correttamente. Una corretta configurazione del set di trasformazioni consente di risolvere il problema.

Accesso remoto e utenti EZVPN si connettono alla VPN ma non possono accedere alle risorse esterne

Problema

Gli utenti di Accesso remoto non dispongono di connettività Internet una volta connessi alla VPN.

Gli utenti di Accesso remoto non possono accedere alle risorse che si trovano dietro altre VPN sullo stesso dispositivo.

Gli utenti di Accesso remoto possono accedere solo alla rete locale.

Soluzioni

Per risolvere il problema, provare le soluzioni seguenti:

- Impossibile accedere ai server in DMZ
- Client VPN: impossibile risolvere il DNS
- Split-Tunnel: impossibile accedere a Internet o alle reti escluse
- Accesso LAN locale
- Sovrapposizione di reti private

Impossibile accedere ai server in DMZ

Una volta che il client VPN ha stabilito il tunnel IPsec con il dispositivo headend VPN (ASA / Cisco IOS® Router), gli utenti del client VPN possono accedere alle risorse della rete INTERNA

(10.10.10.0/24), ma non alla rete DMZ (10.1.1.0/24).

Diagramma

Verificare che nel dispositivo headend non sia stata aggiunta la configurazione NAT del tunnel suddiviso per accedere alle risorse della rete DMZ.

Esempio:

Configurazione ASA:

Questa configurazione mostra come configurare l'esenzione NAT per la rete DMZ in modo da consentire agli utenti VPN di accedere alla rete DMZ:

```
object network obj-dmz
subnet 10.1.1.0 255.255.255.0
object network obj-vpnpool
subnet 192.168.1.0 255.255.255.0
nat (inside,dmz) 1 source static obj-dmz obj-dmz destination static obj-vpnpool obj-vpnpool
```

Dopo aver aggiunto una nuova voce per la configurazione NAT, cancellare la conversione NAT.

```
Clear xlate
Clear local
```

Verifica:

Se il tunnel è stato stabilito, andare sul client VPN Cisco e scegliere Stato > Dettagli route per verificare che i percorsi protetti siano visualizzati sia per la rete DMZ che per la rete INSIDE.

Per informazioni sulla procedura da seguire per aggiungere un nuovo tunnel VPN o una VPN ad accesso remoto a una configurazione VPN da L a L2L esistente, fare riferimento a ASA: Add a New Tunnel or Remote Access to an Existing L2L VPN - Cisco (ASA: Add a New Tunnel or Remote Access to an Existing L2L VPN - Cisco).

Fare riferimento all'esempio di configurazione ASA: Allow Split Tunneling for VPN Client for ASA Configuration Exampleper istruzioni dettagliate su come consentire ai client VPN di accedere a Internet e contemporaneamente eseguire il tunneling in una appliance Cisco Adaptive Security Appliance (ASA) serie 5500.

Client VPN: impossibile risolvere il DNS

Dopo aver stabilito il tunnel, se i client VPN non sono in grado di risolvere il DNS, il problema può essere la configurazione del server DNS nel dispositivo headend (ASA).

Verificare inoltre la connettività tra i client VPN e il server DNS. La configurazione del server DNS deve essere configurata in base ai Criteri di gruppo e applicata in base ai Criteri di gruppo negli attributi generali del gruppo di tunnel, ad esempio:

<#root>

```
!--- Create the group policy named vpn3000 and !--- specify the DNS server IP address(172.16.1.1) !--- a


group-policy vpn3000 internal
group-policy vpn3000 attributes
 dns-server value 172.16.1.1
 default-domain value cisco.com


!--- Associate the group policy(vpn3000) to the tunnel group !--- with the default-group-policy.


tunnel-group vpn3000 general-attributes
 default-group-policy vpn3000
```

I client VPN non sono in grado di connettere i server interni per nome

Il client VPN non è in grado di eseguire il ping degli host o dei server della rete remota o della rete interna del headend per nome. Per risolvere il problema, è necessario abilitare le configurazioni split-dns sull'appliance ASA.

Split-Tunnel: impossibile accedere a Internet o alle reti escluse

Lo split tunnel consente ai client IPsec di accesso remoto di indirizzare condizionalmente i pacchetti sul tunnel IPsec in forma crittografata o su un'interfaccia di rete in forma non crittografata, decrittografata, dove vengono indirizzati a una destinazione finale.

Per impostazione predefinita, lo split-tunnel è disabilitato, il che comporta l'unnelall traffic.

```
split-tunnel-policy {tunnelall | tunnelspecified | excludespecified}
```

L'opzione excludespecified è supportata solo per i client VPN Cisco, non per i client EZVPN.

```
ciscoasa(config-group-policy)#split-tunnel-policy excludespecified
```

Per esempi dettagliati di configurazione dello split-tunnel, consultare i seguenti documenti:

- ASA: esempio di configurazione dell'appliance ASA che consente il tunneling suddiviso per i

client VPN

- Il router consente ai client VPN di connettersi a IPsec e a Internet utilizzando un esempio di configurazione del tunneling ripartito

Soluzione a fermaglio

Questa funzionalità è utile per il traffico VPN che entra in un'interfaccia ma che viene quindi instradato all'esterno della stessa interfaccia.

Ad esempio, in una rete VPN hub e spoke, in cui l'appliance di sicurezza è l'hub e le reti VPN remote sono spoke, il traffico di comunicazione spoke deve passare all'appliance di sicurezza e quindi uscire di nuovo verso l'altro spoke.

Utilizzare la configurazione same-security-traffico per consentire al traffico di entrare e uscire dalla stessa interfaccia.

<#root>

```
securityappliance(config)#
```

same-security-traffic permit intra-interface

Accesso LAN locale

Gli utenti di Accesso remoto si connettono alla VPN e possono connettersi solo alla rete locale.

Per un esempio di configurazione più dettagliata, fare riferimento a ASA: Allow local LAN access for VPN Client.

Sovrapposizione di reti private

Problema

Se non è possibile accedere alla rete interna dopo la creazione del tunnel, controllare l'indirizzo IP assegnato al client VPN che si sovrappone alla rete interna dietro il dispositivo headend.

Soluzione

Verificare che gli indirizzi IP nel pool da assegnare ai client VPN, la rete interna del dispositivo headend e la rete interna del client VPN si trovino in reti diverse.

È possibile assegnare la stessa rete principale con subnet diverse, ma talvolta si verificano problemi di routing.

Per ulteriori esempi, vedere il diagramma e l'esempio della sezione Impossibile accedere ai server nella DMZ.

Impossibile connettere più di tre utenti client VPN

Problema

Solo tre client VPN possono connettersi ad ASA/; la connessione del quarto client non riesce. In caso di errore, viene visualizzato il seguente messaggio di errore:

```
Secure VPN Connection terminated locally by the client.
     Reason 413: User Authentication failed.
```

```
tunnel rejected; the maximum tunnel count has been reached
```

Soluzioni

Nella maggior parte dei casi, questo problema è correlato a un'impostazione di accesso simultaneo in Criteri di gruppo e al limite massimo di sessione.

Per risolvere il problema, provare le soluzioni seguenti:

- Configura accessi simultanei
- Configurazione dell'ASA con CLI
- Configurazione

Configura accessi simultanei

Se la casella di controllo Eredita in ASDM è selezionata, è consentito solo il numero predefinito di accessi simultanei per l'utente. Il valore predefinito per gli accessi simultanei è tre (3).

Per risolvere il problema, aumentare il valore per gli accessi simultanei.

1. Avviare ASDM, quindi selezionare Configurazione > VPN > Criteri di gruppo.
2. Scegliere il raggruppamento appropriato e fare clic sul pulsante Modifica.
3. Nella scheda Generale, annullare la casella di controllo Eredita per Login simultanei in Impostazioni connessione. Scegliere un valore appropriato nel campo.

   Il valore minimo per questo campo è zero (0), che disabilita l'accesso e impedisce l'accesso degli utenti.

   Quando si accede con lo stesso account utente da un PC diverso, la sessione corrente (la connessione stabilita da un altro PC con lo stesso account utente) viene terminata e la

nuova sessione viene stabilita.

Questo è il comportamento predefinito ed è indipendente dagli accessi simultanei VPN.

Configurazione dell'ASA con CLI

Completare la procedura seguente per configurare il numero desiderato di accessi simultanei. Nell'esempio, è stato scelto venti (20) come valore desiderato.

```
<#root>

ciscoasa(config)#

group-policy Bryan attributes

ciscoasa(config-group-policy)#

vpn-simultaneous-logins 20
```

Per ulteriori informazioni sul comando, consultare la guida di riferimento dei comandi di Cisco Security Appliance.

Utilizzare il comando vpn-sessiondb max-session-limiter nella modalità di configurazione globale per limitare le sessioni VPN a un valore inferiore a quello consentito dall'appliance di sicurezza.

Usare la versione di questo comando per rimuovere il limite di sessione. Utilizzare nuovamente il comando per sovrascrivere l'impostazione corrente.

```
vpn-sessiondb max-session-limit {session-limit}
```

Nell'esempio viene mostrato come impostare un limite massimo di sessioni VPN di 450:

```
<#root>

hostname#

vpn-sessiondb max-session-limit 450
```

Configurazione

Messaggio di errore

```
20932 10/26/2007 14:37:45.430 SEV=3 AUTH/5 RPT=1863 10.19.187.229
Authentication rejected: Reason = Simultaneous logins exceeded for user
```

```
handle = 623, server = (none), user = 10.19.187.229, domain = <not
specified>
```

Soluzione

Completare questa procedura per configurare il numero desiderato di accessi simultanei. È inoltre possibile provare a impostare l'opzione Accessi simultanei su 5 per questa associazione di protezione:

Scegliere Configurazione > Gestione utente > Gruppi > Modifica 10.19.187.229 > Generale > Accessi simultanei e modificare il numero di accessi in 5.

Impossibile avviare la sessione o un'applicazione e rallentare il trasferimento dopo l'istituzione del tunnel

Problema

Dopo aver stabilito il tunnel IPsec, l'applicazione o la sessione non viene avviata attraverso il tunnel.

Soluzioni

Utilizzare il comando ping per controllare la rete o verificare se il server applicazioni è raggiungibile dalla rete.

Può trattarsi di un problema con le dimensioni massime del segmento (MSS) per i pacchetti temporanei che attraversano un router o un dispositivo /ASA, in particolare i segmenti TCP con bit SYN impostato.

Cisco IOS® Router: per modificare il valore MSS nell'interfaccia esterna (interfaccia tunnel) del router

Per modificare il valore MSS nell'interfaccia esterna (interfaccia terminale del tunnel) del router, eseguire questi comandi:

<#root>

```
Router>
enable

Router#
configure terminal
Router(config)#
interface ethernet0/1
```

```
Router(config-if)#ip tcp adjust-mss 1300
Router(config-if)#
end
```

Questi messaggi mostrano l'output del comando debug per TCP MSS:

<#root>

```
Router#debug ip tcp transactions
Sep 5 18:42:46.247: TCP0: state was LISTEN -> SYNRCVD [23 -> 10.0.1.1(38437)]
Sep 5 18:42:46.247: TCP: tcb 32290C0 connection to 10.0.1.1:38437, peer MSS 1300, MSS is
1300
Sep 5 18:42:46.247: TCP: sending SYN, seq 580539401, ack 6015751
Sep 5 18:42:46.247: TCP0: Connection to 10.0.1.1:38437, advertising MSS 1300
Sep 5 18:42:46.251: TCP0: state was SYNRCVD -> ESTAB [23 -> 10.0.1.1(38437)]
```

Il valore MSS viene impostato su 1300 sul router come configurato.

Per ulteriori informazioni, fare riferimento a ASA e Cisco IOS®: VPN Fragmentation.

ASA - Fare riferimento alla documentazione di /ASA

Non è possibile accedere a Internet correttamente o il trasferimento viene rallentato tramite il tunnel perché viene visualizzato il messaggio di errore MTU e i problemi di MSS.

Per risolvere il problema, consultare il documento:

- ASA e Cisco IOS®: frammentazione VPN

Impossibile avviare il tunnel VPN da ASA

Problema

Non è possibile avviare il tunnel VPN dall'interfaccia ASA e, dopo aver stabilito il tunnel, il client VPN/estremità remota non può eseguire il ping sull'interfaccia interna dell'ASA sul tunnel VPN.

Ad esempio, il client VPN può non essere in grado di avviare una connessione SSH o HTTP alle appliance ASA all'interno dell'interfaccia sul tunnel VPN.

Soluzione

Non è possibile eseguire il ping dell'interfaccia interna del router dall'altra estremità del tunnel a meno che il comando management-access non sia configurato in modalità di configurazione

globale.

```
<#root>

ASA-02(config)#

management-access inside


ASA-02(config)#

show management-access

management-access inside
```

Questo comando aiuta anche con l'avvio ssh o la connessione http all'interfaccia interna dell'ASA tramite un tunnel VPN.

Queste informazioni sono valide anche per l'interfaccia DMZ. Ad esempio, se si desidera eseguire il ping dell'interfaccia DMZ di /ASA o avviare un tunnel dall'interfaccia DMZ, è necessario il comando DMZ management-access.

```
<#root>

ASA-02(config)#

management-access DMZ
```

Se il client VPN non è in grado di connettersi, verificare che le porte ESP e UDP siano aperte.

Tuttavia, se tali porte non sono aperte, provare a connettersi al protocollo TCP 10000 selezionando questa porta nella voce VPN client connection.

Fare clic con il pulsante destro del mouse su Modifica > scheda Trasporto > IPsec su TCP.

Impossibile passare il traffico attraverso il tunnel VPN

Problema

Non è possibile passare il traffico attraverso un tunnel VPN.

Soluzione

Questo problema può verificarsi anche quando i pacchetti ESP sono bloccati. Per risolvere il problema, riconfigurare il tunnel VPN.

Questo problema può verificarsi quando i dati non sono crittografati, ma solo decrittografati sul tunnel VPN, come mostrato nell'output:

<#root>

```
ASA# sh crypto ipsec sa peer x.x.x.x
peer address: y.y.y.y
    Crypto map tag: IPSec_map, seq num: 37, local addr: x.x.x.x
      access-list test permit ip host xx.xx.xx.xx host yy.yy.yy.yy
      local ident (addr/mask/prot/port): (xx.xx.xx.xx/255.255.255.255/0/0)
      remote ident (addr/mask/prot/port): (yy.yy.yy.yy/255.255.255.255/0/0)
      current_peer: y.y.y.y



 #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 393, #pkts decrypt: 393, #pkts verify: 393

      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0
```

Per risolvere il problema, verificare le seguenti condizioni:

1. Se gli elenchi degli accessi crittografici corrispondono al sito remoto e gli elenchi degli accessi NAT 0 sono corretti.
2. Se il routing è corretto e il traffico colpisce l'interfaccia esterna che passa attraverso l'interfaccia interna. Nell'output di esempio viene mostrato che la decrittografia è stata eseguita, ma non viene eseguita.
3. Se il comando show enable connection-vpn è stato configurato sull'appliance ASA. Se non è configurato, configurare questo comando perché consente all'ASA di esentare il traffico VPN/crittografato dal controllo ACL dell'interfaccia.

Configura il peer di backup per il tunnel VPN sulla stessa mappa crittografica

Problema

Si desidera utilizzare più peer di backup per un singolo tunnel VPN.

Soluzione

La configurazione di più peer equivale al provisioning di un elenco di fallback. Per ogni tunnel, l'appliance di sicurezza tenta di negoziare con il primo peer dell'elenco.

Se il peer non risponde, l'appliance di sicurezza scorre verso il basso fino a quando un peer non risponde o non ci sono altri peer nell'elenco.

L'ASA ha una mappa crittografica già configurata come peer primario. È possibile aggiungere il

peer secondario dopo quello primario.

In questa configurazione di esempio il peer primario viene indicato come X.X.X.X e il peer di backup come Y.Y.Y.Y:

<#root>

ASA(config)#

crypto map mymap 10 set peer X.X.X.X Y.Y.Y.Y

Disabilita/Riavvia tunnel VPN

Problema

Per disabilitare temporaneamente il tunnel VPN e riavviare il servizio, completare la procedura descritta in questa sezione.

Soluzione

Usare il comando crypto map interface in modalità di configurazione globale per rimuovere una mappa crittografica precedentemente definita impostata su un'interfaccia.

Usare la forma di questo comando per rimuovere la mappa crittografica impostata dall'interfaccia.

<#root>

hostname(config)#

no crypto map

map-name

interface

interface-name

Questo comando rimuove una mappa crittografica impostata su un'interfaccia dell'appliance di sicurezza attiva e rende il tunnel VPN IPsec inattivo nell'interfaccia.

Per riavviare il tunnel IPsec su un'interfaccia, è necessario assegnare una mappa crittografica impostata a un'interfaccia prima che quest'ultima possa fornire i servizi IPsec.

<#root>

hostname(config)#

crypto map

map-name

interface

interface-name

Alcuni tunnel non crittografati

Problema

Quando sul gateway VPN è configurato un numero elevato di tunnel, alcuni tunnel non passano il traffico. L'ASA non riceve pacchetti crittografati per questi tunnel.

Soluzione

Questo problema si verifica perché l'ASA non riesce a passare i pacchetti crittografati attraverso i tunnel. Nella tabella ASP vengono create regole di crittografia duplicate.

Errore:- %ASA-5-713904: gruppo = DefaultRAGroup, IP = x.x.x.x, ... modalità di transazione non supportata versione v2. Tunnel terminato.

Problema

Viene visualizzato il messaggio di errore **%ASA-5-713904: Group = DefaultRAGroup, IP = 192.0.2.0,... non supportato dalla modalità di transazione v2.Tunnel** terminatederror.

Soluzione

Il motivo `del` messaggio di errore `Transaction Mode v2` è che ASA supporta solo la configurazione in modalità IKE V6 e non la versione precedente in modalità V2.

Per risolvere l'errore, utilizzare la versione V6 della configurazione della modalità IKE.

Errore:- %ASA-6-72036: gruppo client-gruppo utente xxxx IP x.x.x.x Trasmissione pacchetto di grandi dimensioni 1220 (soglia 1206)

Problema

Nei log dell'ASA viene visualizzato il messaggio di errore **%ASA-6-72036: Group < gruppo client > Utente < xxxx > IP < x.x.x> Transmitting large packet 1220 (soglia 1206).**

Che cosa significa questo registro e come è possibile risolverlo?

Soluzione

Questo messaggio di registro indica al client è stato inviato un pacchetto grande. L'origine del pacchetto non conosce il valore MTU del client.

L'errore potrebbe anche dipendere dalla compressione di dati non comprimibili. Per risolvere il problema, disattivare la compressione SVC con il comando vc compression noneper risolvere il problema.

Messaggio di errore quando QoS è abilitato in un'estremità del tunnel VPN

Problema

Se si è abilitato QoS in un'estremità del tunnel VPN, è possibile ricevere questo messaggio di errore:

```
IPSEC: Received an ESP packet (SPI= 0xDB6E5A60, sequence number= 0x7F9F) from
10.18.7.11 (user= ghufhi) to 172.16.29.23 that failed anti-replay check
```

Soluzione

Questo messaggio viene in genere generato quando un'estremità del tunnel esegue la funzionalità QoS. Questo si verifica quando viene rilevato un pacchetto non in ordine.

È possibile disabilitare QoS per arrestare questa operazione, ma può essere ignorato finché il traffico è in grado di attraversare il tunnel.

AVVISO: voce della mappa crittografica incompleta

Problema

Quando si esegue il comando crypto map mymap 20 ipsec-isakmpè possibile ricevere questo errore:

`AVVISO: voce della mappa crittografica incompleta`

Ad esempio:

<#root>

```
ciscoasa(config)#
```

crypto map mymap 20 ipsec-isakmp

WARNING: crypto map entry incomplete

Soluzione

Si tratta di un avviso comune quando si definisce una nuova mappa crittografica; un promemoria che ricorda che parametri come l'elenco degli accessi (indirizzo corrispondente), il set di trasformazioni e l'indirizzo del peer devono essere configurati prima che funzionino.

È inoltre normale che la prima riga digitata per definire la mappa crittografica non venga visualizzata nella configurazione.

Errore:- %ASA-4-400024: IDS:2151 Pacchetto ICMP di grandi dimensioni da a su interfaccia esterna

Problema

Impossibile passare un pacchetto ping di grandi dimensioni attraverso il tunnel VPN. Quando si tenta di passare pacchetti ping di grandi dimensioni, viene visualizzato l'errore**%ASA-4-40024: IDS:2151 Large ICMP packet from to on interface outside.**

Soluzione

Per risolvere il problema, disabilitare le firme 2150 e 2151.Dopo aver disabilitato le firme, il comando ping funziona correttamente.

Per disabilitare le firme, utilizzare i comandi seguenti:

ASA(config)#ip audit signature 2151 disable

ASA(config)#ip audit signature 2150 disable

Errore:- %ASA-4-402119: IPSEC: ricevuto un pacchetto di protocollo (SPI=spi, numero di sequenza= num_seq) da remote_IP (nome utente) a local_IP che non ha superato il controllo anti-replay.

Problema

Nei messaggi di log dell'appliance ASA è stato visualizzato questo messaggio:

Errore:- %|ASA-4-402119: IPSEC: ricevuto un pacchetto di protocollo (SPI=spi, numero di sequenza= num_seq) da remote_IP (nome utente) a local_IP che non ha superato il controllo anti-replay.

Soluzione

Per risolvere il problema, usare il comando crypto ipsec security-association replay window-sizeper modificare le dimensioni della finestra.

<#root>

```
hostname(config)#
crypto ipsec security-association replay window-size 1024
```

Cisco consiglia di utilizzare la finestra full 1024 per eliminare eventuali problemi di anti-replay.

Messaggio di errore - %ASA-4-407001: negazione del traffico per l'interfaccia host locale nome_interfaccia:indirizzo_interno, limite di numero di licenze superato

Problema

Pochi host non sono in grado di connettersi a Internet e nel syslog viene visualizzato questo messaggio di errore:

Messaggio di errore - %ASA-4-407001: negazione del traffico per l'interfaccia host locale nome_interfaccia:indirizzo_interno, limite di numero di licenze superato

Soluzione

Questo messaggio di errore viene visualizzato quando il numero di utenti supera il limite di utenti della licenza utilizzata. Questo errore può essere risolto aggiornando la licenza a un numero maggiore di utenti.

La licenza utente può includere 50, 100 o un numero illimitato di utenti, in base alle esigenze.

Messaggio di errore - %VPN_HW-4-PACKET_ERROR:

Problema

`Il messaggio di errore - %VPN_HW-4-PACKET_ERROR:`error indica che il pacchetto ESP con HMAC ricevuto dal router non corrisponde. Questo errore può essere causato dai problemi seguenti:

- Modulo hardware VPN difettoso
- Pacchetto ESP danneggiato

Soluzione

Per risolvere questo messaggio di errore:

- Ignorare i messaggi di errore a meno che non vi siano interruzioni del traffico.
- In caso di interruzione del traffico, sostituire il modulo.

Messaggio di errore: comando rifiutato: eliminare prima la connessione crittografica tra la VLAN XXXX e XXXX.

Problema

Questo messaggio di errore viene visualizzato quando si cerca di aggiungere una VLAN consentita sulla porta trunk di uno switch:`Comando rifiutato: delete crypto connection between VLAN XXXX and VLAN XXXX, first..`

Non è possibile modificare il trunk del limite della WAN per consentire altre VLAN. In altre parole, non è possibile aggiungere le VLAN nel trunk della VPN IPSEC.

Il comando è stato rifiutato in quanto restituisce una VLAN di interfaccia connessa tramite crittografia appartenente all'elenco di VLAN consentite e ciò rappresenta una potenziale violazione della sicurezza IPSec.

Si noti che questo comportamento si applica a tutte le porte trunk.

Soluzione

Anziché usare il comando `switchport trunk allowed vlan (vlanlist)`, usare il comando `switchport trunk allowed vlan` senza comando o il comando`"switchport trunk allowed vlan remove (vlan list)"`.

Messaggio di errore - % FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE: pacchetto ignorato - opzione di scala finestra non valida per la sessione da x.x.x.x:27331 a x.x.x.x:23 [iniziatore (flag 0,fattore 0) risponditore (flag 1, fattore 2)]

Problema

Questo errore si verifica quando si tenta di eseguire il telnet da un dispositivo all'estremità remota di un tunnel VPN o quando si tenta di eseguire il telnet dal router stesso:

`Messaggio di errore - % FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE: pacchetto ignorato - opzione di scala finestra non valida per la sessione da x.x.x.x:27331 a x.x.x.x:23 [iniziatore (flag`

0,fattore 0) risponditore (flag 1, fattore 2)]

Soluzione

La licenza utente può includere 50, 100 o un numero illimitato di utenti, in base alle esigenze. È stata aggiunta la funzione di ridimensionamento della finestra per consentire la trasmissione rapida di dati su reti LFN (Long FAT networks).

Si tratta in genere di connessioni con una larghezza di banda molto elevata, ma anche con un'alta latenza.

Le reti con connessioni satellitari sono un esempio di rete LFN, dal momento che i collegamenti satellitari hanno sempre alti ritardi di propagazione ma in genere hanno un'elevata larghezza di banda.

Per abilitare la funzione di ridimensionamento della finestra per il supporto delle LFN, la dimensione della finestra TCP deve essere maggiore di 65.535. Questo messaggio di errore può essere risolto aumentando le dimensioni della finestra TCP a più di 65.535.

%ASA-5-305013: Regole NAT asimmetriche corrispondenti per forward e reverse. Aggiornare i flussi di problemi

Problema

Questo messaggio di errore viene visualizzato quando viene visualizzato il tunnel VPN:

%ASA-5-305013: Regole NAT asimmetriche corrispondenti per forward e reverse. Aggiornare i flussi di problemi

Soluzione

Per risolvere il problema quando non si trova sulla stessa interfaccia dell'host con NAT, utilizzare l'indirizzo mappato anziché l'indirizzo effettivo per connettersi all'host.

Inoltre, abilitare il comando inspectse l'applicazione incorpora l'indirizzo IP.

%ASA-5-713068: ricevuto messaggio di notifica non di routine: notification_type

Problema

Questo messaggio di errore viene visualizzato se il tunnel VPN non si attiva:

%ASA-5-713068: ricevuto messaggio di notifica non di routine: notification_type

Soluzione

Questo messaggio viene generato a causa di una configurazione errata, ovvero quando i criteri o gli ACL non sono configurati come gli stessi nei peer.

Dopo aver trovato la corrispondenza tra le policy e gli ACL, il tunnel viene attivato senza alcun problema.

%ASA-5-72012: (VPN-Secondario) non è stato possibile aggiornare i dati di runtime del failover IPSec sull'unità in standby o %ASA-6-72012: (unità VPN) non è stato possibile aggiornare i dati di runtime del failover IPSec sull'unità in standby

Problema

Quando si cerca di aggiornare Cisco Adaptive Security Appliance (ASA), viene visualizzato uno dei seguenti messaggi di errore:

%ASA-5-72012: (VPN-Secondario) non è stato possibile aggiornare i dati di runtime del failover IPSec sull'unità in standby.

%ASA-6-72012: (unità VPN) non è possibile aggiornare i dati di runtime del failover IPsec sull'unità in standby.

Soluzione

Questi messaggi di errore sono di tipo informativo. I messaggi non influiscono sulla funzionalità dell'ASA o della VPN.

Questi messaggi vengono visualizzati quando il sottosistema di failover VPN non è in grado di aggiornare i dati di runtime relativi a IPSec perché il tunnel IPSec correlato è stato eliminato dall'unità di standby.

Per risolvere questi problemi, usare il comando wr standby sull'unità attiva.

Errore:- %ASA-3-713063: indirizzo peer IKE non configurato per la destinazione 0.0.0.0

Problema

Viene visualizzato il messaggio di errore **%ASA-3-713063: indirizzo peer IKE non configurato per la destinazione 0.0.0.0**e il tunnel non riesce a comparire.

Soluzione

Questo messaggio viene visualizzato quando l'indirizzo peer IKE non è configurato per un tunnel

L2L.

Per risolvere questo errore, è possibile modificare il numero di sequenza della mappa crittografica, quindi rimuovere e riapplicare la mappa crittografica.

Errore: %ASA-3-752006: impossibile per Tunnel Manager inviare un messaggio KEY_ACQUIRE.

Problema

In `%ASA-3-752006: Tunnel Manager non è stato in grado di inviare un messaggio KEY_ACQUIRE.Probabile errore di configurazione della mappa crittografica o del gruppo di tunnel."`Il messaggio di errore è registrato in Cisco ASA.

Soluzione

Questo messaggio di errore può essere causato da una configurazione errata della mappa crittografica o del gruppo di tunnel. Accertarsi che entrambi siano configurati correttamente. Per ulteriori informazioni su questo messaggio di errore, fare riferimento all'errore 752006 .

Di seguito sono elencate alcune delle azioni correttive:

- Rimuovere l'ACL crittografico (ad esempio, associato alla mappa dinamica).
- Rimuovere la configurazione IKEv2 non utilizzata, se presente.
- Verificare che l'ACL crittografico corrisponda correttamente.
- Rimuovere le eventuali voci duplicate dall'elenco degli accessi.

Errore: %ASA-4-402116: IPSEC: ricevuto pacchetto ESP (SPI= 0x99554D4E, numero di sequenza= 0x9E) da XX.XX.XX.XX (utente= XX.XX.XX.XX) a YY.YY.YY.YY

In una configurazione del tunnel VPN da LAN a LAN, questo errore viene ricevuto su un'estremità dell'appliance ASA:

`Il pacchetto interno decapsulato non corrisponde ai criteri negoziati nell'associazione di protezione.`

`Il pacchetto specifica la sua destinazione come 10.32.77.67, l'origine come 10.105.30.1 e il suo protocollo come icmp.`

`L'associazione di protezione specifica il proxy locale come 10.32.77.67/255.255.255.255/ip/0 e il relativo remote_proxy come 10.105.42.192/255.255.255.224/ip/0.`

Soluzione

È necessario verificare gli elenchi degli accessi al traffico interessanti definiti su entrambe le estremità del tunnel VPN. Entrambi devono corrispondere esattamente come immagini speculari.

Impossibile avviare il programma di installazione VA a 64 bit per abilitare la scheda virtuale a causa dell'errore 0xffffffff

Problema

`Impossibile avviare il programma di installazione VA a 64 bit per abilitare la scheda virtuale.` Viene visualizzato il messaggio di `errore 0`xffffffflog quando AnyConnect non riesce a connettersi.

Soluzione

Per risolvere il problema, completare i seguenti passaggi:

1. Selezionare Sistema > Gestione delle comunicazioni Internet > Impostazioni di comunicazione Internet e assicurarsi che Disattiva aggiornamento automatico certificati radice sia disattivato.
2. Se è disattivata, disattivare l'intero modello amministrativo dell'oggetto Criteri di gruppo assegnato al computer interessato e ripetere il test.

Per ulteriori informazioni, fare riferimento a Disattivazione dell'aggiornamento automatico dei certificati radice.

Cisco VPN Client non funziona con la scheda dati in Windows 7

Problema

Cisco VPN Client non funziona con la scheda dati in Windows 7.

Soluzione

Il client VPN Cisco installato in Windows 7 non funziona con le connessioni 3G poiché le schede dati non sono supportate nei client VPN installati in un computer Windows 7.

Avviso: "la funzionalità VPN potrebbe non funzionare affatto"

Problema

Durante i tentativi di abilitazione del protocollo isakmp sull'interfaccia esterna dell'appliance ASA, viene ricevuto questo messaggio di avviso:

```
ASA(config)# crypto isakmp enable outside
WARNING, system is running low on memory.  Performance may start to degrade.
VPN functionality may not work at all.
```

A questo punto, è possibile accedere all'appliance ASA tramite ssh. HTTPS è stato arrestato e sono interessati anche altri client SSL.

Soluzione

Questo problema è dovuto ai requisiti di memoria di diversi moduli, ad esempio logger e crypto.

Accertarsi di non avere il comando 0della coda di registrazione. La dimensione della coda viene impostata su 8192 e l'allocazione della memoria aumenta.

Nelle piattaforme come ASA5505 e ASA5510, questa allocazione di memoria tende a ridurre la memoria di altri moduli.

Errore di Padding IPSec

Problema

Viene ricevuto questo messaggio di errore:

```
%ASA-3-402130: CRYPTO: Received an ESP packet (SPI =
     0xXXXXXXX, sequence number= 0xXXXX) from x.x.x.x (user= user) to y.y.y.y with
     incorrect IPsec padding
```

Soluzione

Il problema si verifica perché la VPN IPSec esegue la negoziazione senza un algoritmo hash. L'hash del pacchetto garantisce il controllo dell'integrità per il canale ESP.

Pertanto, senza hash, i pacchetti in formato errato vengono accettati come non rilevati da Cisco ASA e tentano di decrittografarli.

Tuttavia, poiché i pacchetti sono in formato non corretto, l'ASA rileva dei problemi durante la decrittografia. In questo modo vengono visualizzati i messaggi di errore relativi alla spaziatura interna.

Si consiglia di includere un algoritmo hash nel set di trasformazioni per la VPN e di garantire che il collegamento tra i peer includa un minimo di malformazione del pacchetto.

Il tunnel VPN viene disconnesso ogni 18 ore

Problema

Il tunnel VPN viene disconnesso ogni 18 ore, anche se la durata è impostata su 24 ore.

Soluzione

La durata è il tempo massimo per cui l'associazione di protezione può essere utilizzata per la reimpostazione della chiave. Il valore immesso nella configurazione come durata è diverso dal tempo di rigenerazione della chiave dell'associazione di protezione.

È pertanto necessario negoziare una nuova associazione di protezione (o una coppia di associazioni di protezione nel caso di IPSec) prima della scadenza di quella corrente.

Il tempo di rigenerazione della chiave deve essere sempre inferiore alla durata per consentire più tentativi nel caso in cui il primo tentativo di rigenerazione della chiave non riesca.

Le RFC non specificano come calcolare il tempo di reimpostazione della chiave. Questo è lasciato alla discrezione degli implementatori.

Pertanto, il tempo varia a seconda della piattaforma in uso. Alcune implementazioni possono utilizzare un fattore casuale per calcolare il timer di reimpostazione chiavi.

Ad esempio, se l'ASA avvia il tunnel, è normale che reimposti le chiavi a 64800 secondi = 75% di 86400.

Se il router si avvia, l'ASA può attendere più a lungo per concedere al peer un tempo maggiore per avviare la reimpostazione della chiave.

Pertanto, è normale che la sessione VPN venga disconnessa ogni 18 ore per utilizzare un'altra chiave per la negoziazione VPN. Ciò non deve causare problemi o interruzioni della VPN.

Il flusso del traffico non viene mantenuto dopo la rinegoziazione del tunnel LAN-LAN

Problema

Il flusso del traffico non viene mantenuto dopo la rinegoziazione del tunnel LAN-LAN.

Soluzione

L'ASA controlla tutte le connessioni che passano attraverso di essa e mantiene una voce nella relativa tabella di stato in conformità alla funzione di ispezione dell'applicazione.

I dettagli del traffico crittografato che passano attraverso la VPN vengono gestiti sotto forma di database delle associazioni di sicurezza (SA, Security Association). Per le connessioni VPN da LAN a LAN, mantiene due flussi di traffico diversi.

La prima è il traffico crittografato tra i gateway VPN. L'altro è il flusso di traffico tra la risorsa di rete dietro il gateway VPN e l'utente finale dietro l'altra estremità.

Quando la VPN viene terminata, i dettagli del flusso per questa particolare associazione di protezione vengono eliminati.

Tuttavia, la voce della tabella di stato gestita dall'ASA per questa connessione TCP non è più aggiornata a causa dell'assenza di attività che impedisce il download.

Ciò significa che l'ASA mantiene la connessione TCP per quel particolare flusso mentre l'applicazione utente termina.

Tuttavia, le connessioni TCP diventano inattive e alla fine si interrompe dopo la scadenza del timer di inattività TCP.

Per risolvere il problema, è stata introdotta una funzionalità denominata Persistent IPSec Tunneled Flows (Flussi di tunneling IPSec persistenti).

Un nuovo comando, syspot connection preserve-vpn-flows , è stato integrato nell'appliance Cisco ASA per conservare le informazioni della tabella dello stato durante la rinegoziazione del tunnel VPN.

Per impostazione predefinita, questo comando è disattivato. Per abilitare questa funzione, quando la VPN L2L si riattiva e ristabilisce il tunnel, Cisco ASA conserva le informazioni della tabella di stato TCP.

Il messaggio di errore indica che la larghezza di banda è stata raggiunta per la funzionalità di crittografia

Problema

Questo messaggio di errore viene ricevuto sul router serie 2900:

Errore: mar 20 10:51:29: %CERM-4-TX_BW_LIMIT: è stato raggiunto il limite massimo di larghezza di banda Tx di 85000 Kbps per la funzionalità di crittografia con licenza del pacchetto con tecnologia SecurityKey9.

Soluzione

Si tratta di una questione nota che si verifica a causa delle rigide linee guida emesse dal governo degli Stati Uniti.

Di conseguenza, la licenza securityk9 può consentire la crittografia del payload solo fino a velocità vicine a 90 Mbps e limitare il numero di tunnel crittografati/sessioni TLS per il dispositivo.

Per ulteriori informazioni sulle restrizioni all'esportazione basate sulla crittografia, fare riferimento alle licenze Cisco ISR G2 SEC e HSEC.

Nel caso di dispositivi Cisco, il traffico unidirezionale in entrata e in uscita dal router ISR G2 è inferiore a 85 Mbps, con un totale bidirezionale di 170 Mbps.

Questo requisito si applica alle piattaforme Cisco 1900, 2900 e 3900 ISR G2. Questo comando consente di visualizzare le seguenti limitazioni:

<#root>

```
Router#

show platform cerm-information

Crypto Export Restrictions Manager(CERM) Information:
CERM functionality: ENABLED
 ---------------------------------------------------------------
 Resource                      Maximum Limit          Available
 ---------------------------------------------------------------
 Tx Bandwidth(in kbps)         85000                  85000
 Rx Bandwidth(in kbps)         85000                  85000
 Number of tunnels               225                    225
 Number of TLS sessions         1000                   1000
---Output truncated----
```

Per evitare questo problema, acquistare una licenza HSECK9. La licenza per la funzionalità "hseck9" offre funzionalità avanzate di crittografia del payload con un numero maggiore di tunnel VPN e sessioni vocali sicure.

Per ulteriori informazioni sulle licenze dei router Cisco ISR, consultare il documento su Attivazione del software.

Problema: il traffico di crittografia in uscita in un tunnel IPsec non riesce, anche se il traffico di decrittografia in entrata funziona.

Soluzione

Il problema è stato rilevato su una connessione IPSec dopo più reimpostazioni di chiave, ma la condizione di attivazione non è chiara.

Per verificare la presenza di questo problema, controllare l'output del comando show asp drop e verificare che il contatore del contesto VPN scaduto aumenti per ciascun pacchetto in uscita inviato.

Varie

AG_INIT_EXCH Messaggio visualizzato nell'output dei comandi "show crypto isakmp sa" e "debug"

Se il tunnel non viene avviato, il messaggio**AG_INIT**_EXCH viene visualizzato anche nell'output del

comando show crypto isakmp sacommand e indebugooutput.

Il motivo può essere una mancata corrispondenza dei criteri isakmp o il blocco della porta udp 500.

Viene Visualizzato Il Messaggio Di Debug "Received an IPC message while invalid state"

Questo messaggio è informativo e non ha nulla a che fare con la disconnessione del tunnel VPN.

Informazioni correlate

- ASA e Cisco IOS®: frammentazione VPN
- Cisco ASA serie 5500 Security Appliance
- Negoziazione IPSec/protocolli IKE
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).