Risposta alle domande frequenti su AnyConnect - Tunnel, DPD e timer di inattività

Sommario

Introduzione

In questo documento vengono descritti i tunnel Cisco AnyConnect Secure Mobility Client, il comportamento della riconnessione e il DPD (Dead Peer Detection) e il timer di inattività.

Premesse

Tipi di tunnel

Per connettere una sessione AnyConnect, è possibile usare due metodi:

- Tramite il portale (senza client)
- Tramite l'applicazione standalone

In base al modo in cui ci si connette, vengono creati tre tunnel (sessioni) diversi su Cisco Adaptive Security Appliance (ASA), ciascuno con uno scopo specifico:

1. Senza client o tunnel padre: si tratta della sessione principale creata nella negoziazione per impostare il token di sessione necessario nel caso in cui sia necessaria una riconnessione a causa di problemi di connettività di rete o ibernazione. In base al meccanismo di connessione, l'ASA elenca la sessione come senza client (Weblaunch tramite il portale) o padre (AnyConnect standalone).

   Nota: AnyConnect-Parent rappresenta la sessione quando il client non è connesso in modo attivo. In effetti, funziona come un cookie, in quanto è una voce di database sull'appliance ASA che mappa la connessione di un particolare client. Se il client è in stato di sospensione o ibernazione, i tunnel (protocolli IPsec/IKE (Internet Key Exchange)/TLS (Transport Layer Security)/DTLS (Datagram Transport Layer Security) vengono disattivati, ma il padre rimane attivo fino a quando il timer di inattività o il tempo massimo di connessione non diventa effettivo. In questo modo l'utente può riconnettersi senza ripetere l'autenticazione.

2. Tunnel SSL (Secure Sockets Layer): la connessione SSL viene stabilita per prima e i dati vengono passati attraverso questa connessione mentre quest'ultima tenta di stabilire una connessione DTLS. Una volta stabilita la connessione DTLS, il client invia i pacchetti tramite la connessione DTLS anziché tramite la connessione SSL. I pacchetti di controllo, d'altra parte, passano sempre attraverso la connessione SSL.

3. DTLS-Tunnel: quando il tunnel DTLS-Tunnel è completamente stabilito, tutti i dati vengono trasferiti al tunnel DTLS-Tunnel e il tunnel SSL viene utilizzato solo per il traffico del canale di controllo occasionale. Se succede qualcosa al protocollo UDP (User Datagram Protocol), il tunnel DTLS viene demolito e tutti i dati passano di nuovo attraverso il tunnel SSL.

Output di esempio dell'appliance ASA

Di seguito viene riportato un esempio di output dei due metodi di connessione.

AnyConnect Connected tramite lancio sul Web:

```
ASA5520-C(config)# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : walter Index : 1435
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Protocol : Clientless SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : Clientless: (1)RC4 SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing : Clientless: (1)SHA1 SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 335765 Bytes Rx : 31508
Pkts Tx : 214 Pkts Rx : 18
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : My-Network Tunnel Group : My-Network
Login Time : 22:13:37 UTC Fri Nov 30 2012
Duration : 0h:00m:34s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none

Clientless Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

Clientless:
Tunnel ID : 1435.1
Public IP : 172.16.250.17
Encryption : RC4 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : Web Browser
Client Ver : Mozilla/5.0 (Windows NT 5.1; rv:16.0) Gecko/20100101 Firefox/16.0
Bytes Tx : 329671 Bytes Rx : 31508

SSL-Tunnel:
Tunnel ID : 1435.2
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Encryption : RC4 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Src Port : 1241
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.01065
Bytes Tx : 6094 Bytes Rx : 0
Pkts Tx : 4 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 1435.3
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Encryption : AES128 Hashing : SHA1
Encapsulation: DTLSv1.0 Compression : LZS
UDP Src Port : 1250 UDP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : DTLS VPN Client
Client Ver : Mozilla/5.0 (Windows NT 5.1; rv:16.0) Gecko/20100101 Firefox/16.0
Bytes Tx : 0 Bytes Rx : 0
Pkts Tx : 0 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

AnyConnect connesso tramite l'applicazione standalone:

```
ASA5520-C(config)# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : walter Index : 1436
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 12244 Bytes Rx : 777
Pkts Tx : 8 Pkts Rx : 1
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : My-Network Tunnel Group : My-Network
Login Time : 22:15:24 UTC Fri Nov 30 2012
Duration : 0h:00m:11s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
Tunnel ID : 1436.1
Public IP : 172.16.250.17
Encryption : none Hashing : none
TCP Src Port : 1269 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : AnyConnect
Client Ver : 3.1.01065
Bytes Tx : 6122 Bytes Rx : 777
Pkts Tx : 4 Pkts Rx : 1
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 1436.2
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Encryption : RC4 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Src Port : 1272
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.01065
Bytes Tx : 6122 Bytes Rx : 0
Pkts Tx : 4 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 1436.3
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Encryption : AES128 Hashing : SHA1
Encapsulation: DTLSv1.0 Compression : LZS
UDP Src Port : 1280 UDP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : DTLS VPN Client
Client Ver : 3.1.01065
Bytes Tx : 0 Bytes Rx : 0
Pkts Tx : 0 Pkts Rx : 0
```

```
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

DPD e timer di inattività

Quando una sessione viene considerata inattiva?

La sessione è considerata inattiva (e il timer inizia ad aumentare) solo quando il tunnel SSL non esiste più nella sessione. Quindi, ogni sessione è contrassegnata dall'ora di rilascio del tunnel SSL.

```
ASA5520-C# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : walter Index : 1336
Public IP : 172.16.250.17
Protocol : AnyConnect-Parent <- Here just the AnyConnect-Parent is active
but not SSL-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none
Hashing : AnyConnect-Parent: (1)none
Bytes Tx : 12917 Bytes Rx : 1187
Pkts Tx : 14 Pkts Rx : 7
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : My-Network Tunnel Group : My-Network
Login Time : 17:42:56 UTC Sat Nov 17 2012
Duration : 0h:09m:14s
Inactivity : 0h:01m:06s <- So the session is considered Inactive
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
```

Quando l'ASA elimina il tunnel SSL?

Èpossibile disconnettere un tunnel SSL in due modi:

1. **DPD**: le DPD vengono usate dal client per rilevare un errore nelle comunicazioni tra il client AnyConnect e l'headend ASA. Le DPD vengono usate anche per pulire le risorse sull'appliance ASA. In questo modo, l'headend non manterrà le connessioni nel database se l'endpoint non risponde ai ping DPD. Se l'ASA invia un DPD all'endpoint e risponde, non viene intrapresa alcuna azione. Se l'endpoint non risponde, dopo il numero massimo di ritrasmissioni (dipende dal fatto che venga utilizzato IKEv1 o IKEv2) l'ASA demolisce il tunnel nel database di sessione e sposta la sessione in modalità "In attesa di ripresa". Ciò significa che la DPD è stata avviata dall'headend e che quest'ultimo non comunica più con il client. In queste situazioni, l'ASA mantiene attivo il tunnel padre per consentire all'utente di eseguire il roaming delle reti, passare alla modalità sospensione e ripristinare la sessione. Queste sessioni vengono conteggiate rispetto alle sessioni connesse attivamente e vengono cancellate nelle seguenti condizioni:
   Timeout di inattività utenteIl client riprende la sessione originale e si disconnette correttamente
   Per configurare i DPD, utilizzare il **anyconnect dpd-interval** negli attributi WebVPN nelle impostazioni dei Criteri di gruppo. Per impostazione predefinita, il DPD è abilitato e impostato su 30 secondi sia per l'ASA (gateway) che per il client.

Attenzione: prestare attenzione all'ID bug Cisco CSCts6926 - DPD non riesce a terminare il tunnel DTLS dopo la perdita della connessione client.

2. **Timeout di inattività**: il secondo modo in cui il tunnel SSL viene disconnesso è quando scade il timeout di inattività per questo tunnel. Tuttavia, tenere presente che non deve essere inattivo solo il tunnel SSL, ma anche il tunnel DTLS. A meno che la sessione DTLS non scada in tempo, il tunnel SSL viene mantenuto nel database.

Perché è necessario abilitare i pacchetti keepalive se i DPD sono già abilitati?

Come spiegato in precedenza, la DPD non interrompe la sessione AnyConnect stessa. ma semplicemente elimina il tunnel all'interno della sessione in modo che il client possa ristabilire il tunnel. Se il client non riesce a ristabilire il tunnel, la sessione rimane attiva fino alla scadenza del timer di inattività sull'appliance ASA. Poiché i DPD sono abilitati per impostazione predefinita, i client possono spesso disconnettersi a causa di flussi che si chiudono in una direzione con dispositivi NAT (Network Address Translation), firewall e proxy. Per evitare questo inconveniente, attivare l'opzione keepalive a intervalli bassi, ad esempio 20 secondi.

I pacchetti keepalive vengono attivati negli attributi WebVPN di un determinato criterio di gruppo con **anyconnect ssl keepalive** Per impostazione predefinita, i timer sono impostati su 20 secondi.

Comportamento del client AnyConnect in caso di riconnessioni

AnyConnect tenta di riconnettersi se la connessione viene interrotta. Questa operazione non è configurabile automaticamente. Se la sessione VPN sull'appliance ASA è ancora valida e se AnyConnect può ristabilire la connessione fisica, la sessione VPN viene ripresa.

La funzione di riconnessione continua finché non scade il timeout della sessione o di disconnessione, che in realtà è il timeout di inattività (o 30 minuti se non sono configurati timeout). Dopo la scadenza, il client non può continuare perché le sessioni VPN sono già state eliminate sull'appliance ASA. Il client continua finché ritiene che l'ASA abbia ancora una sessione VPN.

AnyConnect si riconnette indipendentemente dalle modifiche apportate all'interfaccia di rete. Non importa se l'indirizzo IP della scheda di interfaccia di rete (NIC, Network Interface Card) cambia o se la connettività passa da una NIC a un'altra (da wireless a cablata o viceversa).

Se si considera il processo di riconnessione di AnyConnect, occorre ricordare tre livelli di sessione. Inoltre, il comportamento di riconnessione di ciascuna di queste sessioni è vagamente accoppiato, in quanto qualsiasi di esse può essere ristabilita senza una dipendenza dagli elementi della sessione del livello precedente:

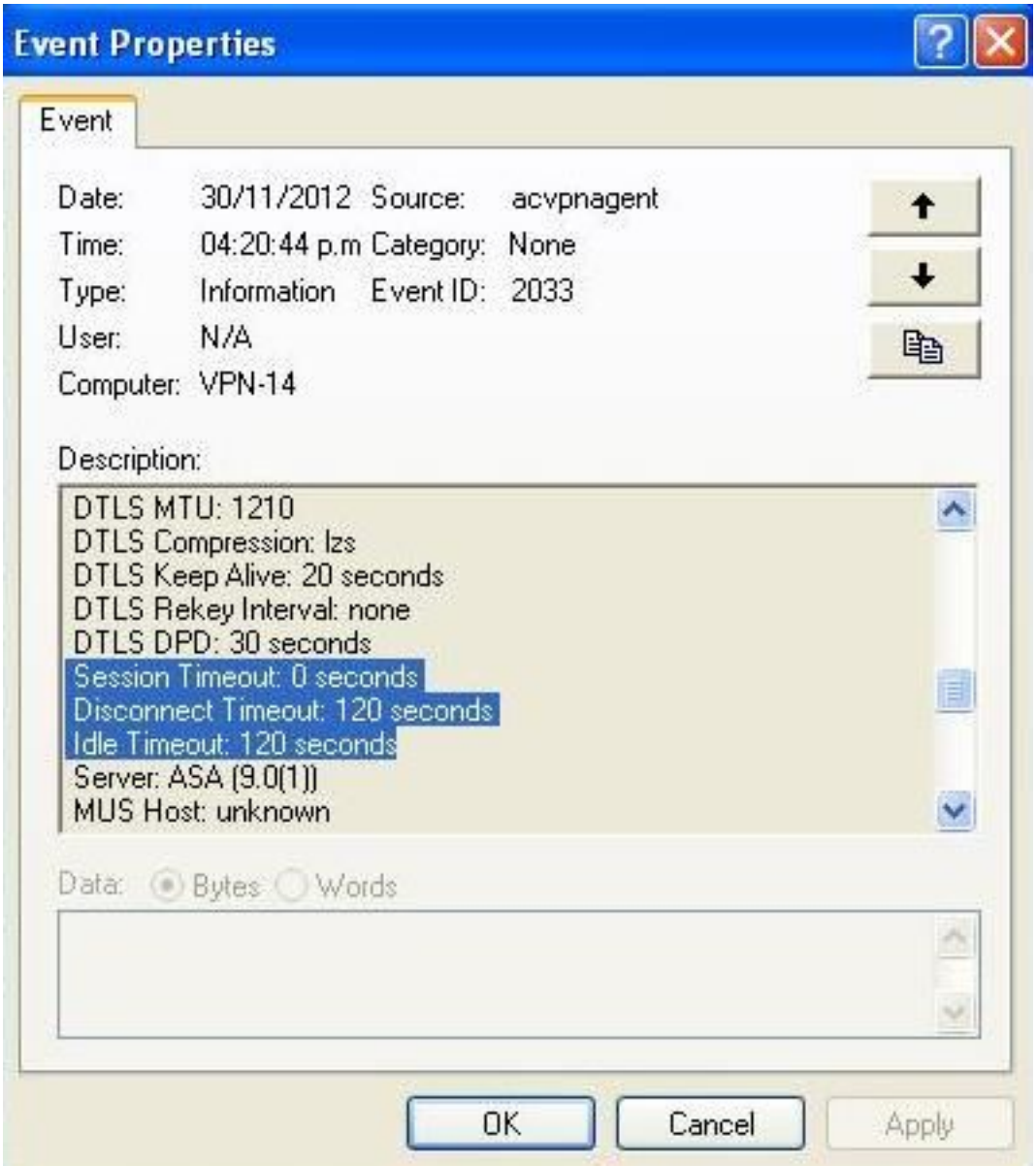
1. Riconnessioni TCP o UDP [OSI Layer 3]
2. TLS, DTLS o IPSec(IKE+ESP) [OSI Layer 4] - Ripresa TLS non supportata.
3. VPN [OSI layer 7] - Il token di sessione VPN viene utilizzato come token di autenticazione per ristabilire la sessione VPN su un canale protetto in caso di interruzione. Si tratta di un meccanismo proprietario molto simile, dal punto di vista concettuale, all'utilizzo di un token Kerberos o di un certificato client per l'autenticazione. Il token è univoco e generato crittograficamente dall'headend, che contiene l'ID sessione e un payload casuale generato crittograficamente. Viene passato al client come parte della configurazione iniziale della VPN dopo aver stabilito un canale sicuro per l'headend. Rimane valida per tutta la durata della

sessione sull'headend e viene archiviata nella memoria client, che è un processo privilegiato.
Suggerimento: queste versioni di ASA e successive contengono un token di sessione crittografica più avanzato: 9.1(3) e 8.4(7.1)

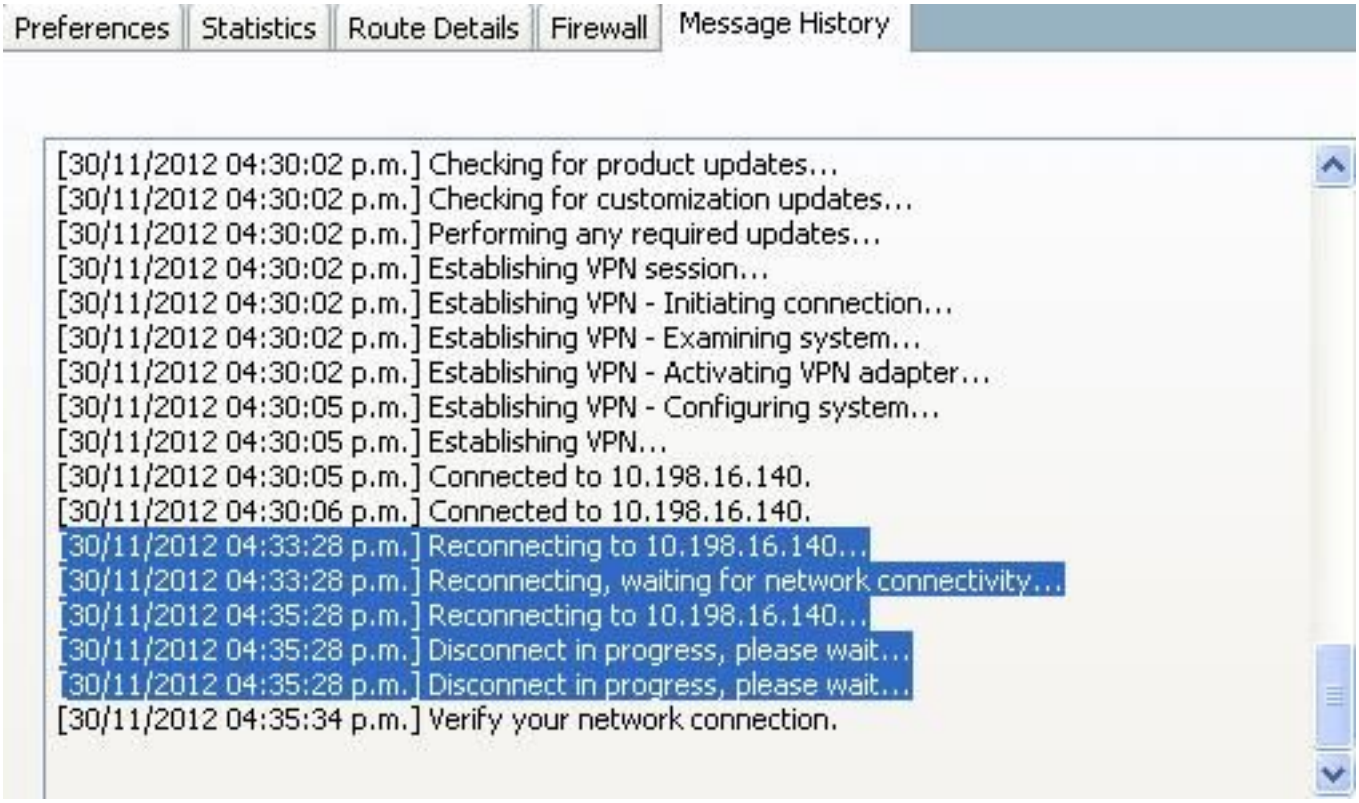
Processo effettivo

Il timer per il timeout di disconnessione viene avviato non appena la connessione di rete viene interrotta. Il client AnyConnect continua a provare a riconnettersi finché il timer non scade. Il valore di Timeout disconnessione è impostato sul valore più basso tra il valore di **Timeout di inattività di** Criteri di gruppo o il valore di **Tempo massimo di connessione**.

Il valore di questo timer viene visualizzato nel Visualizzatore eventi per la sessione AnyConnect nella negoziazione:



Nell'esempio, la sessione si disconnette dopo due minuti (120 secondi), che possono essere controllati nella Cronologia messaggi di AnyConnect:



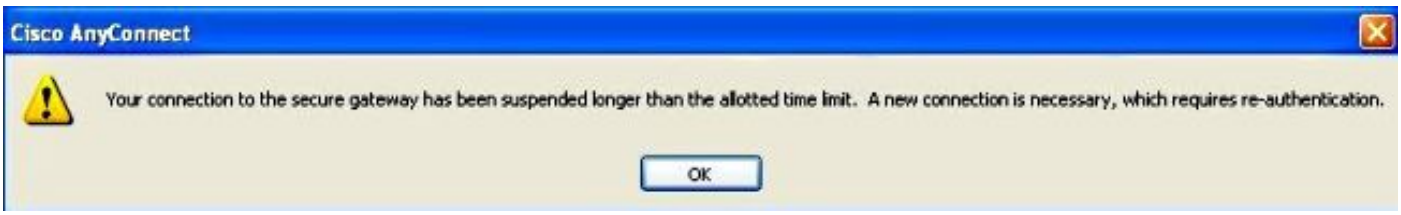
Suggerimento: affinché l'ASA risponda al client che tenta di riconnettersi, la sessione del tunnel padre deve essere ancora presente nel database ASA. In caso di failover, è inoltre necessario abilitare i DPD affinché il comportamento di riconnessione funzioni.

Come risulta dai messaggi precedenti, la riconnessione non è riuscita. Tuttavia, se la riconnessione ha esito positivo, viene eseguita la procedura seguente:

1. Il tunnel padre-tunnel rimane invariato. La negoziazione non viene eseguita perché il tunnel mantiene il token di sessione necessario per la sessione per riconnettersi.
2. Vengono generate nuove sessioni SSL e DTLS e vengono utilizzate porte di origine diverse nella riconnessione.
3. Vengono ripristinati tutti i valori di Idle-Timeout.
4. Timeout di inattività ripristinato.

Attenzione: prestare attenzione all'ID bug Cisco CSCtg3110. Il database delle sessioni VPN non aggiorna l'indirizzo IP pubblico nel database delle sessioni ASA quando AnyConnect si riconnette.

Se i tentativi di riconnessione non riescono, viene visualizzato questo messaggio:



Nota: questa richiesta di miglioramento è stata inviata per rendere il problema più granulare: Cisco bug ID CSCsl52873 - L'appliance ASA non ha un timeout di disconnessione configurabile per AnyConnect.

Comportamento del client AnyConnect in caso di sospensione del sistema

Una funzionalità di roaming consente a AnyConnect di riconnettersi dopo una sospensione del PC. Il client continua i tentativi fino alla scadenza dei timeout di inattività o di sessione e non chiude immediatamente il tunnel quando il sistema entra in modalità di sospensione o standby. Per gli utenti che non desiderano questa funzionalità, impostare il timeout della sessione su un valore basso per impedire le riconnessioni di sospensione/ripresa.

> **Nota**: dopo la correzione dell'ID bug Cisco CSCso17627 (versione 2.3(11)+), è stata introdotta una manopola di controllo per disabilitare la funzione di riconnessione al ripristino.

Il comportamento di riconnessione automatica per AnyConnect può essere controllato tramite il profilo XML AnyConnect con questa impostazione:

```
      <AutoReconnect UserControllable="true">true
<AutoReconnectBehavior>ReconnectAfterResume</AutoReconnectBehavior>
</AutoReconnect>
```

Con questa modifica, AnyConnect tenta di riconnettersi quando il computer viene riattivato dalla modalità sospensione. Per impostazione predefinita, la preferenza AutoReconnectBehavior è DisconnectOnSuspend. Questo comportamento è diverso da quello di AnyConnect Client release 2.2. Per riconnettersi dopo la ripresa, l'amministratore di rete deve impostare ReconnectAfterResume nel profilo o rendere le preferenze di riconnessione automatica e di riconnessione automatica controllabili dall'utente nel profilo per consentire agli utenti di impostarle.

Domande frequenti

D1. Anyconnect DPD ha un intervallo che non prevede tentativi: quanti pacchetti deve perdere prima di segnare il terminale remoto come inattivo?

R. Dal punto di vista del client, i DPD distruggono un tunnel solo durante la fase di definizione del tunnel. Se il client rileva tre tentativi (invia quattro pacchetti) durante la fase di definizione del tunnel e non riceve una risposta dal server VPN primario, torna a utilizzare uno dei server di backup, se configurato. Tuttavia, una volta stabilito il tunnel, le DPD perse non avranno alcun impatto sul tunnel dal punto di vista dei client. L'impatto reale delle DPD è sul server VPN, come spiegato nella sezione DPD e timer di inattività.

D2. L'elaborazione DPD è diversa per AnyConnect con IKEv2?

R. Sì, IKEv2 ha un numero fisso di tentativi - sei tentativi/sette pacchetti.

D3. Esiste un altro scopo per AnyConnect Parent-Tunnel?

R. Oltre a essere un mapping sull'appliance ASA, il tunnel padre viene usato per eseguire il push degli aggiornamenti dell'immagine AnyConnect dall'appliance ASA al client, in quanto il client non è connesso attivamente durante il processo di aggiornamento.

D4. È possibile filtrare e disconnettere solo le sessioni inattive?

R. È possibile filtrare le sessioni inattive con il comando **show vpn-sessiondb anyconnect filter inactive**. Tuttavia, non è disponibile alcun comando per disconnettere solo le sessioni inattive. È invece necessario disconnettere sessioni specifiche o tutte le sessioni per utente (indice - nome), protocollo o gruppo di tunnel. È stata inoltrata una richiesta di miglioramento, con ID bug Cisco CSCuh55707 , per aggiungere l'opzione di disconnessione solo delle sessioni inattive.

D5. Cosa succede al tunnel padre quando scade il timeout di inattività del tunnel DTLS o TLS?

R. Il timer "Idle TO Left" (Inattività a sinistra) della sessione padre di AnyConnect viene reimpostato dopo lo spegnimento del tunnel SSL o del tunnel DTLS. Ciò permette al timeout di inattività di agire come timeout di disconnessione. Questo diventa effettivamente il tempo consentito al client per riconnettersi. Se il client non si riconnette entro il timer, il tunnel padre viene terminato.

D6. Perché mantenere la sessione una volta che i timer DPD hanno disconnesso la sessione e perché l'ASA non rilascia l'indirizzo IP?

R. L'headend non ha alcuna conoscenza dello stato del cliente. In questo caso, l'ASA attende che il client si riconnetta finché la sessione non scade con il timer di inattività. Il DPD non termina una sessione AnyConnect, ma semplicemente termina il tunnel (all'interno della sessione) in modo che il client possa ristabilire il tunnel. Se il client non ristabilisce un tunnel, la sessione rimane attiva fino alla scadenza del timer di inattività.

Se il problema riguarda le sessioni esaurite, impostare gli accessi simultanei su un valore basso, ad esempio uno. Con questa impostazione, gli utenti che dispongono di una sessione nel database della sessione vengono eliminati dalla sessione precedente al successivo accesso.

D7. Qual è il comportamento in caso di failover dell'ASA da Attivo a Standby?

R. Inizialmente, quando viene stabilita la sessione, i tre tunnel (Parent, SSL e DTLS) vengono replicati sull'unità in standby. Una volta eseguito il failover dell'ASA, le sessioni DTLS e TLS vengono ristabilite in quanto non sincronizzate con l'unità in standby, ma i flussi di dati attraverso i tunnel devono funzionare senza interruzioni dopo la riattivazione della sessione AnyConnect.

Le sessioni SSL/DTLS non sono con conservazione dello stato, quindi lo stato SSL e il numero di sequenza non vengono mantenuti e possono essere molto tassativi. Pertanto, tali sessioni devono essere ristabilite da zero, il che avviene con la sessione padre e il token di sessione.

> **Suggerimento**: nel caso di un evento di failover, le sessioni client VPN SSL non vengono trasferite al dispositivo in standby se i pacchetti keepalive sono disabilitati.

D8. Perché ci sono due timeout diversi, il timeout di inattività e il timeout di disconnessione, se entrambi hanno lo stesso valore?

R. Quando i protocolli sono stati sviluppati, sono stati forniti due timeout diversi:

- Timeout di inattività: il timeout di inattività si verifica quando non vengono passati dati su una connessione.
- Timeout disconnessione: il timeout di disconnessione si riferisce al momento in cui si rinuncia alla sessione VPN perché la connessione è stata persa e non può essere ristabilita.

Il timeout di disconnessione non è mai stato implementato sull'appliance ASA. L'ASA invia invece al client il valore del timeout di inattività per i timeout di inattività e di disconnessione.

Il client non usa il timeout di inattività, perché l'ASA gestisce il timeout di inattività. Il client usa il valore di timeout di disconnessione, che è lo stesso del valore di timeout di inattività, per sapere quando interrompere i tentativi di riconnessione dopo che l'ASA ha interrotto la sessione.

Anche se non è connessa attivamente al client, l'ASA esegue il timeout della sessione tramite il timeout di inattività. La ragione principale per non implementare il timeout di disconnessione sull'appliance ASA è stata quella di evitare l'aggiunta di un altro timer per ciascuna sessione VPN e l'aumento del sovraccarico sull'appliance (anche se lo stesso timer può essere usato in entrambe le istanze, solo con valori di timeout diversi, perché i due casi si escludono a vicenda).

L'unico valore aggiunto con il timeout di disconnessione è quello di consentire a un amministratore di specificare un timeout diverso per i casi in cui il client non è connesso in modo attivo o inattivo. Come accennato in precedenza, è stato archiviato l'ID bug Cisco CSCsl52873.

D9. Cosa succede quando il computer client viene sospeso?

R. Per impostazione predefinita, AnyConnect tenta di ristabilire una connessione VPN quando si perde la connettività. Non tenta di ristabilire una connessione VPN dopo la ripresa di un sistema per impostazione predefinita. Per ulteriori informazioni, fare riferimento a Comportamento del client AnyConnect in caso di sospensione del sistema.

D10. In caso di riconnessione, la scheda virtuale AnyConnect è instabile o la tabella di routing cambia?

R. Una riconnessione a livello di tunnel non funziona. Questa è una riconnessione solo su SSL o DTLS. Questi vanno circa 30 secondi prima che si arrendano. Se il DTLS ha esito negativo, viene eliminato. Se SSL non riesce, viene stabilita una riconnessione a livello di sessione. Una riconnessione a livello di sessione ripristina completamente il routing. Se l'indirizzo del client assegnato alla riconnessione o qualsiasi altro parametro di configurazione che influisce sulla scheda virtuale (VA) non è stato modificato, la VA non viene disabilitata. Anche se è improbabile che siano state apportate modifiche ai parametri di configurazione ricevuti dall'ASA, è possibile che una modifica all'interfaccia fisica utilizzata per la connessione VPN (ad esempio, se si disinserisce la connessione e si passa da rete cablata a rete WiFi) possa generare un valore MTU (Maximum Transmission Unit) diverso per la connessione VPN. Il valore MTU influisce sull'VA e una modifica apportata allo stesso determina la disabilitazione e la riabilitazione dell'MTU.

D11. La riconnessione automatica garantisce la continuità della sessione? In caso affermativo, sono state aggiunte funzionalità aggiuntive nel client AnyConnect?

R. AnyConnect non offre alcuna "magia" extra per supportare la persistenza delle sessioni per le applicazioni. Tuttavia, la connettività VPN viene ripristinata automaticamente poco dopo la ripresa della connettività di rete al gateway sicuro, a condizione che i timeout di inattività e di sessione configurati sull'appliance ASA non siano scaduti. A differenza del client IPSec, la riconnessione

automatica produce lo stesso indirizzo IP del client. Mentre AnyConnect tenta di riconnettersi, la scheda virtuale AnyConnect rimane abilitata e nello stato connesso, quindi l'indirizzo IP del client rimane presente e abilitato sul PC client per tutto il tempo, consentendo la persistenza dell'indirizzo IP del client. Le applicazioni PC client, tuttavia, continuano a percepire la perdita di connettività ai server sulla rete aziendale se il ripristino della connettività VPN richiede troppo tempo.

D12. Questa funzionalità è disponibile in tutte le versioni di Microsoft Windows (Vista a 32 bit e 64 bit, XP). E il Macintosh? Funziona su OS X 10.4?

R. Questa funzione funziona su Mac e Linux. Ci sono stati problemi con Mac e Linux, ma sono stati fatti recenti miglioramenti, in particolare per il Mac. Linux richiede ancora un po' di supporto aggiuntivo (ID bug Cisco CSCsr16670, ID bug Cisco CSCsm69213), ma sono disponibili anche le funzionalità di base. Per quanto riguarda Linux, AnyConnect non riconosce che si è verificata una sospensione/ripresa (sleep/wake). Questo ha fondamentalmente due effetti:

- L'impostazione di profilo/preferenza AutoReconnectBehavior non può essere supportata in Linux senza il supporto di sospensione/ripresa, pertanto la riconnessione si verifica sempre dopo la sospensione/ripresa.
- In Microsoft Windows e Macintosh, le riconnessioni vengono eseguite immediatamente a livello di sessione dopo la ripresa, consentendo un passaggio più rapido a un'interfaccia fisica diversa. Su Linux, poiché AnyConnect non è completamente a conoscenza della sospensione o della ripresa, le riconnessioni vengono effettuate prima a livello di tunnel (SSL e DTLS), e ciò può significare che le riconnessioni richiedono più tempo. Ma le riconnessioni avvengono ancora su Linux.

D13. Sono previste limitazioni in termini di connettività (cablata, wi-fi, 3G e così via)? Supporta la transizione da una modalità all'altra (da Wi-Fi a 3G, 3G a cablata e così via)?

R. AnyConnect non è collegato a una particolare interfaccia fisica per tutta la durata della connessione VPN. Se l'interfaccia fisica utilizzata per la connessione VPN viene persa o i tentativi di riconnessione superano una determinata soglia di errore, AnyConnect non utilizza più quell'interfaccia e cerca di raggiungere il gateway sicuro con tutte le interfacce disponibili finché i timer di sessione o di inattività non scadono. Si noti che una modifica nell'interfaccia fisica potrebbe determinare un valore MTU diverso per VA, il che rende necessario disabilitare e riabilitare VA, ma con lo stesso indirizzo IP del client.

In caso di interruzioni della rete (interfaccia inattiva, reti modificate, interfacce modificate), AnyConnect tenta di riconnettersi; non è necessaria una nuova autenticazione alla riconnessione. Ciò vale anche per uno switch di interfacce fisiche:

Esempio:

```
1. wireless off, wired on: AC connection established
2. disconnect wired physically, turn wired on: AC re-established connection in
30 seconds
3. connect wired, turn off wireless: AC re-established connection in 30 secs
```

D14. Come viene autenticata l'operazione di ripresa?

R. In un curriculum, è possibile inviare nuovamente il token autenticato che rimane per tutta la durata della sessione e la sessione viene quindi ristabilita.

D15. L'autorizzazione LDAP viene eseguita anche dopo la riconnessione o solo durante l'autenticazione?

R. Questa operazione viene eseguita solo nella connessione iniziale.

D16. Il pre-login e/o l'hostscan vengono eseguiti alla ripresa?

R. No, vengono eseguiti solo sulla connessione iniziale. Una cosa simile sarebbe prevista per la futura funzione di valutazione della postura periodica.

D17. Per quanto riguarda il bilanciamento del carico (LB) della VPN e la ripresa della connessione, il client si connette direttamente al membro del cluster a cui era connesso in precedenza?

R: Sì, è corretto in quanto non si risolve il nome host tramite DNS per ristabilire una sessione corrente.

Informazioni correlate

- Riferimento DPD ASA: Cisco bug ID CSCsr63074 - DPD non inviato quando il peer è inattivo e tunnel non inattivo su s2s con 7.2.4
- 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).