スタティックにアドレス指定された ASA と、 CCP を使用するダイナミックにアドレス指定さ れた Cisco IOS ルータ間における、ダイナミッ ク IPSec トンネルの設定例

内容

概要
前提条件
要件
使用するコンポーネント
表記法
背景説明
設定
ネットワーク図
設定
確認
CCPを使用したトンネル パラメータの確認
ASA CLIを使用したトンネル ステータスの確認
ルータの CLIを使用したトンネルパラメータの確認
トラブルシュート
関連情報

<u>概要</u>

このドキュメントでは、PIX/ASA セキュリティ アプライアンスが Cisco IOS® ルータからのダイ ナミック IPSec 接続の受け入れを可能にする方法の設定例を示します。このシナリオでは、ルー タ側からトンネルが開始された場合にのみ IPSec トンネルが確立されます。ダイナミック IPSec 設定のため、ASA は VPN トンネルを開始できません。

この設定は、PIX セキュリティ アプライアンスが VPN ルータを使用してダイナミック IPsec LAN-to-LAN(L2L)トンネルを作成できるようにします。このルータは、インターネット サービ ス プロバイダーから外部のパブリック IP アドレスをダイナミックに受信します。プロバイダー からダイナミックに IP アドレスを割り当てる目的で、Dynamic Host Configuration Protocol(DHCP)がこのメカニズムを提供します。これにより、ホストで使用されなくなった IP アドレスを再利用できます。

ルータ上の設定は、<u>Cisco Configuration Professional</u>(CCP)を使用して実行されます。CCP と は、Cisco IOS ベースのアクセス ルータを設定する GUI ベースのデバイス管理ツールです。CCP を使用したルータの設定方法の詳細については、『<u>Cisco Configuration Professional を使用した</u> 基本的なルータ設定』を参照してください。 ASA および Cisco IOS ルータを使用する IPSec トンネルの確立に関する情報および設定例につい ては、『<u>ASA によるサイト間 VPN(L2L)</u>』を参照してください。

PIX および Cisco IOS ルータを使用する IPSec トンネルの確立に関する情報および設定例については、『IOS によるサイト間 VPN(L2L)』を参照してください。

前提条件

<u>要件</u>

この設定を実行する前に、IPSec トンネルを確立するためのインターネット接続が ASA およびル ータに用意されていることを確認します。

<u>使用するコンポーネント</u>

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco IOS ソフトウェア リリース 12.4 が稼働する Cisco IOS ルータ 1812
- Cisco ASA 5510 ソフトウェア リリース 8.0.3

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『<u>シスコ テクニカル ティップスの表記法</u>』を参照してくだ さい。

<u>背景説明</u>

このシナリオでは、192.168.100.0 ネットワークが ASA の背後にあり、192.168.200.0 ネットワ ークは Cisco IOS ルータの背後にあります。ルータは ISP から DHCP を使用してパブリック ア ドレスを取得することを前提とします。ASA 側ではスタティック ピアの設定に問題が発生するた め、ASA と Cisco IOS ルータ間のサイト間トンネルを確立するには、ダイナミック クリプト設 定を使用する必要があります。

ASA 側のインターネット ユーザは、その outside インターフェイスの IP アドレスに変換されます。NAT は Cisco IOS 側に設定されないものとします。

次に、ダイナミック トンネルを確立するために ASA 側で設定する主なステップを示します。

1. フェーズ 1 の ISAKMP 関連の設定

- 2. NAT 免除の設定
- 3. ダイナミック クリプト マップの設定

ASA がスタティックなパブリック IP アドレスを保持していると見なされるため、Cisco IOS ルー タにはスタティック クリプト マップが設定されています。次に、ダイナミック IPSec トンネル を確立するために Cisco IOS ルータ側で設定する主なステップのリストを示します。 1. フェーズ 1 の ISAKMP 関連の設定

2. スタティック クリプト マップ関連の設定

これらのステップは、下記の設定で詳しく説明します。

<u>設定</u>

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供して います。

注:このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool(登録ユーザ専用)を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

<u>ネットワーク図</u>

このドキュメントでは、次のネットワーク セットアップを使用します。



<u>設定</u>

これは、CCP を使用した VPN ルータ上の IPsec VPN 設定です。次のステップを実行します。

1. CCP アプリケーションを起動し、[Configure] > [Security] > [VPN] > [Site to Site VPN] の順 に選択します。[Launch the selected tab] をクリックします。



2. [Step-by-step wizard] をクリックして、[Next] をクリックします。



3. 認証についての詳細に従って、リモート ピアの IP アドレスを入力します。

Site-to-Site VPN Wiza	rd	
VPN Wizard	VPN Connection Information Select the interface for this VPN connection	n: FastEthemet1 💌 Details
	Peer Identity Select the type of peer(s) used for this cannection: Enter the IP address of the remote peer.	VPN Peer with static P address 💉
	Authentication Authentication ensures that each end o key.	f the VPN connection uses the same secret
NA	Pre-shared Keys pre-shared keys Re-enter Key:	C Digital Certificates
	2.2	- Back Next - Firms Cancel Help

4. IKE プロポーザルを選択し、[Next] をクリックします。

VPN Wizard	IKE P IKE pr metho device device	oposals oposals of that is For the should t	specify the en used by this r VPN connecti ae configured	cryption algo outer when n on to be esta with at least	rithm, authentical egotialing a VPN blished with the r one of the policie	ion algorithm and connection with t ernote device, the s listed below.	d key exchange he remote a remote
2 Million	Click	Priority 1 2	Encryption 3DES DES	Hash SHA_1 MD5	D-H Group group2 group2	Authentication	Type Cisco CP Defa User Defined
N.		Add	Edit.	1			
			Larra	-			

5. トランスフォーム セットの詳細を決定し、[Next] をクリックします。

	A transform set specifi data in the VPN tunnel communicate, the rem one selected below. Click the Add button t	les the encryption and aut . Since the two devices mi lote device must be config to add a new transform se	tentication algorit ust use the same ured with the sam t and the Edit bu	rms used to protect the algorithms to e transform set as the tton to edit the specified
	bansform set. Select Transform Set:			
a	myset	3		
	Details of the spec	ified transform set		
	Name	ESP Encryption	ESP Integrity	AH Integrity
	myset	ESP_DES	ESP_MD6_HMAC	
NA	3			3
	Add	Edit		

6. 暗号化が必要なトラフィックを決定し、[Next] をクリックします。

Protect all traffic between the following subnets Local Network Enter the IP address and subnet mask of the network where IPSec traffic originates. IP Address: 192 168 200.0 Subnet Mask: 255 255 255.0 or 24	/bnet, or
Enter the IP address and subnet mask of the network where IPSec traffic originates. IP Address: 182 168 200.0 Subnet Mask: 295 255 255 0 or 24	
IP Address: IP Address: IP Address: 192 168.200.0 Subnet Mask: 192.168.100.0 Subnet Mask: 255.255.0 or 24	net Mask of
192 168 200.0 192 168 100.0 Subnet Mask: 255 255 255.0 255 255 255.0 or 24	
Subnet Mask: Subnet Mask 255.255.255.0 or 24	
255.255.255.0 or 24 🖁 255.255.0 or	
	24
Create/Select an access-list for IPSec traffic	r 24 📕

7. crypto IPsec 設定のサマリーを確認し、[Finish] をクリックします。

te-to-Site VPN Wizar	rð				
VPN Wizard	Summary of the	Configuration			
	Click Finish to de	liver the configurat	on to the router.		
	IKE Policies:			~	
	Hash	DH Group	Authentication	Encryption	
	MD5 SHA_1	group2 group2	PRE_SHARE PRE_SHARE	DES 3DES	
N	Transform Sets Namer ESP En ESP Int Mode:T	nyset cryption:ESP_DES egrity:ESP_MD5_H UNNEL	мас	- -	
N.A	IPSec Rule: permit :	all ip traffic from 193	1.168.200.0 0.0.0.255 to	192.168.100.0 0.0	
	<			3	
	Test VPN con	nectivity after config	uting]		
	4.51		<back med<="" td=""><td>Finish Cancel</td><td>He</td></back>	Finish Cancel	He

8. [Deliver] をクリックして、設定を VPN ルータに送信します。

crypto ipsec transform-set myset esp-md5-hmac esp-des mode tunnel exit crypto map SDM_CMAP_1 1 ipsec-isakmp description Tunnel to209.165.201.2 set transform-set myset set peer 209.165.201.2 match address 101 exit interface FastEthernet1 Soc crypto man		oto ipsec transform-set myset esp-md5-hmac esp-des de tunnel scription Tunnel to209.165.201.2 transform-set myset peer 209.165.201.2 ch address 101
match address 101 exit interface FastEthernet1 Ro cryste man		tch address 101
	<u>></u>	face FastEthernet1 crunto men
The differences between the running configuration and the startup configuration are he router is turned off.	lost whenever	differences between the running configuration and the startup configuration router is turned off.
This operation can take several minutes.		This operation can take several minutes.

		_
Submitting 31 control Configuration del Copying the Run Running config c	internets, please wat ivered to router. ring config to Startup config of your router. Please wat opied successfully to Startup Config of your router.	1
		1

9. [OK] をクリックします。 CLI での設定

- <u>Ciscoasa</u>
- <u>VPN ルータ</u>

Ciscoasa

```
ciscoasa(config)#show run
: Saved
:
ASA Version 8.0(3)
1
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
1
interface Ethernet0/0
nameif outside
security-level 0
ip address 209.165.201.2 255.255.254
!
interface Ethernet0/1
nameif inside
security-level 100
ip address 192.168.100.1 255.255.255.0
Ţ
interface Ethernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
1
interface Management0/0
shutdown
no nameif
no security-level
no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
!--- Output suppressed access-list nonat extended permit
```

```
ip 192.168.100.0 255.255.255.0 192.168.200.0
255.255.255.0
no pager
mtu outside 1500
mtu inside 1500
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-613.bin
no asdm history enable
arp timeout 14400
!!--- Define the nat-translation for Internet users
global (outside) 1 interface
nat (inside) 1 192.168.100.0 255.255.255.0
!!--- Define the nat-exemption policy for VPN traffic
nat (inside) 0 access-list nonat
route outside 0.0.0.0 0.0.0.0 209.165.201.1 1
1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
!!--- Configure the IPsec transform-set crypto ipsec
transform-set myset esp-des esp-md5-hmac
!!--- Configure the dynamic crypto map crypto dynamic-
map mymap 1 set transform-set myset
crypto dynamic-map mymap 1 set reverse-route
crypto map dyn-map 10 IPSec-isakmp dynamic mymap
crypto map dyn-map interface outside
!!--- Configure the phase I ISAKMP policy crypto isakmp
policy 10
authentication pre-share
encryption des
hash md5
group 2
lifetime 86400
!!--- Configure the default L2L tunnel group parameters
tunnel-group DefaultL2LGroup IPSec-attributes
pre-shared-key *
1
class-map inspection_default
match default-inspection-traffic
1
1
policy-map type inspect dns preset_dns_map
parameters
 message-length maximum 512
policy-map global_policy
class inspection_default
 inspect dns preset_dns_map
 inspect ftp
 inspect h323 h225
```

inspect	h323 ras
inspect	netbios
inspect	rsh
inspect	rtsp
inspect	skinny
inspect	esmtp
inspect	sqlnet
inspect	sunrpc
inspect	tftp
inspect	sip
inspect	xdmcp
!	
service-po	olicy global_policy global
prompt hos	stname context
Cryptoched	ksum:d41d8cd98f00b204e9800998ecf8427e
: end	
ciscoasa(c	config)#

CCP により、VPN ルータにこの内容が設定されます。

```
VPN ルータ
VPN-Router#show run
Building configuration...
1
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname VPN-Router
1
1
username cisco privilege 15 secret 5
$1$UQxM$WvwDZbfDhK3wS26C9xYns/
username test12 privilege 15 secret 5
$1$LC0U$ex3tp4hM8CYD.HJSRDfQ01
1
!!--- Output suppressed no aaa new-model ip subnet-zero
! ip cef ! crypto isakmp enable outside
!
crypto isakmp policy 1
encrypt 3des
 authentication pre-share
group 2
!
crypto isakmp policy 2
hash md5
authentication pre-share
group 2
!
1
crypto isakmp key cisco123 address 209.165.201.2
1
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
1
1
crypto map SDM_CMAP_1 1 IPSec-isakmp
description Tunnel to209.165.201.2
 set peer 209.165.201.2
 set transform-set myset
```

```
match address 101
1
1
interface BRI0
no ip address
shutdown
!
interface Dot11Radio0
no ip address
shutdown
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0
12.0 18.0 24.0 36.0 48.0 54.0
station-role root
!
interface Dot11Radio1
no ip address
 shutdown
speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0
48.0 54.0
station-role root
!
interface FastEthernet0
ip address 192.168.200.1 255.255.255.0
 duplex auto
speed auto
1
interface FastEthernet1
ip address dhcp
duplex auto
 speed auto
 crypto map SDM_CMAP_1
!
interface FastEthernet2
no ip address
shutdown
!
interface FastEthernet3
no ip address
shutdown
!
interface FastEthernet4
no ip address
shutdown
interface FastEthernet5
no ip address
shutdown
1
interface FastEthernet6
no ip address
shutdown
1
interface FastEthernet7
no ip address
shutdown
!
interface FastEthernet8
no ip address
shutdown
ļ
interface FastEthernet9
no ip address
 shutdown
```

```
interface Vlan1
no ip address
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.200.1
!!--- Output suppressed ! ip http server ip http
authentication local ip http secure-server ! access-list
100 permit ip 0.0.0.0 255.255.255.0 0.0.0.0
255.255.255.0
access-list 101 remark CCP_ACL Category=4
access-list 101 remark IPSEC Rule
access-list 101 permit ip 192.168.200.0 0.0.0.255
192.168.100.0 0.0.0.255
1
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
privilege level 15
login local
transport input telnet ssh
line vty 5 15
privilege level 15
 login local
 transport input telnet ssh
1
no scheduler allocate
end
```

<u>確認</u>

ここでは、設定が正常に機能しているかどうかを確認します。

<u>アウトプット インタープリタ ツール(登録ユーザ専用)(OIT)は、特定の show コマンドをサ</u> <u>ポートします。</u>OIT を使用して、show コマンドの出力の分析を表示します。

- <u>CCP を使用したトンネル パラメータの確認</u>
- ASA CLI を使用したトンネル ステータスの確認
- <u>ルータの CLI を使用したトンネルパラメータの確認</u>

<u>CCP を使用したトンネル パラメータの確認</u>

•トラフィックが IPSec トンネルを通過することを監視します。

Image:	
Image: Second processing or Web Status > Web S	sional dis
Binder	
Bit Met Descenter Presente Bit Mut Presente Bit Mut Descenter Descenter <td>_</td>	_
Statute	
Interact Bundle Default Workshow Very Status Default Show Default Show Default Show	and Tannel. Update
Interformation Inter	April at
Interact Number Image: Status Image: Stat	Packets
Become Travelit P Send Error Packet: Barry Starts P Received Error Packet: Data Starts P Received Error Packet:	Packets
In the second	rioti
In Strate Interest Au Interest Strate	(Facility)
Der Sterben / Der St	
Interference Found State Interference Pounders also evany 13 sec Interference Interpretation Pecters Interpretation Pecters Received from Pecters <td< td=""><td></td></td<>	
Intervent Voter Withmall Ford size size a non-yr 13 too Intervent Ford size size non-yr 13 too Intervent of the pro-process Reserved the pro-process Intervent Ford size size non-yr 13 too Intervent of the pro-process Reserved the pro-process Intervent Ford size size non-yr 13 too Intervent of the pro-process Reserved the pro-process Intervent Ford size size non-yr 13 too Ford size size non-yr 13 too Intervent of the pro-process Intervent Ford size size non-yr 13 too Ford size size non-yr 13 too Intervent of the pro-process Intervent Ford size size non-yr 13 too Ford size size non-yr 13 too Intervent of the pro-process Intervent Ford size size non-yr 13 too Ford size non-yr 13 too Ford size non-yr 13 too Intervent Ford size non-yr 13 too Ford size non-yr 13 too Ford size non-yr 13 too Intervent Ford size non-yr 13 too Ford size non-yr 13 too Ford size non-yr 13 too Intervent Ford size non-yr 14 too Ford size non-yr 14 too Ford size non-yr 14 too Intervent Ford size non-yr 14 too Ford size non-yr 14 too Ford size non-yr 14 too Intervent Ford size non-yr	
Image: addition Packets Send Grave Packets Send	
Image: default of patients Image: default of patients Image: default of patients Image: default o	Envir Packate
	CALCULATION .
Image: indication indicatione indindindication indication indication indication indication in	
	ala.
Image: second	
ability bility bility </td <td></td>	
set set set	
edu/	
40() 41() 41() 41() 12() <td< td=""><td></td></td<>	
Intribution Introduction Sector from Proceeding Sector from Proceeding Introduction Sector from Proceeding <td></td>	
The [percent tage The [percent tage 12:01:20 The [percent set] The [percent set]	
Send train Packets	
12:55:25 The [recent S2]	arta
12:57:25 The [recent st]	
12:57:20 The (PECPH SE)	
12:57:25 The [Income 55]	
12:51:25 The [http://doi.org/10.15]	
12/37/25 Taile (http://doi.org/10.1011/10.1001/1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/1000/10000/1000000	
12/51/20 Taxe (https://www.stg	
N	

・フェーズ1ISAKMP SA のステータスを監視します。

Reading and the last					
anne 🖉 terlipes 📳 terder	1 🛣 🗠 😣		Cisco Co	nfiguration Professional	cisco
Balast Conversity Parolaut 18,27,000,000 [m	Resider > Security > 984 Mate	e > 1Plac Tanish		E	
hute	by VPH Status				
Percette	OMUNIS Turnets	Cech row represents one HE GA	<u>K</u>	Q ² static carries to one	Nobel 14 C
Transal Statio	C C C C C C C C C C C C C C C C C C C	fourse P	Ovstination IP	200	
Transis Januar Marc Baba Marc Baba	Sin Proportaniato				

<u>ASA CLI を使用したトンネル ステータスの確認</u>

•フェーズ1ISAKMP SA のステータスを確認します。

ciscoasa#show crypto isakmp sa

```
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
```

```
1 IKE Peer: 209.165.200.12

Type : L2L Role : responder

Rekey : no State : MM_ACTIVE

ciscoasa#
```

注:応答側の役割を確認します。この役割は、このトンネルの発信側がもう一方の端 (VPNルータなど)にあることを示します。

```
    フェーズ2 IPSEC SA のパラメータを確認します。

 ciscoasa#show crypto ipsec sa
 interface: outside
     Crypto map tag: mymap, seq num: 1, local addr: 209.165.201.2
       local ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0)
       remote ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0)
       current_peer: 209.165.200.12
       #pkts encaps: 29, #pkts encrypt: 29, #pkts digest: 29
       #pkts decaps: 29, #pkts decrypt: 29, #pkts verify: 29
       #pkts compressed: 0, #pkts decompressed: 0
       #pkts not compressed: 29, #pkts comp failed: 0, #pkts decomp failed: 0
       #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
       #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
       #send errors: 0, #recv errors: 0
       local crypto endpt.: 209.165.201.2, remote crypto endpt.: 209.165.200.12
       path mtu 1500, IPSec overhead 58, media mtu 1500
       current outbound spi: E7B37960
     inbound esp sas:
       spi: 0xABB49C64 (2880740452)
          transform: esp-des esp-md5-hmac none
          in use settings ={L2L, Tunnel, }
          slot: 0, conn_id: 4096, crypto-map: mymap
          sa timing: remaining key lifetime (kB/sec): (4274997/3498)
          IV size: 8 bytes
          replay detection support: Y
     outbound esp sas:
       spi: 0xE7B37960 (3887298912)
          transform: esp-des esp-md5-hmac none
          in use settings ={L2L, Tunnel, }
          slot: 0, conn_id: 4096, crypto-map: mymap
          sa timing: remaining key lifetime (kB/sec): (4274997/3498)
          IV size: 8 bytes
          replay detection support: Y
```

<u>ルータの CLI を使用したトンネルパラメータの確認</u>

・フェーズ1ISAKMP SA のステータスを確認します。

VPN-Router#show crypto isakmp sa

dst	src	state	conn-id	slot	status
209.165.201.2	209.165.200.12	QM_IDLE	1	0	ACTIVE

・フェーズ 2 IPSEC SA のパラメータを確認します。

VPN-Router#show crypto ipsec sa

```
interface: FastEthernet1
   Crypto map tag: SDM_CMAP_1, local addr 209.165.200.12
  protected vrf: (none)
  local ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0)
  current_peer 209.165.201.2 port 500
     PERMIT, flags={origin_is_acl,}
   #pkts encaps: 39, #pkts encrypt: 39, #pkts digest: 39
   #pkts decaps: 39, #pkts decrypt: 39, #pkts verify: 39
   #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.: 209.165.200.12, remote crypto endpt.: 209.165.201.2
    path mtu 1500, ip mtu 1500
     current outbound spi: 0xABB49C64(2880740452)
     inbound esp sas:
     spi: 0xE7B37960(3887298912)
        transform: esp-des esp-md5-hmac ,
       in use settings ={Tunnel, }
       conn id: 2001, flow_id: C18XX_MBRD:1, crypto map: SDM_CMAP_1
        sa timing: remaining key lifetime (k/sec): (4481818/3375)
        IV size: 8 bytes
       replay detection support: Y
       Status: ACTIVE
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
     spi: 0xABB49C64(2880740452)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
       conn id: 2002, flow_id: C18XX_MBRD:2, crypto map: SDM_CMAP_1
        sa timing: remaining key lifetime (k/sec): (4481818/3371)
       IV size: 8 bytes
       replay detection support: Y
        Status: ACTIVE
     outbound ah sas:
     outbound pcp sas:
```

<u>トラブルシュート</u>

ここでは、設定のトラブルシューティングに使用できる情報を示します。

既存のクリプト接続を切断します。
 ciscoasa#clear crypto ipsec sa
 ciscoasa#clear crypto isakmp sa

VPN-Router#clear crypto isakmp

・VPN トンネルに関する問題をトラブルシューティングするには、debug コマンドを使用します。注:デバッグを有効にすると、インターネットワークで高負荷状態が発生したときにルータの動作が中断する可能性があります。debugコマンドは使用注意してください。一般に、これらのコマンドは、特定の障害をトラブルシューティングする場合に限り、必ずルータの技術サポート担当者の指示に従って使用することをお勧めします。 ciscoasa#debug crypto engine

ciscoasa#debug crypto isakmp ciscoasa#debug crypto IPSec ciscoasa#

VPN-Router#debug crypto engine Crypto Engine debugging is on VPN-Router#debug crypto isakmp Crypto ISARMP debugging is on VPN-Router#debug crypto ipsec Crypto IPSEC debugging is on VPN-Router#

debug コマンドの詳細については、『<u>debug コマンドの説明と使用』の「debug crypto isakmp」</u>

<u>を参照してください。関連情報</u>

- <u>IPsec ネゴシエーション/IKE プロトコルに関するサポート ページ</u>
- <u>Cisco ASA セキュリティ アプライアンス OS ソフトウェアに関するドキュメント</u>
- 最も一般的な IPSec VPN のトラブルシューティング方法
- Requests for Comments (RFCs)