Configurazione iniziale di Cisco VPN 5000 Concentrator per l'accesso client remoto

Sommario

Introduzione

Questa guida spiega la configurazione iniziale di Cisco VPN 5000 Concentrator, in particolare come configurarlo per connettersi alla rete tramite IP e offrire connettività client remota.

Èpossibile installare il concentratore in una di due configurazioni, a seconda della connessione alla rete in relazione a un firewall. Il concentratore dispone di due porte Ethernet, una delle quali (Ethernet 1) passa solo il traffico IPSec. L'altra porta (Ethernet 0) instrada tutto il traffico IP. Se si intende installare VPN Concentrator in parallelo con il firewall, è necessario utilizzare entrambe le porte in modo che Ethernet 0 sia rivolto alla LAN protetta e Ethernet 1 sia rivolto a Internet tramite il router gateway Internet della rete. È inoltre possibile installare il concentratore dietro il firewall nella LAN protetta e collegarlo tramite la porta Ethernet 0, in modo che il traffico IPSec che passa da Internet al concentratore passi attraverso il firewall.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Per la stesura del documento, è stato usato Cisco VPN 5000 Concentrator.

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.

Configurazione connettività di base

Il modo più semplice per stabilire la connettività di rete di base è collegare un cavo seriale alla porta console sul concentratore e usare il software del terminale per configurare l'indirizzo IP sulla porta Ethernet 0. Dopo aver configurato l'indirizzo IP sulla porta Ethernet 0, è possibile utilizzare Telnet per connettersi al concentratore e completare la configurazione. Potete anche generare un file di configurazione in un editor di testo appropriato e inviarlo al concentratore utilizzando il protocollo TFTP.

Se si utilizza un software terminale attraverso la porta console, inizialmente viene richiesto di immettere una password. Utilizzare la password "letmein". Dopo aver risposto con la password, usare il comando **configure ip Ethernet 0**, rispondendo alle richieste con le informazioni di sistema. La sequenza dei prompt dovrebbe essere simile alla seguente:

```
*[ IP Ethernet 0 ]# configure ip ethernet 0
      Section 'ip ethernet 0' not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
      <Keyword> = <Value>
      To find a list of valid keywords and additional help enter "?"
      *[ IP Ethernet 0 ]# ipaddress=192.168.233.1
      *[ IP Ethernet 0 ]# subnetmask=255.255.255.0
      *[ IP Ethernet 0 ]# ipbroadcast=192.168.233.255
      *[ IP Ethernet 0 ]# mode=routed
      *[ IP Ethernet 0 ]#
```

A questo punto è possibile configurare la porta Ethernet 1.

Ethernet 1 porta

Le informazioni relative all'indirizzo TCP/IP sulla porta Ethernet 1 sono l'indirizzo TCP/IP esterno con routing a Internet assegnato al concentratore. Evitare di utilizzare un indirizzo nella stessa rete TCP/IP di Ethernet 0, in quanto ciò disabiliterà TCP/IP nel concentratore VPN.

Immettere i comandi **configure ip ethernet 1**, rispondendo alle richieste con le informazioni di sistema. La sequenza dei prompt dovrebbe essere simile alla seguente:

```
*[ IP Ethernet 0 ]# configure ip ethernet 1
      Section 'ip ethernet 1' not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
      <Keyword> = <Value>
      To find a list of valid keywords and additional help enter "?"
```

```
*[ IP Ethernet 1 ]# ipaddress=206.45.55.1
*[ IP Ethernet 1 ]# subnetmask=255.255.255.0
*[ IP Ethernet 1 ]# ipbroadcast=206.45.55.255
*[ IP Ethernet 1 ]# mode=routed
*[ IP Ethernet 1 ]#
```

A questo punto è necessario configurare il percorso predefinito.

Route predefinita

Ènecessario configurare una route predefinita che il concentratore possa utilizzare per inviare tutto il traffico TCP/IP destinato a reti diverse da quelle a cui è direttamente connesso o per le quali dispone di route dinamiche. Il percorso predefinito punta indietro a tutte le reti trovate sulla porta interna. In seguito, si configurerà Intraport per inviare traffico IPSec da e verso Internet utilizzando il parametro Gateway IPSec. Per avviare la configurazione predefinita del percorso, immettere il comando edit config ip static in risposta alle richieste con le informazioni di sistema. La sequenza dei prompt dovrebbe essere simile alla seguente:

```
*IntraPort2+_A56CB700# edit config ip static
      Section 'ip static' not found in the config.
      Do you want to add it to the config? y
      Configuration lines in this section have the following format:
      <Destination> <Mask> <Gateway> <Metric> [<Redist=(RIP|none)>]
      Editing "[ IP Static ]"...
      1: [ IP Static ]
      End of buffer
      Edit [ IP Static ]> append 1
      Enter lines at the prompt. To terminate input, enter
      a . on a line all by itself.
      Append> 0.0.0.0 0.0.0.0 192.168.233.2 1
      Append> .
      Edit [ IP Static ]> exit
      Saving section...
      Checking syntax...
      Section checked successfully.
      *IntraPort2+_A56CB700#
```

A questo punto è necessario configurare il gateway IPSec.

Gateway IPSec

Il gateway IPSec controlla il punto in cui il concentratore invia tutto il traffico IPSec, o tunneling. Questa opzione è indipendente dalla route predefinita appena configurata. Iniziare immettendo il comando **configure general**, rispondendo ai prompt con le informazioni di sistema. La sequenza dei prompt dovrebbe essere simile alla seguente:

```
* IntraPort2+_A56CB700#configure general
      Section 'general' not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
       =
      To find a list of valid keywords and additional help enter "?"
      *[ General ]# ipsecgateway=206.45.55.2
      *[ General ]# exit
      Leaving section editor.
      * IntraPort2+_A56CB700#
```

Configurare quindi il criterio IKE.

Criteri IKE

Impostare i parametri ISAKMP/IKE (Internet Security Association Key Management Protocol/Internet Key Exchange) per il concentratore. Queste impostazioni controllano il modo in cui il concentratore e il client si identificano e si autenticano a vicenda per stabilire sessioni tunnel. Questa negoziazione iniziale è denominata Fase 1. I parametri della Fase 1 sono globali per il dispositivo e non sono associati a una particolare interfaccia. Di seguito sono descritte le parole chiave riconosciute in questa sezione. I parametri di negoziazione della fase 1 per i tunnel da LAN a LAN possono essere impostati nella sezione [Tunnel Partner<Section ID>].

La negoziazione IKE fase 2 controlla il modo in cui il concentratore VPN e il client gestiscono le singole sessioni del tunnel. I parametri di negoziazione IKE fase 2 per il concentratore VPN e il client sono impostati nel dispositivo [VPN Group <Nome>]

La sintassi per i criteri IKE è la seguente:

```
Protection = [ MD5_DES_G1 | MD5_DES_G2 | SHA_DES_G1 | SHA_DES_G2 ]
```

La parola chiave protection specifica una suite di protezione per la negoziazione ISAKMP/IKE tra il concentratore VPN e il client. Questa parola chiave può apparire più volte in questa sezione, nel qual caso il concentratore propone tutte le suite di protezione specificate. Il client accetta una delle opzioni per la negoziazione. La prima parte di ciascuna opzione, MD-5 (message-digest 5), è l'algoritmo di autenticazione utilizzato per la negoziazione. SHA è l'acronimo di Secure Hash Algorithm, considerato più sicuro di MD5. Il secondo elemento di ciascuna opzione è l'algoritmo di crittografia. DES (Data Encryption Standard) utilizza una chiave a 56 bit per codificare i dati. Il terzo elemento di ciascuna opzione è il gruppo Diffie-Hellman, utilizzato per lo scambio di chiavi. Poiché i numeri maggiori vengono utilizzati dall'algoritmo Gruppo 2 (G2), questo risulta più sicuro rispetto al Gruppo 1 (G1).

Per avviare la configurazione, immettere il comando **configure IKE policy**, in risposta alle richieste con le informazioni di sistema.

```
* IntraPort2+_A56CB700# configure IKE policy
      Section 'IKE Policy' was not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
      <Keyword> = <Value>
      To find a list of valid keywords and additional help enter "?"
      *[ IKE Policy ] Protection = MD5_DES_G1
      *[ IKE Policy ] exit
      Leaving section editor.
      * IntraPort2+_A56CB700#
```

Dopo aver configurato le nozioni di base, immettere i parametri di gruppo.

Configurazione gruppo VPN

Quando si immettono i parametri di gruppo, tenere presente che il nome del gruppo VPN non deve contenere spazi, anche se il parser della riga di comando consente di immettere spazi nel nome del gruppo VPN. Il nome del gruppo VPN può contenere lettere, numeri, trattini e caratteri di sottolineatura.

In ciascun gruppo VPN per il funzionamento IP sono richiesti quattro parametri di base:

- Numero massimo di connessioni
- StartIPaddress or LocalIPNet
- Trasforma
- IPNet

Il parametro Maxconnections è il numero massimo di sessioni client simultanee consentite in questa particolare configurazione del gruppo VPN. Tenere presente questo numero, in quanto viene utilizzato insieme al parametro StartIPAddress o LocalIPNet.

VPN Concentrator assegna indirizzi IP ai client remoti in base a due schemi diversi, StartIPAddress e LocalIPNet. StartIPAddress assegna i numeri IP dalla subnet connessa a Ethernet 0 e i proxy-arp per i client connessi. LocalIPNet assegna i numeri IP ai client remoti da una subnet univoca ai client VPN e richiede che il resto della rete sia a conoscenza dell'esistenza della subnet VPN tramite il routing statico o dinamico. StartIPAddress semplifica la configurazione, ma può limitare le dimensioni dello spazio degli indirizzi. LocalIPNet offre una maggiore flessibilità di indirizzamento per gli utenti remoti, ma richiede una quantità leggermente maggiore di lavoro per configurare il routing necessario.

Per StartIPAddress, utilizzare il primo indirizzo IP assegnato a una sessione tunnel client in ingresso. In una configurazione di base, questo deve essere un indirizzo IP sulla rete TCP/IP interna (la stessa rete della porta Ethernet 0). Nell'esempio riportato di seguito, alla prima sessione client viene assegnato l'indirizzo 192.168.233.50, alla successiva sessione client simultanea viene assegnato 192.168.233.51 e così via. È stato assegnato un valore Maxconnections di 30, pertanto è necessario disporre di un blocco di 30 indirizzi IP inutilizzati (inclusi gli eventuali server DHCP) a partire da 192.168.233.50 fino a 192.168.233.79. Evitare di sovrapporre gli indirizzi IP utilizzati in configurazioni di gruppi VPN diverse.

LocalIPNet assegna indirizzi IP ai client remoti da una subnet che deve essere inutilizzata in un'altra posizione della LAN. Ad esempio, se si specifica il parametro "LocalIPNet=182.168.1.0/24" nella configurazione del gruppo VPN, il concentratore assegna gli indirizzi IP ai client a partire da 192.168.1.1. È quindi necessario assegnare "Maxconnections=254", in quanto il concentratore non tiene conto dei limiti della subnet quando assegna i numeri IP utilizzando LocalIPNet.

La parola chiave Transform specifica i tipi di protezione e gli algoritmi utilizzati dal concentratore per le sessioni client IKE. Le opzioni sono le seguenti:

```
Transform = [ ESP(SHA,DES) | ESP(SHA,3DES) | ESP(MD5,DES) | ESP(MD5,3DES)
 | ESP(MD5) | ESP(SHA) | AH(MD5) | AH(SHA) |AH(MD5)+ESP(DES) | AH(MD5)+ESP(3DES)
 | AH(SHA)+ESP(DES) | AH(SHA)+ESP(3DES) ]
```

Ogni opzione è un elemento di protezione che specifica i parametri di autenticazione e crittografia. Questa parola chiave può apparire più volte all'interno di questa sezione, nel qual caso il concentratore propone i pezzi di protezione specificati nell'ordine in cui sono analizzati, fino a quando non ne viene accettato uno dal client per l'uso durante la sessione. Nella maggior parte dei casi, è necessaria una sola parola chiave Transform.

ESP(SHA,DES), ESP(SHA,3DES), ESP(MD5,DES) ed ESP(MD5,3DES) denotano l'intestazione Encapsulating Security Payload (ESP) per crittografare e autenticare i pacchetti. DES (Data Encryption Standard) utilizza una chiave a 56 bit per codificare i dati. 3DES utilizza tre chiavi diverse e tre applicazioni dell'algoritmo DES per codificare i dati. MD5 è l'algoritmo hash message-digest 5 e SHA è l'algoritmo hash sicuro, considerato più sicuro di MD5.

ESP(MD5,DES) è l'impostazione predefinita ed è consigliata per la maggior parte delle

installazioni. ESP(MD5) ed ESP(SHA) utilizzano l'intestazione ESP per autenticare i pacchetti senza crittografia. AH(MD5) e AH(SHA) utilizzano l'intestazione AH (Authentication Header) per autenticare i pacchetti. AH(MD5)+ESP(DES), AH(MD5)+ESP(3DES), AH(SHA)+ESP(DES) e AH(SHA)+ESP(3DES) utilizzano l'intestazione di autenticazione per autenticare i pacchetti e l'intestazione ESP per crittografarli.

Nota: il software client Mac OS non supporta l'opzione AH. È necessario specificare almeno un'opzione ESP se si utilizza il software client Mac OS.

Il campo IPNet è importante in quanto consente di controllare la posizione dei client del concentratore. I valori immessi in questo campo determinano il traffico TCP/IP da sottoporre a tunneling o, più comunemente, la posizione in cui un client appartenente a questo gruppo VPN può passare sulla rete.

Cisco consiglia di configurare la rete interna (nell'esempio 192.168.233.0/24), in modo che tutto il traffico proveniente da un client diretto alla rete interna venga inviato attraverso il tunnel e quindi autenticato e crittografato (se si abilita la crittografia). In questo scenario, non viene tunneling di altro traffico; invece, viene indirizzato normalmente. È possibile inserire più voci, inclusi indirizzi singoli o host. Il formato è l'indirizzo (nell'esempio riportato l'indirizzo di rete 192.168.233.0) e quindi la maschera associata a tale indirizzo in bit (/24, che è una maschera di classe C).

Per avviare questa parte della configurazione, immettere il comando **configure VPN group basic-user**, quindi rispondere alle richieste con le informazioni di sistema. Di seguito è riportato un esempio dell'intera sequenza di configurazione:

```
*IntraPort2+_A56CB700# configure VPN group basic-user
      Section 'VPN Group basic-user' not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
      <Keyword> = <Value>
      To find a list of valid keywords and additional help enter "?"
      *[ VPN Group "basic-user" ]# startipaddress=192.168.233.50
                                   or
      *[ VPN Group "basic-user" ]# localipnet=192.168.234.0/24
      *[ VPN Group "basic-user" ]# maxconnections=30
      *[ VPN Group "basic-user" ]# Transform=ESP(SHA,DES)
      *[ VPN Group "basic-user" ]# ipnet=192.168.233.0/24
      *[ VPN Group "basic-user" ]# exit
      Leaving section editor.
      *IntraPort2_A51EB700#
```

Il passaggio successivo consiste nella definizione del database dell'utente.

Configurazione utente VPN

In questa sezione della configurazione si definisce il database degli utenti VPN. Ogni riga definisce un utente VPN insieme alla configurazione e alla password del gruppo VPN di tale utente. Le voci su più righe devono avere interruzioni di riga che terminano con una barra rovesciata. Le interruzioni di riga racchiuse tra virgolette doppie vengono tuttavia mantenute.

Quando un client VPN inizia una sessione tunnel, il nome utente del client viene trasmesso al dispositivo. Se il dispositivo rileva l'utente in questa sezione, utilizza le informazioni riportate nella voce per configurare il tunnel. È inoltre possibile utilizzare un server RADIUS per l'autenticazione degli utenti VPN. Se il dispositivo non trova il nome utente e non è stato configurato un server

RADIUS per eseguire l'autenticazione, la sessione del tunnel non verrà aperta e verrà restituito un errore al client.

Avviare la configurazione immettendo il comando **edit config VPN users**. Di seguito viene illustrato un esempio che aggiunge un utente denominato "User1" al gruppo VPN "basic-user".

```
*IntraPort2+_A56CB700# edit config VPN users
      Section 'VPN users' not found in the config.
      Do you want to add it to the config? y
      <Name> <Config> <SharedKey>
      Editing "[ VPN Users ]"...
      1: [ VPN Users ]
      End of buffer
      Edit [ VPN Users ]> append 1
      Enter lines at the prompt. To terminate input, enter
      a . on a line all by itself.
      Append> User1 Config="basic-user" SharedKey="Burnt"
      Append> .
      Edit [ VPN Users ]> exit
      Saving section...
      Checking syntax...
      Section checked successfully.
      *IntraPort2+_A56CB700#
```

SharedKey dell'utente è "Masterizzato". Per tutti questi valori di configurazione viene fatta distinzione tra maiuscole e minuscole. se si configura "User1", l'utente deve immettere "User1" nel software client. Se si immette "user1" viene visualizzato un messaggio di errore utente non valido o non autorizzato. È possibile continuare a immettere gli utenti invece di uscire dall'editor, ma è necessario immettere un punto per uscire dall'editor. In caso contrario, è possibile che vengano immesse voci non valide nella configurazione.

Completamento

L'ultimo passaggio consiste nel salvare la configurazione. Quando viene richiesto se si desidera scaricare la configurazione e riavviare il dispositivo, digitare y e premere Invio. Non spegnere il concentratore durante il processo di avvio. Una volta riavviato il concentratore, gli utenti possono connettersi utilizzando il software VPN Client del concentratore.

Per salvare la configurazione, immettere il comando **save**, come indicato di seguito:

```
*IntraPort2+_A56CB700# save
      Save configuration to flash and restart device? y
```

Se si è collegati al concentratore mediante Telnet, l'output precedente sarà visibile. Se si è connessi tramite una console, verrà visualizzato un output simile al seguente, solo molto più lungo. Alla fine di questo output, il concentratore restituisce "Hello Console..." e richiede una password. Questo è come sai che hai finito.

```
Codesize => 0 pfree => 462
      Updating Config variables...
      Adding section '[ General ]' to config
      Adding -- ConfiguredFrom = Command Line, from Console
      Adding -- ConfiguredOn = Timeserver not configured
      Adding -- DeviceType = IntraPort2
```

```
Adding -- SoftwareVersion = IntraPort2 V4.5
Adding -- EthernetAddress = 00:00:a5:6c:b7:00
Not starting command loop: restart in progress.
Rewriting Flash....
```

Informazioni correlate

- Cisco VPN serie 5000 concentrator: annuncio di fine vendita
- Pagina di supporto per Cisco VPN 5000 Concentrator
- Pagina di supporto per i client Cisco VPN 5000
- Pagina di supporto per IPsec
- Documentazione e supporto tecnico – Cisco Systems