ASA/PIX: CLI および ASDM による VPN Client トラフィック用の着信 NAT を使用したリモート VPN サーバの設定例

目次

概要
前提条件
要件
使用するコンポーネント
関連製品
表記法
背景説明
設定
ASDM を使用した、リモート VPN サーバとしての ASA/PIX の設定
ASDM を使用した、着信 VPN クライアント トラフィックを NAT するための ASA/PIX の設定
CLI を使用した、リモート VPN サーバとして、および着信を NAT するための ASA/PIX の設定
確認
ASA/PIX セキュリティ アプライアンス - show コマンド
トラブルシューティング
関連情報

概要

このドキュメントでは、Adaptive Security Device Manager (ASDM)か CLI を使用して、リモー ト VPN サーバとして機能し、着信 VPN Client トラフィックに NAT を実行するように Cisco 5500 シリーズ適応型セキュリティ アプライアンス (ASA)を設定する方法について説明します 。 ASDM では、直感的で使用が容易な Web ベースの管理インターフェイスにより、ワールドク ラスのセキュリティ管理と監視機能が提供されています。 Cisco ASA の設定が完了したら、 Cisco VPN Client を使用して設定を検証できます。

<u>前提条件</u>

<u>要件</u>

このドキュメントでは、ASA が完全に動作していて、Cisco ASDM か CLI で設定を変更できるように設定されていることを想定しています。 また、ASA をアウトバウンド NAT に関して設定することも想定しています。 アウトバウンド NAT の設定方法の詳細については、「<u>PAT を使用し</u> て内部ホストから外部ネットワークへアクセスを許可」を参照してください。

注: 「ASDM 用の HTTPS アクセスの許可」または「PIX/ASA 7.x: 内部および外部インターフェ

<u>イスの SSH の設定例</u>」を参照してください。

<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くものです。

- Cisco 適応型セキュリティ アプライアンス ソフトウェア バージョン 7.x 以降
- Adaptive Security Device Manager バージョン 5.x 以降
- Cisco VPN Client バージョン 4.x 以降

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たものです。 このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

関連製品

この設定は、Cisco PIX セキュリティ アプライアンス バージョン 7.x 以降にも適用できます。

表記法

ドキュメント表記の詳細は、『<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。

背景説明

リモート アクセス設定により、モバイル ユーザなどの Cisco VPN Client にセキュアなリモート アクセスが提供されます。 リモート アクセス VPN により、リモート ユーザが中央のネットワー ク リソースに安全にアクセスできるようになります。 Cisco VPN Client は IPSec プロトコルに 準拠しており、特にセキュリティ アプライアンスと連動する設計になっています。 一方、セキュ リティ アプライアンスは、多様なプロトコルに準拠するクライアントと IPSec 接続を確立できま す。 IPSec の詳細については、『<u>ASA 構成ガイド</u>』を参照してください。

グループとユーザは、VPN のセキュリティの管理とセキュリティ アプライアンスの設定では中 心となる概念です。 これらにより、ユーザによる VPN へのアクセスと使用を決定する属性が指 定されます。 グループはユーザの集合で、単一のエンティティとして扱われます。 ユーザは自身 の属性をグループのポリシーから取得します。 トンネル グループでは、特定の接続のグループ ポリシーが識別されます。 特定のグループ ポリシーをユーザに割り当てない場合は、その接続の デフォルトのグループ ポリシーが適用されます。

トンネル グループは、トンネル接続のポリシーを決定するレコードのセットで構成されています 。これらのレコードにより、トンネル ユーザが認証されているサーバ、および接続情報の送信先 となるアカウンティング サーバ(存在する場合)が識別され、 接続のデフォルトのグループ ポ リシーも識別されます。レコードには、プロトコル固有の接続パラメータも含まれています。 ト ンネル グループには、トンネル自体の作成に関連した少数の属性が含まれています。 トンネル グループには、ユーザ指向の属性を定義するグループ ポリシーに対するポインタが含まれていま す。

<u>設定</u>

<u>ASDM を使用した、リモート VPN サーバとしての ASA/PIX の設定</u>

ASDM を使用して Cisco ASA をリモート VPN サーバとして設定するには、次の手順を実行します。

 ブラウザを開き、https://<ASDM アクセス用に設定された ASA のインターフェイスの IP ア ドレス> を入力して、ASA 上の ASDM にアクセスします。SSL 証明書の信頼性に関連して ブラウザから出力されるすべての警告を承認します。 デフォルトのユーザ名とパスワード は、両方とも空白です。ASA がこのウィンドウを表示するのは、ASDM アプリケーション のダウンロードを許可するためです。 次の例の場合、アプリケーションはローカル コンピ ュータにロードされ、Java アプレットでは動作しません。

Sisco ASDM 6.1	cisco
Cisco ASDM 6.1(3) provides an intuitive graphical user interface that make configure and manage your Cisco Security Appliances.	es it easy to set up,
Cisco ASDM runs as either a local application or Java Web Start.	
 When you run Cisco ASDM as a local application, it connects to your Se your desktop via SSL. Running Cisco ASDM as an application has these You can invoke ASDM from desktop shortcuts. No browser is rec One desktop shortcut allows you to connect to <i>multiple</i> Security 	ecurity Appliance from advantages: quired. Appliances.
Install ASDM Launcher and Run ASDM	
 Running Cisco ASDM as Java Web Start You can run Cisco ASDM as Java Web Start that is dynamically downloat to which you connect. Click Run ASDM to run Cisco ASDM. Click Run Startup Wizard to run Startup Wizard.Startup Wizard 	aded from the device d walks you through,
step by step, the initial configuration of your security appliance.	_

- 3. ASDM Launcher がダウンロードされたら、プロンプトに従って一連のステップを実行し、 該当ソフトウェアをインストールした後、Cisco ASDM Launcher を起動します。
- 4. http コマンドで設定したインターフェイスの IP アドレスとユーザ名とパスワード(指定した場合)を入力します。次の例では、ユーザ名として cisco123 、パスワードとして cisco123 を使用しています。

	🖆 Cisco ASDM Launch	er v1.5(30)	
			cisco
	Device IP Address / Name:	10.77.241.111	_
	Username:	cisco123	
	Password:	* * * * * * *	
	🔲 Run in Demo Mode		
		ů.	1 🗐 🖆
5.	[Home] ウィンドウで、[Wi	zards] > [IPsec VPN Wizar	d] の順に選択します。
	🚰 Cisco ASDM 6.1 for	ASA - 10.77.241.111	

CIGCO ASDIN 0.1101 ASA - 10.77.241.111				
File View Tools	Wizards Window Help			
Home 🖧 Cor	Startup Wizard			
Device List	IPsec VPN Wizard			
	SSL VPN Wizard			
🔁 Add 🔟 Delete	High Availability and Scalability Wizard			
10.77.241.1	Packet Capture Wizard			

6. 次に示すように、[Remote Access] VPN トンネル タイプを選択し、VPN トンネル インター フェイスが意図どおりに設定されていることを確認し、[Next] をクリックします。

🖆 VPN Wizard			
VPN Wizard	VPN Tunnel Type (Step 1 of)		
Brandh Br	Use this wizard to configure new site-to-site VPN tunnels or new remote access VPN tunnels. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A tunnel established by calls from remote users such as telecommuters is called remote access tunnel. This wizard creates basic tunnel configurations that you can edit later using the ASDM.		
Corporate	VPN Tunnel Type: Site-to-Site VPN		
THE REAL	Site-to-Site		
	Remote Access		
	VPN Tunnel Interface: Outside		
	< Back Next > Finish Cancel Help		

7. 次に示すとおり、VPN クライアント タイプが選択されています。 ここでは、[Cisco VPN <u>Client]</u> が選択されています。 [Next] をクリックします。

🖆 VPN Wizard	
VPN Wizard	Remote Access Client (Step 2 of)
Branch	Remote access users of various types can open VPN tunnels to this ASA. Select the type of VPN client for this tunnel.
	VPN Client Type:
Home	
Corporate Norwork	Cisco VPN Client, Release 3.x or higher,
North	or other Easy VPN Remote product
THE THE	Microsoft Windows client using L2TP over IPsec
	Specify the PPP authentication protocol. If a protocol is not specified on the remote client, do not specify it.
- THUM	PAP V CHAP V MS-CHAP-V1 MS-CHAP-V2 EAP-PROXY
	Specify if the client will send tunnel group name as - username@tunnelgroup.
- 6	Client will send tunnel group name as username@tunnelgroup.
	If pre-shared authentication is used with this option then DefaultRAGroup's pre-shared key and ppp authentication are also modified.
	< Back Next > Finish Cancel Help

8. [Tunnel Group Name] の名前を入力します。 使用する認証情報(この例では**事前共有キー**)を入力します。 次の例では、cisco123 という事前共有鍵を使用しています。 この例で使 用しているトンネル グループ名は cisco です。 [Next] をクリックします。

🖆 VPN Wizard	
VPN Wizard	VPN Client Authentication Method and Tunnel Group Name (Step 3 of)
Branch Branch Horne Horne	The ASA allows you to group remote access tunnel users based on common connection parameters attributes configured in the subsequent screens. Configure authentication method and tunel group for this remote connection. Use the same tunnel group name for the device and the remote cient. Authentication Method Pre-shared key Pre-Shared Key: cisco123 Certificate Certificate Signing Algorithm: rsa-sig Certificate Name: Challenge/response authentication (CRACK)
	< Back Next > Finish Cancel Help

9. リモート ユーザの認証用にローカル ユーザのデータベースか外部 AAA サーバ グループを 選択します。注: ステップ 10 で、ローカル ユーザのデータベースにユーザを追加します。 注: ASDM で外部 AAA サーバ グループを設定する方法の詳細については、「<u>PIX/ASA</u> <u>7.x : ASDM での VPN ユーザの認証と認可サーバ グループの設定例</u>」を参照してください

o

🖆 VPN Wizard		×
VPN Wizard	Client Authentication (Step 4 of)	
Branch Branch Home Home Home Home	To authenticate remote users using local device user database, select the first option below. You can create user accounts in the next step. To use external AAA servers instead, select the second option. You can select an existing AAA server group or create a new one using the New button below. To manage all other AAA settings, go to Configuration > Device Management > Users/AAA in the main ASDM window.	
	< Back Next > Finish Cancel He	þ

10. [Username] とオプションの [Password] を入力し、[Add] をクリックして、ユーザ認証デー タベースに新しいユーザを追加します。 [Next] をクリックします。注: このウィンドウで 既存のユーザを削除しないようにしてください。 データベースの既存エントリを編集する 、またはデータベースから既存エントリを削除するには、メインの [ASDM] ウィンドウで 、[Configuration] > [Device Management] > [Users/AAA] > [User Accounts] の順に選択しま す。

🖆 VPN Wizard			×
VPN Wizard	User Accounts (Step 5 of 11)		
	Add new users into the user authe or to remove them from the datab Users/AAA > User Accounts in the	entication database. To edit existing entries in the database ase, go to Configuration > Device Management > main ASDM window.	
Home	User to Be Added		
Corporate Network	Username:	dsco123	4
THE THE	cisco	Add >>	
	Password (optional):	Delete	
THUM	•••••		
THEFT	Confirm Password (optional):		
	•••••		
		< Back Next > Finish Cancel Hei	P

11. リモート VPN クライアントに動的に割り当てられるローカル アドレスのプールを定義す <u>るには、[New] をクリックして、新しい IP プール</u>を作成します。

🖆 VPN Wizard		Σ	<
VPN Wizard	Address Pool	(Step 6 of 11)	
Branch Branch Designed Home Corporate	Enter a po clients.	ol of local addresses to be used for assigning dynamic IP addresses to remote VPN Tunnel Group Name : cisco	
Notwork		Pool Name: New	
		Subnet Mask:	
		< Back Next > Finish Cancel Help	

12. [Add IP Pool] という名前の新しいウィンドウに以下の情報が表示されたら、[OK] をクリックします。IP プールの名前開始 IP アドレス終了 IP アドレスサブネット マスク

1	Add IP Pool	2	×
	Name:	vpnpool	
	Starting IP Address:	192.168.1.1	
	Ending IP Address:	192.168.1.254	
	Subnet Mask:	255.255.255.0	
	ОКЪС	Cancel Help	

13. リモート VPN クライアントの接続時に動的に割り当てられるローカル アドレスのプール を定義したら、[Next] をクリックします。

🖆 VPN Wizard					×
VPN Wizard	Address Pool	(Step 6 of 11)			
Branch Branch Branch Branch Home Home	Enter a po clients.	ol of local addresses to be use	ed for assigning dynamic IP	addresses to remote VPN	
Corporate Network		Tunnel Group Name :	cisco		
CUTT IN		Pool Name:	vpnpool	New	
		Pool Settings Range Start Address:	192.168.1.1		
		Range End Address:	192.168.1.254		
		Subnet Mask:	255.255.255.0		
	L				-
			< Back Next >	Finish Cancel He	Þ

14. オプション:DNS と WINS のサーバ情報、およびリモート VPN Client にプッシュするデ

フォルトのドメイン名を指定します。

🖆 VPN Wizard		
VPN Wizard	Attributes Pushed to Client (Optional)(Step 7 of 11)
Bronch Bronch Bronch Bronch Bronch Bronch Bronch Bronch Bronch Bronch Bronch	Attributes you configure below are push ASA. If you do not want an attribute pus	ed to the VPN client when the client connects to the shed to the client, leave the corresponding field blank.
Corporate	Tunnel Group:	cisco
The states in	Primary DNS Server:	I
	Secondary DNS Server:	
TIMU	Primary WINS Server:	
TIT	Secondary WINS Server:	
	Default Domain Name:	
		< Back Next > Finish Cancel Help

15. IKE のパラメータを指定します。これは IKE フェーズ 1 とも呼ばれます。トンネルの両側 の設定は完全に一致している必要があります。 ただし、Cisco VPN Client では適切な設定 が自動的に選択されます。 そのため、クライアント PC で IKE を設定する必要はありませ ん。

🖆 VPN Wizard		×
VPN Wizard	IKE Policy (Step 8 of 11)	
Branch Branch F F F F F F F F F F F F F F F F F F F	Select the encryption algorithm, authentication algorithm, and Diffie-Hellman group for the devices to use to negotiate an Internet Key Exchange (IKE) security association between them. Configurations on both sides of the connection must match exactly.	
Network	Encryption: DES	
	Authentication:	
	Diffie-Helman Group: 2	
	< Back Next Finish Cancel Help	,

16. このウィンドウにはユーザが行った操作の概要が表示されます。 設定に問題がなければ、 [Finish] をクリックします。



<u>ASDM を使用した、着信 VPN クライアント トラフィックを NAT するための</u> <u>ASA/PIX の設定</u>

ASDM を使用して、着信 VPN クライアント トラフィックを NAT するために Cisco ASA を設定 するには、次の手順を実行します。

1. [Configuration] > [Firewall] > [Nat Rules] の順に選択し、[Add] をクリックします。 ドロップ ダウンリストで、[Add Dynamic NAT Rule] を選択します。



2. [Add Dynamic NAT Rule] ウィンドウで、インターフェイスとして [Outside] を選択し、 [Source] ボックスの横にある [Browse] ボタンをクリックします。

G	Add Dyna	amic NAT Rule		
Or	iginal Interface: Source:	Outside		
Tra	anslated — Select a glo	bal pool for dynamic tr	anslation.	
	Pool ID	Interface	Addresses Pool	
	0	(outbound)	Same as original address (identity)	
	0	(inbound)	Same as original address (identity)	
				Manage
6	onnectio	n Settings		*
			OK Cancel Help	

3. [Browse Source] ウィンドウで適切なネットワーク オブジェクトを選択し、[Selected Source] セクションの下で [Source] を選択し、[OK] をクリックします。 ここでは、 192.168.1.0 ネットワーク オブジェクトが選択されています。

🖆 Browse Source				
🗣 Add 📝 Edit 📋 Dele	te Q			
Filter:				Filter Clear
Name ^1	IP Address	Netmask	Description	
⊡ Network Objects				
- 🌍 any	0.0.0	0.0.0.0		
📲 inside-network	172.16.1.0	255.255.255.0		
- 🚮 Outside-network	10.10.10.0	255.255.255.0		
- 1 92.168.1.0	192.168.1.0	255.255.255.0		
			-	
Selected Source				
	8.1.0/24			
				Cancel

4. [Manage] をクリックします。

🖆 Add Dy	namic NAT Rule		X
Original Interface Source: Translated - Select a g	: Outside 192.168.0.0	translation.	
Pool ID 0	Interface (outbound) (inbound)	Addresses Pool Same as original address (identity) Same as original address (identity)	Manage
Connecti	on Settings		۲
		OK Cancel Help	

5. [Manage Global Pool] ウィンドウで、[Add] をクリックします。

🖆 Manage Global Pool 🛛 🛛 🔀				
🕂 Add 🗹 Eo	lit 💼 Delete			
Pool ID	Interface	Addresses Pool	1	
			_	
-				
	ОК	Cancel Help		

6. [Add Global Address Pool] ウィンドウで、インターフェイスとして [Inside] を選択し、[Pool ID] として 2を選択します。 [Port Address Translation (PAT) using IP Address of the interface] の横のオプション ボタンが選択されていることも確認してください。 [Add>>] を クリックして、[OK] をクリックします。

📧 Add Global Address Pool		X
Interface: inside Pool ID: 2		
IP Addresses to Add Range Starting IP Address: Ending IP Address: Netmask (optional): IP Address Translation (PAT) IP Address: Netmask (optional):	Add >> << Delete	Addresses Pool
Port Address Translation (PAT) using IP Address of the interface OK OK	Cancel	Help

7. 前のステップで設定した**Pool ID 2** が設定されたグローバル プールを選択したら、[OK] をク リックします。

🕵 Add Dyn	amic NAT Rule		
Original			
Interface:	Outside	~	
Source:	192.168.1.0/24		
Translated -			
Select a glo	obal pool for dynamic	translation.	
Pool ID	Interface	Addresses Pool	
0	(outbound)	Same as original address (identity)	
0	(inbound)	Same as original address (identity)	
2	inside	🔤 inside	Manage
Connectio	n Settings		8
Connectio			
		OK Cancel Help	

8. ここで、[Apply] をクリックすると、設定が ASA に適用されます。これで設定は終了です。

Configura	Configuration > Firewall > NAT Rules					
💠 Add	🝷 📑 Edit 🎁 Dele	te 🛧 🗸 🕉 🖿	n 💼 - 🛛 🔍 Find 🗄	🔁 Diagram 🗐	Packet Trace	
	Turne	Original			Translated	
*	туре	Source	Destination	Service	Interface	Addre
🖬 Outsid	le (1 Dynamic rules)					
1	Dynamic	192.168.1.0/24			inside	🛲 insia
⊡ inside	(1 Exempt rules, 1 Dy	namic rules)				
1	🔁 Exempt	🏈 any	192.168.1.0/24		(outbound)	
2	📊 Dynamic	🏈 any			Outside	🎫 Out
Epabl	e traffic through the	firewall without address	translation			<u>(*)</u>
	a dan con ough dio		y Reset]		

<u>CLI を使用した、リモート VPN サーバとして、および着信を NAT するための</u> <u>ASA/PIX の設定</u>

ASA デバイスでの設定の実行
ciscoasa# show running-config : Saved ASA Version 8.0(3)
! hostname ciscoasa enable password 8Ry2YjIyt7RRXU24
encrypted names ! interface Ethernet0/0 nameif Outside
security-level 0 ip address 10.10.10.2 255.255.255.0 !
interface Ethernet0/1 nameif inside security-level 100
ip address 172.16.1.2 255.255.255.0 ! ! passwd
2KFQnbNIdI.2KYOU encrypted boot system disk0:/asa803-
k8.bin ftp mode passive access-list inside_nat0_outbound
extended permit ip any 192.168.1.0 255.255.255 0 pager
lines 24 logging enable mtu Outside 1500 mtu inside 1500
ip local pool vpnpool 192.168.1.1-192.168.1.254 mask
255.255.255.0 no failover icmp unreachable rate-limit 1
burst-size 1 asdm image disk0:/asdm-615.bin asdm history
enable arp timeout 14400 nat-control global (Outside) 1
interface global (inside) 2 interface nat (Outside) 2

192.168.1.0 255.255.255.0 outside nat (inside) 0 accesslist inside_nat0_outbound nat (inside) 1 0.0.0.0 0.0.0.0 route Outside 0.0.0.0 0.0.0.0 10.10.10.3 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 sipdisconnect 0:02:00 timeout uauth 0:05:00 absolute dynamic-access-policy-record DfltAccessPolicy http server enable no snmp-server location no snmp-server contact !--- Configuration for IPsec policies. !---Enables the crypto transform configuration mode, !--where you can specify the transform sets that are used !--- during an IPsec negotiation. crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set pfs group1 crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set transform-set ESP-DES-SH ESP-DES-MD5 crypto map Outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP crypto map Outside_map interface Outside crypto isakmp enable Outside !---Configuration for IKE policies. !--- Enables the IKE policy configuration (config-isakmp) !--- command mode, where you can specify the parameters that !--- are used during an IKE negotiation. Encryption and !--- Policy details are hidden as the default values are chosen. crypto isakmp policy 10 authentication pre-share encryption des hash sha group 2 lifetime 86400 crypto isakmp policy 30 authentication pre-share encryption des hash md5 group 2 lifetime 86400 telnet timeout 5 ssh timeout 60 console timeout 0 management-access inside threat-detection basic-threat threat-detection statistics access-list group-policy cisco internal group-policy cisco attributes vpn-tunnel-protocol IPSec !--- Specifies the username and password with their !--respective privilege levels username cisco123 password ffIRPGpDSOJh9YLq encrypted privilege 15 username cisco password ffIRPGpDSOJh9YLq encrypted privilege 0 username cisco attributes vpn-group-policy cisco tunnel-group cisco type remote-access tunnel-group cisco generalattributes address-pool vpnpool default-group-policy cisco !--- Specifies the pre-shared key "cisco123" which must !--- be identical at both peers. This is a global !--- configuration mode command. tunnel-group cisco ipsec-attributes pre-shared-key * ! class-map inspection_default match default-inspection-traffic ! ! policy-map type inspect dns migrated_dns_map_1 parameters message-length maximum 512 policy-map global_policy class inspection_default inspect dns migrated_dns_map_1 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 ! servicepolicy global_policy global prompt hostname context Cryptochecksum:f2ad6f9d5bf23810a26f5cb464e1fdf3 : end ciscoasa#



ASA の設定に成功したことを検証するには、Cisco VPN Client を使用して Cisco ASA に接続して

みます。

1. [New] をクリックします。

VPN Client - Version 5.0.03.0530			
Connection Entries Status Certificates Log Options	Help		
Connect News Import Modify) Delete		cisco
Connection Entries Certificates Log			
Connection Entry	Host	Transport	
I Not connected			

2. 新しい接続の詳細情報を入力します。[Host] フィールドには、設定済みの Cisco ASA の IP アドレスまたはホスト名が含まれている必要があります。 グループ認証情報は、ステップ 4 で使用した情報と一致している必要があります。 終了したら、[Save] をクリックします。

VPN Client Create New VPN Connection Entry				
Connection Entry: MyVPNClient				
Description:				
Host: 10.10.10.2	cisco			
Authentication Transport Backup Servers Dial-Up				
Group Authentication	Authentication			
Name: cisco				
Password: ******				
Confirm Password:				
Certificate Authentication Name: Send CA Certificate Chain				
Erase User Password Save	Cancel			

3. 新しく作成した接続を選択し、Connect をクリックします。

🥔 status: Disconnected VPN Client	- Version 5.0.03.0530		
Connection Entries Status Certificates Log	Options Help		
Confuct New Import	Kodify Delete		cisco
Connection Entries Certificates Log			
Connection Entry	Host	Transport	
MyVPNClient	10.10.10.2	IPSec/UDP	
Not connected.			

4. 拡張認証用のユーザ名とパスワードを入力します。 この情報は、**ステップ5と6**で指定した情報と一致している必要があります。

VPN Client User Authentication for "MyVPNC	Client" 🛛 🔀
The server has requested the following information to complete t authentication.	he user
Cisco Cisco Password:	
ОК	Cancel

5. 接続が正常に確立されたら、[Status] メニューから [Statistics] を選択し、トンネルの詳細情 報を確認します。

🥔 status: Connected V	PN Client - Version 5.	0.03.0530				
Connection Entries Status Ce	ertificates Log Options H	Help				
Disconnect N	tics Ctrl+S cations Ctrl+N	Delete		() (ı. 0
Connection Entries	stats					
Connection Entry	Δ	Host		Transport		
MyVPNClient		10.10.10.2		IPSec/UDP		
Connected to "My¥PNClient".			Connected Ti	me: 0 day(s), 00:00.36		▼ //

次のウィンドウには、トラフィックと暗号の情報が表示されています。

VPN Client Statistics						
Tunnel Details Route Details	Firewall					
ہج Address Information Client: 192.168.1.1 Server: 10.10.10.2 Butes	Connection Inform Entry: Time: Crypto	ation MyVPNClient 0 day(s), 00:01.13				
Received: 5412	Encryption:	56-bit DES				
Packets Encrypted: 39 Decrypted: 31 Discarded: 8 Bypassed: 22	Transport Transparent Tunn Local LAN: Compression:	eling:Inactive Disabled None Reset Close				
└────────────────────────────────────						
VPN Client Statistics						
Tunnel Details Route Details	Firewall					
Local LAN Routes	Secured Ro	utes				
Network Subnet Mask	k Network	Subnet Mask				
	0.0.0	0.0.0.0				

ASA/PIX セキュリティ アプライアンス - show コマンド

Close

[•] show crypto isakmp sa:現在ピアにあるすべての IKE SA を表示します。ASA#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: 10.10.10.1 Type : user Role : responder Rekey : no State : AM_ACTIVE

- show crypto ipsec sa: 現在ピアにあるすべての IPSec SA を表示します。ASA#show crypto ipsec sa interface: Outside Crypto map tag: SYSTEM_DEFAULT_CRYPTO_MAP, seq num: 65535, local addr: 10.10 .10.2 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0) current_peer: 10.10.10.1, username: ciscol23 dynamic allocated peer ip: 192.168.1.1 #pkts encaps: 20, #pkts encrypt: 20, #pkts digest: 20 #pkts decaps: 74, #pkts decrypt: 74, #pkts verify: 74 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 20, #pkts comp failed: 0, #pkts decomp failed: 0 #prefrag 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.: 10.10.10.2, remote crypto endpt.: 10.10.10.1 path mtu 1500, ipsec overhead 58, media mtu 1500 current outbound spi: F49F954C inbound esp sas: spi: 0x3C10F9DD (1007745501) transform: esp-des esp-md5-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 24576, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP sa timing: remaining key lifetime (sec): 27255 IV size: 8 bytes replay detection support: Y outbound esp sas: spi: 0xF49F954C (4104099148) transform: esp-des esp-md5-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 24576, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP sa timing: remaining key lifetime (sec): 27255 IV size: 8 bytes replay detection support: Y
- ciscoasa(config)#debug icmp trace !--- Inbound Nat Translation is shown below for Outside to Inside ICMP echo request translating Outside:192.168.1.1/768 to inside:172.16.1.2/1 ICMP echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=7936 len=3 2 !--- Inbound Nat Translation is shown below for Inside to Outside ICMP echo reply untranslating inside:172.16.1.2/1 to Outside:192.168.1.1/768 ICMP echo request from Outside:192.168.1.1 to inside:172.16.1.3 ID=768 seq=8192 len=32 ICMP echo request translating Outside:192.168.1.1/768 to inside:172.16.1.2/1 ICMP echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=8192 len=3 2 ICMP echo reply untranslating inside:172.16.1.2/1 to Outside:192.168.1.1/768 ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8448 len=32 ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8448 len=32 ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8704 len=32 ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8704 len=32 ICMP echo reply from 172.16.1.2 ID=768 seq=8960 len=32 ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8960 len=32

<u>トラブルシューティング</u>

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

<u>Output Interpreter Tool</u>(OIT)(<u>登録</u>ユーザ専用)では、特定の show コマンドがサポートされ ています。 OIT を使用して、show コマンド出力の解析を表示できます。

サイト間 VPN のトラブルシューティングの詳細については、「<u>一般的な L2L およびリモート ア</u> <u>クセス IPSec VPN のトラブルシューティング ソリューション</u>」を参照してください。

関連情報

- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- <u>Cisco Adaptive Security Device Manager</u>
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス(ASA)のトラブルシューテ ィングとアラート
- ・<u>テクニカルサポートとドキュメント Cisco Systems</u>