ASA 8.x:ASA で AnyConnect VPN Client のス プリット トンネリングを許可するための設定例

内容

概要 <u>前提条件</u> <u>要件</u> 使用するコンポーネント 表記法 <u>背景説明</u> 設定 <u>ネットワーク図</u> ASDM 6.0(2) を使用した ASA 設定 ASDM 6.0(2) を使用した ASA 設定 ASA CLI の設定 SVC との SSL VPN 接続の確立 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、Cisco Adaptive Security Appliance(ASA)8.0.2にトンネル接続されている 状態でCisco AnyConnect VPNクライアントからインターネットにアクセスする方法を順を追って 説明します。この設定では、スプリットトンネリングを使用してセキュアでないアクセスを許可 します。

<u>前提条件</u>

<u>要件</u>

この設定を行う前に、次の要件が満たされていることを確認します。

- ASA セキュリティ アプライアンスはバージョン 8.x を稼動する必要があります。
- Cisco AnyConnect VPN Client 2.x注: AnyConnect VPN Clientパッケージ(anyconnectwin*.pkg)は、Cisco Software Download(登録ユーザ<u>専用</u>)からダウンロードします。
 AnyConnect VPN クライアントを ASA のフラッシュ メモリにコピーします。これは、ASA との SSL VPN 接続を確立するためにリモート ユーザ コンピュータにダウンロードされます。
 詳細については、ASA コンフィギュレーション ガイドの「AnyConnect クライアントのインストール」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いています。

- ・ソフトウェア バージョン 8.0(2) が稼働している Cisco 5500 シリーズ ASA
- Windows 2.0.0343 用のバージョンの Cisco AnyConnect SSL VPN Client
- Microsoft Installer バージョン 3.1 によって Microsoft Visa、Windows XP SP2、または Windows 2000 Professional SP4 が稼動している PC
- Cisco Adaptive Security Device Manager (ASDM) $\mathcal{N} \mathcal{V} = \mathcal{V} 6.0(2)$

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。

<u>表記法</u>

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>

Cisco AnyConnect VPN Client は、リモート ユーザのためにセキュリティ アプライアンスへのセ キュアな SSL 接続を提供しています。以前にインストールしたクライアントがない場合、リモー ト ユーザは SSL VPN 接続を受け入れるように設定したインターフェイスのブラウザに IP アドレ スを入力します。セキュリティ アプライアンスが http:// 要求を https:// にリダイレクトするよう に設定されていない場合、ユーザは https://<address> の形式で URL を入力する必要があります 。

URL を入力した後、ブラウザは、そのインターフェイスに接続し、ログイン画面を表示します。 ユーザがログインと認証を満たし、セキュリティアプライアンスがユーザをクライアントが必要 であると識別すると、リモートコンピュータのオペレーティングシステムに一致するクライアン トをダウンロードします。ダウンロード後、クライアントは自身をインストールして設定し、セ キュアな SSL 接続を確立して、接続が終了したときに自身を残すか、アンインストールします (これは、セキュリティ アプライアンスの設定に従います)。

以前にインストールされているクライアントの場合、ユーザが認証を行うと、セキュリティ アプ ライアンスはクライアントのリビジョンを調査して、必要に応じてクライアントをアップグレー ドします。

クライアントは、セキュリティ アプライアンスと SSL VPN 接続をネゴシエートすると、 Transport Layer Security(TLS)を使って接続し、オプションで Datagram Transport Layer Security(DTLS)に接続します。DTLS は、SSL 接続の一部に関連する遅延と帯域幅の問題を回 避し、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスを向上 させます。

AnyConnect クライアントは、セキュリティ アプライアンスからダウンロードすることも、シス テム管理者がリモートの PC に手動でインストールすることもできます。クライアントを手動で イ<u>ンストールする方法の詳細について</u>は、『<u>Cisco AnyConnect VPN Client管理者ガイド</u>』を参照 してください。 セキュリティ アプライアンスは、グループ ポリシーや接続を確立するユーザのユーザ名属性に基 づいてクライアントをダウンロードします。セキュリティ アプライアンスは、クライアントを自 動的にダウンロードするように設定することも、クライアントをダウンロードするかどうかをユ ーザにプロンプトで表示してから設定することもできます。後者の場合、ユーザが応答しないと きには、タイムアウト期間が経過した後にクライアントをダウンロードするか、ログイン ページ を表示するか、いずれかを実行するようにセキュリティ アプライアンスを設定できます。

<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。



注:この設定で使用されるIPアドレッシング方式は、インターネット上で正式にルーティング可 能なものではありません。これらは、ラボ環境で使用された <u>RFC 1918</u> のアドレスです。

<u>ASDM 6.0(2) を使用した ASA 設定</u>

このドキュメントは、インターフェイス設定などの基本設定がすでに行われていて適切に動作し ていることを前提としています。

注:ASAをASDMで設定<u>するには、『</u>ASDMでのHTTPSアクセスの許可』を参照してください。

注:ポート番号を変更しない限り、WebVPNとASDMを同じASAインターフェイスで有効にする ことはできません。詳細は、「<u>ASA の同じインターフェイスでイネーブルになる ASDM および</u> <u>WebVPN」を参照してください。</u> 次の手順を実行すると、ASA 上でスプリット トンネリングを備えた SSL VPN を設定できます。

1. [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Management] > [Address Pools] > [Add] を選択し、IP アドレス プール vpnpool を作成しま

	付 Add IP Pool		
	Name:	vpnpool	
	Starting IP Addr	ess: 192.168.10.1	
	Ending IP Addre	ss: 192.168.10.2	54
	Subnet Mask:	255.255.255.0	
व 。	ок	Cancel	Help

- 2. [Apply] をクリックします。同等の CLI 設定
- 3. WebVPN をイネーブルにします。[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [SSL VPN Connection Profiles] を選択し、[Access Interfaces] の下で、外 部インターフェイスに対して [Allow Acces] と [Enable DTLS] のチェックボックスをオンに します。また、[Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interface selected in the table below] チェックボックスをオンにし、外部インターフェイ スで SSL VPN を有効にします。

Configuration > Remo	ote Access VPN > Net	work (Client) Access > SSL VPN	l Connection Profiles		
The security applianc client deployment rec Layer Security (DTLS)	e automatically deploys juires end-user administ) tunneling options.	the Cisco AnyConnect VPN Client or rative rights. The Cisco AnyConnect	r legacy SSL VPN Client to VPN Client supports the		
(More client-related)	parameters, such as clie	nt images and client profiles, can be	e found at <u>Client Settings</u>		
Access Interfaces –					
Enable Cisco Any	Connect VPN Client or le	gacy SSL VPN Client access on the i	nterfaces selected in the		
Interface	Allow Access	Require Client Certificate	Enable DTLS		
outside					
inside					
Access Port: 443 DTLS Port: 443					
Click here to Assign (Certificate to Interface.				

[Apply] をクリックします。[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [SSL VPN] > [Client Settings] > [Add] を選択し、次に示すように Cisco AnyConnect VPN のクライアント イメージを ASA のフラッシュ メモリから追加しま す。

줄 Add SSL VPN Client Image		X SSL VPN > Clie	nt Settings
Flash SVC Image:	Browse Flash Upload	Duntered operati	on system to the top of the
🔂 Browse Flash			×
Folders	Files		
e→ eisk0:	FileName ▲ □ crypto_archive □ □ log asdm-603.bin asa803-k8.bin admin.cfg anyconnect-win-2.0.03 asdm-602.bin asadm-602.bin asa722-k8.bin asa802-k8.bin old_running.cfg sslclient-win-1.1.4.179 sslclient-win-1.1.4.179	Size (bytes) 6,851,212 14,635,008 1,220 2,635,734 6,889,764 8,312,832 5,623,108 14,524,416 1,841 418,765	Date Modified 07/24/07 05:21:48 07/24/07 05:21:36 01/04/08 18:07:02 01/04/08 17:49:50 09/20/07 09:51:38 08/13/07 04:14:50 01/03/08 21:38:26 02/13/07 04:16:30 02/12/07 05:53:48 01/03/08 21:24:42 09/20/07 09:51:38 03/14/08 13:47:58
File Name: [OK] をクリックします。 ide Add SSL VPN Client Ime Flash SVC Image: ct-win-2.	anyconnect-win-2.0.0343-k9.p age 0.0343-k9.pkg Uploa	kg =lash	
ОК	Cancel Help		クリックします。
Configuration > Remote Access	VPN > Network (Client) Acce	ess > Advanced > SS	ノファフレます。 L VPN > Client Settings
Identify SSL VPN Client (SVC) rel	ated files.		Ŭ
CEL VDN Client Images			
Minimize connection setup time b	y moving the image used by the	most commonly encour	tered operation system to t
	shake in the image dated by the t	nose commonly encour	korod operation system to t
🗘 Add 🧭 Replace 🕅 D	elete 😙 Move UP 🗣 Move	Down	

disk0:/anyconnect-win-2.0.0343-k9.pkg

同等の CLI 設定

4. グループ ポリシーを設定します。[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] を選択し、内部グループ ポリシー clientgroup を作成しま す。[General] タブの下で、[SSL VPN Client] チェックボックスをオンにし、トンネリング プロトコルとして WebVPN を有効にします。

🗯 Add Internal Group Policy	
General	Name: (clientgroup
-Advanced	Banner: 🔽 Inherit
	Address Pools: 🔽 Inherit
H-IPsec Clienc	More Options
	Tunneling Protocols: 🔲 Inherit 🔲 Clientless SSL VPN 💭 SSL VPN Client 🔲 IPsec

[Advanced] > [Split Tunneling] タブで、スプリット トンネル ポリシー用の [Inherit] チェック ボックスをオフにして、ドロップダウン リストから [Tunnel Network List Below] を選択しま

す。		
🔂 Add Internal Group Policy		×
General Servers Advanced	Split tunneling network lists distinguish networks that require traffic to go through the tunnel and those that do not require tunneling. The security appliance makes split tunneling decisions on the basis of a network list, which is an ACL that consists of list of addresses on the private network.	
B−SSL VPN Client B−IPsec Client	Policy: Inherit Tunnel All Networks Network List: Inherit Tunnel All Networks Tunnel Network List Below Manage Exclude Network List Below Exclude Network List Below	

[Split Tunnel Network List] の [Inherit] チェック ボックスをオフにして [Manage] をクリック することで、ACL Manager を起動します。 がEdit Internal Group Policy: hivalleyypn

General Servers Advanced	Split tunneling network lists distinguish networks that require traffic to go through the tunnel and those that do not require tunneling. The security appliance makes split tunneling decisions on the basis of a network list, which is an ACL that consists of list of addresses on the private network.
IE Browser Proxy	DNS Names: 🔽 Inherit
E IPsec Client	Policy: Inherit Tunnel Network List Below
Client Access Rule Client Firewall Hardware Client	Network List: None Manage

[ACL Manager] で、[Add] > [Add ACL...] の順に選択して、新しいアクセス リストを作成し ます。

is ALL Manager				
Standard ACL Extended	ACL			
💠 Add 🕞 🗹 Edit 📋	Delete 🛧 🗲	1 % 🖻 🛍	-	
🔂 Add ACL	dress	Action	De	scription
🔂 Add ACE				

ACL に名前を指定して [OK] をクリックします。

i	ACL Manag	er				
	Standard AC	エ Extende	HACL			
	💠 Add 🕞	💣 Edit 🥤	🕽 Delete 🕈 🔸	- X == == -	-	
	No	Д	ddress.	Action		Description
	🔂 Add A	EL			×	
	ACL Nar	ne: split-tuni	nel			

ACL 名が作成されてから、[Add] > [Add ACE] を選択して Access Control Entry (ACE; アク セス コントロール エントリ)を追加します。ASA の背後にある LAN に対応する ACE を定 義します。この場合、ネットワークは 10.77.241.128/26 であり、[Action] として [Permit] を 選択します。[OK] をクリックして [ACL Manager] を終了します。

		_ · · · _	-		
No	Address	Action	C	escription	
split-tunnel					
🔄 Add ACE					
Action					
Action:	🖌 Permit 🔄				
Host/Netv	vork				
IP Addre	ess: 10.77.241.128				-
Netmasl	k 255.255.255.192				_
	· ·				
Description:	:				

作成したばかりの ACL が split-tunnel ネットワーク リスト用に選択されていることを確認し ます。[OK] をクリックして、グループ ポリシー設定に戻ります。

Ī	Add Internal Group Policy									×
	General Servers Advanced Splt Tunneling IE Browser Proxy SSL VPN Client	Split tunneling require tunne ACL that com DNS Names: Policy:	g network lists ling. The sect sists of list of Inherit Inherit	s distinguish nei urity appliance i addresses on t	works that red nakes split tun he private net ork List Below	uire traffic to neling decision work.	go through the t s on the basis of	unnel and tho a network list	ise that do not t, which is an	
		Network List:	🕅 Inherit	split-tunnel				V	Manage	
		Intercept	DHCP Confi	uration Mes	sage from M	icosoft Clien	ts		8	

メインページで、[Apply]をクリックしてから [Send](必要な場合)をクリックして、コマ ンドを ASA に送信します。グループ ポリシー モードで SSL VPN を設定します。[Keep Installer on Client System] オプションで、[Inherit]チェック ボックスをオフにし、[Yes] オプ ション ボタンをクリックします。この操作によって、SVC ソフトウェアはクライアント マ シン上に留まります。これにより、ASA は接続が確立するたびに SVC ソフトウェアをクラ イアントにダウンロードする必要がなくなります。このオプションは、社内ネットワークに 頻繁にアクセスするリモート ユーザが選択するのに適しています。 Edit Internal Group Policy: clientgroup

General	Keep Installer on Client System:	🔲 Inherit	• Yes	C No
Servers	Compression:	🔽 Inherit	C Enable	C Disab
-Split Tunneling 	Datagram TLS:	🔽 Inherit	C Enable	C Disab
	Keepalive Messages:	🔽 Inherit	🔲 Disable	Interval:

[Login Setting] をクリックして、次に示すように [Post Login Setting] と [Default Post Login Selection] を設定します。

-General -Servers	After successfully logging in, user can have the choice to download the client software, or g portal page. The following settings decides what will happen.
-Advanced	Inherit
IE Browser Proxy	Post Login Setting
	Do not prompt user to choose
Key Regeneration	C Prompt user to choose
Dead Peer Detecti	
	User has seconds to choose, or Default Post Login belection below is take
	Default Post Login Selection
	C Go to Clientless SSL VPN portal
	Download SSL VPN Client

[Renegotiation Interval] オプションで、[Inherit]チェック ボックスをオフにし、[Unlimited] チ ェックボックスをオフにし、キーの再生成が行われるまでの時間(分)を入力します。セ キュリティは、キーが有効である時間に制限を設けることで強化されます。[Renegotiation] Method] オプションで、[Inherit]チェック ボックスをオフにして、[SSL] オプション ボタン **をクリックします。**再ネゴシエーションは、現在の SSL トンネルまたは再ネゴシエーショ ン用に明示的に作成された新しいトンネルを使用できます。

General	Renegotia	tion Interval:	🔲 Inherit	🔲 Unlimited	1 30	minutes	
-Servers							
🗄 Advanced	Renegotia	ation Method:	🔲 Inherit	🔿 None	SSL .	O New	Tunnel
-Split Tunneling							
IE Browser Proxy							
SSL VPN Client							
Login Setting							
Key Regeneration)						
[OK] をクリックし、次に	[Apply] を	クリックし	ます。				
Configuration > Remote Acces	ss VPN > Neti	vork (Client) A	\ccess > Gra	up Policies			
Manage VPN group policies. A externally on a RADIUS/LDAP :	/PN group polic server. The gro	y is a collection oup policy inform	of user-orient ation is refere	ed attribute/val inced by VPN tu	ue pairs that n nnel groups ar	nay be stor nd user acc	ed inter ounts.
🗣 Add 🔻 🗹 Edit 📋 D	elete						
Name		Туре		Tunneli	ing Protocol		
		Interna	svc				N/A -
DfltGrpPolicy (System Default))	Interna	L2TF	-IPSec,IPSec,w	ebvpn		N/A -

同等の CLI 設定

5. [Configuration] > [Remote Access VPN] > [AAA Setup] > [Local Users] > [Add]を選択し、新 しいユーザアカウントssluser1を作成します。[OK]をクリックし、次に[Apply]をクリックし ます。

🔄 Add User Account	
Identity 	Username: ssluser1 Password: ****** Confirm Password: ****** User authenticated using MSCHAP
	Member-of
	Member-of: Add >> Delete
	Access Restriction
	Note: All users have betwork access, regardless of these settings
	Eull access(ASDM_SSH_Telpet and Console)
	Privilege level is used with command authorization. Privilege Level: 2
	CLI login prompt for SSH, Telnet and console (no ASDM access)
	This setting is effective only if AAA authenticate console command is configured.
	C No ASDM, SSH, Telnet or Console access
	This setting is effective only if AAA authenticate console command is configured.

6. [Configuration] > [Remote Access VPN] > [AAA Setup] > [AAA Servers Groups] > [Edit] を選 択し、[Enable Local User Lockout] チェック ボックスをオンにして最大試行値の 16 に設定 することで、デフォルトのサーバ グループ I OCAL を変更します。

Config	guration > Remote	Access VPN > AA	A Setup > AAA Server	Groups	
AAA :	Server Groups —				
	Server Group	Protocol	Accounting Mode	Reactivation Mode	
LO	CAL	LOCAL			
4	This feature before lockin when the loc Enable L Maximum	Allows you to speci g out and denying al database is used ocal User Lockout Attempts: 16	fy the maximum number of access to the user. This li I for authentication.	of failed attempts to allow mit is applicable only Help	×

- 7. [OK] をクリックし、次に [Apply] をクリックします。**同等の CLI 設定**
- 8. トンネル グループを設定します。[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [SSL VPN Connection Profiles Connection Profiles] > [Add] を選択し、新 しいトンネル グループ sslgroup を作成します。[Basic] タブで、次に示すように設定のリス トを実行できます。トンネル グループに sslgroup という名前を付けます。[Client Address Assignment] の下でドロップダウン リストからアドレス プール vpnpool を選択します。 [Default Group Policy] の下でドロップダウン リストからグループ ポリシー clientgroup を選 択します。

E Add SSL VPN Connection	Profile		
Basic	Name:	ssigroup	
E Advanced	Aliases:		
	Authentication —		
	Method:	🛈 AAA 🔿 Certificate 🔿 Both	
	AAA Server Group:	LOCAL	Manag
		Use LOCAL if Server Group fails	
	Client Address Assign	ment	
	DHCP Servers:		
	Client Address Pools:	vpnpool	Select
	Default Group Policy		
	Group Policy:	clientgroup	Manag
	SSL VPN Client Protoco	ol: 🔽 Enabled	
	ОК	Cancel Help	

[SSL VPN] > [Connection Aliases] タブの下で、グループ エイリアス名に **sslgroup_users** と 指定して [OK] をクリックします。

🔁 Add SSL VPN Connection Profile

Basic	Portal Page Customization: DfltCustomization
E-Advanced	
General	CSD Alternate Group Policy: [DfltGrpPolicy
Client Addressing Authentication	\square Enable the display of Radius Reject-Message on the
-Authorization Accounting	Connection Aliases
	Add E Delete
	🚰 Add Connection Alias 🛛 🔀
	Alias: sslgroup_users
	Enabled
	G OK Cancel Help
	Add 🗹 Delete [OK] をク

リックし、次に [Apply] をクリックします。**同等の CLI 設定**

9. NAT を設定します。[Configuration] > [Firewall] > [NAT Rules] > [Add Dynamic NAT Rule] を 選択し、Inside ネットワークからのトラフィックが Outside IP アドレス 172.16.1.5 で変換 できるようにします。

Add Dynamic	NAT Rule		
Driginal —			
Interface: insi	de	T	
Source: any	()		
franslated —			
Select a global (pool for dynamic translation.		
Pool ID	Interface	Addresses Poo	ol
0	(outbound)	Same as original address (identit	y)
0	(inbound)	Same as original address (identit	y)
	outcido		

クリックします。[OK] をクリックします。

ion > Firewall > NA	T Rules				
🕶 🗹 Edit 📋 De	lete 🛧 🗲 👗	🖻 💼 🛛 🔍 Q	Find 🔛 Diag	gram 🛛 🟹 Packet Tr	ace
Tupe		Original			
туре	Source	Destination	Service	Interface	
1 Dynamic rules)					
Dynamic	🌍 any			outside	
	ion > Firewall > NA • 2 Edit 1 De Type L Dynamic rules) Dynamic	ion > Firewall > NAT Rules ✓ ☑ Edit	ion > Firewall > NAT Rules ✓ Z Edit	ion > Firewall > NAT Rules ✓ Z Edit Delete	ion > Firewall > NAT Rules ✓ Z Edit

[Apply] をクリックします。**同等の CLI 設定**

10. VPN クライアントにネットワーク内から戻るトラフィックの NAT 免除を設定します。 ciscoasa(config)#access-list nonat permit ip 10.77.241.0 192.168.10.0 ciscoasa(config)#access-list nonat permit ip 192.168.10.0 10.77.241.0 ciscoasa(config)#nat (inside) 0 access-list nonat

<u>ASA CLI の設定</u>

Cisco ASA 8.0(2) ciscoasa(config)#show running-config : Saved : ASA Version 8.0(2) ! hostname ciscoasa domain-name default.domain.invalid enable password 8Ry2YjIyt7RRXU24 encrypted names 1 interface Ethernet0/0 nameif inside security-level 100 ip address 10.77.241.142 255.255.255.192 1 interface Ethernet0/1 nameif outside security-level 0 ip address 172.16.1.1 255.255.255.0 ! 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 boot system disk0:/asa802-k8.bin

ftp mode passive clock timezone IST 5 30 dns server-group DefaultDNS domain-name default.domain.invalid access-list split-tunnel standard permit 10.77.241.128 255.255.255.192 !--- ACL for Split Tunnel network list for encryption. access-list nonat permit ip 10.77.241.0 192.168.10.0 access-list nonat permit ip 192.168.10.0 10.77.241.0 !--- ACL to define the traffic to be exempted from NAT. pager lines 24 logging enable logging asdm informational mtu inside 1500 mtu outside 1500 ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0 !--- The address pool for the Cisco AnyConnect SSL VPN Clients no failover icmp unreachable rate-limit 1 burstsize 1 asdm image disk0:/asdm-602.bin no asdm history enable arp timeout 14400 global (outside) 1 172.16.1.5 !--- The global address for Internet access used by VPN Clients. !--- Note: Uses an RFC 1918 range for lab setup. !--- Apply an address from your public range provided by your ISP. nat (inside) 0 access-list nonat !--- The traffic permitted in "nonat" ACL is exempted from NAT. nat (inside) 1 0.0.0.0 0.0.0.0 route outside 0.0.0.0 0.0.0.0 172.16.1.2 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 http server enable http 0.0.0.0 0.0.0.0 inside no snmp-server location no snmp-server contact snmp-server enable traps snmp authentication linkup linkdown coldstart no crypto isakmp nat-traversal telnet timeout 5 ssh timeout 5 console timeout 0 threat-detection basic-threat threat-detection statistics access-list 1 class-map inspection_default match default-inspection-traffic 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 rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
webvpn enable outside
<pre>! Enable WebVPN on the outside interface svc image disk0:/anyconnect-win-2.0.0343-k9.pkg 1</pre>
<pre>! Assign an order to the AnyConnect SSL VPN Client image svc enable</pre>
<pre>! Enable the security appliance to download SVC images to remote computers tunnel-group-list enable</pre>
<pre>! Enable the display of the tunnel-group list on the WebVPN Login page group-policy clientgroup internal</pre>
<pre>! Create an internal group policy "clientgroup" group-policy clientgroup attributes vpn-tunnel-protocol svc</pre>
<pre>! Specify SSL as a permitted VPN tunneling protocol split-tunnel-policy tunnelspecified split-tunnel-network-list value split-tunnel</pre>
! Encrypt the traffic specified in the split tunnel
<pre>! Encrypt the traffic specified in the split tunnel ACL only webvpn</pre>
<pre>! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed</pre>
<pre>! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and</pre>
<pre>! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the</pre>
<pre>! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30</pre>
<pre>! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30</pre>
<pre>! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ! Command that specifies the number of minutes from the start of the location working the relevant to be</pre>
<pre>! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ! Command that specifies the number of minutes from the start of the ! session until the rekey takes place from 1 to 10080 (1 week) svc rekey method ssl</pre>
<pre>! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ! Command that specifies the number of minutes from the start of the ! session until the rekey takes place, from 1 to 10080 (1 week). svc rekey method ssl</pre>
<pre>! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ! Command that specifies the number of minutes from the start of the ! session until the rekey takes place, from 1 to 10080 (1 week). svc rekey method ssl ! Command that specifies that SSL renegotiation takes place during SVC rekey. svc ask none default svc</pre>
<pre>! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ! Command that specifies the number of minutes from the start of the ! session until the rekey takes place, from 1 to 10080 (1 week). svc rekey method ssl ! Command that specifies that SSL renegotiation takes place during SVC rekey. svc ask none default svc username ssluser1 password ZRhW85jZqEaVd5P. encrypted</pre>
<pre>! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ! Command that specifies the number of minutes from the start of the ! session until the rekey takes place, from 1 to 10080 (1 week). svc rekey method ssl ! Command that specifies that SSL renegotiation takes place during SVC rekey. svc ask none default svc username ssluser1 password ZRhW85jZqEaVd5P. encrypted ! Create a user account "ssluser1" tunnel-group</pre>
<pre>! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ! Command that specifies the number of minutes from the start of the ! session until the rekey takes place, from 1 to 10080 (1 week). svc rekey method ssl ! Command that specifies that SSL renegotiation takes place during SVC rekey. svc ask none default svc username ssluser1 password ZRhW85jZqEaVd5P. encrypted ! Create a user account "ssluser1" tunnel-group sslgroup type remote-access</pre>
<pre>! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ! Command that specifies the number of minutes from the start of the ! session until the rekey takes place, from 1 to 10080 (1 week). svc rekey method ssl ! Command that specifies that SSL renegotiation takes place during SVC rekey. svc ask none default svc username ssluser1 password ZRhW85jZqEaVd5P. encrypted ! Create a user account "ssluser1" tunnel-group sslgroup type remote-access</pre>
<pre>! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ! Command that specifies the number of minutes from the start of the ! session until the rekey takes place, from 1 to 10080 (1 week). svc rekey method ssl ! Command that specifies that SSL renegotiation takes place during SVC rekey. svc ask none default svc username ssluser1 password ZRhW85jZqEaVd5P. encrypted ! Create a user account "ssluser1" tunnel-group sslgroup type remote-access ! Create a tunnel group "sslgroup" with type as</pre>
<pre>! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ! Command that specifies the number of minutes from the start of the ! session until the rekey takes place, from 1 to 10080 (1 week). svc rekey method ssl ! Command that specifies that SSL renegotiation takes place during SVC rekey. svc ask none default svc username ssluser1 password ZRhW85jZqEaVd5P. encrypted ! Create a user account "ssluser1" tunnel-group sslgroup type remote-access ! Create a tunnel group "sslgroup" with type as remote access tunnel-group sslgroup general-attributes</pre>
<pre>! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ! Command that specifies the number of minutes from the start of the ! session until the rekey takes place, from 1 to 10080 (1 week). svc rekey method ssl ! Command that specifies that SSL renegotiation takes place during SVC rekey. svc ask none default svc username ssluser1 password ZRhW85jZqEaVd5P. encrypted ! Create a user account "ssluser1" tunnel-group sslgroup type remote-access ! Create a tunnel group "sslgroup" with type as remote access tunnel-group sslgroup general-attributes address-pool vpnpool</pre>
<pre>! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ! Command that specifies the number of minutes from the start of the ! session until the rekey takes place, from 1 to 10080 (1 week). svc rekey method ssl ! Command that specifies that SSL renegotiation takes place during SVC rekey. svc ask none default svc username ssluser1 password ZRhW85jZqEaVd5P. encrypted ! Create a user account "ssluser1" tunnel-group sslgroup type remote-access ! Create a tunnel group "sslgroup" with type as remote access tunnel-group sslgroup general-attributes address-pool vpnpool ! Associate the address pool vpnpool created default- group-policy clientgroup</pre>
<pre>! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ! Command that specifies the number of minutes from the start of the ! session until the rekey takes place, from 1 to 10080 (1 week). svc rekey method ssl ! Command that specifies that SSL renegotiation takes place during SVC rekey. svc ask none default svc username ssluser1 password ZRhW85jZqEaVd5P. encrypted ! Create a user account "ssluser1" tunnel-group sslgroup type remote-access ! Create a tunnel group "sslgroup" with type as remote access tunnel-group sslgroup general-attributes address-pool vpnpool ! Associate the address pool vpnpool created default- group-policy clientgroup</pre>

tunnel-group sslgroup webvpn-attributes

group-alias sslgroup_users enable
I Configure the group alias as selgroup-users prompt
hostname context
Cryptochecksum:af3c4bfc4ffc07414c4dfbd29c5262a9 : end
ciscoasa(config)#

<u>SVC との SSL VPN 接続の確立</u>

次の手順を実行して、ASA との SSL VPN 接続を確立します。



2. ユーザ名とパスワードを入力します。また、次に示すようにドロップダウン リストからそ れぞれのグループを選択します。

	Login	
Please enter you	r username and pa	issword.
USERNAME:	ssluser1	
PASSWORD:	••••••	
GROUP:	sslgroup_users	~
	Login	Clear

される前に次のウィンドウが表示されます。

SSL VPN 接続が確立

Cisco	AnyConnect VPN Client
VPN Client Download Please v	der vait while the VPN connection is established.
- : - Microsoft Java	Cancel
🔄 - Sun Java	
Download	
Connected	Help Cancel

注:SVCをダウンロードする前に、コンピュータにActiveXソフトウェアをインストールす る必要があります。接続が確立されると、このウィンドウが表示されます。



3. コンピュータのタスクバーに表示される錠をクリックします。

🐴 Cisco AnyConnect VPN Client	
🗞 Connection 🕕 Statistics 🚕 About	
cisco	
Connect to: 172.16.1.1	*
Disconnect	
PN session established.	

接続についての情報が提供されます。たとえば、192.168.10.1 は ASA によって割り当てら

Cisco AnyConnect VPN Clie	ent 📃 🗖 🔽
🔌 Connection 🕕 Statistics) 🧯	about
cisco	1 i D
Tunnel State:	Connected
Client Address: Server Address:	192.168.10.1 172.16.1.1
Bytes Sent:	23461
Bytes Received:	1111
Time Connected:	00:04:51
Details	
とです。 VPN session established.	

ィンドウは、Cisco AnyConnect VPN Client バージョンの情報を示しています。





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> ポートします。OIT を使用して、show コマンドの出力の分析を表示します。

- show webvpn svc: ASA フラッシュ メモリに格納された SVC イメージを表示します。 ciscoasa#show webvpn svc
 - 1. disk0:/anyconnect-win-2.0.0343-k9.pkg 1
 CISCO STC win2k+
 2,0,0343
 Mon 04/23/2007 4:16:34.63
 - 1 SSL VPN Client(s) installed
- show VPN-sessiondb svc:現在の SSL 接続についての情報を表示します。 ciscoasa#show vpn-sessiondb svc

Session Type: SVC

Username : **ssluser1**

Assigned IP	:	192.168.10.1	E	Public IP	:	192.168.1.1
Protocol	:	Clientless SSL-Tunnel	D	LS-Tunnel		
Encryption	:	RC4 AES128	F	lashing	:	SHA1
Bytes Tx	:	194118	E	Bytes Rx	:	197448
Group Policy	:	clientgroup]	Funnel Group	:	sslgroup
Login Time	:	17:12:23 IST Mon Mar 2	24	2008		
Duration	:	0h:12m:00s				
NAC Result	:	Unknown				
VLAN Mapping	:	N/A	7	/LAN	:	none
			-			

・show webvpn group-alias:さまざまなグループに対する設定済みのエイリアスを表示します

ciscoasa#**show webvpn group-alias** Tunnel Group: **sslgroup** Group Alias: **sslgroup_users enabled**

• ASDM で、[Monitoring] > [VPN] > [VPN Statistics] > [Sessions] を選択すると、ASA の現在の WebVPN セッションがわかります。

onitoring > VF	PN > VPN S	tatistic	s > Sessions)				
Sessions								
Remote	Site	Site	SSL VPN			E-mail Drows	VDN Load Palancin	_
Access	Sice-co-	Site	Clientless	With Client	Total	E-mail Proxy	VPN LOAD Balancin	g
0	0		0	0	0	0	0	
Filter By: SSL	VPN Client	•	All Sessions			Fi	lter	
Userna VD Addu	Username Gr		aroup Policy Protocol		col	Login Time		B
IP Addr	IP Address		Connection	Encryp	tion	Duration		B
ssluser1 192.168.10.1	sluser1 clientgroup 192.168.10.1 sslgroup		Clientless SSL- RC4 AES128	Clientless SSL-Tunnel DT RC4 AES128		. 17:12:23 IST Mon Mar 24 2008 0h:03m:31s		

<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。
 - 1. **vpn-sessiondb logoff name <ユーザ名>**:特定のユーザ名の SSL VPN セッションをログオフ するコマンドです。

ciscoasa#vpn-sessiondb logoff name ssluser1 Do you want to logoff the VPN session(s)? [confirm] Y INFO: Number of sessions with name "ssluser1" logged off : 1

ciscoasa#Called vpn_remove_uauth: success!
webvpn_svc_np_tear_down: no ACL
webvpn_svc_np_tear_down: no IPv6 ACL
np_svc_destroy_session(0xB000)

同様に、vpn-sessiondb logoff svc コマンドを使用すると、すべての SVC セッションを終了 できます。

2. 注: PCがスタンバイモードまたは休止モードになると、SSL VPN接続を終了できます。

webvpn_rx_data_cstp webvpn_rx_data_cstp: got message SVC message: t/s=5/16: Client PC is going into suspend mode (Sleep, Hibernate, e tc) Called vpn_remove_uauth: success! webvpn_svc_np_tear_down: no ACL webvpn_svc_np_tear_down: no IPv6 ACL ciscoasa#**show vpn-sessiondb svc** INFO: There are presently no active sessions

3. debug webvpn svc <1-255> : セッションを確立するために、リアルタイムの webvpn イベ ントを提供します。

Ciscoasa#debug webvpn svc 7

webvpn_rx_data_tunnel_connect CSTP state = HEADER_PROCESSING http_parse_cstp_method() ... input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1' webvpn_cstp_parse_request_field() ...input: 'Host: 172.16.1.1' Processing CSTP header line: 'Host: 172.16.1.1' webvpn_cstp_parse_request_field() ...input: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343' Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343 Setting user-agent to: 'Cisco AnyConnect VPN Client 2, 0, 0343' webvpn_cstp_parse_request_field() ...input: 'Cookie: webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B 7D75F4EDEF26 ' Processing CSTP header line: 'Cookie: webvpn=16885952@12288@1206098825@D251883E8 625B92C1338D631B08B7D75F4EDEF26 ' Found WebVPN cookie: 'webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B 08B7D75F4EDEF26 ' WebVPN Cookie: 'webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B7D7 5F4EDEF26' webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Version: 1' Processing CSTP header line: 'X-CSTP-Version: 1' Setting version to '1' webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Hostname: tacweb' Processing CSTP header line: 'X-CSTP-Hostname: tacweb' Setting hostname to: 'tacweb' webvpn_cstp_parse_request_field() ... input: 'X-CSTP-Accept-Encoding: deflate;q=1.0' Processing CSTP header line: 'X-CSTP-Accept-Encoding: deflate;q=1.0' webvpn_cstp_parse_request_field() ...input: 'X-CSTP-MTU: 1206' Processing CSTP header line: 'X-CSTP-MTU: 1206' webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Address-Type: IPv4' Processing CSTP header line: 'X-CSTP-Address-Type: IPv4' webvpn_cstp_parse_request_field() ...input: 'X-DTLS-Master-Secret: CE151BA2107437EDE5EC4F5EE6AEBAC12031550B1812D40 642E22C6AFCB9501758FF3B7B5545973C06F6393C92E59693 ' Processing CSTP header line: 'X-DTLS-Master-Secret: CE151BA2107437EDE5EC4F5EE6AE BAC12031550B1812D40642E22C6AFCB9501758FF3B7B5545973C06F6393C92E59693 ' webvpn_cstp_parse_request_field() ...input: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA' Processing CSTP header line: 'X-DTLS-CipherSuite: AES256-SHA: AES128-SHA: DES-CBC3 -SHA:DES-CBC-SHA' Validating address: 0.0.0.0 CSTP state = WAIT_FOR_ADDRESS webvpn_cstp_accept_address: 192.168.10.1/0.0.0.0 CSTP state = HAVE_ADDRESS No subnetmask... must calculate it SVC: NP setup

np_svc_create_session(0x3000, 0xD41611E8, TRUE)
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
SVC ACL ID: -1
vpn_put_uauth success!
SVC IPv6 ACL Name: NULL
SVC IPv6 ACL ID: -1
SVC: adding to sessmgmt
SVC: Sending response
Unable to initiate NAC, NAC might not be enabled or invalid policy
CSTP state = CONNECTED
webvpn_rx_data_cstp: got internal message
Unable to initiate NAC, NAC might not be enabled or invalid policy

4. ASDM で、[Monitoring] > [Logging] > [Real-time Log Viewer] > [View] を選択してリアルタイ

Ь.	イベントを表示します。		
1	lisco ASDM 6.0 for ASA - 10.77.241.14	2	
Eile	<u>View T</u> ools Wi <u>z</u> ards <u>W</u> indow <u>H</u> e	lp .	Look For:
C) Home 🦓 Configuration 🔯 Monitori	ng 🔚 Save 🔇 Refresh 🔇 Bad	K 🚫 Forward 💡 Help
	Logging 🗗 🕂 🗡	Monitoring > Logging > Real-Time L	og Viewer
e Lis	Real-Time Log Viewer	Real-Time Log Viewer	
Devi		Click the View button below desired logging level to see r Logging Level:	to start displaying syslog messages in real time. Select the messages at that severity or higher. Debugging
		Buffer Limit:	1000
			View

この例では、ヘッドエンド デバイスで SSL セッションが確立されていることを示します。

ter By: Filter 🗐 Show All Find:							
Severity	Date	Time	Syslog ID	Source IP	Destination IP		
<u>i</u> 6	Mar 21 2008	20:03:36	725007	10.77.233.74		55L session with dient inside:10.77.233.74/1026 terminated.	
<u>k</u> 6	Mar 21 2008	20:03:35	106015	10.77.233.74	10.77.241.142	Deny TCP (no connection) from 10.77.233.74/1026 to 10.77.241.142/44	
<u>k</u> 6	Mar 21 2008	20:03:35	302014	10.77.233.74	10.77.241.142	Teardown TCP connection 700 for inside:10.77.233.74/1026 to NP Ident	
<u>k</u> 6	Mar 21 2008	20:03:35	605005	0.0.0.0	0.0.0.0	Login permitted from 0.0.0.0/1026 to inside:0.0.0.0/https.for.user "enab	
<u>4</u> 6	Mar 21 2008	20:03:35	725002	10.77.233.74		Device completed 55L handshake with client inside:10.77.233.74/1026	
<u>i</u> 6	Mar 21 2008	20:03:35	725003	10.77.233.74		55L client inside:10.77.233.74/1026 request to resume previous session.	
<u>k</u> 6	Mar 21 2008	20:03:35	725001	10.77.233.74		Starting SSL handshake with client inside:10.77.233.74/1026 for TLSv1 s	
<u>4</u> 6	Mar 21 2008	20:03:35	302013	10.77.233.74	10.77.241.142	Built inbound TCP connection 700 for inside:10.77.233.74/1026 (10.77.2	
4				1			

<u>関連情報</u>

- <u>Cisco 5500 シリーズ適応型セキュリティ アプライアンスに関するサポート ページ</u>
- <u>AnyConnect VPN クライアント リリース 2.0 のリリース ノート</u>
- ASA/PIX: PIX/ASA 7.x: ASA で VPN クライアントのスプリット トンネリングを許可するた めの設定例
- <u>スプリット トンネリングを使用する VPN クライアントが IPSec とインターネットに接続するのをルータで許可する設定例</u>
- 公衆インターネット VPN on a Stick のための PIX/ASA 7.x および VPN クライアント間の設 定例
- ASDM を使用した ASA での SSL VPN Client (SVC)の設定例
- <u>テクニカル サポートとドキュメント Cisco Systems</u>