Configurazione di un tunnel IPsec - Cisco VPN 5000 Concentrator su firewall Checkpoint 4.1

Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Convenzioni Configurazione Esempio di rete Configurazioni Firewall checkpoint 4.1 Verifica Risoluzione dei problemi Comandi per la risoluzione dei problemi di VPN 5000 Concentrator Riepilogo della rete Debug del firewall di Checkpoint 4.1 Output di esempio del comando debug Informazioni correlate

Introduzione

In questo documento viene illustrato come formare un tunnel IPsec con chiavi già condivise per collegarsi a due reti private. Si unisce a una rete privata all'interno di Cisco VPN 5000 Concentrator (192.168.1.x) e a una rete privata all'interno del firewall di Checkpoint 4.1 (10.32.50.x). Si presume che il traffico tra l'interno del concentratore VPN e il checkpoint e diretto a Internet (rappresentato in questo documento dalle reti 172.18.124.x) scorra prima di avviare questa configurazione.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

- Cisco VPN 5000 Concentrator
- Cisco VPN 5000 Concentrator software versione 5.2.19.0001
- Firewall checkpoint 4.1

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 <u>Cisco sulle convenzioni</u> nei suggerimenti tecnici.

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 questo documento, 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 viene usata questa configurazione.

Cisco VPN 5000 Concentrator

[IP Ethernet 0:0] Mode SubnetMask IPAddress	= Routed = 255.255.255.0 = 192.168.1.1
[General] EthernetAddress DeviceType ConfiguredOn ConfiguredFrom DeviceName IPSecGateway	<pre>= 00:00:a5:e9:c8:00 = VPN 5002/8 Concentrator = Timeserver not configured = Command Line, from Console = "cisco_endpoint" = 172.18.124.34</pre>
[IKE Policy] Protection	= SHA_DES_G2
[Tunnel Partner VPN 1] KeyLifeSecs LocalAccess Peer BindTo SharedKey KeyManage Transform Partner Mode	<pre>= 28800 = "192.168.1.0/24" = "10.32.50.0/24" = "ethernet 1:0" = "ciscorules" = Auto = esp(sha,des) = 172.18.124.157 = Main</pre>
[IP VPN I] Numbered Mode	= Off = Routed
[IP Ethernet 1:0] IPAddress SubnetMask Mode [IP Static]	= 172.18.124.35 = 255.255.255.240 = Routed
Configuration size is 113	VPN I I 31 out of 65500 bytes.

Firewall checkpoint 4.1

Completare la procedura seguente per configurare il firewall di Checkpoint 4.1.

 Selezionare Proprietà > Crittografia per impostare la durata di IPSec del checkpoint in modo che corrisponda al comando KeyLifeSecs = 28800 VPN Concentrator.Nota: lasciare invariata la durata predefinita di Scambio chiave Internet (IKE) del punto di

Properties Setup		X
High Availability IP Pool NAT Access Security Policy Traffic Control Services L Authentication SYNDefender LDAP	s Lists og and Alert Encryption	Desktop Security Security Servers ConnectControl
SKIP Enable Exportable SKIP Change SKIP Session Key :	- Manual IF SPI alloc	SEC
<u>Every</u> 120 Seconds (0 for infinity)	<u>F</u> rom	100
E⊻ery 10485760 Bytes (0 for infinity)	Īo	
Renegotiate I <u>K</u> E Security Associations every	440	minutes
Renegotiate I <u>P</u> SEC Security Associations every	8800	seconds
	Hala	1
	пер	

 Selezionare Gestisci > Oggetti di rete > Nuovo (o Modifica) > Rete per configurare l'oggetto per la rete interna ("cpinside") dietro il checkpoint. In questo caso, il comando deve essere Peer = "10.32.50.0/24" VPN

General NAT Name: cpinside IP Address: 10.32.50.0 Mat Marky 255.255.0	
<u>Name:</u> cpinside <u>IP Address:</u> 10.32.50.0 <u>G</u> et address Net Mark: 255.255.0	
IP Address: 10.32.50.0	
Mark Markur 255 255 0	
Net <u>Mask:</u> [200.200.200.0	
Color: Color:	
Location: Broadcast:	
Internal ○ External Internal Internal ○ External Internal Internal ○ External Internal Interna	

 Selezionare Gestisci > Oggetti di rete > Modifica per modificare l'oggetto per l'endpoint gateway (checkpoint "RTPCPVPN") a cui punta il concentratore VPN nel comando Partner = <ip>.Selezionare Interno in Posizione.Selezionare Gateway per Type (Tipo di gateway).Controllare VPN-1 e FireWall-1 e la stazione di gestione sotto Moduli

General Interfaces SNMP NAT Certificates VPN Authe
Name: RTPCPVPN
IP Address: 172.18.124.157 Get address
Comment: Firewalled gateway to internet
- Location:
Modules Installed
✓ VPN-1 & FireWall-1 Version: 4.1 ▼ Get
□ FloodGate-1 Version: 4.1 ▼
Compression Version: 4.1
Management Station Color:
OK Cancel Help

- 4. Selezionare Gestisci > Oggetti di rete > Nuovo (o Modifica) > Rete per configurare l'oggetto per la rete esterna ("inside cisco") dietro al concentratore VPN In questo caso, si deve
 - per la rete esterna ("inside_cisco") dietro al concentratore VPN.In questo caso, si deve accettare il comando LocalAccess = <192.168.1.0/24> VPN

	Network Properties
	General NAT
	<u>Name:</u> inside_cisco
	IP Address: 192.168.1.0 Get address
	Net <u>M</u> ask: 255.255.255.0
	Color:
	Location: Broadcast:
	○ Internal ● External ● Allowed ● Disallowed
	OK Cancel Help
trator.	

5. Selezionare Gestisci > Oggetti di rete > Nuovo > Workstation per aggiungere un oggetto per il gateway VPN Concentrator esterno ("cisco_endpoint").Questa è l'interfaccia "esterna" del concentratore VPN con connettività al checkpoint (in questo documento, 172.18.124.35 è l'indirizzo IP nel comando IPAddress = <ip>).Selezionare Esterno in Posizione. Selezionare Gateway per Type (Tipo di gateway).Nota: non selezionare VPN-1/FireWall-

Workstation Properties	×
General Interfaces SNMP 1	NAT VPN
Name: cisco endpoint	
IP Address: 172.18.124.35	Get address
Location:	– Туре: –
O <u>I</u> nternal ⊙ <u>E</u> xternal	⊂ <u>H</u> ost
Modules Installed	
VPN-1 & <u>F</u> ireWall-1	Version: 4.1 🔽 Ge <u>t</u>
FloodGate-1	Version: 4.1
Compression	Version: 4.1
Management Station	Color:
	Cancel Help

6. Selezionare Gestisci > Oggetti di rete > Modifica per modificare la scheda VPN dell'endpoint del gateway del checkpoint (chiamata "RTPCPVPN"). In Dominio selezionare Altro, quindi selezionare dall'elenco a discesa l'interno della rete del checkpoint (denominata "cpinside"). In Definizione schemi di crittografia selezionare IKE, quindi fare clic su

General Interfaces SNMP NAT Certificates VPN Authe
Domain: Encryption schemes defined: O Disabled Image: Marceletee schemes defined:
○ Valid Addresses(of Interfaces) □ Image: Manual IPSEC ○ Other: □ Image: SKIP □ Exportable for SecuRemote Edit

 Modificare le proprietà IKE in crittografia DES e hashing SHA1 per accettare il comando SHA_DES_G2 VPN Concentrator.Nota: la sigla "G2" si riferisce al gruppo Diffie-Hellman 1 o 2. Durante il test è stato rilevato che il checkpoint accetta "G2" o "G1".Cambia le impostazioni:Deselezionare Modalità aggressiva.Selezionare Supporta le subnet.Selezionare Segreto precondiviso in Metodo di

	General Interfaces SNMP NAT Certificates VPN Authe
	KE Properties 🔪 🔹 🔀
	General
	Key <u>N</u> egotiation Encryption Method(s): <u>H</u> ash Method: _
	- Authentication Method:
	Public Key Signatures Configure
	Supports Aggresive Mode Supports Subnets
	OK Cancel Help
autenticazione.	

8. Fare clic su **Edit Secrets** (Modifica segreti) per impostare la chiave già condivisa in modo che accetti il comando **SharedKey = <key>** VPN

Workstation Properties
General Interfaces SNMP NAT Certificates VPN Authe
IKE Properties 💦 🗶
General
Shared Secret 🔀
Shared Secrets List:
Peer Name Shared Secret
OK Cancel
OK Cancel Help
OK Cancel Help

Concentrator.

Selezionare Gestisci > Oggetti di rete > Modifica per modificare la scheda VPN
 "cisco_endpoint". In Dominio selezionare Altro, quindi selezionare l'interno della rete VPN
 Concentrator (denominata "inside_cisco"). In Definizione schemi di crittografia selezionare
 IKE, quindi fare clic su

	Workstation Properties	>
	General Interfaces SNMP NAT VPN	
		1
	O Disabled	
	O ⊻alid Addresses(of Interfaces)	
	● <u>O</u> ther:	
	🖳 inside_cisco 💌	
	Exportable for SecuRemote Edit	
	Traffic Control Logging	1
	✓ Ium on Traffic Control Logging	
	OK Cancel Help	
a.		

 Modificare le proprietà IKE in crittografia DES e hashing SHA1 per accettare il comando SHA_DES_G2 VPN Concentrator.Nota: la sigla "G2" si riferisce al gruppo Diffie-Hellman 1 o 2. Durante il test, è stato rilevato che il checkpoint accetta "G2" o "G1".Cambia le impostazioni:Deselezionare Modalità aggressiva.Selezionare Supporta le subnet.Selezionare Segreto precondiviso in Metodo di

ſ	General Interfaces SNMP NAT Certificates VPN Authe	
	KE Properties	×
i	General	
	Key Negotiation Encryption Method(s): Hash Method: Image: DES Image: MD5 Image: CAST Image: SHA1	
	Authentication Method: ✓ Pre-Shared Secret □ Public Key Signatures Configure	
	Supports Aggresive Mode 🔽 Supports Subnets	
	OK Cancel Help	
autenticazione.		

11. Fare clic su **Edit Secrets** (Modifica segreti) per impostare la chiave già condivisa in modo che accetti il comando **SharedKey = <key>** VPN

	IKE Properties	×
	General	
	Shared Secret	×
	Shared Secrets List:	
	Peer Name Shared Secret	
	<u>Edit</u>	
	<u>R</u> emove	
	OK Cancel	
Concentrator	OK Cancel Help	

12. Nella finestra Editor dei criteri inserire una regola con Origine e Destinazione come "inside_cisco" e "cpinside" (bidirezionale). Set **Service=Any**, **Action=Encrypt** e **Track=Long**.

T	'RTP(CPVPN - Check Po	oint Policy Editor				- 🗆 🗡
Ei	e <u>E</u> di	t <u>V</u> iew <u>M</u> anage	Policy Window <u>H</u>	elp			
6] 🖨	🖪 🕹 🕻	E 💁 🕉 🕉	B. 🐬 🌆 🖆	🗏 🖀 🖷 🖷	T. 🔫 🖦 🛃	🐻 🎹 🚯
ž	Seci	urity Policy - Standard	🕂 🖶 Address Trans	slation - Standard 🛛 😿	Bandwidth Policy - S	tandard	
	No.	Source	Destination	Service	Action	Track	In
Ì	1	🚆 inside_cisco	👷 cpinside 👷 inside_cisco	Any	Encrypt	Long	
							•
Fo	r Help,	press F1		RTPC	PVPN Rea	d/Write	

13. Sotto l'intestazione Azione, fare clic sull'icona **Encrypt** verde e selezionare **Modifica proprietà** per configurare i criteri di crittografia.

chillograna.				
rrity Policy - Standard	📇 Address Translation	- Standard 👭 Ban	dwidth Policy - Standard	-12-
∼ FVV1 Host	∼ Ldap-Servers	😰 Idap	accept	
∼ FVV1 Host	∼ Logical-Servers	∼ load_agent	accept	5
nside_cisco	🖶 cpinside 💂 inside_cisco	Any	Adit properties	ng .
		icmp dest-unreach	Edit Encryption	
		icmp echo-request	accept	am 🗂
		imp-proto	drop	
Any	Any	imp mask-reply	🚺 😑 reject	ng l am l
•		P Higer Participet		

14. Selezionare IKE, quindi fare clic su

	Encryption Properties	×
	General Encryption schemes defined:	
Modifica	OK Cancel Help	

15. Nella finestra Proprietà IKE modificare queste proprietà in modo che corrispondano al comando Transform = esp(sha,des) VPN Concentrator.In Trasforma, selezionare Crittografia + integrità dei dati (ESP). L'algoritmo di crittografia deve essere DES, l'integrità dei dati deve essere SHA1 e il gateway peer consentito deve essere il gateway del concentratore VPN esterno (denominato "cisco_endpoint"). Fare clic su

IKE Properties	
General	
Transform:	
Encryption + Data Integrit	y (ESP)
C Data Integrity Only (AH)	
Encryption Algorithm:	DES
Data Integrity	SHA1
Allowed Peer Gateway:	cisco_endpo
Use Perfect Forward Sec	recy
OK Ca	ancel Help

16. Dopo aver configurato il checkpoint, selezionare **Criterio > Installa** nel menu del checkpoint per rendere effettive le modifiche.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Comandi per la risoluzione dei problemi di VPN 5000 Concentrator

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**.

- vpn trace dump all: visualizza le informazioni su tutte le connessioni VPN corrispondenti, incluse le informazioni sull'ora, il numero VPN, l'indirizzo IP reale del peer, gli script eseguiti e, in caso di errore, la routine e il numero di riga del codice software in cui si è verificato l'errore.
- show system log buffer: visualizza il contenuto del log buffer interno.
- show vpn statistics: visualizza queste informazioni per utenti, partner e il totale di entrambi. Per i modelli modulari, il display include una sezione per ogni slot del modulo. Fare riferimento alla sezione <u>Output di esempio del comando debug</u>.)Attivo corrente (Current Active) -Connessioni attive correnti.In Negot - Connessioni attualmente in fase di negoziazione.Acqua alta (High Water) - Numero massimo di connessioni attive simultanee dall'ultimo riavvio.Totale parziale: il numero totale di connessioni riuscite dall'ultimo riavvio.Tunnel ok: il numero di tunnel per i quali non si sono verificati errori.Tunnel starts: il numero di avvii del tunnel.Errore tunnel: il numero di tunnel con errori.
- **show vpn statistics verbose**: visualizza le statistiche di negoziazione ISAKMP e molte altre statistiche di connessione attive.

Riepilogo della rete

Quando più reti interne adiacenti sono configurate nel dominio di crittografia sul checkpoint, il dispositivo potrebbe riepilogarle automaticamente in relazione al traffico interessante. Se VPN Concentrator non è configurato per la corrispondenza, è probabile che il tunnel non riesca. Ad esempio, se le reti interne 10.0.0.0 /24 e 10.0.1.0 /24 sono configurate per essere incluse nel tunnel, è possibile riepilogarle in 10.0.0.0 /23.

Debug del firewall di Checkpoint 4.1

Si tratta di un'installazione di Microsoft Windows NT. Poiché il rilevamento è stato impostato per Long nella finestra Editor dei criteri (come illustrato nel <u>passaggio 12</u>), il traffico negato dovrebbe essere visualizzato in rosso nel Visualizzatore log. Per ottenere un debug più dettagliato, procedere come segue:

C:\WINNT\FW1\4.1\fwstop C:\WINNT\FW1\4.1\fw d -d e in un'altra finestra:

$C:\WINNT\FW1\4.1\fwstart$

Utilizzare i seguenti comandi per cancellare le associazioni di sicurezza (SA) sul checkpoint:

fw tab -t IKE_SA_table -x
fw tab -t ISAKMP_ESP_table -x
fw tab -t inbound_SPI -x
fw tab -t ISAKMP_AH_table -x
Rispondi sì al messaggio..

Output di esempio del comando debug

```
cisco_endpoint#vpn trac dump all
         4 seconds -- stepmngr trace enabled --
   new script: lan-lan primary initiator for <no id> (start)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing l2lp_init, (0 @ 0)
         38 seconds doing l2lp_do_negotiation, (0 @ 0)
   new script: ISAKMP secondary Main for lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_init, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
        38 seconds doing isa_i_main_process_pkt_2, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_process_pkt_4, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing isa_i_main_process_pkt_6, (0 @ 0)
         39 seconds doing isa_i_main_last_op, (0 @ 0)
   end script: ISAKMP secondary Main for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
   next script: lan-lan primary initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
         39 seconds doing l2lp_phase_1_done, (0 @ 0)
         39 seconds doing l2lp_start_phase_2, (0 @ 0)
   new script: phase 2 initiator for lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing iph2_init, (0 @ 0)
         39 seconds doing iph2_build_pkt_1, (0 @ 0)
         39 seconds doing iph2_send_pkt_1, (0 @ 0)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing iph2_pkt_2_wait, (0 @ 0)
         39 seconds doing ihp2_process_pkt_2, (0 @ 0)
         39 seconds doing iph2_build_pkt_3, (0 @ 0)
         39 seconds doing iph2_config_SAs, (0 @ 0)
         39 seconds doing iph2_send_pkt_3, (0 @ 0)
         39 seconds doing iph2_last_op, (0 @ 0)
   end script: phase 2 initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
   next script: lan-lan primary initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
         39 seconds doing l2lp_open_tunnel, (0 @ 0)
         39 seconds doing l2lp_start_i_maint, (0 @ 0)
   new script: initiator maintenance for lan-lan-VPN0:1:[172.18.124.157] (start)
        39 seconds doing imnt_init, (0 @ 0)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
```

cisco_endpoint#show vpn stat

	Current Active	In Negot	High Water	Running Total	Tunnel Starts	Tunnel OK	Tunnel Error
Users	0	0	0	0	0	0	0
Partners	1	0	1	1	1	0	0
Total	1	0	1	1	1	0	0

	Current Active	In Negot	High Water	Running Total	Tunnel Starts	Tunnel OK	Tunnel Error
Users	0	0	0	0	0	0	0
Partners	0	0	0	0	0	0	0
Total	0	0	0	0	0	0	0

cisco_endpoint#**show vpn stat verb**

	Current Active	In Negot	High Water	Running Total	Tunnel Starts	Tunnel OK	Tunnel Error
Users	0	0	0	0	0	0	0
Partners	1	0	1	1	1	0	0
Total	1	0	1	1	1	0	0

Stats	VPN0:1
Wrapped	13
Unwrapped	9
BadEncap	0
BadAuth	0
BadEncrypt	0
rx IP	9
rx IPX	0
rx Other	0
tx IP	13
tx IPX	0
tx Other	0
IKE rekey	0

Input VPN pkts dropped due to no SA: 0

Input VPN pkts dropped due to no free queue entries: 0

ISAKMP Negotiation stats Admin packets in 4 Fastswitch packets in 0 0 No cookie found Can't insert cookie 0 Inserted cookie(L) 1 Inserted cookie(R) 0 Cookie not inserted(L) 0 Cookie not inserted(R) 0 Cookie conn changed 0 Cookie already inserted 0 Deleted cookie(L) 0 Deleted cookie(R) 0 Cookie not deleted(L) 0 Cookie not deleted(R) 0 Forwarded to RP 0 Forwarded to IOP 0 0 Bad UDP checksum Not fastswitched 0 Bad Initiator cookie 0 Bad Responder cookie 0 0 Has Responder cookie No Responder cookie 0 No SA 0 Bad find conn 0 0 Admin queue full Priority queue full 0 Bad IKE packet 0 No memory 0

Bad Admin Put	0
IKE pkt dropped	0
No UDP PBuf	0
No Manager	0
Mgr w/ no cookie	0
Cookie Scavenge Add	1
Cookie Scavenge Rem	0
Cookie Scavenged	0
Cookie has mgr err	0
New conn limited	0

IOP slot 1:

	Current Active	In Negot	High Water	Running Total	Tunnel Starts	Tunnel OK	Tunnel Error
Users	0	0	0	0	0	0	0
Partners	0	0	0	0	0	0	0
Total	0	0	0	0	0	0	0

Stats Wrapped Unwrapped BadEncap BadAuth BadEncrypt rx IP rx IPX rx Other tx IP tx IPX tx Other IKE rekey Input VPN pkts dropped due to no SA: $\ensuremath{\texttt{0}}$ Input VPN pkts dropped due to no free queue entries: 0 ISAKMP Negotiation stats Admin packets in 0 Fastswitch packets in 3

Pastswitten packets in	5
No cookie found	0
Can't insert cookie	0
Inserted cookie(L)	0
Inserted cookie(R)	1
Cookie not inserted(L)	0
Cookie not inserted(R)	0
Cookie conn changed	0
Cookie already inserted	0
Deleted cookie(L)	0
Deleted cookie(R)	0
Cookie not deleted(L)	0
Cookie not deleted(R)	0
Forwarded to RP	0
Forwarded to IOP	3
Bad UDP checksum	0
Not fastswitched	0
Bad Initiator cookie	0
Bad Responder cookie	0
Has Responder cookie	0
No Responder cookie	0
No SA	0
Bad find conn	0
Admin queue full	0

Priority queue full	0
Bad IKE packet	0
No memory	0
Bad Admin Put	0
IKE pkt dropped	0
No UDP PBuf	0
No Manager	0
Mgr w/ no cookie	0
Cookie Scavenge Add	1
Cookie Scavenge Rem	0
Cookie Scavenged	0
Cookie has mgr err	0
New conn limited	0

Informazioni correlate

- Cisco VPN serie 5000 concentrator: annuncio di fine vendita
- Negoziazione IPSec/protocolli IKE
- Documentazione e supporto tecnico Cisco Systems