Configurazione del concentratore Cisco VPN 5000 e implementazione della connettività VPN da LAN a LAN in modalità principale IPSec

Sommario

Introduzione

Questo documento spiega la configurazione iniziale di Cisco VPN 5000 Concentrator e mostra come connettersi alla rete utilizzando l'IP e come offrire la connettività VPN da LAN a LAN in modalità principale IPSec.

Èpossibile installare VPN Concentrator in una di due configurazioni, a seconda del punto di connessione alla rete in relazione a un firewall. VPN Concentrator ha 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 VPN 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

Non sono previsti prerequisiti specifici 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 VPN e utilizzare 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 a VPN Concentrator e completare la configurazione. È inoltre possibile generare un file di configurazione in un editor di testo appropriato e inviarlo al concentratore VPN 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 a quella dell'esempio 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.

Configurazione di Ethernet 1 Port

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

Immettere i comandi **configure ip ethernet 1**, rispondendo alle richieste con le informazioni di sistema. La sequenza dei prompt dovrebbe essere simile a quella dell'esempio 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 gateway IPSec.

Configurazione del gateway IPSec

Il gateway IPSec controlla la posizione in cui il concentratore VPN invia tutto il traffico IPSec, o tunneled. Questa opzione è indipendente dalla route predefinita che si configura in seguito. Iniziare immettendo il comando **configure general**, rispondendo ai prompt con le informazioni di sistema. La sequenza dei prompt dovrebbe essere simile a quella illustrata di seguito.

```
* 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#
```

Nota: nelle versioni 6.x e successive, il comando **ipsecgateway** è stato modificato in **vpngateway**.

A questo punto è necessario configurare il criterio IKE (Internet Key Exchange).

Configurazione del criterio IKE

I parametri ISAKMP (Internet Security Association Key Management Protocol)/IKE controllano il modo in cui il concentratore VPN 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 VPN gestiscono le singole sessioni del tunnel. I parametri di negoziazione IKE fase 2 per il concentratore VPN e il client VPN sono impostati nel dispositivo [VPN Group <Nome>].

La sintassi del criterio 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 VPN Concentrator e VPN Client. Questa parola chiave può essere visualizzata più volte all'interno di questa sezione, nel qual caso VPN Concentrator propone tutte le suite di protezione specificate. Il client VPN accetta una delle opzioni per la negoziazione. La prima parte di ciascuna opzione, MD5 (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. Di seguito è riportato un esempio.

```
* 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, è possibile definire i parametri di comunicazione IP e del tunnel.

Configurazione da sito a sito in modalità principale

Per configurare VPN Concentrator in modo da supportare le connessioni LAN a LAN, è necessario definire la configurazione del tunnel e i parametri di comunicazione IP da utilizzare nel tunnel. Questa operazione viene eseguita in due sezioni, la sezione [Tunnel Partner VPN x] e la sezione [IP VPN x]. Per ogni configurazione da sito a sito, le *x* definite in queste due sezioni devono corrispondere, in modo che la configurazione del tunnel sia associata correttamente alla configurazione del protocollo.

Esaminiamo in dettaglio ognuna di queste sezioni.

Sezione Configurazione del partner del tunnel

Nella sezione partner tunnel è necessario definire almeno gli otto parametri seguenti.

- Trasforma
- Partner
- Gestione chiavi
- ChiaveCondivisa
- Modalità
- Accesso locale
- Peer
- Associa a

Trasforma

La parola chiave Transform specifica i tipi di protezione e gli algoritmi utilizzati per le sessioni client IKE. Ogni opzione associata a questo parametro è una protezione che specifica i parametri di autenticazione e crittografia. Il parametro Transform può essere visualizzato più volte all'interno di questa sezione, nel qual caso VPN Concentrator propone le parti di protezione specificate nell'ordine in cui vengono analizzate, fino a quando non ne viene accettato l'utilizzo da parte del

client durante la sessione. Nella maggior parte dei casi, è necessaria una sola parola chiave Transform.

Le opzioni per la parola chiave Transform sono le seguenti.

```
[ 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) ]
```

ESP è l'acronimo di Encapsulating Security Payload, mentre AH è l'acronimo di Authentication Header. Entrambe queste intestazioni vengono utilizzate 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. SHA è l'algoritmo Secure Hash Algorithm, considerato più sicuro di MD5.

ESP(MD5,DES) è l'impostazione predefinita ed è consigliata per la maggior parte delle impostazioni. ESP(MD5) ed ESP(SHA) utilizzano ESP per autenticare i pacchetti (senza crittografia). AH(MD5) e AH(SHA) utilizzano AH per autenticare i pacchetti. AH(MD5)+ESP(DES), AH(MD5)+ESP(3DES), AH(SHA)+ESP(DES) e AH(SHA)+ESP(3DES) utilizzano AH per autenticare i pacchetti ed ESP per crittografarli.

Partner

La parola chiave Partner definisce l'indirizzo IP dell'altro terminatore di tunnel nella relazione del tunnel. Questo numero deve essere un indirizzo IP pubblico instradabile con il quale il concentratore VPN locale può creare una connessione IPSec.

Gestione chiavi

La parola chiave KeyManage definisce il modo in cui i due concentratori VPN in una relazione tunnel determinano il dispositivo che avvia il tunnel e il tipo di procedura di definizione del tunnel da seguire. Le opzioni disponibili sono Automatico, Avvio, Risposta e Manuale. È possibile usare le prime tre opzioni per configurare i tunnel IKE e la parola chiave Manual per configurare i tunnel a crittografia fissa. In questo documento non viene spiegato come configurare i tunnel a crittografia fissa. Auto specifica che il partner del tunnel può avviare e rispondere alle richieste di configurazione del tunnel. L'opzione Avvia specifica che il partner del tunnel invia solo richieste di configurazione del tunnel, ma non risponde. Rispondi specifica che il partner del tunnel deve rispondere alle richieste di installazione del tunnel, ma non le avvia mai.

ChiaveCondivisa

La parola chiave SharedKey viene utilizzata come segreto condiviso IKE. È necessario impostare lo stesso valore SharedKey su entrambi i partner del tunnel.

Modalità

La parola chiave Mode definisce il protocollo di negoziazione IKE. Poiché l'impostazione predefinita è Aggressivo, per impostare il concentratore VPN per la modalità di interoperabilità è necessario impostare la parola chiave Mode su Main.

Accesso locale

LocalAccess definisce i numeri IP a cui è possibile accedere tramite il tunnel, da una maschera host a una route predefinita. La parola chiave LocalProto definisce i numeri di protocollo IP a cui è possibile accedere tramite il tunnel, ad esempio ICMP(1), TCP(6), UDP(17) e così via. Se si desidera passare tutti i numeri IP, impostare LocalProto=0. LocalPort determina i numeri di porta che è possibile raggiungere tramite il tunnel. Sia LocalProto che LocalPort hanno come valore predefinito 0 o hanno accesso completo.

Peer

La parola chiave Peer specifica quali subnet vengono trovate attraverso un tunnel. PeerProto specifica i protocolli consentiti tramite l'endpoint del tunnel remoto e PeerPort imposta i numeri di porta a cui è possibile accedere all'altra estremità del tunnel.

Associa a

BindTo specifica quale porta Ethernet termina le connessioni da sito a sito. È consigliabile impostare sempre questo parametro su Ethernet 1, ad eccezione del caso in cui VPN Concentrator sia in esecuzione in modalità a porta singola.

Configurazione dei parametri

Per configurare questi parametri, immettere il comando **configure Tunnel Partner VPN 1** in risposta alle richieste con le informazioni di sistema.

La sequenza dei prompt dovrebbe essere simile a quella riportata nell'esempio seguente.

```
*IntraPort2+_A56CB700# configure Tunnel Partner VPN 1
      Section ?config Tunnel Partner VPN 1? 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 "?"
      *[ Tunnel Partner VPN 1 ]# transform=ESP(MD5,DES)
      *[ Tunnel Partner VPN 1 ]# sharedkey=letmein
      *[ Tunnel Partner VPN 1 ]# partner=208.203.136.10
      *[ Tunnel Partner VPN 1 ]# mode=main
      *[ Tunnel Partner VPN 1 ]# peer=10.0.0.0/8
      *[ Tunnel Partner VPN 1 ]# localaccess=192.168.233.0/24
      *[ Tunnel Partner VPN 1 ]# bindto=Ethernet 1
      *[ Tunnel Partner VPN 1 ]# exit
      Leaving section editor.
```

A questo punto è necessario configurare la sezione IP.

Configurazione della sezione IP

Èpossibile utilizzare connessioni numerate o senza numero (come nella configurazione IP su connessioni WAN) nella sezione di configurazione IP di ciascuna relazione tunnel. Qui abbiamo usato numeri senza numeri.

La configurazione minima per una connessione da sito a sito senza numero richiede due istruzioni: numeroed=false e mode=routed. Iniziare immettendo i comandi **configure ip vpn 1** e rispondere ai prompt del sistema come segue.

```
*[ IP Ethernet 0 ]# configure ip vpn 1
      Section ?IP VPN 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 VPN 1 ]# mode=routed
      *[ IP VPN 1 ]# numbered=false
```

A questo punto è possibile impostare un percorso predefinito.

Configurazione della route predefinita (tabella route TCP/IP)

Ènecessario configurare una route predefinita che il concentratore VPN può utilizzare per inviare tutto il traffico TCP/IP destinato a reti diverse da quelle a cui è connesso direttamente o per le quali dispone di route dinamiche. Il percorso predefinito punta indietro a tutte le reti trovate sulla porta interna. Intraport è già stato configurato per l'invio di traffico IPSec da e verso Internet utilizzando il parametro IPSec Gateway. 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 a quella riportata nell'esempio 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#
```

Completamento

L'ultimo passaggio consiste nel salvare la configurazione. Alla richiesta di conferma del download della configurazione e del riavvio del dispositivo, digitare **y** e premere **Invio**. Non disattivare VPN Concentrator 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 connessi a VPN Concentrator utilizzando Telnet, l'output riportato sopra è tutto ciò che viene visualizzato. Se si è connessi tramite una console, verrà visualizzato un output simile al

seguente, solo molto più lungo. Al termine di questo output, VPN Concentrator 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