Esempio di tunnel IPsec LAN a LAN tra un concentratore Cisco VPN 3000 e un router con configurazione AES

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Configurazione Esempio di rete Configurazioni **Configurare VPN Concentrator** Verifica Verifica della configurazione del router Verifica della configurazione di VPN Concentrator Risoluzione dei problemi Risoluzione dei problemi del router Risoluzione dei problemi di VPN Concentrator Informazioni correlate

Introduzione

In questo documento viene spiegato come configurare un tunnel IPsec tra un concentratore Cisco VPN 3000 e un router Cisco con Advanced Encryption Standard (AES) come algoritmo di crittografia.

AES è una nuova pubblicazione FIPS (Federal Information Processing Standard) creata dal National Institute of Standards and Technology (NIST) per essere utilizzata come metodo di crittografia. Questo standard specifica un algoritmo di crittografia simmetrica AES che sostituisce Data Encryption Standard (DES) come trasformazione della privacy sia per IPsec che per IKE (Internet Key Exchange). AES ha tre diverse lunghezze di chiave, una a 128 bit (predefinita), una a 192 bit e una a 256 bit. La funzionalità AES di Cisco IOS® aggiunge il supporto per il nuovo standard di crittografia AES, con modalità CBC (Cipher Block Chaining), a IPsec.

Per ulteriori informazioni su AES, fare riferimento al <u>sito Centro risorse per la sicurezza dei</u> <u>computer NIST</u>.

Per ulteriori informazioni sulla configurazione del tunnel LAN-LAN tra un concentratore VPN 3000 e un firewall PIX, fare riferimento agli <u>esempi di tunnel IPsec LAN-LAN tra un concentratore VPN</u>

Per ulteriori informazioni sulla versione del PIX con software 7.1, fare riferimento all'<u>esempio di</u> <u>configurazione del tunnel IPsec tra i PIX 7.x e</u> la <u>VPN 3000 Concentrator</u>.

Prerequisiti

Requisiti

Questo documento richiede una comprensione di base del protocollo IPsec. per ulteriori informazioni su IPSec, fare riferimento a <u>Introduzione alla crittografia IPSec</u>.

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Requisiti del router La funzione AES è stata introdotta nel software Cisco IOS versione 12.2(13)T. Per abilitare AES, il router deve supportare IPsec ed eseguire un'immagine IOS con chiavi lunghe "k9" (sottosistema "k9").Nota: il supporto hardware per AES è disponibile anche sui moduli VPN in accelerazione AES Cisco 2600XM, 2691, 3725 e 3745. Questa funzione non ha implicazioni sulla configurazione e il modulo hardware viene selezionato automaticamente se sono disponibili entrambi.
- VPN Concentrator Requirements II supporto software per la funzione AES è stato introdotto nella versione 3.6. Il supporto hardware è fornito dal nuovo processore di crittografia scalabile (SEP-E). Questa funzionalità non ha implicazioni a livello di configurazione.Nota: in Cisco VPN 3000 Concentrator versione 3.6.3, i tunnel non vengono negoziati su AES a causa dell'ID bug Cisco <u>CSCdy88797</u> (solo utenti registrati). Questa condizione è stata risolta dalla release 3.6.4.Nota: Cisco VPN 3000 Concentrator utilizza moduli SEP o SEP-E, non entrambi. Non installare entrambi sulla stessa periferica. Se si installa un modulo SEP-E in un concentratore VPN che contiene già un modulo SEP, il concentratore VPN disabilita il modulo SEP e utilizza solo il modulo SEP-E.

Componenti usati

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

- Cisco serie 3600 Router con software Cisco IOS versione 12.3(5)
- Cisco VPN 3060 Concentrator con software versione 4.0.3

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

Fare riferimento a <u>Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.</u>

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo <u>strumento di</u> <u>ricerca</u> dei comandi (solo utenti <u>registrati</u>).

Esempio di rete



Nel documento viene usata questa impostazione di rete:

Configurazioni

Nel documento vengono usate queste configurazioni:

- Router IPsec
- <u>VPN Concentrator</u>

| Configurazione ipsec_router | | | |
|--------------------------------------|--|--|--|
| | | | |
| version 12.3 | | | |
| service timestamps debug uptime | | | |
| service timestamps log datetime msec | | | |
| no service password-encryption | | | |
| 1 | | | |
| hostname ipsec_router | | | |
| ! | | | |
| memory-size iomem 10 | | | |
| no aaa new-model | | | |
| ip subnet-zero | | | |
| ! | | | |

```
!--- Configuration for IKE policies. crypto isakmp
policy 1
!--- Enables the IKE policy configuration (config-
isakmp) command mode, !--- where you can specify the
parameters to be used during !--- an IKE negotiation.
encryption aes 256
!--- Specifies the encryption algorithm as AES with a
256 !--- bit key within an IKE policy. authentication
pre-share
group 2
crypto isakmp key cisco123 address 20.20.20.1
!--- Specifies the preshared key "cisco123" which !---
should be identical at both peers. !
!--- Configuration for IPsec policies. crypto ipsec
security-association lifetime seconds 28800
!--- Specifies the lifetime of the IPsec security
association (SA). ! crypto ipsec transform-set vpn esp-
aes 256 esp-md5-hmac
!--- Enables the crypto transform configuration mode,
where you can !--- specify the transform sets to be used
during an IPsec negotiation. ! crypto map vpn 10 ipsec-
isakmp
!--- Indicates that IKE is used to establish the IPsec
SA for protecting !--- the traffic specified by this
crypto map entry. set peer 20.20.20.1
!--- Sets the IP address of the remote end (VPN
Concentrator). set transform-set vpn
!--- Configures IPsec to use the transform-set "vpn"
defined earlier. ! !--- Specifies the traffic to be
encrypted. match address 110
I
interface Ethernet1/0
ip address 30.30.30.1 255.255.255.0
ip nat outside
half-duplex
crypto map vpn
!--- Configures the interface to use the crypto map
"vpn" for IPsec. !
interface FastEthernet2/0
ip address 192.168.20.1 255.255.255.0
ip nat inside
duplex auto
speed auto
!
ip nat pool mypool 30.30.30.3 30.30.30.3 netmask
255.255.255.0
ip nat inside source route-map nonat pool mypool
overload
ip http server
no ip http secure-server
in classless
ip route 0.0.0.0 0.0.0.0 30.30.30.2
!
access-list 110 permit ip 192.168.20.0 0.0.0.255
172.16.0.0 0.0.255.255
!--- This crypto ACL-permit identifies the matching
traffic !--- flows to be protected via encryption. !---
Specifies the traffic not to be encrypted. access-list
120 deny ip 192.168.20.0 0.0.0.255 172.16.0.0
0.0.255.255
!--- This crypto ACL-deny identifies the matching
traffic flows not to be encrypted. !
access-list 120 permit ip 192.168.20.0 0.0.0.255 any
!--- The access control list (ACL) used in the NAT
```

```
configuration exempts !--- the LAN-to-LAN traffic from
the NAT process, !--- but allows all traffic going to
the Internet to be translated. !
route-map nonat permit 10
!--- The traffic flows not encrypted from the !--- peer
network are allowed. match ip address 120
!
line con 0
line aux 0
line vty 0 4
login
!
end
```

Nota: anche se la sintassi degli ACL non è stata modificata, i significati sono leggermente diversi per gli ACL crittografici. Negli ACL crittografici, il comando **allow** specifica che i pacchetti corrispondenti devono essere crittografati, mentre il comando **deny** specifica che non è necessario crittografare i pacchetti corrispondenti.

Configurare VPN Concentrator

I concentratori VPN non sono pre-programmati con indirizzi IP nelle impostazioni di fabbrica. È necessario utilizzare la porta della console per configurare le configurazioni iniziali, che sono un'interfaccia della riga di comando (CLI) basata su menu. Per informazioni su come configurare i concentratori VPN tramite la console, consultare il documento sulla <u>configurazione dei</u> <u>concentratori VPN</u> tramite la console.

Dopo aver configurato l'indirizzo IP sull'interfaccia Ethernet 1 (privata), il resto può essere configurato sia dalla CLI che dall'interfaccia del browser. L'interfaccia del browser supporta sia HTTP che HTTP su SSL (Secure Sockets Layer).

Questi parametri vengono configurati tramite la console:

• **Ora/Data** - L'ora e la data corrette sono molto importanti. Garantiscono l'accuratezza delle voci di registrazione e di accounting e la possibilità di creare un certificato di protezione valido.

• Ethernet 1 (private) interface - Indirizzo IP e maschera (dalla topologia di rete 172.16.1.1/24).

A questo punto, VPN Concentrator è accessibile dalla rete interna tramite un browser HTML. Per informazioni sulla configurazione di VPN Concentrator in modalità CLI, consultare il documento sulla <u>configurazione rapida tramite CLI</u>.

 Digitare l'indirizzo IP dell'interfaccia privata dal browser Web per abilitare l'interfaccia GUI.Fare clic sull'icona Save needed (Salva le modifiche necessarie) per salvare le modifiche in memoria. Il nome utente e la password predefiniti di fabbrica sono "admin", che fa distinzione tra maiuscole e minuscole.

| | VPN 3000 | | Main Help Support Logout |
|---|--|--|--|
| | Concentrator Series Mana | iger | Looped in: admir |
| | | Confi | guration Administration Monitoring |
| 8:Configuration 17:Administration 17:Mentiorina | Main Welcome to the VFN 3000 Concern In the left forme or the consignion b • <u>Configuration</u> – to configu- • <u>Administration</u> – to configu- • <u>Montoring</u> – to view staff The bar at the top right has: • <u>Montoring</u> – to view staff The bar at the top right has: • <u>Montoring</u> – to view staff The bar at the top right has: • <u>Montoring</u> – to view staff • <u>Montoring</u> – to view staff • <u>Montoring</u> – to some VFN • <u>Logari</u> – to some VFN • <u>Logari</u> – to some VFN • <u>Save Finisted</u> – as due • <u>Restain</u> – to temporarily • <u>Restain</u> – to temporarily • <u>Restain</u> – to temporarily | ntrator Manager. bar okova, elick the function you want: no administrative functions on this device. It administrative functions on this device. It administrative functions on this device. It administrative state of the second output streen. 2000 Concentrator support and documentation. Is season and sector. In the Manager logis sectors. Is right, these icons may appear. Click to: Is configuration and make it the boot configuration. Is influenting you have changed the active configuration. Is presentabilities to zero. Influenties from their reset values. | |

2. Dopo aver avviato la GUI, selezionare **Configuration > Interfaces > Ethernet 2 (Public)** per configurare l'interfaccia Ethernet

| 2. | | | | |
|------------------------|---|---------------------------------|--|--|
| <u>Configuration</u> | | 154 | | |
| | figuration Interfaces | s Ethernet 2 | | |
| EHUser Management Conf | guring Ethernet Interfa | ce 2 (Public). | | |
| | •• | | | |
| - Administration Gen | ieral RIP OSPF B | andwidth | | |
| | | Gener | ral Parameters | |
| Sel | Attribute | Value | | Description |
| | Disabled | | | Select to disable this interface. |
| (| DHCP Client | | | Select to obtain the IP Address, Subnet Mask and Default Geterory via DHCP. |
| | G Static IP Addressing | | | |
| | IP Address | 20.20.20.1 | | Enter the IP Address and Subnet Mask, for this |
| | Subnet Mask | 255.255.255.0 | | 200011800. |
| | Public Interface | Public Interface 🗹 🔿 | | Check to make this interface a "public" interface. |
| | MAC Address | MAC Address 00.90.A4.00.41 F9 0 | | The MAC address for this interface. |
| | Filter | Filter 2. Public (Defoult) | | Select the filter for this interface. |
| | Speed | 10/100 auto 💌 | | Select the speed for this interface. |
| | Duplex | Auto 💌 | | Select the duplex mode for this interface. |
| | мто | 1500 | | Enter the Maximum Transmit Unit for this interface (68 - 1500). |
| | C Do not fragment prior to IPSec encapsulation; fit | | agment prior to interface transmission. | |
| | Public Interface IPSec Fragmentation Policy | C Fragment prior to IPSec end | Fragment prior to IPSec encapsulation with Path MTU Discovery (ICMP) | |
| | | C Fragment prior to IPSec enc | opsulatics, without F | ath MTU Discovery (Clear DF bit) |
| CISCO SYSTEMS | Apply Cancel | | | |

3. Selezionare Configurazione > Sistema > Routing IP > Gateway predefiniti configurare il gateway predefinito (Internet) e il gateway predefinito del tunnel (interno) in modo che IPsec raggiunga le altre subnet nella rete privata.In questo scenario, nella rete interna è disponibile una sola subnet.

| <u>Configuration</u> | | |
|----------------------------|---|---|
| | Configuration System IP Routing De | efault Gateways |
| - () System | | |
| - Bervers | Configure the default sateways for your system. | |
| Address Management | | |
| - El-Tunneting Protocols | | |
| - CP Routing | Default Gateway 20.20.20.2 | Enter the IP address of the default gateway or router. Enter 0.0.0.0 for an default router. |
| Static Routes | Matrix 1 | Enter the metric from 1 to 16 |
| Default Gateways | Nor unit: | Enter the metric, from t to ro. |
| OSPE | Tunnel Default 172 16 1 2 | Enter the IP address of the default gateway or router for tunnels. Enter 0.0.0.0 for no |
| OSPE Areas | Gateway Trainer | default router. |
| DHCP Parameters | Override Default | Check to allow bound default externance to councils the confirmed default externan |
| DHCP Retay | Gateway 🖻 | Check to many learnes determ gareways to overtale the configures determ gareway. |
| Redunciancy | Annta Canad | |
| Reverse Route Injection | Appiy Concei | |
| - III-Management Protocols | | |
| - Events | | |
| General | | |
| - El Client Lipdate | | |
| Load Balancing | | |
| El-User Management | | |
| Policy Management | | |
| +++Administration | | |
| -E-Monitoring | | |
| | | |

4. Selezionare Configurazione > Gestione policy > Gestione traffico > Elenchi di rete > Aggiungi per creare gli elenchi di rete che definiscono il traffico da crittografare.Le reti menzionate nell'elenco sono raggiungibili dalla rete remota. Le reti mostrate nell'elenco seguente sono reti locali. È inoltre possibile generare automaticamente l'elenco delle reti locali tramite RIP quando si fa clic su Genera elenco

| locale. | | | |
|---|----------------|--|--|
| - Configuration | | | |
| | Configurati | on Policy Management Traffic Manage | ment Network Lists Modify |
| - (I) System | | | |
| - (E) User Management | Modify a confi | gued Network List, Click on Generate Local List to | o generate a network list based on routing entries on the Private interface. |
| | | , | · · |
| Access Hours | | | |
| ———————————————————————————————————— | List Name | vpn_local_network | Name of the Network List you are adding. The name must be unique. |
| Network Lists | | 172, 16, 0, 0/0, 0, 255, 255 | The state of the S |
| Rules | | 172.10.0.0/0.0/200.200 | Ealer the Networks and Wildcard masks using the following Consult a provide a provide a 10 10 0 00 0 355 355. |
| <u>SAs</u> | | | Note: Entrance wildow describe a birth in the second of a |
| <u>— Fiters</u> | | | INDEX EDIET & WARRANT MARK, WHEN IS DE FEVELSE OF A submat mark. A univiouri mark has is in hit positions to |
| -DNAT | | | imore 0s in hit positions to match. For example |
| BYV Policies | Notwork List | | 10.10.10000255 = all 10.10.1 res addresses. |
| Group Matching | Demote LD1 | | Bach Network and Wildcard mask pair must be entered on a |
| - Administration | | | single line. |
| Honitoring | | | The Wildrard mask may be omitted if the natural Wildrard |
| | | | mask is to be used. |
| | | | <u> </u> |
| | | | |
| | Apply | Concel Generate Local List | |
| | . 449 | | |

5. Le reti in questo elenco sono reti remote e devono essere configurate manualmente. A tale scopo, immettere il valore network/wildcard per ciascuna subnet

| raggiungibile. | |
|------------------------|--|
| Configuration | |
| | Configuration Policy Management Traffic Management Network Lists Modify |
| | |
| - 3Huser Management | Modify a configured Network List. Cluck on Generate Local List to generate a network list based on routing entries on the Private interface. |
| | |
| El Tratific Magazanest | List Name won remote network. Name of the Network List you are adding. The using must be unions. |
| Network Lists | |
| Bules | 192.168.20.0/0.0.0.255 |
| -SAz | Bates the Networks and Wildowid masks using the following format: |
| Elbers | a a a n'n n n n n (e.g. 10, 10, 0, 00, 0, 255 253). |
| - GNAT | Done: Earler a Ward/or Doask, Which is the reverse of a source mask. A, unident much has been been being much has been being and the source of the source much has been been been been been been been bee |
| EV/(Foliples | Nature First |
| - E-Group Matching | Each Network and Wildrard mask pair multiple schemes in a single line |
| + Administration | The Wildcard enastic may be omitted if the nutrual Wildcard mode is to be |
| - Monitoring | used. |
| | × |
| | z z |
| | And County Developed List |
| | Appy Cancel Generale Local List |

Al termine, questi sono i due elenchi di reti:

| ER <u>Configuration</u> Interloces Interloces | Configuration Policy Managem | ent Traffic Management Netw | ork Lists | Save |
|---|--|---|----------------|------|
| | This section lets you add, modify, copy, a | and delete Network Lists. | | |
| Rubonik Liste | Clink Add to create a Network List, or sel | eet a Network List and click Moduly, Copy Network List | Actions | |
| Tiletz - (TMAI - (TMAI - (TMAI) - | | VPN Client Local LAN (Defaulf) Vpn_remote_network Vpn_local_network | Add | |
| Administration Hentering | | | Modity Copy | |
| | | | Delete | |

6. Selezionare Configurazione > Sistema > Protocolli di tunneling > IPSec da LAN a LAN > Aggiungi e definire il tunnel da LAN a LAN.Questa finestra è suddivisa in tre sezioni. La sezione superiore si riferisce alle informazioni di rete, mentre le due sezioni inferiori si riferiscono agli elenchi delle reti locali e remote. Nella sezione Informazioni di rete selezionare la crittografia AES, il tipo di autenticazione, la proposta IKE e digitare la chiave già condivisa. Nelle sezioni inferiori selezionare gli elenchi Rete già creati, ovvero gli elenchi Locale e

| Remoto. | | |
|---|---|---|
| -B <u>Configuration</u> | Configuration System Tunneling Protoco | uls IPSec LAN-to-LAN Add |
| Address: Management | Add a new Lifer LAB-to-LAN connection | |
| | Enable 🖂 | Check to enable this LAN-to-LAN connection. |
| | Name test | Enter the name for this LAN-to-LAN connection. |
| LAN-to-LAN | Interface Ethernet 2 (Public) (20.20.20 | Select the interface for this LAN-to-LAN connection. |
| <u>IKE Proposelo</u> <u>NAT Transparency</u> Alasta | Connection Type Bi-directional | Choose the type of LAN-to-LAN connection. An $Originate-Only connection may have multiple passe specified below.$ |
| | 30.30.30.1 Peen | Enter the remote peer IP addresses for this LAN-to-LAN connection. Originate- Days connection may specify up to tan peer IP addresses. Eater one IP address per line. |
| | Digital Certificate None (Use Preshared Keyr | Solart the digital contificate to use. |
| - stantoring | Certificate C Entire certificate chain. Transmission © Identity certificate only | Choose how to send the digital certificate to the DCE peer. |
| | Preshared Key cisco123 | Enter the possbared key for this LAN-to-LAN connection. |
| | Authentication ESP/MD5/HMAC-128 - | Specify the packet authentication mechanism to use. |
| CISCO SYSTEMS | Encryption AES-256 💌 | Specify the encryption mechanism to use. |
| | IKE Proposal KE-AES256-SHA 💌 | Select the IKE Proposal to use for this LAN-to-LAN econection. |

| - Denfiguration Interfaces - Devices | | |
|--|---|--|
| - E-Servers | | |
| | | |
| E-Tunneling Protocols | | |
| Pette | | Change the filterate combines the meffle that is translad through this [). If its [) its |
| | Filter -None- | capital in an in the second seco |
| EUDSer. | | DOBRECIDO. |
| | | Check to let NAT-T compatible IPSec peers establish this LAN-to-LAN |
| Longeton | IPSer NAT-T | reamentiza, theough a NAT device. You must also enable IPSec over NAT-T under |
| HE Proposals | | NAT Transparency. |
| NAT Transporency | Bandwidth Policy | Danage the keeping of a noticy to couly to this 1 AN-to-1 AN conception |
| Alerta | 14010 | come or construction band or abbill or one random state or other state |
| - E-P Routing | Boutine Mano | Choose the routing mechanism to use Parameters below are ignored if Network |
| El-Management Protocols | interior interior | Autodiscovery is chosen. |
| - Events | | |
| - E-General | Local Neinark: If a LAN-to-LAN NAT rule is used, this is the Translat | ted Natwork address. |
| -E-Client Update | | Provide the free wetweet address list or the 10 address and wildered used. On this |
| Load Balancing | Network List Vpn_local_network | Specify the local intervent datases lat of the re-annex data whether must for this |
| | | Lon-to-Lon volustica. |
| T-Policy Management | IP Address | |
| topage House | - | Note: Enter a wildcard mask, which is the ownerse of a subast mask. A |
| Fi Tendio Management | Wildcard Mask | wikinged mesks has 1s in bit positions to ignore, Us in bit positions to realth. For |
| | | szaruple, 10.10.1.000.0.0.255 = all 10.10.1 mm addresses. |
| - E-Group Matching | | |
| | Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remo | te Network address. |
| - 3 Monitoring | | I Specify the proste returnsk address list or the IP address and uddress mask for |
| | Network List Vpn_remote_network | this LAN-to-LAN concertion. |
| | | |
| | IP Address | N. N |
| | | Note: Enter a minimum mask, which is the private of a submet mask. A |
| | Wildcard Mask | wildcard mask has is in bit positions to gnote, is in bit positions to match. For |
| 0 | | enrepie, 10.10.1.00.0.0.255 = all 10.10.1 faith alleresses. |
| CISCO SISTEMS | Add Coorel | |
| du du | | |
| ومتل التبيين اللتي | | |

7. Dopo aver fatto clic su Add, se la connessione è corretta, viene visualizzata la finestra IPSec LAN-to-LAN-Add-Done.In questa finestra viene presentata una sintesi delle informazioni di configurazione del tunnel. Vengono inoltre configurati automaticamente il Nome gruppo, il Nome associazione di protezione e il Nome filtro. È possibile modificare qualsiasi parametro di questa

| tabella. | |
|---------------------------|---|
| Configuration | |
| | Configuration System Tunneling Protocols IPSec LAN to LAN Add Done |
| - Constant | Save Needed |
| - I Servers | |
| - (T) Acidress Management | An IPSec LAN-to-LAN connection has been successfully configured. The following have been added to your configuration: |
| Tunneting Protocols | |
| | Authentication Server Internal |
| | Genue 30 30 30 1 |
| L CALLON L AND | Repurity Association 1.7 - for |
| ICE Bronowair | |
| NAT Transportney | Filter Rules L2L test Out |
| -Verts | |
| - CHP Routing | Modificies one of loss tone will effect the LOM to LEM conference. The Grammin Telescore as using LEM build Misses. The Recentler Accessication and |
| - GIManagement Protocols | where all start with "124" in information that the Links for a LANA start should be start as your interview part. The information and |
| - CEventa | |
| - Gl-General | or l |
| - Client Update | |
| Load Balancing | |
| | |
| LetPolicy Management | |
| | |
| (4)-Monitoring | |

A questo punto, è stato configurato il tunnel IPsec LAN-LAN e si può iniziare a lavorare. Se per qualche motivo il tunnel non funziona, è possibile verificare la presenza di configurazioni errate.

 Per visualizzare o modificare i parametri IPsec da LAN a LAN creati in precedenza, selezionare Configurazione > Sistema > Protocolli di tunneling > IPSec da LAN a LAN.L'immagine mostra "test" come nome del tunnel e l'interfaccia pubblica dell'estremità remota è 30.30.30.1 come nell'esempio.

| - Configuration | | |
|------------------------|---|---|
| | Configuration System Tunneling Protocols IPSec LAN-to-LAN | |
| -G-System | | Save |
| - @Servers | | |
| | This section late unu configure IESsc LAN-to-LAN connections LAN-to-LAN connections are set | shlished with other VPN 3000 Concentrators |
| | PIX firewalls, 7100/4000 series conters and other IPSec-compliant security gateways. To configure | a VPN 3002 or other remote access |
| EPTP | connection, go to User Management and configure a Group and User. To configure NAT over LAN | -to-LAN, go to LAN-to-LAN NAT Rules. |
| L2TP | | |
| - EHESee | If you want to define a set of actworks on the local or remote side of the LAN-to-LAN connection. | configure the necessary Network Lists prior |
| LAN-to-LAN | to creating the connection. | |
| IKE Proposals | | |
| | Click the Add button to add a LAN-to-LAN connection, or select a connection and click Modify or | Delete. |
| -FIP Bruting | | |
| - Management Protocols | (D) indicates a disabled LAN-to-LAN connection. | |
| - (Events | | |
| - @ General | LAN-to-LAN | |
| - I Client Update | Connection | Actions |
| Load Balancing | test (30.30.30.1) on Ethernet 2 (Public) | |
| | | 4 -1-1 |
| - GEolicy Management | | Add |
| Access Hours | | Modiky |
| - Tratfic Management | | mouny |
| Network Lists | | Delete |
| Hules | | |
| - Char | | |
| TINAT | | |
| ENV Policies | | |
| FFGroup Metching | | |
| Administration | | |
| - Monitoring | | |
| | | |

 9. In alcuni casi, il tunnel potrebbe non essere disponibile se la proposta IKE è inclusa nell'elenco Proposte inattive. Selezionare Configurazione > Sistema > Protocolli di tunneling > IPSec > Proposte IKE per configurare la proposta IKE attiva.Se la proposta IKE è inclusa

nell'elenco "Proposte inattive", è possibile abilitarla selezionando la proposta IKE e facendo clic sul pulsante **Attiva**. In questo grafico la proposta selezionata "IKE-AES256-SHA" è inclusa nell'elenco Proposte

| allive. | | | | | |
|--------------------------|--|---|---------------------------------|--------|--|
| -p- <u>Configuration</u> | | | | | |
| | Configuration System Tunneling Protoco | ls IPSec IKE Propos | als | | |
| | | | | Save 📊 | |
| Servers | | | | | |
| - C-Address Management | Add, delete, prioritize, and configure IKE Proposals. | | | | |
| | | | | | |
| <u>PPTP</u> | Select an Inactive Proposal and click Artivate to make it | ect as Inactive Proposal and click Artivate to make it Artive, or click Modify. Copy or Delete as antoportate, | | | |
| | ect as Artive Proposal and click Deactivate to make it Inartive, or click Move Up or Move Down to change its priceity. | | | | |
| | Click Add or Copy to add a new Inactive Proposal. IKE | lick Add or Copy to add a new Inactive Proposal. IKE Proposals are used by Security Associations to specify IKE parameters. | | | |
| LAN-TO-LAN | | | | | |
| NE Projections | Active | | Inactive | | |
| Alerte | Proposals | Actions | Proposals | | |
| Cill Parties | CiscoVPNClipst-3DES-MD5 | 1 | IKE-IDES-SHA-DSA | | |
| CI-Management Evolution | IKE-3DES-MD5 | << Activate | IKE-1DES-MD5-BSA-DH1 | | |
| - TEPvento | IKE-3DES-MD5-DH1 | 0 | IKE-DES-MD5-DH7 | | |
| - (#General | IKE-DES-MD5 | Deactivele >> | CiscoVPNClient-3DES-MD5-BSA | | |
| -rit-Client Lodate | IKE-3DES-MD5-DH7 | Mauel In | CiscoVPNClient-3DES-SHA-DSA | | |
| Load Balancing | CiscoVPNClient3DES-MD5-DH5 | MOVE OP | CiscoVPNClient-3DES-MD5-RSA-DH5 | | |
| - E-User Management | CiscoVPNClient-AES128-SHA | Move Down | CiscoVPNClient-3DES-SHA-DSA-DH5 | | |
| - E-Policy Management | IKE-AES128-SHA | | CiscoVPNClient-AES256-SHA | | |
| - Administration | IKE-3DES-MD5-RSA | Add | | | |
| • Monitoring | KE-AES255-SHA | 1. f = 116 - | | | |
| | | Madity | | | |
| | | Conv | | | |
| | | | | | |
| | | Delete | | | |
| | | | I | | |

 Selezionare Configurazione > Gestione criteri > Gestione traffico > Associazioni di sicurezza per verificare se i parametri SA sono corretti.

| 다. 다. Configuration | | | | |
|------------------------------|---|------------------|---|-----|
| | Configuration Policy Management Traffic Manageme | ent Security | ty Associations | |
| - Gyzlen | | | Sav | 6 🗖 |
| - ErServers | | | | |
| - EB-Address Management | This section lats you add, configure, modify, and delete IPSec Security I | Associations (SA | As). Security Associations use <u>IKE Proposals</u> to negotiate IK | E |
| | parameters. | | · / · · · | |
| - PPTP | - | | | |
| LZTP | Click Add to add an SA, or select an SA and click Modify or Delete | | | |
| PPSec | contrast to see at this of control and the set of the set of the set | | | |
| LAN-to-LAN | me | | 4-4 | |
| KE Proposals | LPSec SA | 8 | 70019 | |
| NAT Transparency | ESP-3DES-MD5 | | | |
| <u>Alerts</u> | ESP-3DES-MD5-0 | DH5 | | |
| - EIP Routing | ESP-3DES-MD5-1 | DH7 | | |
| EHManagement Protocols | ESP-3DES-NONE | E I | Add | |
| - EV <u>Events</u> | ESP-AES128-SH/ | A I | Mada | |
| - E General | ESP-DES-MD5 | | Modily. | |
| Client Update | ESP4_2TP-TRAN | ISPORT | Delete | |
| Load Balancing | ESP/KE-3DES-M | 105 | 00100 | |
| - ER <u>liser Manacement</u> | L2L: test | | | |
| Policy Management | | | | |
| Access Hours | | | | |
| -EFiraffic Management | | | | |
| Metwork Lista | | | | |
| - Bulica | | | | |
| | | | | |
| <u>Filters</u> | | | | |
| - E-NAT | | | | |
| BW Policies | | | | |
| ElGroup Matching | | | | |
| - Administration | | | | |
| Monitoring | | | | |
| | | | | |

11. Fare clic sul nome dell'associazione di protezione (in questo caso, L2L: test) e quindi fare clic su Modifica per verificare le associazioni di protezione.Se uno dei parametri non corrisponde alla configurazione peer remota, è possibile modificarlo qui

| qui. | | |
|---|---|--|
| Configuration | Configuration Policy Management Traffic Manage | ement Security Associations Modify |
| | Modify a configured Security Association. | |
| | SA Name L2L: test Inheritance From Rule | Specify the name of this Security Association (SA). Select the granularity of this SA. |
| CHPSec CAN-ID-LAN HOL Promosels NAT Transporency | IPSec Parameters Authentication Algorithm ESP/MD5/HMAC-128 | Select the peaket authentication algorithm to use. |
| <u>Alerts</u> | Encryption Algorithm AES-256 | Select the ESP encryption algorithm to use. |
| El-Management Protocols | Encapsulation Mode Tunnel | Select the Encapsulation Mode for this SA. |
| - Erents - Er-General - Er-Clarit Lindale | Perfect Ferreard Secrecy Disabled | Select the use of Perfect Forward Secury. |
| Load Balancing | Lifetime Time | Select the lifetime measurement of the IPSec keys. |
| - (Huser Management | Data Lifetime 10000 | Scrarific the data lifetime in hilderiter (ICD) |
| - Access Hours - D'Instite Management | Time Lifetime 28800 | Specify the time lifetime in seconds. |
| Bules | IKE Parameters | |
| Elters | Connection Type Historetional IKE Process 31 31 31 1 | The Connection Type and IKE Peers cannot be modified on IFSe: SA that is part of a LAN-to-LAN Connection. |
| - GALAT - GALPolicies | Negatiation Mode Main | Select the IKE Negotiation mode to use |
| -E-Group Matching -E-Administration | Digital Certificate None (Use Preshared Keys) 💌 | Select the Digital Certificate to use. |
| - Monitoring | Certificate C Entire certificate chain. Transmission © Identity certificate only | Chooses how to send the digital cartificate to the IKE press. |
| | IKE Proposal IKE-AES256-SHA | Select the IKE Proposal to use as IKE isitiator. |
| Cisco Systems | Apply Concel | |

Verifica

Verifica della configurazione del router

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Alcuni comandi show sono supportati dallo strumento Output Interpreter (solo utenti registrati); lo strumento permette di visualizzare un'analisi dell'output del comando show.

 show crypto isakmp sa: visualizza tutte le SA IKE correnti in un peer. Lo stato QM_IDLE indica che l'associazione di sicurezza rimane autenticata con il peer e può essere utilizzata per successivi scambi in modalità rapida. È in uno stato silenzioso.
 ipsec_router#show crypto isakmp sa

```
dst src state conn-id slot
20.20.20.1 30.30.30.1 QM_IDLE 1 0
```

 show crypto ipsec sa: visualizza le impostazioni utilizzate dalle associazioni di protezione correnti. Verificare gli indirizzi IP dei peer, le reti accessibili sia a livello locale che remoto e il set di trasformazioni utilizzato. Esistono due associazioni di protezione ESP, una per ogni direzione. Poiché vengono utilizzati set di trasformazioni AH, è vuoto.
 ipsec_router#show crypto ipsec sa

```
interface: Ethernet1/0
```

Crypto map tag: vpn, local addr. 30.30.30.1

protected vrf:

local ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (172.16.0.0/255.255.0.0/0/0)

current_peer: 20.20.20.1:500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 145, #pkts encrypt: 145, #pkts digest 145

#pkts decaps: 51, #pkts decrypt: 51, #pkts verify 51

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 6, #recv errors 0

local crypto endpt.: 30.30.30.1, remote crypto endpt.: 20.20.20.1

path mtu 1500, media mtu 1500

current outbound spi: 54FA9805

inbound esp sas:

spi: 0x4091292(67703442)

transform: esp-256-aes esp-md5-hmac ,

in use settings ={Tunnel, }

slot: 0, conn id: 2000, flow_id: 1, crypto map: vpn

sa timing: remaining key lifetime (k/sec): (4471883/28110)

```
IV size: 16 bytes
replay detection support: Y
inbound ah sas:
inbound pcp sas:
outbound esp sas:
spi: 0x54FA9805(1425709061)
transform: esp-256-aes esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2001, flow_id: 2, crypto map: vpn
sa timing: remaining key lifetime (k/sec): (4471883/28110)
IV size: 16 bytes
replay detection support: Y
outbound ah sas:
```

outbound pcp sas:

• **show crypto engine connections active**: visualizza le connessioni correnti attive alle sessioni crittografate per tutti i motori di crittografia. Ogni ID connessione è univoco. Il numero di pacchetti crittografati e decrittografati viene visualizzato nelle ultime due colonne.

| ID | Interface | IP-Address | State | Algorithm | Encrypt | Decrypt |
|------|-------------|------------|-------|--------------------|---------|---------|
| 1 | Ethernet1/0 | 30.30.30.1 | set | HMAC_SHA+AES_256_C | 0 | 0 |
| 2000 | Ethernet1/0 | 30.30.30.1 | set | HMAC_MD5+AES_256_C | 0 | 19 |
| 2001 | Ethernet1/0 | 30.30.30.1 | set | HMAC_MD5+AES_256_C | 19 | 0 |

Verifica della configurazione di VPN Concentrator

Completare questa procedura per verificare la configurazione di VPN Concentrator.

 Analogamente ai comandi show crypto ipsec sa e show crypto isakmp sa sui router, è possibile visualizzare le statistiche IPsec e IKE quando si seleziona Monitoraggio > Statistiche > IPSec sui concentratori VPN.

| -= Configuration | Monitoring Statistics IPSec Thursd | ay, U1 J. | anuary 2004-19:32:36 |
|--------------------------|--|-----------|----------------------|
| ElStaten . | | | Reset 🥔 Refresh 🔞 |
| -FiUser Management | IKE (Phase 1) Statistics IPSec (Phase 2) Statistics | | |
| Effolicy Management | Active Tunnels I Active Tunnels | 1 | |
| Access Hours | Total Tunnels 2 Total Tunnels | 2 | |
| Network Lists | Received Bytes 5545268 Received Bytes | 3608 | |
| Bulez | Sent Bytes 5553204 Sent Bytes | 5376 | |
| <u></u> | Received Packets 60187 Received Packets | 145 | |
| Eitera John T | Sent Packets 60299 Sent Packets | 51 | |
| BAY Policies | Received Parkets Dropped 0 Received Parkets Dropped | 0 | |
| Group Matching | Sent Parkets Dropped 0 Received Parkets Dropped (Anti-Rep | ay) 0 | |
| G Administration | Received Notifies 60084 Sent Packets Dropped | 0 | |
| ErSoftware Undate | Sent Notifies 120172 Inhound Authentirations | 145 | |
| Concentrator | Received Phase-2 Eachanges 2 Failed Inbound Authentications | 0 | |
| Clients | Sent Phase-2 Exchanges 49 Outbound Authentications | SL | |
| Reboot Status | Invalid Phase-2 Exchanges Received D Failed Outbound Authentications | 0 | |
| Elba | Invalid Phase 2 Exchanges Sent 0 Decryptions | 145 | |
| Monitoring Refresh | Rejected Received Phase-2 Exchanges 0 Failed Decryptions | 0 | |
| EFF is Management | Rejected Sent Please-2 Exchanges 0 Encryptions | 51 | |
| Swap Confio File | Phase-2 SA Delete Requests Received 0 Failed Encryptions | 0 | |
| <u>TFTP_Tranzler</u> | Phase-2 SA Delete Requests Sent 30 System Capability Failures | 0 | |
| XML Export | Initiated Tunnels 0 No. SA Failures | 0 | |
| EPCertificate Management | Failed initiated Tunnels 0 Protorol Use Failures | 0 | |
| Enrollment | Failed Benuite Tunnels 0 | | , |
| | Authentication Failures 0 | | |
| -Routing Table | Decryption Failures 0 | | |
| Dynamic Filters | Hash Validation Failures 0 | | |
| Cisco Systems | System Capability Failures 0 | | |
| adhoadhoa | No-SA Failures 0 | | |

2. Analogamente al comando **show crypto engine connections active** sui router, è possibile utilizzare la finestra Administration-Sessions su VPN Concentrator per visualizzare i parametri e le statistiche di tutte le connessioni o i tunnel IPsec LAN a LAN attivi.

| attivit | | | | | | | | | | |
|---|---|--|--|--|--------------------------------------|--|---------------------------------|--|--|--|
| Configuration Interfaces Extern Extern Constraint Constraint | Administration Ad This screen shows statis on that essector's name. T Group [-All- Legour All: <u>PPTP User</u> | indusister Sessions. too for sessions. To log out a session 1277F User DS | sions To refiech the m, click Lege r <u>lec User</u> <u>T</u> Se | statistics, clic rt in the table c LAN-to-LA | ik Refresh below. To t | Select a Group t est the activation | a filter the se camection to | Thursday ssions Form a session, cliv | , 01 Janu Re ore informe 's Ping, | any 2004–19430-200 eset 🥜 Refresh 🕲 ticu on a sessicu, click |
| Group Matching | Active LAN-to- LAN Sessions | Active Remot Access Session | e Active IS S | Management essions | Total A Sessi | artive Peak (ous Se | Concurrent ssions | Concur Sessions | tent 1 Limit | fotal Cumulative Sessions |
| Arithin inter Sessions | 1 | 0 | | 1 | 2 | | 3 | 4000 |) | 19 |
| Contentiatie | | | | | | angement Sessions] | | | | |
| | Connection Name | IP Address | Protoco | d E | aryption | Logia Tinos | Duration | Bytes Tx | Bytes Rx | Actions |
| -Ping | test | 30.30.30.1 | IPSec/LAN-t | o-LAN 8 | ES-256 | Jan 1 19:57:29 | 0:02:51 | 2128 | 2128 | [Logent Ping] |
| Monitorine Setreati Bis <u>Access Matter</u> Offic Management Officiale Management (Hentinate Management) | Remaie Access Sess | iions Assigned IP Add Public IP Add | dress ress | Googe No S | Protocol Encryption Cemole Acc | Login Tr Durati 155 Sessions | ine Q | N-to-LAN Se lient Type Version | smons Mu Dytes Dytes | nagement Sessions) Tx Rx Artions |
| | Management Sessio | AS | | | | | [LAN- | to-LAN See | ione Remo | ta Accese Sessione] |
| | Administrator | IP Addre | ss Pro | ncol I | nryption | Legia | Time | Duration | h | Artions |
| | admin. | 172.161.1 | HTTP | Non | 8 | Jan.01 19:17 | 42 | 0:12:38 | [Logs | ot Ping] |
| | - | | | | | | | | 112 | |

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Risoluzione dei problemi del router

Lo <u>strumento Output Interpreter</u> (solo utenti <u>registrati</u>) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Nota: consultare le <u>informazioni importanti sui comandi di debug</u> prima di usare i comandi di **debug**.

- debug crypto engine: visualizza il traffico crittografato. Il motore di crittografia è il meccanismo che esegue la crittografia e la decrittografia. Un motore di crittografia può essere un acceleratore software o hardware.
- **debug crypto isakmp**: visualizza le negoziazioni ISAKMP (Internet Security Association and Key Management Protocol) della fase 1 di IKE.
- debug crypto ipsec: visualizza le negoziazioni IPsec di IKE fase 2.

Per informazioni più dettagliate e un output di esempio, fare riferimento a <u>Risoluzione dei problemi</u> <u>di IPSec - Comprensione e uso dei comandi di **debug**.</u>

Risoluzione dei problemi di VPN Concentrator

Analogamente ai comandi **debug** sui router Cisco, è possibile configurare le classi Event per visualizzare tutti gli allarmi.

 Selezionare Configurazione > Sistema > Eventi > Classi > Aggiungi per attivare la registrazione delle classi di evento.Le classi seguenti sono disponibili per IPSec:IKEIKEDBGCODICE

IKEDECODEIPSECIPSECDBGCODICEIPSEC

| Configuration | | | | |
|------------------------------|--|--|--|--|
| | Configuration System Events Classes | | | |
| | Save Needed | | | |
| -EX <u>Servers</u> | | | | |
| E)Address Monogement | This section lets you configure special handling of specific event classes. | | | |
| E <u>Tunnelina Protocots</u> | | | | |
| EHP Routine | Click far Add button to odd as event class, or select as event class and thick Modiffy or Defects. | | | |
| E Management Protocols | | | | |
| -DEvents | Click here to configure superal event parameters. | | | |
| General | | | | |
| ETP Beckup | Configurad | | | |
| | Perint Classes Actions | | | |
| Service Services | | | | |
| GMED Cacava | IKEDECODE | | | |
| Engl Recipiento | PECUBIC | | | |
| - ElGeneral | MB2TRAP Add | | | |
| -FiCient Undate | | | | |
| Load Balancing | Modily | | | |
| - (7) User Management | | | | |
| -GHPolicy Management | Detete | | | |
| Administration | | | | |
| ##Monitoring | | | | |
| | | | | |

2. Durante l'aggiunta, è inoltre possibile selezionare il livello di gravità per ogni classe, in base al livello di gravità inviato dall'allarme.Gli allarmi possono essere gestiti usando uno dei seguenti metodi:Per registroVisualizzato sulla consoleInviato al server Syslog UNIXInviato come messaggio di posta elettronicaInviato come trap a un server SNMP (Simple Network Management Protocol)

| -E-Configuration | | | | | | |
|--|---|--|--|--|--|--|
| | Configuration System Events Classes Add | | | | | |
| - DSystem | | | | | | |
| - EFGenvers | This screen lets you add and configure an event class for special handling. | | | | | |
| Address Management | | | | | | |
| Tunneling Protocols | Class Name KEDDC | Estat the sumst sizes to confirm | | | | |
| - EHP Routing | Class Hane NEDBG | Select the event class to cooligure. | | | | |
| | Enable 🖂 | Check to enable special handling of this class. | | | | |
| - P <u>events</u> | | | | | | |
| General | Hone of the following values has been out to Hug | Event List the Event List can be easn by viewing Configuration 1 System Events General | | | | |
| FTP Backup | a site of the reasoning range the control to our prior and, an area of the reasoning range and a prior in the reasoning range and a | | | | | |
| <u></u> | Changing a value set to Use Svent List will override the sections of the Event List referring to this event class. | | | | | |
| Irao Destinations | Transfer Lee Course Street C | 1 Standa mutata ministratura | | | | |
| System Servers | Figure to Fog Seventies 1-2 | Select the events to enter in the log. | | | | |
| SMIP Servers | Events to Consols Severities 1-3 | Select the events to display on the consols. | | | | |
| | | | | | | |
| The Section Se | Events to Syslog None | Select the events to send to a Syslog Server. | | | | |
| i cad Galapabay | Events to Email None | Select the events to send to an Ersail Registerit. | | | | |
| Thilling Versenant | 11010 | | | | | |
| EDolou Management | Events to Trap None 💌 | Select the events to send to an SNMP Trap Destination. | | | | |
| El Administration | | | | | | |
| | Add Cancel | | | | | |
| La <u>montante da la</u> | | | | | | |

3. Selezionare Monitoraggio > Registro eventi filtrabile per monitorare gli allarmi



Informazioni correlate

- Advanced Encryption Standard (AES)
- DES/3DES/AES VPN Encryption Module
- <u>Configurazioni di esempio IPSec</u>
- <u>Cisco VPN serie 3000 Client Support Page</u>
- Pagina di supporto per la negoziazione IPSec/i protocolli IKE

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).