Configurazione e risoluzione dei problemi di Cisco Network-Layer Encryption: Contesto - Parte 1

Sommario

Introduzione

In questo documento viene descritto come configurare Cisco Network-Layer Encryption con IPSec e Internet Security Association e il protocollo ISAKMP (Key Management Protocol) e vengono fornite informazioni di base sulla crittografia a livello di rete e sulla configurazione di base insieme a IPSec e ISAKMP.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

- Software Cisco IOS® versione 11.2 e successive

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.

Informazioni di base e configurazione di Crittografia a livello di rete

La funzionalità Crittografia a livello di rete è stata introdotta nel software Cisco IOS® versione 11.2. Fornisce un meccanismo per la trasmissione sicura dei dati e consiste di due componenti:

- **Autenticazione router:** Prima di passare il traffico crittografato, due router eseguono un'autenticazione unica e bidirezionale utilizzando le chiavi pubbliche DSS (Digital Signature Standard) per firmare richieste casuali.
- **Crittografia a livello di rete:** Per la crittografia del payload IP, i router utilizzano lo scambio di chiavi Diffie-Hellman per generare in modo sicuro una chiave di sessione DES (40 o 56 bit), Triple DES - 3DES (168 bit) o la più recente Advanced Encryption Standard - AES (128 bit (predefinito) o 192 bit, o 256 bit), introdotta nella versione 12.2(13)T. Le nuove chiavi di sessione vengono generate su base configurabile. I criteri di crittografia vengono impostati dalle mappe crittografiche che utilizzano elenchi di accesso IP estesi per definire le coppie di rete, subnet, host o protocollo da crittografare tra i router.

Sfondo crittografia

Il campo della crittografia riguarda la riservatezza delle comunicazioni. La protezione delle comunicazioni sensibili è stata l'enfasi della crittografia per gran parte della sua storia. La crittografia è la trasformazione dei dati in una forma illeggibile. Il suo scopo è quello di garantire la privacy mantenendo le informazioni nascoste a chiunque non sia per chi esse non sono destinate, anche se possono vedere i dati crittografati. La decrittografia è l'inverso della crittografia: è la trasformazione dei dati crittografati in forma comprensibile.

La crittografia e la decrittografia richiedono l'utilizzo di alcune informazioni segrete, generalmente definite "chiavi". A seconda del meccanismo di crittografia utilizzato, è possibile utilizzare la stessa chiave sia per la crittografia che per la decrittografia; mentre per altri meccanismi, le chiavi utilizzate per la crittografia e la decrittografia potrebbero essere diverse.

Una firma digitale consente di associare un documento al proprietario di una chiave specifica,

mentre un timestamp digitale consente di associare un documento alla relativa creazione in un determinato momento. Questi meccanismi di crittografia possono essere utilizzati per controllare l'accesso a un'unità disco condivisa, a un'installazione ad alta sicurezza o a un canale televisivo pay-per-view.

Mentre la crittografia moderna è sempre più diversificata, la crittografia è fondamentalmente basata su problemi difficili da risolvere. Un problema può essere difficile perché la soluzione richiede la conoscenza della chiave, ad esempio la decrittografia di un messaggio crittografato o la firma di un documento digitale. Il problema può anche essere difficile perché è intrinsecamente difficile da completare, ad esempio trovare un messaggio che produce un determinato valore hash.

Con l'avanzare del campo della crittografia, le linee di divisione tra ciò che è e ciò che non è crittografia sono diventate meno nitide. La crittografia odierna potrebbe essere riassunta come lo studio di tecniche e applicazioni che dipendono dall'esistenza di problemi matematici difficili da risolvere. Un crittoanalista tenta di compromettere i meccanismi crittografici, e la crittografia è la disciplina combinata della crittografia e della crittanalisi.

Definizioni

In questa sezione vengono definiti i termini correlati utilizzati nel presente documento.

- **Autenticazione:** Proprietà di sapere che i dati ricevuti sono effettivamente inviati dal mittente richiesto.
- **Riservatezza:** La proprietà di comunicare in modo che i destinatari siano a conoscenza di ciò che viene inviato, ma le parti non intenzionali non possono determinare ciò che viene inviato.
- **DES (Data Encryption Standard):** Il DES utilizza un metodo a chiave simmetrica, noto anche come metodo a chiave segreta. Ciò significa che se un blocco di dati viene crittografato con la stessa chiave, il blocco crittografato deve essere decrittografato con la stessa chiave, quindi sia il componente di crittografia che il decrittografatore devono utilizzare la stessa chiave. Anche se il metodo di cifratura è noto e ben pubblicato, il metodo di attacco più noto al pubblico è la forza bruta. Le chiavi devono essere verificate rispetto ai blocchi crittografati per verificare se sono in grado di risolverli correttamente. Con l'aumento della potenza dei processori, la vita naturale di DES sta per finire. Ad esempio, un'attività coordinata che utilizza la potenza di elaborazione di riserva di migliaia di computer in Internet è in grado di trovare la chiave a 56 bit per un messaggio codificato DES in 21 giorni.Il DES è convalidato ogni cinque anni dalla National Security Agency (NSA) degli Stati Uniti ai fini della conformità con gli obiettivi del governo statunitense. L'attuale approvazione scade nel 1998 e la NSA ha dichiarato che non procederà alla nuova certificazione DES. Oltre a DES, esistono altri algoritmi di cifratura che non hanno alcun punto debole se non gli attacchi di forza bruta. Per ulteriori informazioni, vedere DES FIPS 46-2 del National Institute of Standards and Technology (NIST) .
- **Decrittografia:** Applicazione inversa di un algoritmo di crittografia ai dati crittografati, ripristinando in tal modo i dati allo stato originale non crittografato.
- **DSS e Digital Signature Algorithm (DSA):** Il DSA è stato pubblicato dal NIST nel Digital Signature Standard (DSS), che fa parte del progetto Capstone del governo degli Stati Uniti. Il DSS è stato scelto dal NIST, in collaborazione con la NSA, come standard di autenticazione digitale del governo degli Stati Uniti. Lo standard è stato rilasciato il 19 maggio 1994.
- **Crittografia:** L'applicazione di uno specifico algoritmo ai dati in modo da alterarne l'aspetto

rendendoli incomprensibili per coloro che non sono autorizzati a visualizzare le informazioni.

- **Integrità:** La proprietà di garantire che i dati vengano trasmessi dall'origine alla destinazione senza alterazioni non rilevate.
- **Non ripudio:** Proprietà di un destinatario in grado di provare che il mittente di alcuni dati ha effettivamente inviato i dati anche se il mittente potrebbe in seguito voler negare di aver mai inviato tali dati.
- **Crittografia a chiave pubblica:** La crittografia tradizionale si basa sulla conoscenza e sull'utilizzo della stessa chiave segreta da parte del mittente e del destinatario del messaggio. Il mittente utilizza la chiave segreta per crittografare il messaggio, mentre il destinatario utilizza la stessa chiave segreta per decrittografare il messaggio. Questo metodo è noto come "chiave segreta" o "crittografia simmetrica". Il problema principale è far sì che il mittente e il destinatario concordino sulla chiave segreta senza che nessun altro lo scopra. Se si trovano in posizioni fisiche separate, devono fidarsi di un corriere, di un sistema telefonico o di un altro mezzo di trasmissione per impedire la divulgazione della chiave segreta comunicata. Chiunque ascolti o intercetti la chiave in transito può leggere, modificare e falsificare tutti i messaggi crittografati o autenticati utilizzando tale chiave. La generazione, la trasmissione e l'archiviazione di chiavi è detta gestione delle chiavi; tutti i sistemi crittografici devono risolvere i problemi di gestione delle chiavi. Poiché tutte le chiavi di un sistema di crittografia a chiave segreta devono rimanere segrete, la crittografia a chiave segreta ha spesso difficoltà a fornire una gestione sicura delle chiavi, soprattutto nei sistemi aperti con un elevato numero di utenti.Il concetto di crittografia a chiave pubblica è stato introdotto nel 1976 da Whitfield Diffie e Martin Hellman per risolvere il problema della gestione delle chiavi. Nella loro concezione, ogni persona ottiene una coppia di chiavi, una chiamata chiave pubblica e l'altra chiamata chiave privata. La chiave pubblica di ogni utente viene pubblicata mentre la chiave privata viene mantenuta segreta. Non è più necessario che il mittente e il destinatario condividano informazioni segrete e tutte le comunicazioni riguardano solo chiavi pubbliche e non viene mai trasmessa o condivisa alcuna chiave privata. Non è più necessario fidarsi di alcuni canali di comunicazione per essere sicuri da intercettazioni o tradimenti. L'unico requisito è che le chiavi pubbliche siano associate agli utenti in modo attendibile (autenticate), ad esempio in una directory attendibile. Chiunque può inviare un messaggio confidenziale semplicemente utilizzando informazioni pubbliche, ma il messaggio può essere decriptato solo con una chiave privata, che è in possesso esclusivo del destinatario. Inoltre, la crittografia a chiave pubblica può essere utilizzata non solo per la privacy (crittografia), ma anche per l'autenticazione (firme digitali).
- **Firme digitali a chiave pubblica:** Per firmare un messaggio, una persona esegue un calcolo che coinvolge sia la propria chiave privata che il messaggio stesso. L'output viene denominato firma digitale e viene allegato al messaggio, che viene quindi inviato. Una seconda persona verifica la firma eseguendo un calcolo del messaggio, della firma presunta e della chiave pubblica della prima persona. Se il risultato è contenuto in una semplice relazione matematica, la firma viene verificata come autentica. In caso contrario, la firma potrebbe essere fraudolenta o il messaggio potrebbe essere stato alterato.
- **Crittografia a chiave pubblica:** Quando una persona desidera inviare un messaggio segreto a un'altra persona, la prima persona cerca la chiave pubblica della seconda in un elenco, la utilizza per crittografare il messaggio e lo invia. La seconda persona quindi utilizza la propria chiave privata per decrittografare il messaggio e leggerlo. Nessuno che ascolta in può decrittografare il messaggio. Chiunque può inviare un messaggio crittografato all'altra persona, ma solo quest'ultima può leggerlo. Chiaramente, un requisito è che nessuno possa calcolare la chiave privata dalla chiave pubblica corrispondente.

- **Analisi del traffico:** Analisi del flusso del traffico di rete allo scopo di dedurre informazioni utili per un avversario. Esempi di tali informazioni sono la frequenza di trasmissione, l'identità delle parti che conversano, le dimensioni dei pacchetti, gli identificatori di flusso utilizzati e così via.

Informazioni preliminari

In questa sezione vengono illustrati alcuni concetti di base relativi alla crittografia a livello di rete. Contiene gli aspetti della crittografia che è necessario tenere in considerazione. Inizialmente, questi problemi potrebbero non avere senso per voi, ma è una buona idea leggerli adesso ed essere consapevoli di loro perché avranno più senso dopo che avete lavorato con la crittografia per diversi mesi.

- Èimportante notare che la crittografia si verifica solo sull'output di un'interfaccia e la decrittografia si verifica solo sull'input dell'interfaccia. Questa distinzione è importante quando si pianificano le regole. La policy per la crittografia e la decrittografia è simmetrica. Ciò significa che definendo uno si ottiene automaticamente l'altro. Con le mappe crittografiche e i loro elenchi degli accessi estesi associati, solo il criterio di crittografia è definito in modo esplicito.I criteri di decrittografia utilizzano le stesse informazioni, ma quando corrispondono ai pacchetti, inverte gli indirizzi e le porte di origine e di destinazione. In questo modo, i dati vengono protetti in entrambe le direzioni di una connessione duplex. L'istruzione *match address x* nel comando **crypto map** viene usata per descrivere i pacchetti in uscita da un'interfaccia. In altre parole, descrive la crittografia dei pacchetti. Tuttavia, quando i pacchetti entrano nell'interfaccia, devono anche essere abbinati per la decrittografia. Questa operazione viene eseguita automaticamente attraversando l'elenco degli accessi con gli indirizzi di origine e di destinazione invertiti e le porte invertite. Questo fornisce la simmetria per la connessione. L'elenco degli accessi a cui punta la **mappa crittografica** deve descrivere il traffico in una sola direzione (in uscita). I pacchetti IP che non corrispondono all'elenco degli accessi definito verranno trasmessi ma non crittografati. Se l'elenco degli accessi contiene il messaggio "Deny" (Nega), gli host non devono essere abbinati, ossia non verranno crittografati. Il "rifiuto", in questo contesto, non significa che il pacchetto venga scartato.
- Fai molta attenzione a usare la parola "qualsiasi" negli elenchi degli accessi estesi. Se si utilizza "any" (qualsiasi), il traffico viene interrotto a meno che non venga indirizzato all'interfaccia "non crittografata" corrispondente. Inoltre, con IPSec nel software Cisco IOS versione 11.3(3)T, la parola "any" (qualsiasi) non è consentita.
- L'uso della parola chiave "any" (qualsiasi) è sconsigliato nello specificare indirizzi di origine o di destinazione. Se si specifica "any" (qualsiasi), potrebbero verificarsi problemi con i protocolli di routing, il protocollo NTP (Network Time Protocol), l'eco, la risposta echo e il traffico multicast, in quanto il router ricevente scarta automaticamente il traffico. Se si deve utilizzare "any" (qualsiasi), deve essere preceduto da istruzioni "deny" (nega) per il traffico che non deve essere crittografato, ad esempio "ntp".
- Per risparmiare tempo, verificare di poter eseguire il **ping** sul router peer con cui si sta tentando di ottenere un'associazione di crittografia. Inoltre, chiedere ai dispositivi terminali (che dipendono dalla crittografia del traffico) di eseguire il ping tra loro prima di dedicare troppo tempo alla risoluzione del problema sbagliato. In altre parole, verificare che il routing funzioni prima di provare a eseguire la **crittografia**. Il peer remoto potrebbe non disporre di un percorso per l'interfaccia in uscita, nel qual caso non è possibile avere una sessione di crittografia con il peer (potrebbe essere possibile utilizzare **ip senza numero** sull'interfaccia seriale).

- Molti collegamenti WAN point-to-point utilizzano indirizzi IP non instradabili e il software Cisco IOS versione 11.2 Encryption si basa sul protocollo ICMP (Internet Control Message Protocol), ossia utilizza l'indirizzo IP dell'interfaccia seriale in uscita per ICMP. In questo caso, è possibile che si debba usare il comando **ip senza numero** sull'interfaccia WAN. Eseguire sempre i comandi **ping** e **traceroute** per verificare che il routing sia in uso per i due router peer (crittografia/decrittografia).
- Solo due router possono condividere una chiave di sessione Diffie-Hellman. Ossia, un router non può scambiare pacchetti crittografati con due peer che usano la stessa chiave di sessione; ogni coppia di router deve disporre di una chiave di sessione risultante da uno scambio Diffie-Hellman tra i router.
- Il motore di crittografia è in Cisco IOS, il VIP2 Cisco IOS o nell'hardware l'ESA (Encryption Services Adapter) su un VIP2. Senza un VIP2, il motore di crittografia Cisco IOS gestisce i criteri di crittografia su tutte le porte. Sulle piattaforme che utilizzano il VIP2, sono presenti più motori di crittografia: una in Cisco IOS e una in ciascun VIP2. Il motore di crittografia di un VIP2 gestisce la crittografia sulle porte che risiedono sulla scheda.
- Verificare che il traffico sia impostato in modo da raggiungere un'interfaccia preparata per la crittografia. Se il traffico può in qualche modo arrivare su un'interfaccia diversa da quella a cui è applicata la **mappa crittografica**, viene scartato automaticamente.
- Consente l'accesso da console (o alternativo) a entrambi i router durante lo scambio di chiavi; è possibile far impiccare il lato passivo mentre si aspetta una chiave.
- Il **cfb-64** è più efficiente da elaborare rispetto al **cfb-8** in termini di carico della CPU.
- Il router deve eseguire l'algoritmo che si desidera utilizzare con la modalità cipher-feedback (CFB); i valori predefiniti per ciascuna immagine sono il nome dell'immagine (ad esempio "56") con **cfb-64**.
- Provare a modificare il timeout della chiave. Il valore predefinito di 30 minuti è molto breve. Provate ad aumentarlo di un giorno (1440 minuti).
- Il traffico IP viene interrotto durante la rinegoziazione delle chiavi a ogni scadenza della chiave.
- Selezionare solo il traffico che si desidera crittografare, in modo da risparmiare cicli di CPU.
- Con il routing DDR (dial-on-demand routing), rendere l'ICMP interessante o non comporre mai il numero.
- Per crittografare il traffico diverso da IP, utilizzare un tunnel. Con i tunnel, applicare le mappe crittografiche sia all'interfaccia fisica che a quella del tunnel. Vedere il Campione 5: crittografia del traffico IPX in un tunnel IP.
- I due router peer di crittografia non devono essere connessi direttamente.
- Un router di fascia bassa può inviare un messaggio di "mancato utilizzo della CPU". Questo argomento può essere ignorato perché indica che la crittografia utilizza molte risorse della CPU.
- Non posizionare i router di crittografia in modo ridondante in modo da decrittografare e ricrittografare il traffico e lo spreco di CPU. È sufficiente crittografare i dati a due endpoint. Vedere il Campione 3: Crittografia su e attraverso un router per ulteriori informazioni.
- Al momento, la crittografia dei pacchetti broadcast e multicast non è supportata. Se gli aggiornamenti di routing "sicuri" sono importanti per la progettazione di una rete, è consigliabile utilizzare un protocollo con autenticazione incorporata, ad esempio Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF) o Routing Information Protocol versione 2 (RIPv2) per garantire l'integrità degli aggiornamenti.

Avvertenze

Nota: le avvertenze riportate di seguito sono state tutte risolte.

- Un router Cisco 7200 che usa un'ESA per la crittografia non può decrittografare un pacchetto con una chiave di sessione e quindi crittografarlo nuovamente con una chiave di sessione diversa. Fare riferimento all'ID bug Cisco CSCdj82613 (solo utenti registrati).
- Quando due router sono connessi da una linea assegnata in leasing crittografata e da una linea di backup ISDN, in caso di interruzione della linea assegnata, il collegamento ISDN viene attivato correttamente. Tuttavia, quando la linea dedicata torna disponibile, il router che ha effettuato la chiamata ISDN si blocca. Fare riferimento all'ID bug Cisco CSCdj00310 (solo utenti registrati).
- Per i router Cisco serie 7500 con più VIP, se una **mappa crittografica** viene applicata anche a un'interfaccia di qualsiasi VIP, si verifica un arresto anomalo di uno o più VIP. Fare riferimento all'ID bug Cisco CSCdi88459 (solo utenti registrati).
- Per i router Cisco serie 7500 con VIP2 e ESA, il comando **show crypto card** non visualizza l'output a meno che l'utente non si trovi sulla porta della console. Fare riferimento all'ID bug Cisco CSCdj89070 (solo utenti registrati).

Configurazione della crittografia a livello di rete Cisco IOS

Gli esempi di configurazione di Cisco IOS descritti in questo documento provengono direttamente da router di laboratorio. L'unica modifica apportata è stata la rimozione di configurazioni di interfaccia non correlate. Tutto il materiale qui reperito proviene da risorse liberamente disponibili su Internet o nella sezione Informazioni correlate alla fine di questo documento.

Tutte le configurazioni di esempio riportate in questo documento fanno riferimento al software Cisco IOS versione 11.3. Sono state apportate diverse modifiche ai comandi del software Cisco IOS versione 11.2, ad esempio l'aggiunta delle seguenti parole:

- dss in alcuni comandi di configurazione key.
- cisco in alcuni comandi **show** e **crypto map** per distinguere tra la crittografia proprietaria di Cisco (come trovata nel software Cisco IOS versione 11.2 e successive) e IPSec che è nel software Cisco IOS versione 11.3(2)T.

Nota: gli indirizzi IP utilizzati in questi esempi di configurazione sono stati scelti casualmente nel laboratorio di Cisco e sono stati progettati per essere completamente generici.

Passaggio 1: Genera manualmente coppie di chiavi DSS

Una coppia di chiavi DSS (una chiave pubblica e una chiave privata) deve essere generata manualmente su ciascun router che partecipa alla sessione di crittografia. In altre parole, ogni router deve avere le proprie chiavi DSS per poter partecipare. Un motore di crittografia può disporre di una sola chiave DSS che la identifica in modo univoco. La parola chiave "dss" è stata aggiunta nel software Cisco IOS versione 11.3 per distinguere le chiavi DSS dalle chiavi RSA. È possibile specificare qualsiasi nome per le chiavi DSS del router (anche se, si consiglia di utilizzare il nome host del router). Su una CPU meno potente (ad esempio, Cisco serie 2500), la generazione della coppia di chiavi richiede circa 5 secondi o meno.

Il router genera una coppia di chiavi:

- Una chiave pubblica (inviata in seguito ai router che partecipano alle sessioni di crittografia).

- Una chiave privata (che non può essere vista né scambiata con altri; infatti, è memorizzata in una sezione separata della NVRAM (che non può essere visualizzata).

Dopo aver generato la coppia di chiavi DSS del router, questa è associata in modo univoco al motore di crittografia di quel router. La generazione della coppia di chiavi è illustrata nell'output del comando di esempio riportato di seguito.

```
dial-5(config)#crypto key generate dss dial5
Generating DSS keys ....
 [OK]

dial-5#show crypto key mypubkey dss
crypto public-key dial5 05679919
 160AA490 5B9B1824 24769FCD EE5E0F46 1ABBD343 4C0C4A03 4B279D6B 0EE5F65F
 F64665D4 1036875A 8CF93691 BDF81722 064B51C9 58D72E12 3E1894B6 64B1D145
quit


dial-5#show crypto engine configuration
slot:               0
engine name:        dial5
engine type:        software
serial number:      05679919
platform:           rp crypto engine
crypto lib version: 10.0.0

Encryption Process Info:
input queue top:    43
input queue bot:    43
input queue count:  0

dial-5#
```

Poiché è possibile generare una sola coppia di chiavi che identifica il router, è possibile che la chiave originale venga sovrascritta e che sia necessario inviare nuovamente la chiave pubblica a ogni router nell'associazione di crittografia. Come mostrato nell'output del comando di esempio riportato di seguito:

```
StHelen(config)#crypto key generate dss barney
% Generating new DSS keys will require re-exchanging
   public keys with peers who already have the public key
   named barney!
Generate new DSS keys? [yes/no]: yes
Generating DSS keys ....
 [OK]


StHelen(config)#
Mar 16 12:13:12.851: Crypto engine 0: create key pairs.
```

Passaggio 2: Scambio manuale di chiavi pubbliche DSS con peer (fuori banda)

La generazione della coppia di chiavi DSS del router è il primo passaggio per stabilire un'associazione di sessione di crittografia. Il passaggio successivo è lo scambio di chiavi pubbliche con ogni altro router. È possibile immettere manualmente queste chiavi pubbliche immettendo prima il comando **show crypto mypubkey** per visualizzare la chiave pubblica DSS del router. È quindi possibile scambiare queste chiavi pubbliche (ad esempio tramite posta elettronica) e, con il comando **crypto key pubkey-chain dss**, tagliare e incollare la chiave pubblica del router peer nel router.

Èinoltre possibile utilizzare il comando **crypto key exchange dss** per fare in modo che i router scambino automaticamente le chiavi pubbliche. Se si utilizza il metodo automatico, verificare che non vi siano istruzioni **mappa crittografica** sulle interfacce utilizzate per lo scambio di chiavi. In questo caso, è utile la **chiave di crittografia** di **debug**.

Nota: è consigliabile eseguire il **ping** del peer prima di provare a scambiare le chiavi.

```
Loser#ping 19.19.19.20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 19.19.19.20, timeout is 2 seconds:
!!!!!

Loser(config)#crypto key exchange dss passive
Enter escape character to abort if connection does not complete.
Wait for connection from peer[confirm]
Waiting ....


  StHelen(config)#crypto key exchange dss 19.19.19.19 barney
  Public key for barney:
  Serial Number 05694352
  Fingerprint   309E D1DE B6DA 5145 D034

  Wait for peer to send a key[confirm]


Public key for barney:
   Serial Number 05694352
   Fingerprint   309E D1DE B6DA 5145 D034

Add this public key to the configuration? [yes/no]:yes


         Mar 16 12:16:55.343: CRYPTO-KE: Sent 2 bytes.
         Mar 16 12:16:55.343: CRYPTO-KE: Sent 4 bytes.
         Mar 16 12:16:55.343: CRYPTO-KE: Sent 2 bytes.
         Mar 16 12:16:55.347: CRYPTO-KE: Sent 64 bytes.


Mar 16 12:16:45.099: CRYPTO-KE: Received 4 bytes.
Mar 16 12:16:45.099: CRYPTO-KE: Received 2 bytes.
Mar 16 12:16:45.103: CRYPTO-KE: Received 6 bytes.
Mar 16 12:16:45.103: CRYPTO-KE: Received 2 bytes.
Mar 16 12:16:45.107: CRYPTO-KE: Received 50 bytes.
Mar 16 12:16:45.111: CRYPTO-KE: Received 14 bytes.

Send peer a key in return[confirm]
Which one?

fred? [yes]:
Public key for fred:
   Serial Number 02802219
   Fingerprint   2963 05F9 ED55 576D CF9D


         Waiting ....
         Public key for fred:
           Serial Number 02802219
         Fingerprint   2963 05F9 ED55 576D CF9D
```

```
         Add this public key to the configuration? [yes/no]:

Loser(config)#
Mar 16 12:16:55.339: CRYPTO-KE: Sent 4 bytes.
Mar 16 12:16:55.343: CRYPTO-KE: Sent 2 bytes.
Mar 16 12:16:55.343: CRYPTO-KE: Sent 4 bytes.
Mar 16 12:16:55.343: CRYPTO-KE: Sent 2 bytes.
Mar 16 12:16:55.347: CRYPTO-KE: Sent 64 bytes.
Loser(config)#

Mar 16 12:16:56.083: CRYPTO-KE: Received 4 bytes.
Mar 16 12:16:56.087: CRYPTO-KE: Received 2 bytes.
Mar 16 12:16:56.087: CRYPTO-KE: Received 4 bytes.
Mar 16 12:16:56.091: CRYPTO-KE: Received 2 bytes.
Mar 16 12:16:56.091: CRYPTO-KE: Received 52 bytes.
Mar 16 12:16:56.095: CRYPTO-KE: Received 12 bytes.
Add this public key to the configuration? [yes/no]: yes
StHelen(config)#^Z
StHelen#
```

Ora che le chiavi DSS pubbliche sono state scambiate, verificare che entrambi i router dispongano delle rispettive chiavi pubbliche e che corrispondano, come mostrato nell'output del comando seguente.

```
Loser#show crypto key mypubkey dss
crypto public-key fred 02802219
 79CED212 AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8 05D4930C CE891810
 C0064492 5F6684CD 3FC326E5 679BCA46 BB155402 D443F68D 93487F7E 5ABE182E
quit

Loser#show crypto key pubkey-chain dss
crypto public-key barney 05694352
 B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A 3232EBA2 F2D31D21 53AE24ED
 732EA43D 484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477 91810341
quit

--------

StHelen#show crypto key mypubkey dss
crypto public-key barney 05694352
 B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A 3232EBA2 F2D31D21 53AE24ED
 732EA43D 484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477 91810341
quit

StHelen#show crypto key pubkey-chain dss
crypto public-key fred 02802219
 79CED212 AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8 05D4930C CE891810
 C0064492 5F6684CD 3FC326E5 679BCA46 BB155402 D443F68D 93487F7E 5ABE182E
quit
```

Campione 1: Configurazione Cisco IOS per collegamento dedicato

Dopo aver generato le chiavi DSS su ciascun router e aver scambiato le chiavi pubbliche DSS, è possibile applicare il comando **crypto map** all'interfaccia. La sessione crittografica inizia generando il traffico che corrisponde all'elenco degli accessi utilizzato dalle mappe crittografiche.

```
Loser#write terminal
Building configuration...

Current configuration:
```

```
!
! Last configuration change at 13:01:18 UTC Mon Mar 16 1998
! NVRAM config last updated at 13:03:02 UTC Mon Mar 16 1998
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
!
hostname Loser
!
enable secret 5 $1$AeuFSMx7O/DhpqjLKc2VQVbeC0
!
ip subnet-zero
no ip domain-lookup
crypto map oldstyle 10
 set peer barney
 match address 133
!
crypto key pubkey-chain dss
 named-key barney
  serial-number 05694352
  key-string
   B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A 3232EBA2 F2D31D21 53AE24ED
   732EA43D 484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477 91810341
  quit
!
interface Ethernet0
 ip address 40.40.40.41 255.255.255.0
 no ip mroute-cache
!
interface Serial0
 ip address 18.18.18.18 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 shutdown
!
interface Serial1
 ip address 19.19.19.19 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 clockrate 2400
 no cdp enable
 crypto map oldstyle
!
ip default-gateway 10.11.19.254
ip classless
ip route 0.0.0.0 0.0.0.0 19.19.19.20
access-list 133 permit ip 40.40.40.0 0.0.0.255 30.30.30.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
 no exec
 transport input all
line vty 0 4
 password ww
 login
!
end

Loser#
--------------------------

StHelen#write terminal
```

```
Building configuration...

Current configuration:
!
! Last configuration change at 13:03:05 UTC Mon Mar 16 1998
! NVRAM config last updated at 13:03:07 UTC Mon Mar 16 1998
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
!
hostname StHelen
!
boot system flash c2500-is56-l
enable password ww
!
partition flash 2 8 8
!
no ip domain-lookup
crypto map oldstyle 10
 set peer fred
 match address 144
!
crypto key pubkey-chain dss
 named-key fred
  serial-number 02802219
  key-string
   79CED212 AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8 05D4930C CE891810
   C0064492 5F6684CD 3FC326E5 679BCA46 BB155402 D443F68D 93487F7E 5ABE182E
  quit
 !
 !
interface Ethernet0
 ip address 30.30.30.31 255.255.255.0
!
interface Ethernet1
 no ip address
 shutdown
!
interface Serial0
 no ip address
 encapsulation x25
 no ip mroute-cache
 shutdown
!
interface Serial1
 ip address 19.19.19.20 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 load-interval 30
 compress stac
 no cdp enable
 crypto map oldstyle
!
ip default-gateway 10.11.19.254
ip classless
ip route 0.0.0.0 0.0.0.0 19.19.19.19
access-list 144 permit ip 30.30.30.0 0.0.0.255 40.40.40.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
 transport input all
line vty 0 4
```

```
 password ww
 login
!
end

StHelen#
```

Esempio 2: Configurazione Cisco IOS per Multipoint Frame Relay

L'output del comando di esempio seguente è stato preso dal router HUB.

```
Loser#write terminal
Building configuration...

Current configuration:
!
! Last configuration change at 10:45:20 UTC Wed Mar 11 1998
! NVRAM config last updated at 18:28:27 UTC Tue Mar 10 1998
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
!
hostname Loser
!
enable secret 5 $1$AeuFSMx7O/DhpqjLKc2VQVbeC0
!
ip subnet-zero
no ip domain-lookup
!
crypto map oldstuff 10
 set peer barney
 match address 133
crypto map oldstuff 20
 set peer wilma
 match address 144
!
crypto key pubkey-chain dss
 named-key barney
  serial-number 05694352
  key-string
   1D460DC3 BDC73312 93B7E220 1861D55C E00DA5D8 DB2B04CD FABD297C 899D40E7
   D284F07D 6EEC83B8 E3676EC2 D813F7C8 F532DC7F 0A9913E7 8A6CB7E9 BE18790D
  quit
 named-key wilma
  serial-number 01496536
  key-string
   C26CB3DD 2A56DD50 CC2116C9 2697CE93 6DBFD824 1889F791 9BF36E70 7B29279C
   E343C56F 32266443 989B4528 1CF32C2D 9E3F2447 A5DBE054 879487F6 26A55939
  quit
!
crypto cisco pregen-dh-pairs 5
!
crypto cisco key-timeout 1440
!
interface Ethernet0
 ip address 190.190.190.190 255.255.255.0
 no ip mroute-cache
!
interface Serial1
 ip address 19.19.19.19 255.255.255.0
 encapsulation frame-relay
```

```
 no ip mroute-cache
 clockrate 500000
 crypto map oldstuff
!
!
ip default-gateway 10.11.19.254
ip classless
ip route 200.200.200.0 255.255.255.0 19.19.19.20
ip route 210.210.210.0 255.255.255.0 19.19.19.21
access-list 133 permit ip 190.190.190.0 0.0.0.255 200.200.200.0 0.0.0.255
access-list 144 permit ip 190.190.190.0 0.0.0.255 210.210.210.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
 no exec
 transport input all
line vty 0 4
 password ww
 login
!
end

Loser#
```

L'output del comando di esempio seguente è stato preso dal sito remoto A.

```
WAN-2511a#write terminal
Building configuration...

Current configuration:
!
version 11.3
no service password-encryption
!
hostname WAN-2511a
!
enable password ww
!
no ip domain-lookup
!
crypto map mymap 10
 set peer fred
 match address 133
!
crypto key pubkey-chain dss
 named-key fred
  serial-number 02802219
  key-string
   56841777 4F27A574 5005E0F0 CF3C33F5 C6AAD000 5518A8FF 7422C592 021B295D
   D95AAB73 01235FD8 40D70284 3A63A38E 216582E8 EC1F8B0D 0256EFF5 0EE89436
  quit
!
interface Ethernet0
 ip address 210.210.210.210 255.255.255.0
 shutdown
!
interface Serial0
 ip address 19.19.19.21 255.255.255.0
 encapsulation frame-relay
 no fair-queue
 crypto map mymap
!
```

```
ip default-gateway 10.11.19.254
ip classless
ip route 190.190.190.0 255.255.255.0 19.19.19.19
access-list 133 permit ip 210.210.210.0 0.0.0.255 190.190.190.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line 1
 no exec
 transport input all
line 2 16
 no exec
line aux 0
line vty 0 4
 password ww
 login
!
end

WAN-2511a#
```

L'output del comando di esempio riportato di seguito è stato ottenuto dal sito remoto B.

```
StHelen#write terminal
Building configuration...

Current configuration:
!
! Last configuration change at 19:00:34 UTC Tue Mar 10 1998
! NVRAM config last updated at 18:48:39 UTC Tue Mar 10 1998
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
!
hostname StHelen
!
boot system flash c2500-is56-l
enable password ww
!
partition flash 2 8 8
!
no ip domain-lookup
!
crypto map wabba 10
 set peer fred
 match address 144
!
crypto key pubkey-chain dss
 named-key fred
  serial-number 02802219
  key-string
   56841777 4F27A574 5005E0F0 CF3C33F5 C6AAD000 5518A8FF 7422C592 021B295D
   D95AAB73 01235FD8 40D70284 3A63A38E 216582E8 EC1F8B0D 0256EFF5 0EE89436
  quit
!
interface Ethernet0
 ip address 200.200.200.200 255.255.255.0
!
interface Serial1
 ip address 19.19.19.20 255.255.255.0
 encapsulation frame-relay
 no ip mroute-cache
```

```
 crypto map wabba
!
ip default-gateway 10.11.19.254
ip classless
ip route 190.190.190.0 255.255.255.0 19.19.19.19
access-list 144 permit ip 200.200.200.0 0.0.0.255 190.190.190.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
 transport input all
line vty 0 4
 password ww
 login
!
end

StHelen#
```

L'output del comando di esempio seguente è stato preso dallo switch Frame Relay.

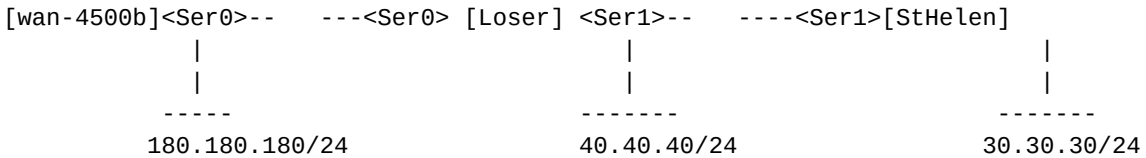
```
Current configuration:
!
version 11.2
no service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname wan-4700a
!
enable password ww
!
no ip domain-lookup
frame-relay switching
!
interface Serial0
 no ip address
 encapsulation frame-relay
 clockrate 500000
 frame-relay intf-type dce
 frame-relay route 200 interface Serial1 100
!
interface Serial1
 no ip address
 encapsulation frame-relay
 frame-relay intf-type dce
 frame-relay route 100 interface Serial0 200
 frame-relay route 300 interface Serial2 200
!
interface Serial2
 no ip address
 encapsulation frame-relay
 clockrate 500000
 frame-relay intf-type dce
 frame-relay route 200 interface Serial1 300
!
```

Campione 3: Crittografia su e tramite un router

I router peer non devono essere a un hop di distanza. È possibile creare una sessione di peering con un router remoto. Nell'esempio che segue, l'obiettivo è crittografare tutto il traffico di rete tra 180.180.180.0/24 e 40.40.40.0/24 e tra 180.180.180.0/24 e 30.30.30.0/24. La crittografia del

traffico tra 40.40.40.0/24 e 30.30.30.0/24 non desta alcuna preoccupazione.

Il router wan-4500b ha una sessione di crittografia associata a Loser e anche a StHelen. Crittografando il traffico tra il segmento Ethernet del wan-4500b e il segmento Ethernet di Sant'Elena, si evita di decrittografare inutilmente il dispositivo Loser. Loser semplicemente trasmette il traffico crittografato all'interfaccia seriale di StHelen, dove viene decriptato. Ciò riduce il ritardo del traffico per i pacchetti IP e i cicli della CPU sul router Loser. E, soprattutto, aumenta notevolmente la sicurezza del sistema, dal momento che un intercettore su Loser non può leggere il traffico. Se Loser decrittografasse il traffico, ci sarebbe la possibilità che i dati decrittografati possano essere deviati.




```
wan-4500b#write terminal
Building configuration...

Current configuration:
!
version 11.3
no service password-encryption
!
hostname wan-4500b
!
enable password 7 111E0E
!
username cse password 0 ww
no ip domain-lookup
!
crypto map toworld 10
 set peer loser
 match address 133
crypto map toworld 20
 set peer sthelen
 match address 144
!
crypto key pubkey-chain dss
 named-key loser
  serial-number 02802219
  key-string
   F0BE2128 752D1A24 F394B355 3216BA9B 7C4E8677 29C176F9 A047B7D9 7D03BDA4
   6B7AFDC2 2DAEF3AB 393EE7C7 802C1A95 B40031D1 908004F9 8A33A352 FF19BC24
  quit
 named-key sthelen
  serial-number 05694352
  key-string
   5C401002 404DC5A9 EAED2360 D7007E51 4A4BB8F8 6F9B1554 51D8ACBB D3964C10
   A23848CA 46003A94 2FC8C7D6 0B57AE07 9EB5EF3A BD71482B 052CF06B 90C3C618
  quit
 !
interface Ethernet0
 ip address 180.180.180.180 255.255.255.0
!
interface Serial0
 ip address 18.18.18.19 255.255.255.0
 encapsulation ppp
 crypto map toworld
```

```
!
router rip
 network 18.0.0.0
 network 180.180.0.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 30.30.30.31
ip route 171.68.118.0 255.255.255.0 10.11.19.254
access-list 133 permit ip 180.180.180.0 0.0.0.255 40.40.40.0 0.0.0.255
access-list 144 permit ip 180.180.180.0 0.0.0.255 30.30.30.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
 password 7 044C1C
line vty 0 4
 login local
!
end

wan-4500b#

--------------------

Loser#write terminal
Building configuration...

Current configuration:
!
! Last configuration change at 11:01:54 UTC Wed Mar 18 1998
! NVRAM config last updated at 11:09:59 UTC Wed Mar 18 1998
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
!
hostname Loser
!
enable secret 5 $1$AeuFSMx7O/DhpqjLKc2VQVbeC0
!
ip subnet-zero
no ip domain-lookup
ip host StHelen.cisco.com 19.19.19.20
ip domain-name cisco.com
!
crypto map towan 10
 set peer wan
 match address 133
!
crypto key pubkey-chain dss
 named-key wan
  serial-number 07365004
  key-string
   A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F
   2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B
  quit
!
interface Ethernet0
 ip address 40.40.40.40 255.255.255.0
 no ip mroute-cache
!
interface Serial0
 ip address 18.18.18.18 255.255.255.0
 encapsulation ppp
```

```
 no ip mroute-cache
 clockrate 64000
 crypto map towan
!
interface Serial1
 ip address 19.19.19.19 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 priority-group 1
 clockrate 64000
!
!
router rip
 network 19.0.0.0
 network 18.0.0.0
 network 40.0.0.0
!
ip default-gateway 10.11.19.254
ip classless
access-list 133 permit ip 40.40.40.0 0.0.0.255 180.180.180.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
 no exec
 transport input all
line vty 0 4
 password ww
 login
!
end

Loser#

-------------------------

StHelen#write terminal
Building configuration...

Current configuration:
!
! Last configuration change at 11:13:18 UTC Wed Mar 18 1998
! NVRAM config last updated at 11:21:30 UTC Wed Mar 18 1998
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
!
hostname StHelen
!
boot system flash c2500-is56-l
enable password ww
!
partition flash 2 8 8
!
no ip domain-lookup
!
crypto map towan 10
 set peer wan
 match address 144
!
crypto key pubkey-chain dss
 named-key wan
  serial-number 07365004
```

```
  key-string
   A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F
   2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B
  quit
!
interface Ethernet0
 no ip address
!
interface Ethernet1
 ip address 30.30.30.30 255.255.255.0
!
interface Serial1
 ip address 19.19.19.20 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 load-interval 30
 crypto map towan
!
router rip
 network 30.0.0.0
 network 19.0.0.0
!
ip default-gateway 10.11.19.254
ip classless
access-list 144 permit ip 30.30.30.0 0.0.0.255 180.180.180.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
 transport input all
line vty 0 4
 password ww
 login
!
end

StHelen#

--------------------------

wan-4500b#show crypto cisco algorithms
  des cfb-64
  40-bit-des cfb-64

wan-4500b#show crypto cisco key-timeout
Session keys will be re-negotiated every 30 minutes

wan-4500b#show crypto cisco pregen-dh-pairs
Number of pregenerated DH pairs: 0

wan-4500b#show crypto engine connections active
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 1    Serial0         18.18.18.19 set    DES_56_CFB64    1683     1682
 5    Serial0         18.18.18.19 set    DES_56_CFB64    1693     1693

wan-4500b#show crypto engine connections dropped-packet
Interface            IP-Address    Drop Count

Serial0              18.18.18.19   52
wan-4500b#show crypto engine configuration
slot:               0
engine name:        wan
engine type:        software
serial number:      07365004
```

```
platform:           rp crypto engine
crypto lib version: 10.0.0

Encryption Process Info:
input queue top:    303
input queue bot:    303
input queue count:  0

wan-4500b#show crypto key mypubkey dss
crypto public-key wan 07365004
 A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F
 2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B
quit

wan-4500b#show crypto key pubkey-chain dss
crypto public-key loser 02802219
 F0BE2128 752D1A24 F394B355 3216BA9B 7C4E8677 29C176F9 A047B7D9 7D03BDA4
 6B7AFDC2 2DAEF3AB 393EE7C7 802C1A95 B40031D1 908004F9 8A33A352 FF19BC24
quit
crypto public-key sthelen 05694352
 5C401002 404DC5A9 EAED2360 D7007E51 4A4BB8F8 6F9B1554 51D8ACBB D3964C10
 A23848CA 46003A94 2FC8C7D6 0B57AE07 9EB5EF3A BD71482B 052CF06B 90C3C618
quit

wan-4500b#show crypto map interface serial 1
No crypto maps found.

wan-4500b#show crypto map
Crypto Map "toworld" 10 cisco
        Connection Id = 1        (1 established,    0 failed)
        Peer = loser
        PE = 180.180.180.0
        UPE = 40.40.40.0
        Extended IP access list 133
            access-list 133 permit ip
                source: addr = 180.180.180.0/0.0.0.255
                dest:   addr = 40.40.40.0/0.0.0.255

Crypto Map "toworld" 20 cisco
        Connection Id = 5        (1 established,    0 failed)
        Peer = sthelen
        PE = 180.180.180.0
        UPE = 30.30.30.0
        Extended IP access list 144
            access-list 144 permit ip
                source: addr = 180.180.180.0/0.0.0.255
                dest:   addr = 30.30.30.0/0.0.0.255

wan-4500b#

-------------------------

Loser#show crypto cisco algorithms
  des cfb-64
  des cfb-8
  40-bit-des cfb-64
  40-bit-des cfb-8

Loser#show crypto cisco key-timeout
Session keys will be re-negotiated every 30 minutes

Loser#show crypto cisco pregen-dh-pairs
Number of pregenerated DH pairs: 10
```

```
Loser#show crypto engine connections active
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 61   Serial0         18.18.18.18 set    DES_56_CFB64    1683     1682

Loser#show crypto engine connections dropped-packet
Interface            IP-Address    Drop Count

Serial0              18.18.18.18   1
Serial1              19.19.19.19   90
Loser#show crypto engine configuration
slot:               0
engine name:        loser
engine type:        software
serial number:      02802219
platform:           rp crypto engine
crypto lib version: 10.0.0

Encryption Process Info:
input queue top:    235
input queue bot:    235
input queue count:  0

Loser#show crypto key mypubkey dss
crypto public-key loser 02802219
 F0BE2128 752D1A24 F394B355 3216BA9B 7C4E8677 29C176F9 A047B7D9 7D03BDA4
 6B7AFDC2 2DAEF3AB 393EE7C7 802C1A95 B40031D1 908004F9 8A33A352 FF19BC24
quit

Loser#show crypto key pubkey-chain dss
crypto public-key wan 07365004
 A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F
 2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B
quit

Loser#show crypto map interface serial 1
No crypto maps found.

Loser#show crypto map
Crypto Map "towan" 10 cisco
        Connection Id = 61       (0 established,    0 failed)
        Peer = wan
        PE = 40.40.40.0
        UPE = 180.180.180.0
        Extended IP access list 133
            access-list 133 permit ip
                source: addr = 40.40.40.0/0.0.0.255
                dest:   addr = 180.180.180.0/0.0.0.255

Loser#

----------------------------------------

StHelen#show crypto cisco algorithms
  des cfb-64

StHelen#show crypto cisco key-timeout
Session keys will be re-negotiated every 30 minutes

StHelen#show crypto cisco pregen-dh-pairs
Number of pregenerated DH pairs: 10

StHelen#show crypto engine connections active

ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
```

```
 58   Serial1         19.19.19.20 set    DES_56_CFB64    1694     1693

StHelen#show crypto engine connections dropped-packet
Interface            IP-Address    Drop Count

Ethernet0            0.0.0.0       1
Serial1              19.19.19.20   80
StHelen#show crypto engine configuration
slot:               0
engine name:        sthelen
engine type:        software
serial number:      05694352
platform:           rp crypto engine
crypto lib version: 10.0.0

Encryption Process Info:
input queue top:    220
input queue bot:    220
input queue count:  0

StHelen#show crypto key mypubkey dss
crypto public-key sthelen 05694352
 5C401002 404DC5A9 EAED2360 D7007E51 4A4BB8F8 6F9B1554 51D8ACBB D3964C10
 A23848CA 46003A94 2FC8C7D6 0B57AE07 9EB5EF3A BD71482B 052CF06B 90C3C618
quit

StHelen#show crypto key pubkey-chain dss
crypto public-key wan 07365004
 A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F
 2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B
quit

StHelen#show crypto map interface serial 1
Crypto Map "towan" 10 cisco
        Connection Id = 58       (1 established,    0 failed)
        Peer = wan
        PE = 30.30.30.0
        UPE = 180.180.180.0
        Extended IP access list 144
            access-list 144 permit ip
                source: addr = 30.30.30.0/0.0.0.255
                dest:   addr = 180.180.180.0/0.0.0.255

StHelen#show crypto map
Crypto Map "towan" 10 cisco
        Connection Id = 58       (1 established,    0 failed)
        Peer = wan
        PE = 30.30.30.0
        UPE = 180.180.180.0
        Extended IP access list 144
            access-list 144 permit ip
                source: addr = 30.30.30.0/0.0.0.255
                dest:   addr = 180.180.180.0/0.0.0.255

StHelen#
```

Campione 4: Crittografia con DDR

Poiché Cisco IOS si basa sull'ICMP per stabilire le sessioni di crittografia, il traffico ICMP deve essere classificato come "interessante" nell'elenco dei dialer quando si esegue la crittografia su un collegamento DDR.

Nota: la compressione funziona correttamente nel software Cisco IOS versione 11.3, ma non è

molto utile per i dati crittografati. Dal momento che i dati crittografati hanno un aspetto abbastanza casuale, la compressione non fa altro che rallentare le operazioni. Tuttavia, è possibile lasciare attiva questa funzione per il traffico non crittografato.

In alcuni casi, è necessario eseguire il dial backup sullo stesso router. Ad esempio, è un carburante d'uso quando gli utenti vogliono proteggere contro il fallimento di un particolare collegamento nelle loro reti WAN. Se due interfacce raggiungono lo stesso peer, la stessa mappa crittografica può essere utilizzata su entrambe le interfacce. Affinché questa funzionalità funzioni correttamente, è necessario utilizzare l'interfaccia di backup. Se il progetto di backup prevede la composizione di un router in una casella diversa, creare mappe crittografiche diverse e impostare i peer di conseguenza. Anche in questo caso, usare il comando **backup interface**.

```
dial-5#write terminal
Building configuration...

Current configuration:
!
version 11.3
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname dial-5
!
boot system c1600-sy56-l 171.68.118.83
enable secret 5 $1$oNe1wDbhBdcN6x9Y5gfuMjqh10
!
username dial-6 password 0 cisco
isdn switch-type basic-ni1
!
crypto map dial6 10
 set peer dial6
 match address 133
!
crypto key pubkey-chain dss
 named-key dial6
  serial-number 05679987
  key-string
   753F71AB E5305AD4 3FCDFB6D 47AA2BB5 656BFCAA 53DBE37F 07465189 06E91A82
   2BC91236 13DC4AA8 7EC5B48C D276E5FE 0D093014 6D3061C5 03158820 B609CA7C
  quit
!
interface Ethernet0
 ip address 20.20.20.20 255.255.255.0
!
interface BRI0
 ip address 10.10.10.11 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 load-interval 30
 dialer idle-timeout 9000
 dialer map ip 10.10.10.10 name dial-6 4724118
 dialer hold-queue 40
 dialer-group 1
 isdn spid1 919472417100 4724171
 isdn spid2 919472417201 4724172
 compress stac
 ppp authentication chap
 ppp multilink
 crypto map dial6
```

```
!
ip classless
ip route 40.40.40.0 255.255.255.0 10.10.10.10
access-list 133 permit ip 20.20.20.0 0.0.0.255 40.40.40.0 0.0.0.255
dialer-list 1 protocol ip permit
!
line con 0
 exec-timeout 0 0
line vty 0 4
 password ww
 login
!
end

dial-5#

-----------------------

dial-6#write terminal
Building configuration...

Current configuration:
!
version 11.3
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname dial-6
!
boot system c1600-sy56-l 171.68.118.83
enable secret 5 $1$VdPYuA/BIVeEm9UAFEm.PPJFc.
!
username dial-5 password 0 cisco
no ip domain-lookup
isdn switch-type basic-ni1
!
 crypto map dial5 10
 set peer dial5
 match address 144
!
crypto key pubkey-chain dss
 named-key dial5
  serial-number 05679919
  key-string
   160AA490 5B9B1824 24769FCD EE5E0F46 1ABBD343 4C0C4A03 4B279D6B 0EE5F65F
   F64665D4 1036875A 8CF93691 BDF81722 064B51C9 58D72E12 3E1894B6 64B1D145
  quit
 !
!
interface Ethernet0
 ip address 40.40.40.40 255.255.255.0
!
interface BRI0
 ip address 10.10.10.10 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 dialer idle-timeout 9000
 dialer map ip 10.10.10.11 name dial-5 4724171
 dialer hold-queue 40
 dialer load-threshold 5 outbound
 dialer-group 1
 isdn spid1 919472411800 4724118
 isdn spid2 919472411901 4724119
```

```
 compress stac
 ppp authentication chap
 ppp multilink
 crypto map dial5
!
ip classless
ip route 20.20.20.0 255.255.255.0 10.10.10.11
access-list 144 permit ip 40.40.40.0 0.0.0.255 20.20.20.0 0.0.0.255
dialer-list 1 protocol ip permit
!
line con 0
 exec-timeout 0 0
line vty 0 4
 password ww
 login
!
end

dial-6#
```

Campione 5: Crittografia del traffico IPX in un tunnel IP

Nell'esempio, il traffico IPX in un tunnel IP è crittografato.

Nota: solo il traffico in questo tunnel (IPX) è crittografato. Tutto il resto del traffico IP viene lasciato da solo.

```
WAN-2511a#write terminal
Building configuration...

Current configuration:
!
version 11.2
no service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname WAN-2511a
!
enable password ww
!
no ip domain-lookup
ipx routing 0000.0c34.aa6a
!
crypto public-key wan2516 01698232
 B1C127B0 78D79CAA 67ECAD80 03D354B1 9012C80E 0C1266BE 25AEDE60 37A192A2
 B066D299 77174D48 7FBAB5FC 2B60893A 37E5CB7B 62F6D902 9495733B 98046962
 quit
!
crypto map wan2516 10
 set peer wan2516
 match address 133
!
!
interface Loopback1
 ip address 50.50.50.50 255.255.255.0
!
interface Tunnel1
 no ip address
 ipx network 100
 tunnel source 50.50.50.50
```

```
 tunnel destination 60.60.60.60
 crypto map wan2516
!
interface Ethernet0
 ip address 40.40.40.40 255.255.255.0
 ipx network 600
!
interface Serial0
 ip address 20.20.20.21 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 crypto map wan2516
!
interface Serial1
 no ip address
 shutdown
!
ip default-gateway 10.11.19.254
ip classless
ip route 0.0.0.0 0.0.0.0 20.20.20.20
access-list 133 permit ip host 50.50.50.50 host 60.60.60.60
!
line con 0
 exec-timeout 0 0
 password ww
 login
line 1 16
line aux 0
 password ww
 login
line vty 0 4
 password ww
 login
!
end

WAN-2511a#

------------------------

WAN-2516a#write terminal
Building configuration...

Current configuration:
!
version 11.2
no service pad
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname WAN-2516a
!
enable password ww
!
no ip domain-lookup
ipx routing 0000.0c3b.cc1e
!
crypto public-key wan2511 01496536
 C8EA7C21 DF3E48F5 C6C069DB 3A5E1B08 8B830AD4 4F1DABCE D62F5F46 ED08C81D
 5646DC78 DDC77EFC 823F302A F112AF97 668E39A1 E2FCDC05 545E0529 9B3C9553
 quit
!
crypto map wan2511 10
```

```
 set peer wan2511
 match address 144
!
!
hub ether 0 1
 link-test
 auto-polarity
!
! <other hub interfaces snipped>
!
hub ether 0 14
 link-test
 auto-polarity
!
interface Loopback1
 ip address 60.60.60.60 255.255.255.0
!
interface Tunnel1
 no ip address
 ipx network 100
 tunnel source 60.60.60.60
 tunnel destination 50.50.50.50
 crypto map wan2511
!
interface Ethernet0
 ip address 30.30.30.30 255.255.255.0
 ipx network 400
!
interface Serial0
 ip address 20.20.20.20 255.255.255.0
 encapsulation ppp
 clockrate 2000000
 crypto map wan2511
!
interface Serial1
 no ip address
 shutdown
!
interface BRI0
 no ip address
 shutdown
!
ip default-gateway 20.20.20.21
ip classless
ip route 0.0.0.0 0.0.0.0 20.20.20.21
access-list 144 permit ip host 60.60.60.60 host 50.50.50.50
access-list 188 permit gre any any
!
line con 0
 exec-timeout 0 0
 password ww
 login
line aux 0
 password ww
 login
 modem InOut
 transport input all
 flowcontrol hardware
line vty 0 4
 password ww
 login
!
end
```

```
WAN-2516a#
----------------------

WAN-2511a#show ipx route
Codes: C - Connected primary network,    c - Connected secondary network
       S - Static, F - Floating static, L - Local (internal), W - IPXWAN
       R - RIP, E - EIGRP, N - NLSP, X - External, A - Aggregate
       s - seconds, u - uses

3 Total IPX routes. Up to 1 parallel paths and 16 hops allowed.

No default route known.

C        100 (TUNNEL),        Tu1
C        600 (NOVELL-ETHER),  Et0
R        400 [151/01] via      100.0000.0c3b.cc1e,   24s, Tu1


WAN-2511a#show crypto engine connections active
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 1    Serial0         20.20.20.21 set    DES_56_CFB64    207      207


WAN-2511a#ping 400.0000.0c3b.cc1e
Translating "400.0000.0c3b.cc1e"

Type escape sequence to abort.
Sending 5, 100-byte IPX cisco Echoes to 400.0000.0c3b.cc1e, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/35/48 ms


WAN-2511a#show crypto engine connections active
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 1    Serial0         20.20.20.21 set    DES_56_CFB64    212      212


WAN-2511a#ping 30.30.30.30

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.30.30.30, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms


WAN-2511a#show crypto engine connections active

ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 1    Serial0         20.20.20.21 set    DES_56_CFB64    212      212

WAN-2511a#
```

Campione 6: Crittografia dei tunnel L2F

In questo esempio, viene tentato solo di crittografare il traffico L2F per gli utenti che effettuano la chiamata. In questo caso, "user@cisco.com" chiama il server di accesso alla rete locale (NAS) denominato "DEMO2" nella propria città e viene inserito nel tunnel del CD del gateway domestico. Tutto il traffico DEMO2 (insieme a quello di altri chiamanti L2F) è crittografato. Poiché L2F utilizza la porta UDP 1701, in questo modo viene costruito l'elenco degli accessi e viene determinato quale traffico è crittografato.

Nota: se l'associazione di crittografia non è già configurata, ovvero il chiamante è la prima persona

a chiamare e creare il tunnel L2F, il chiamante potrebbe essere scartato a causa del ritardo nell'impostazione dell'associazione di crittografia. Questo problema potrebbe non verificarsi sui router con sufficiente potenza della CPU. Inoltre, si potrebbe desiderare di aumentare il **keytimeout** in modo che la configurazione della crittografia e la disinstallazione si verifichino solo nelle ore non di punta.

L'output del comando di esempio seguente è stato preso dal NAS remoto.

```
DEMO2#write terminal
Building configuration...

Current configuration:
!
version 11.2
no service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname DEMO2
!
enable password ww
!
username NAS1 password 0 SECRET
username HomeGateway password 0 SECRET
no ip domain-lookup
vpdn enable
vpdn outgoing cisco.com NAS1 ip 20.20.20.20
!
crypto public-key wan2516 01698232
 B1C127B0 78D79CAA 67ECAD80 03D354B1 9012C80E 0C1266BE 25AEDE60 37A192A2
 B066D299 77174D48 7FBAB5FC 2B60893A 37E5CB7B 62F6D902 9495733B 98046962
 quit
!
crypto map vpdn 10
 set peer wan2516
 match address 133
!
crypto key-timeout 1440
!
interface Ethernet0
 ip address 40.40.40.40 255.255.255.0
!
interface Serial0
 ip address 20.20.20.21 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 crypto map vpdn
!
interface Serial1
 no ip address
 shutdown
!
interface Group-Async1
 no ip address
 encapsulation ppp
 async mode dedicated
 no peer default ip address
 no cdp enable
 ppp authentication chap pap
 group-range 1 16
!
```

```
ip default-gateway 10.11.19.254
ip classless
ip route 0.0.0.0 0.0.0.0 20.20.20.20
access-list 133 permit udp host 20.20.20.21 eq 1701
 host 20.20.20.20 eq 1701
!
!
line con 0
 exec-timeout 0 0
 password ww
 login
line 1 16
 modem InOut
 transport input all
 speed 115200
 flowcontrol hardware
line aux 0
 login local
 modem InOut
 transport input all
 flowcontrol hardware
line vty 0 4
 password ww
 login
!
end

DEMO2#
```

L'output del comando di esempio seguente è stato preso dal gateway principale.

```
CD#write terminal
Building configuration...

Current configuration:
!
version 11.2
no service pad
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname CD
!
enable password ww
!
username NAS1 password 0 SECRET
username HomeGateway password 0 SECRET
username user@cisco.com password 0 cisco
no ip domain-lookup
vpdn enable
vpdn incoming NAS1 HomeGateway virtual-template 1
!
crypto public-key wan2511 01496536
 C8EA7C21 DF3E48F5 C6C069DB 3A5E1B08 8B830AD4 4F1DABCE D62F5F46 ED08C81D
 5646DC78 DDC77EFC 823F302A F112AF97 668E39A1 E2FCDC05 545E0529 9B3C9553
 quit
!
crypto key-timeout 1440
!
crypto map vpdn 10
 set peer wan2511
 match address 144
```

```
!
!
hub ether 0 1
 link-test
 auto-polarity
!
interface Loopback0
 ip address 70.70.70.1 255.255.255.0
!
interface Ethernet0
 ip address 30.30.30.30 255.255.255.0
!
interface Virtual-Template1
 ip unnumbered Loopback0
 no ip mroute-cache
 peer default ip address pool default
 ppp authentication chap
!
interface Serial0
 ip address 20.20.20.20 255.255.255.0
 encapsulation ppp
 clockrate 2000000
 crypto map vpdn
!
interface Serial1
 no ip address
 shutdown
!
interface BRI0
 no ip address
 shutdown
!
ip local pool default 70.70.70.2 70.70.70.77
ip default-gateway 20.20.20.21
ip classless
ip route 0.0.0.0 0.0.0.0 20.20.20.21
access-list 144 permit udp host 20.20.20.20 eq 1701 host 20.20.20.21 eq 1701
!
line con 0
 exec-timeout 0 0
 password ww
 login
line aux 0
 password ww
 login
 modem InOut
 transport input all
 flowcontrol hardware
line vty 0 4
 password ww
 login
!
end
```

Risoluzione dei problemi

In genere, è preferibile iniziare ogni sessione di risoluzione dei problemi raccogliendo informazioni utilizzando i comandi **show** seguenti. Un asterisco (*) indica un comando particolarmente utile. Per ulteriori informazioni, vedere anche Risoluzione dei problemi di sicurezza IP - Comprensione e uso dei comandi di debug.

Alcuni comandi **show sono supportati dallo** strumento Output Interpreter (solo utenti registrati); lo

strumento permette di visualizzare un'analisi dell'output del comando **show.**

Nota: prima di usare i comandi di **debug**, consultare le informazioni importanti sui comandi di debug.

Comandi	
mostra algoritmi crypto cisco	show crypto cisco key-timeout
show crypto cisco pregen-dh-pair	* mostra connessioni del motore di crittografia attive
show crypto engine connections drop-packet	mostra configurazione motore di crittografia
show crypto key mypubkey dss	* show crypto key pubkey-chain dss
show crypto map interface serial 1	* mostra mappa crittografica
debug crypto engine	* debug crypto sess
chiave cry di debug	cancella connessione crittografica
crypto zeroize	nessuna chiave pubblica crittografica

- **mostra algoritmi crypto cisco**- È necessario abilitare tutti gli algoritmi DES (Data Encryption Standard) utilizzati per comunicare con qualsiasi altro router peer per la crittografia. Se non si abilita un algoritmo DES, non sarà possibile utilizzarlo anche se si tenta di assegnarlo a una **mappa crittografica** in un secondo momento.Se il router tenta di configurare una sessione di comunicazione crittografata con un router peer e sui due router non è abilitato lo stesso algoritmo DES su entrambe le estremità, la sessione crittografata ha esito negativo. Se almeno un algoritmo DES comune è abilitato a entrambe le estremità, la sessione crittografata può continuare.**Nota:** la parola extra cisco viene usata nel software Cisco IOS versione 11.3 ed è necessaria per distinguere tra crittografia IPSec e crittografia proprietaria Cisco trovata nel software Cisco IOS versione 11.2.

```
Loser#show crypto cisco algorithms
  des cfb-64
  des cfb-8
  40-bit-des cfb-64
  40-bit-des cfb-8
```

- **show crypto cisco key-timeout**: dopo aver stabilito una sessione di comunicazione crittografata, questa rimane valida per un periodo di tempo specifico. Dopo questo periodo di tempo, la sessione scade. Per continuare la comunicazione crittografata, è necessario negoziare una nuova sessione e generare una nuova chiave DES (session). Utilizzare questo comando per modificare il tempo di durata di una sessione di comunicazione crittografata prima della scadenza (timeout).

```
Loser#show crypto cisco key-timeout
Session keys will be re-negotiated every 30 minutes
```

Utilizzare questi comandi per determinare il periodo di tempo che deve trascorrere prima della rinegoziazione delle chiavi DES.

```
StHelen#show crypto conn
Connection Table
PE              UPE         Conn_id New_id Algorithm    Time
0.0.0.1         0.0.0.1        4    0      DES_56_CFB64 Mar 01 1993 03:16:09
```

```
                flags:TIME_KEYS


StHelen#show crypto key
Session keys will be re-negotiated every 30 minutes

StHelen#show clock
*03:21:23.031 UTC Mon Mar 1 1993
```

- **show crypto cisco pregen-dh-pair** - Ogni sessione crittografata utilizza una coppia univoca di numeri DH. Ogni volta che viene stabilita una nuova sessione, è necessario generare nuove coppie di numeri DH. Al termine della sessione, questi numeri vengono eliminati. La generazione di nuove coppie di numeri DH è un'attività che richiede un utilizzo intensivo della CPU e può rallentare la configurazione delle sessioni, in particolare per i router di fascia bassa.Per accelerare l'impostazione della sessione, è possibile scegliere di pregenerare e tenere in riserva una determinata quantità di coppie di numeri DH. In questo modo, quando si configura una sessione di comunicazione crittografata, viene fornita una coppia di numeri DH dalla riserva. Dopo aver utilizzato una coppia di numeri DH, la riserva viene automaticamente rifornita con una nuova coppia di numeri DH, in modo che vi sia sempre una coppia di numeri DH pronta per l'uso.In genere, non è necessario che siano pregenerate più di una o due coppie di numeri DH, a meno che il router non stia configurando più sessioni crittografate con una frequenza tale che una riserva pregenerata di una o due coppie di numeri DH si esaurisca troppo rapidamente.

```
Loser#show crypto cisco pregen-dh-pairs
Number of pregenerated DH pairs: 10
```

- **mostra connessioni crypto cisco attive**Di seguito viene riportato un esempio di output del comando.

```
Loser#show crypto engine connections active
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 16   Serial1         19.19.19.19 set    DES_56_CFB64    376      884
```

- **show crypto cisco engine connections drop-packet**Di seguito viene riportato un esempio di output del comando.

```
Loser#show crypto engine connections dropped-packet
Interface            IP-Address    Drop Count

Serial1              19.19.19.19   39
```

- **show crypto engine configuration** (era **show crypto engine brief** nel software Cisco IOS versione 11.2.1)Di seguito viene riportato un esempio di output del comando.

```
Loser#show crypto engine configuration
slot:               0
engine name:        fred
engine type:        software
serial number:      02802219
platform:           rp crypto engine
crypto lib version: 10.0.0

Encryption Process Info:
input queue top:    465
input queue bot:    465
input queue count:  0
```

- **show crypto key mypubkey dss**Di seguito viene riportato un esempio di output del comando.

```
Loser#show crypto key mypubkey dss
crypto public-key fred 02802219
 79CED212 AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8 05D4930C CE891810
 C0064492 5F6684CD 3FC326E5 679BCA46 BB155402 D443F68D 93487F7E 5ABE182E
quit
```

- **show crypto key pubkey-chain dss**Di seguito viene riportato un esempio di output del

comando.

```
Loser#show crypto key pubkey-chain dss
crypto public-key barney 05694352
 B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A 3232EBA2 F2D31D21 53AE24ED
 732EA43D 484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477 91810341
quit
```

- **show crypto map interface serial 1**Di seguito viene riportato un esempio di output del comando.

```
Loser#show crypto map interface serial 1
Crypto Map "oldstyle" 10 cisco
        Connection Id = 16       (8 established,    0 failed)
        Peer = barney
        PE = 40.40.40.0
        UPE = 30.30.30.0
        Extended IP access list 133
            access-list 133 permit ip
                source: addr = 40.40.40.0/0.0.0.255
                dest:   addr = 30.30.30.0/0.0.0.255
```

Notare la differenza di tempo quando si usa il comando **ping**.

```
wan-5200b#ping 30.30.30.30

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.30.30.30, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/54/56 ms
wan-5200b#
-----------
wan-5200b#ping 30.30.30.31

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.30.30.31, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/53/56 ms
-----------------

wan-5200b#ping 19.19.19.20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 19.19.19.20, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/21/24 ms
------------
```

- **show crypto map interface serial 1**Di seguito viene riportato un esempio di output del comando.

```
Loser#show crypto map
Crypto Map "oldstyle" 10 cisco
        Connection Id = 16       (8 established,    0 failed)
        Peer = barney
        PE = 40.40.40.0
        UPE = 30.30.30.0
        Extended IP access list 133
            access-list 133 permit ip
                source: addr = 40.40.40.0/0.0.0.255
                dest:   addr = 30.30.30.0/0.0.0.255
```

- **debug crypto engine**Di seguito viene riportato un esempio di output del comando.

```
Loser#debug crypto engine
Mar 17 11:49:07.902: Crypto engine 0: generate alg param

Mar 17 11:49:07.906: CRYPTO_ENGINE: Dh phase 1 status: 0
Mar 17 11:49:07.910: Crypto engine 0: sign message using crypto engine
Mar 17 11:49:09.894: CRYPTO_ENGINE: packets dropped: State = 0
```

```
Mar 17 11:49:11.758: Crypto engine 0: generate alg param

Mar 17 11:49:12.246: CRYPTO_ENGINE: packets dropped: State = 0
Mar 17 11:49:13.342: CRYPTO ENGINE 0: get syndrome for conn id 25
Mar 17 11:49:13.346: Crypto engine 0: verify signature
Mar 17 11:49:14.054: CRYPTO_ENGINE: packets dropped: State = 0
Mar 17 11:49:14.402: Crypto engine 0: sign message using crypto engine
Mar 17 11:49:14.934: Crypto engine 0: create session for conn id 25
Mar 17 11:49:14.942: CRYPTO ENGINE 0: clear dh number for conn id 25
Mar 17 11:49:24.946: Crypto engine 0: generate alg param
```

- **debug crypto sessmgmt**Di seguito viene riportato un esempio di output del comando.

```
StHelen#debug crypto sessmgmt

Mar 17 11:49:08.918: IP: s=40.40.40.40 (Serial1), d=30.30.30.30, len 328,
              Found an ICMP connection message.

Mar 17 11:49:08.922: CRYPTO: Dequeued a message: CIM
Mar 17 11:49:08.926: CRYPTO-SDU: Key Timeout, Re-exchange Crypto Keys
Mar 17 11:49:09.978: CRYPTO: Verify done. Status=OK
Mar 17 11:49:09.994: CRYPTO: DH gen phase 1 status for conn_id 22 slot 0:OK
Mar 17 11:49:11.594: CRYPTO: DH gen phase 2 status for conn_id 22 slot 0:OK
Mar 17 11:49:11.598: CRYPTO: Syndrome gen status for conn_id 22 slot 0:OK
Mar 17 11:49:12.134: CRYPTO: Sign done. Status=OK
Mar 17 11:49:12.142: CRYPTO: ICMP message sent: s=19.19.19.20, d=19.19.19.19
Mar 17 11:49:12.146: CRYPTO-SDU: act_on_nnc_req: NNC Echo Reply sent
Mar 17 11:49:12.154: CRYPTO: Create encryption key for conn_id 22 slot 0:OK
Mar 17 11:49:15.366: CRYPTO: Dequeued a message: CCM
Mar 17 11:49:15.370: CRYPTO: Syndrome gen status for conn_id 22 slot 0:OK
Mar 17 11:49:16.430: CRYPTO: Verify done. Status=OK
Mar 17 11:49:16.434: CRYPTO: Replacing -23 in crypto maps with 22 (slot 0)
Mar 17 11:49:26.438: CRYPTO: Need to pregenerate 1 pairs for slot 0.
Mar 17 11:49:26.438: CRYPTO: Pregenerating DH for conn_id 32 slot 0
Mar 17 11:49:28.050: CRYPTO: DH phase 1 status for conn_id 32 slot 0:OK
                           ~~ <---------- This is good ----------> ~~
```

  Se nella mappa crittografica è impostato il peer errato, viene visualizzato questo messaggio di errore.

```
Mar  2 12:19:12.639: CRYPTO-SDU:Far end authentication error:
          Connection message verify failed
```

  Se gli algoritmi crittografici non corrispondono, viene visualizzato questo messaggio di errore.

```
Mar  2 12:26:51.091: CRYPTO-SDU: Connection
failed due to incompatible policy
```

  Se la chiave DSS è mancante o non valida, viene visualizzato questo messaggio di errore.

```
Mar 16 13:33:15.703: CRYPTO-SDU:Far end authentication error:
           Connection message verify failed
```

- **debug crypto key**Di seguito viene riportato un esempio di output del comando.

```
StHelen#debug crypto key
Mar 16 12:16:45.795: CRYPTO-KE: Sent 4 bytes.
Mar 16 12:16:45.795: CRYPTO-KE: Sent 2 bytes.
Mar 16 12:16:45.799: CRYPTO-KE: Sent 6 bytes.
Mar 16 12:16:45.799: CRYPTO-KE: Sent 2 bytes.
Mar 16 12:16:45.803: CRYPTO-KE: Sent 64 bytes.

Mar 16 12:16:56.083: CRYPTO-KE: Received 4 bytes.
Mar 16 12:16:56.087: CRYPTO-KE: Received 2 bytes.
Mar 16 12:16:56.087: CRYPTO-KE: Received 4 bytes.
Mar 16 12:16:56.091: CRYPTO-KE: Received 2 bytes.
Mar 16 12:16:56.091: CRYPTO-KE: Received 52 bytes.
Mar 16 12:16:56.095: CRYPTO-KE: Received 12 bytes.
```

- **cancella connessione crittografica**Di seguito viene riportato un esempio di output del comando.

```
wan-2511#show crypto engine connections act
```

```
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 9    Serial0         20.20.20.21 set    DES_56_CFB64    29       28

wan-2511#clear crypto connection 9
wan-2511#
*Mar  5 04:58:20.690: CRYPTO: Replacing 9 in crypto maps with 0 (slot 0)
*Mar  5 04:58:20.694: Crypto engine 0: delete connection 9
*Mar  5 04:58:20.694: CRYPTO: Crypto Engine clear conn_id 9 slot 0: OK
wan-2511#
wan-2511#show crypto engine connections act
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt

wan-2511#
```

- **crypto zeroize**Di seguito viene riportato un esempio di output del comando.

```
wan-2511#show crypto mypubkey
crypto public-key wan2511 01496536
 11F43C02 70C0ADB7 5DD50600 A0219E04 C867A5AF C40A4FE5 CE99CCAB A8ECA840
 EB95FBEE D727ED5B F0A6F042 BDB5529B DBB0698D DB0B2756 F6CABE8F 05E4B27F
quit

wan-2511#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
wan-2511(config)#crypto zeroize
Warning! Zeroize will remove your DSS signature keys.
Do you want to continue? [yes/no]: yes
% Keys to be removed are named wan2511.
Do you really want to remove these keys? [yes/no]: yes
% Zeroize done.

wan-2511(config)#^Z
wan-2511#
wan-2511#show crypto mypubkey
wan-2511#
```

- **nessuna chiave pubblica crittografica**Di seguito viene riportato un esempio di output del comando.

```
wan-2511#show crypto pubkey
crypto public-key wan2516 01698232
 B1C127B0 78D79CAA 67ECAD80 03D354B1 9012C80E 0C1266BE 25AEDE60 37A192A2
 B066D299 77174D48 7FBAB5FC 2B60893A 37E5CB7B 62F6D902 9495733B 98046962
quit

wan-2511#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
wan-2511(config)#crypto public-key ?
  WORD  Peer name

wan-2511(config)#
wan-2511(config)#no crypto public-key wan2516 01698232
wan-2511(config)#^Z
wan-2511#
wan-2511#show crypto pubkey
wan-2511#
```

Risoluzione dei problemi di Cisco 7200 con ESA

Cisco fornisce anche un'opzione di assistenza hardware per eseguire la crittografia sui router Cisco serie 7200, chiamata ESA. L'ESA ha la forma di un adattatore di porta per la scheda VIP2-40 o di un adattatore di porta standalone per Cisco 7200. Questa disposizione consente l'uso di un adattatore hardware o del motore software VIP2 per crittografare e decrittografare i dati che entrano o escono dalle interfacce sulla scheda VIP2 di Cisco 7500. Cisco 7200 consente al

supporto hardware di crittografare il traffico per qualsiasi interfaccia sullo chassis Cisco 7200. L'uso di un supporto di crittografia consente di salvare cicli preziosi della CPU che possono essere utilizzati per altri scopi, ad esempio il routing o una qualsiasi delle altre funzioni di Cisco IOS.

Su un Cisco 7200, la scheda di porta standalone è configurata esattamente come il motore di crittografia del software Cisco IOS, ma dispone di alcuni comandi aggiuntivi che vengono utilizzati solo per l'hardware e per decidere quale motore (software o hardware) eseguirà la crittografia.

Innanzitutto, preparare il router per la crittografia hardware:

```
wan-7206a(config)#
%OIR-6-REMCARD: Card removed from slot 3, interfaces disabled
*Mar  2 08:17:16.739: ...switching to SW crypto engine

wan-7206a#show crypto card 3

Crypto card in slot: 3

Tampered:        No
Xtracted:        Yes
Password set:    Yes
DSS Key set:     Yes
FW version       0x5049702
wan-7206a#

wan-7206a(config)#

wan-7206a(config)#crypto zeroize 3
Warning! Zeroize will remove your DSS signature keys.
Do you want to continue? [yes/no]: yes
% Keys to be removed are named hard.
Do you really want to remove these keys? [yes/no]: yes
[OK]
```

Abilitare o disabilitare la crittografia hardware come illustrato di seguito:

```
wan-7206a(config)#crypto esa shutdown 3
...switching to SW crypto engine


wan-7206a(config)#crypto esa enable 3
There are no keys on the ESA in slot 3- ESA not enabled.
```

Quindi, generare le chiavi per l'ESA prima di abilitarla.

```
wan-7206a(config)#crypto gen-signature-keys hard
% Initialize the crypto card password. You will need
   this password in order to generate new signature
   keys or clear the crypto card extraction latch.

Password:
Re-enter password:
Generating DSS keys ....
 [OK]

wan-7206a(config)#
wan-7206a#show crypto mypubkey
crypto public-key hard 00000052
 EE691A1F BD013874 5BA26DC4 91F17595 C8C06F4E F7F736F1 AD0CACEC 74AB8905
```

```
 DF426171 29257F8E B26D49B3 A8E11FB0 A3501B13 D3F19623 DCCE7322 3D97B804
quit

wan-7206a#
wan-7206a(config)#crypto esa enable 3
...switching to HW crypto engine

wan-7206a#show crypto engine brie
crypto engine name:   hard
crypto engine type:   ESA
serial number:        00000052
crypto engine state:  installed
crypto firmware version:  5049702
crypto engine in slot: 3

wan-7206a#
```

Risoluzione dei problemi VIP2 con ESA

L'adattatore della porta hardware ESA sulla scheda VIP2 viene utilizzato per crittografare e decrittografare i dati che entrano o escono dalle interfacce sulla scheda VIP2. Come per Cisco 7200, l'uso di un supporto di crittografia consente di risparmiare preziosi cicli della CPU. In questo caso, il comando **crypto esa enable** non esiste perché l'adattatore della porta ESA esegue la crittografia delle porte sulla scheda VIP2 se l'ESA è collegata. Il dispositivo **crypto clear-latch** deve essere applicato allo slot se l'adattatore della porta ESA è stato appena installato per la prima volta o rimosso e reinstallato.

```
Router#show crypto card 11

Crypto card in slot: 11

Tampered:        No
Xtracted:        Yes
Password set:    Yes
DSS Key set:     Yes
FW version       0x5049702
Router#
```

Poiché il modulo Cripto ESA è stato estratto, verrà visualizzato il seguente messaggio di errore finché non si esegue un comando **crypto clear-latch** su tale slot, come mostrato di seguito.

```
----
*Jan 24 02:57:09.583: CRYPTO: Sign done. Status= Extraction latch set. Request not allowed.
-----
Router(config)#crypto clear-latch ?
  <0-15>  Chassis slot number

Router(config)#crypto clear-latch 11
% Enter the crypto card password.
Password:
Router(config)#^Z
```

Se si dimentica una password assegnata in precedenza, usare il comando **crypto zeroize** invece del comando **crypto clear-latch** per ripristinare l'ESA. Dopo aver eseguito il comando **crypto zeroize**, è necessario rigenerare e scambiare nuovamente le chiavi DSS. Quando si rigenerano le chiavi DSS, viene richiesto di creare una nuova password. Di seguito è riportato un esempio.

```
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#show crypto card 11

Crypto card in slot: 11

Tampered:        No
Xtracted:        No
Password set:    Yes
DSS Key set:     Yes
FW version       0x5049702
Router#

-------------------------------------------------


Router#show crypto engine brief
crypto engine name:   TERT
crypto engine type:   software
serial number:        0459FC8C
crypto engine state:  dss key generated
crypto lib version:   5.0.0
crypto engine in slot: 6

crypto engine name:   WAAA
crypto engine type:   ESA
serial number:        00000078
crypto engine state:  dss key generated
crypto firmware version:  5049702
crypto engine in slot: 11

Router#
-----------
Router(config)#crypto zeroize
Warning! Zeroize will remove your DSS signature keys.
Do you want to continue? [yes/no]: yes
% Keys to be removed are named TERT.
Do you really want to remove these keys? [yes/no]: yes
% Zeroize done.

Router(config)#crypto zeroize  11
Warning! Zeroize will remove your DSS signature keys.
Do you want to continue? [yes/no]: yes
% Keys to be removed are named WAAA.
Do you really want to remove these keys? [yes/no]: yes
[OK]

Router(config)#^Z
Router#show crypto engine brief
crypto engine name:   unknown
crypto engine type:   software
serial number:        0459FC8C
crypto engine state:  installed
crypto lib version:   5.0.0
crypto engine in slot: 6

crypto engine name:   unknown
crypto engine type:   ESA
serial number:        00000078
crypto engine state:  installed
crypto firmware version:  5049702
crypto engine in slot: 11
```

```
Router#
--------------
Router(config)#crypto gen-signature-keys VIPESA 11
% Initialize the crypto card password. You will need
   this password in order to generate new signature
   keys or clear the crypto card extraction latch.

Password:
Re-enter password:
Generating DSS keys ....
 [OK]

Router(config)#
*Jan 24 01:39:52.923: Crypto engine 11: create key pairs.
^Z
Router#
------
Router#show crypto engine brief
crypto engine name:   unknown
crypto engine type:   software
serial number:        0459FC8C
crypto engine state:  installed
crypto lib version:   5.0.0
crypto engine in slot: 6

crypto engine name:   VIPESA
crypto engine type:   ESA
serial number:        00000078
crypto engine state:  dss key generated
crypto firmware version:  5049702
crypto engine in slot: 11

Router#
----------
Router#show crypto engine connections active 11
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 2    Serial11/0/0    20.20.20.21 set    DES_56_CFB64    9996     9996

Router#
Router#clear crypto connection 2 11
Router#
*Jan 24 01:41:04.611: CRYPTO: Replacing 2 in crypto maps with 0 (slot 11)
*Jan 24 01:41:04.611: Crypto engine 11: delete connection 2
*Jan 24 01:41:04.611: CRYPTO: Crypto Engine clear conn_id 2 slot 11: OK
Router#show crypto engine connections active 11
No connections.

Router#
*Jan 24 01:41:29.355: CRYPTO ENGINE:Number of connection entries
received from VIP 0
------------

Router#show crypto mypub
% Key for slot 11:
crypto public-key VIPESA 00000078
 CF33BA60 56FCEE01 2D4E32A2 5D7ADE70 6AF361EE 2964F3ED A7CE08BD A87BF7FE
 90A39F1C DF96143A 9B7B9C78 5F59445C 27860F1E 4CD92B6C FBC4CBCC 32D64508
quit

Router#show crypto pub
crypto public-key wan2516 01698232
 C5DE8C46 8A69932C 70C92A2C 729449B3 FD10AC4D 1773A997 7F6BA37D 61997AC3
 DBEDBEA7 51BF3ADD 2BB35CB5 B9126B4D 13ACF93E 0DF0CD22 CFAAC1A8 9CE82985
```

```
quit

Router#
----------
interface Serial11/0/0
 ip address 20.20.20.21 255.255.255.0
 encapsulation ppp
 ip route-cache distributed
 no fair-queue
 no cdp enable
 crypto map test
!
----------
Router#show crypto eng conn act 11
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 3    Serial11/0/0    20.20.20.21 set    DES_56_CFB64    761      760

Router#
*Jan 24 01:50:43.555: CRYPTO ENGINE:Number of connection
entries received from VIP 1

Router#
```

Informazioni correlate

- Configurazione e risoluzione dei problemi di Cisco Network-Layer Encryption: IPSec e ISAKMP - Parte 2
- DES FIPS 46-2 del National Institute of Standards and Technology (NIST)
- DSS FIPS 186 del National Institute of Standards and Technology (NIST)
- Domande frequenti di RSA Laboratories sulla crittografia attuale
- Standard di sicurezza IETF
- Configurazione del protocollo di protezione di Internet Key Exchange
- Configurazione di IPSec Network Security
- Pagina di supporto per IPSec
- Supporto tecnico – Cisco Systems