# ASA 7.1/7.2:ASA の SVC に対するスプリット トンネリングの許可の設定例

### 内容

概要 <u>前提条件</u> <u>要件</u> <u>使用するコンポーネント</u> <u>表記法</u> <u>背景説明</u> <u>設定</u> <u>ネットワーク図</u> <u>ASDM 5.2(2) を使用した ASA 設定</u> <u>CLI を使用した ASA 7.2(2) の設定</u> <u>SVC との SSL VPN 接続の確立</u> <u>確認</u> <u>トラブルシュート</u> <u>関連情報</u>

## <u>概要</u>

このドキュメントでは、Cisco Adaptive Security Appliance(ASA; 適応型セキュリティ アプライ アンス)にトンネリングされているときに、セキュア ソケット レイヤ(SSL)VPN クライアン ト(SVC)のインターネットへのアクセスを許可する方法の段階的な手順を説明します。 この設 定では、SSL 経由で社内のリソースへの SVC のセキュアなアクセスを可能にし、スプリット ト ンネリングを使用したインターネットへのセキュアではないアクセスを提供します。

同一のインターフェイス上でセキュリティで保護されたトラフィックと保護されていないトラフ ィックの両方を送信する機能は、スプリット トンネリングという名前で知られています。スプリ ット トンネリングでは、どのトラフィックがセキュリティで保護され、そのトラフィックの宛先 はどこであるかをユーザが正確に指定する必要があります。それによって、指定されたトラフィ ックだけがトンネル内に入り、それ以外のトラフィックはパブリック ネットワーク(インターネ ット)経由で暗号化されずに送信されます。

## 前提条件

#### <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。

・すべてのリモート ワークステーション上でのローカルな管理者権限

- ・リモート ワークステーションでの Java コントロールおよび ActiveX コントロール
- •接続パス上のどの場所でも、ポート 443(SSL)がブロックされていないこと

#### 使用するコンポーネント

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 7.2(2) を実行する Cisco 5500 シリーズ適応型セキュリティ アプラ イアンス(ASA)
- Windows 1.1.4.179 用のバージョンの Cisco SSL VPN Client注: SSL VPN Clientパッケージ (sslclient-win\*.pkg)を<u>Cisco Software Download</u>(登録ユーザ<u>専用</u>)からダウンロードします。 SVC 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。詳細は、『ASA コンフ ィギュレーション ガイド』の「SVC ソフトウェアのインストール」セクションを参照してく ださい。
- Windows 2000 Professional SP4 または Windows XP SP2 が稼働している PC
- Cisco Adaptive Security Device Manager (ASDM) バージョン 5.2(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>

SSL VPN Client (SVC)は、ネットワーク管理者によるリモート コンピュータへの IPSec VPN クライアントのインストールおよび設定を必要とせずに、リモート ユーザに IPSec VPN クライ アントのメリットを提供する VPN トンネリング技術です。SVC は、リモート コンピュータに既 存の SSL 暗号化およびセキュリティ アプライアンスの WebVPN ログインおよび認証を使用しま す。

SVC セッションを確立するには、リモート ユーザがブラウザでセキュリティ アプライアンスの IP アドレスを入力し、ブラウザはそのインターフェイスに接続し、WebVPN ログイン画面を表 示します。ログインと認証を完了し、セキュリティ アプライアンスで SVC を必要としているこ とが確認されると、セキュリティ アプライアンスは SVC をリモート コンピュータにダウンロー ドします。セキュリティ アプライアンスが、SVC を使用するオプションがあると確認した場合 、セキュリティ アプライアンスは、SVC のインストールをスキップするリンクをウィンドウに 表示するとともに、SVC をリモート コンピュータにダウンロードします。

ダウンロードが完了すると、SVC はインストールと設定を実行します。接続が終了すると、その 設定に応じて SVC がリモート コンピュータに保持されるか、またはリモート コンピュータから アンインストールされます。



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<u>れるコマンドの詳細を調べる</u>には、<u>Command Lookup Tool(登録</u>ユ ーザ専用)を使用してください。

#### <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 <u>RFC 1918 で使用されているアドレスであり、ラボ環境で使</u> <u>用されたものです。</u>

#### <u>ASDM 5.2(2) を使用した ASA 設定</u>

手順を実行すると、次で示されているように 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。

- 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など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、「 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 WebVPN」を参照してくだ さい。
- 2. IP アドレス プールを作成するために、[Configuration] > [VPN] > [IP Address Management]> [IP Pools] を選択します。vpnpool は VPN クライアント向けです。

Name:	vpnpool		
Starting IP Address:	192.168.10.1		
Ending IP Address:	192.168.10.254		
Subnet Mask:	255.255.255.0	•	
ок	Cancel	Help	[Apply] をクリックします

3. WebVPN の有効化[Configuration] > [VPN] > [WebVPN] > [WebVPN Access] を選択し、マウ スで外部インターフェイスを強調表示して [Enable] をクリックします。ユーザのログイン ページでドロップ ダウン表示を有効にするために [Enable Tunnel Group Drop-down List on WebVPN Login Page] のチェックボックスをオンにして、それぞれのグループを選択します

0		
Configuration > VPN > WebVPN	N > WebVPN Access	
VPN Wizard	-WebVPN Access	
🕀 🚰 General		
te−¶v ke	Configure access parameters for WebVPN.	
🕀 🧤 IPSec		
🖯 🌆 IP Address Management		
Assignment		
P Pools	there is a second in the second is a second se	( market a
- 😽 NAC	Interface WebVPN Enabled	Enspie
E- K VVeb VPN	Inside No	
WebVPN Access	joutside	Disable
Proxies	-	
- APCF		
Auto Signon		
Cache		
- Content Rewrite		
- Java Trustpoint		
	Port Number: 443	
- The Servers and URLs		
Port Forwarding	Default Idle Timeout: 1800 seconds	
ACLs	Max. Sessions Limit: 2	
-B SSL VPN Client	WebVPN Memory Size: 50 % of total physical memory 🔻	
- SSÓ Servers		
🔄 🖓 E-mail Proxy	Enable Tunnel Group Drop-down List on WebVPN Login Page	
	(Arcily) Report	
and the second	Copyry IVeset	

[Apply] をクリックします。[Configuration] > [VPN] > [WebVPN] > [SSL VPN Client] > [Add] を選択し、次に示すように SSL VPN 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。

			sh.
		Upload	
ок	Cancel	Help	
rowse Flash Dialog	Files		
E- disk0:	FileName	Size (bytes)	Da
	asdm-603.bin	6,851,212	01
I ±⊢ crypto_archive		14,635,008	04
1 - 1 - 12 - 18 - 18 - 18 - 18 - 18 - 18	asa803-k8.bin	14,000,000	0
	asa8U3-k8.bin admin.cfg	1,220	0
	asa803-k8.bin admin.cfg anyconnect-win-2.0.0	1,220 2,635,734	0 90 90
	asa803-k8.bin admin.cfg anyconnect-win-2.0.0 asdm-602.bin	1,220 2,635,734 6,889,764	09
	asa803-k8.bin admin.cfg anyconnect-win-2.0.0 asdm-602.bin asa722-k8.bin	1,220 2,635,734 6,889,764 8,312,832	01 09 08 01 01
	asa803-k8.bin admin.cfg anyconnect-win-2.0.0 asdm-602.bin asa722-k8.bin asdm-522.bin	1,220 2,635,734 6,889,764 8,312,832 5,623,108	09 08 01 02 02
	asa803-k8.bin admin.cfg anyconnect-win-2.0.0 asdm-602.bin asa722-k8.bin asadm-522.bin asa802-k8.bin	1,220 2,635,734 6,889,764 8,312,832 5,623,108 14,524,416	01 09 08 01 02 02 02
	asa803-k8.bin admin.cfg anyconnect-win-2.0.0 asdm-602.bin asa722-k8.bin asa802-k8.bin old_running.cfg	1,220 2,635,734 6,889,764 8,312,832 5,623,108 14,524,416 1,841	01 09 01 01 02 01 01

OK] をクリックします。

	Flash SVC Image:	ie disk0:/sslclie	nt-win-1.1.4.179.pkg	Bro	owse Fla Upload.
	クリックします。[SSL VPN	ĸ	Cancel	Help リックします。	[OK] を
	Configuration > VPN > WebVF	N > SSL VPI	N Client		
	VPN Wizard General F General F IKE F F IPSec F IP Address Management F Address Management IP Pools IP Pools NAC F WebVPN WebVPN WebVPN Access [Apply] をクリックします。[	SSL VPN C Config でE SS	Client gure SSL VPN Client pa inable SSL VPN Client L VPN Client Images disk0:/sslclient-win- 設定	arameters.	
4.	クルーフ ホリシーの設定[Co [Add (Internal Group Policy	nfiguration] )]を選択し てーックポッ	> [VPN] > [General 、内部グループ ポ	I] > [Group Policy] リシー clientgroup	> )を作成します
	。[General] で、[WebVPN] 、 WebVPN を有効にします。	<b>Fエック</b> 示ツ	シスをオノにし、	トノネリンク ノレ	
	Add Internal Group Policy				

🚰 Add Internal Group Policy		
Name:		
General IPSec Client Conf	iguration Client Fir	rewall
Check an Inherit checkbox	to let the correspo	nding setting take its value from the default group policy.
Tunneling Protocols:	🗂 Inherit	□ IPSec
Filter:	🔽 Inherit	Manage

[Client Configuration] > [General Client Parameters] タブでスプリット トンネル ポリシー用 の [Inherit] ボックスの選択を解除して、ドロップダウン リストから [Tunnel Network List Below] を選択します。[Split Tunnel Network List] の [Inherit] ボックスをオフにし、[Manage] をクリックして ACL Manager を起動します。

Edit Internal Group Policy: clientgroup		
Name: clientgroup		
eneral   IPSec Client Configuration   Client Firewall	Hardware Client	NAC WebVPN
Check an Inherit checkbox to let the corresponding	setting take its valu	e from the default group policy.
General Client Parameters	- Microsoft Client	Parametere
	T MICLOSOIL CIICH	r urumeters j
Banner:	🔽 Inherit	Edit Banner
Default Domain:	🔽 Inherit	
Split Tunnel DNS Names (space delimited):	🔽 Inherit	
Split Tunnel Policy:	🔲 Inherit	Tunnel Network List Below
Split Tunnel Network List:	🗖 Inherit	None Manage
Address pools		
🔽 Inherit		
Available Pools		Assigned Pools (up to 6 entries)
	Add>>	ſ l
	< <remove< td=""><td></td></remove<>	
	Contract 1	100

[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。

ACL Manager	4.00		
Add - Edit	Delete 🔶 🛧 🤘	F % @ @ -	
🔂 Add ACL	dress	Action	Description
🔂 Add ACE	1		
👲 insert			
👘 Insert After			

#### ACL に名前を指定して [OK] をクリックします。

Add 👻 📝	Edit 📋 Delete 🔶	◆ ※ № 嗯 -	
No	Address	Action	Description
Add ACL			×
0 CL blamar	anlit tumnal		

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、[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	Description	
split-tunnel				
Add ACE				
Action				
Action:	🖌 Permit 🔄			
Linet Minter				
HOSDINETWO				
IP Addres	ss: 10.77.241.128			-
Netmask:	255.255.255.192			•
7.7				
Design and states and				

Split Tunnel Network List で、作成した ACL が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。

🚰 Edit Internal Group Policy: clientgroup		
Name: clientgroup		
General IPSec Client Configuration Client Firew	all Hardware Client	NAC WebVPN
Check an Inherit checkbox to let the correspondin	ig setting take its valu	e from the default group policy.
General Client Parameters Cisco Client Paramete	ers   Microsoft Client	Parameters
Banner:	🔽 Inherit	Edit Banner
Default Domain:	🔽 Inherit	
Split Tunnel DNS Names (space delimited):	🔽 Inherit	
Split Tunnel Policy:	🗖 Inherit	Tunnel Network List Below
Split Tunnel Network List:	🗖 Inherit	split-tunnel 💌 Manage
CAddress pools		
🔽 Inherit		
Available Pools	Add≻>	Assigned Pools (up to 6 entries)
	<-remove	
ок	Cancel	Help

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。[Use SSL VPN Client] オプションで、[Inherit] チェック ボック スをオフにし、[Optional] ラジオ ボタンをクリックします。この選択により、リモート クラ イアントで [WebVPN] > [SSLVPN Client] タブをクリックするかどうかを選択し、これらの オプションを選択できるようになります。SVC はダウンロードしないでください。 [Always]を選択すると、SSL VPN 接続のたびにリモート ワークステーションに SVC がダウ ンロードされるようになります。[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。[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た場合に強化されま 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。SSL VPN ク ライアントの属性は次の図で示すように設定することになります。

N attributes using the f	ollowing tabs .			
heckbox to let the corr				
	esponding setting take	e its value from the	default group polic	у.
tent Filtering Homepa	ge Port Forwarding	Other SSL VPN	Client Auto Signo	n ]
l Client:	🗌 Inherit	C Always	( Optional	C Neve
on Client System:	🔲 Inherit	( Yes	C No	
:	🔽 Inherit	C Enable	C Disable	
ssages:	🔽 Inherit	Enable	Interval:	Sf
iation Settings				_
tion Interval:	🗖 Inherit	🔲 Unlimited	30	minutes
tion Method:	🗖 inherit	C None	( 55L)	C New 1
stection				
Side Detection:	🔽 Inherit	F Enable	Interval:	SI
	Itent Filtering   Homepa Client: r on Client System: ssages: ation Settings ation Interval: ation Method: etection	Itent Filtering   Homepage   Port Forwarding   I Client:  Inherit I I Inherit I I Inherit I I I I I I I I I I I I I I I I I I I	ttent Filtering   Homepage   Port Forwarding   Other (SSL VPN) Client: □ Inherit	tent Filtering Homepage Port Forwarding Other SSL VPN Client Auto Signo   I Client: Inherit Always Optional   r on Client System: Inherit Yes No   c Inherit Yes No   c Inherit Enable Disable   essages: Imherit Enable Interval:   iation Settings Inherit Unlimited 30   ation Method: Inherit None Inherit   etection Inherit Inherit Interval:

<sup>[</sup>OK] をクリックし、次に [Apply] をクリックします。



同等の CLI 設定

5. Configuration > VPN > General > Users > Addの順に選択し、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。

Username:	ssluser1	
Password:	******	
Confirm Password:	*******	
🔲 User authentio	cated using MSCHAP	
Privilege level is used v	with command authorization	•
Privilege Level:	2	<b>*</b>
	Cancel	Heln

#### 同等の CLI 設定

6. [Configuration] > [Properties] > [AAA Setup] > [AAA Servers Groups] > [Edit] を選択してデフ ォルトのサーバ グループ LOCAL を変更し、 [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 に設定します。

Configuration > Properties > A	AA Setup > AAA Server Gro	ups			
Startup Wizard	AAA Server Groups	-			
🕀 🚽 AAA Setup	1				
AAA Server Groups	AAA server groups				
Auth. Prompt	Samuer Group	Destand	Accounting Mode	Reactivation Mode	
LDAP Attribute Map	Server Group	Protocol	Accounting mode	Reactivation mode	Add
Anti-Spoofing	LOCAL	LOCAL			Edit
E-B ARP	🗺 Edit LOCAL Server Gro	oup		>	(
- 🛃 Auto Update	Sector and the sector of the s			-	Delete
Gient Update	This facture allows to		m number of follow offer	unto to ollow kotoro	-
Certificate	Inis reacure allows to locking out a user and	I specify the maxim	ourser. This limit is applied	able only when local	
E Device Access	database is used for	authentication.	e aser. The link is appre-	able only whethood	
AAA Access					
RITPS/ASDM	Enable Local Lise	Lockout			
Secure Shell	ELINER EDGA CODE	LEODING			-
June 1 Virtual Access					Add
The Device Administration	Maximum Attempt	s: (15)			Carles I.
THE DHCP Services					Ear
E-B DNS					Delete
High Availability and Scal					
- Failover	<u> </u>				Move U
Fragment	OF		Cancel H	elp	-
5.0	-				Movie Dis

### 同等の CLI 設定

7. トンネル グループの設定[Configuration] > [VPN] > [General] > [Tunnel Group] > [Add (WebVPN access)] を選択し、新しいユーザ アカウント sslgroup を作成します。 [General] > [Basic] タブで、ドロップダウン リストから clientgroup としてグループ ポリシ ーを選択します。

Name:	ssigroup	, <b>)</b>	Тур	e: webvpn	
General	WebVPN				
Configur	e deneral acc	cess attributes fr	om the following s	uh-tahs	
Configur	e general acc	cess attributes fr	om the following s	:ub-tabs. art Address Assignment	l aduana
Configur Basic A	e general acc	cess attributes fr	om the following s	ent Address Assignment	Advanc
Configur Basic	e general acc Authentication 9 Policy:	cess attributes fr	om the following s	ent Address Assignment	Advanc

[General] > [Client Address Assignment] タブで、[Address Pools] の下から、[Add] >> をク リックして、利用可能なアドレス プール **vpnpool** を割り当てます。

Name:	ssigroup	Түре	e: webvpn	
na series en la serie de la Serie de la serie de la ser	1.2.		- I	
General) v	VebVPN			
Configure	general access attribute	es from the following s	ub-tabs.	
Basic A	uthentication Authoriza	tion Accounting Clie	ent Address Assignment Ad	vanced
		~ <u>~</u>		
To > If	specify whether to use Address Management :	DHCP or address pools - Assignment.	s for address assignment, go	to Configuration :
	DHCP Servers			
	IP Address:	Add	>>	
		Dele	te	
	1913 - A. 19			
[	Address Pools		Walters while south	
	To configure interface-s	specific address pools,	, go to the Advanced tab.	
	Available Pools		Assigned pools	
	<i>v.</i>		vpnpool	X
		A	<< br	
hVPN1 > [G	Iroun Aliases and U	RIslタブで、パ=	━━━━━━━━━ ラメータ ボックス内の ]	「イリアス名;
、[Add] >>	をクリックしてロ	ダイン ページのグ	ループ名のリストに表	示させます。
eral (WebVP	N			
0.1				
onfigure Web\	/PN access attributes fro	om the following sub-ta	abs.	
sic NetBIOS	Servers Group Aliase	s and URLs Web Pac	ie )	
Group Aliase:	3			1
A.F			Alias	Sta
Allas:		Add >>	ssigroup_users	enable
-				

[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. NAT の設定[Configuration] > [NAT] > [Add] > [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

1	Add Dynamic	NAT Rule	2			
1	Real Address					-
	Interface:	inside				
	IP Address:	0.0.0.0			-	
	Netmask:	0.0.0.0			-	
	-Dynamic Tran	slation			- 10 L - 17	
	Interface:	utside			1	-
	🔂 Add 🖸	🖞 Edit 📋	Delete			-
	Select	Pool ID	Addr 1721615	esses Pool		
					_	-
	NAT Options					
す。	ОК		Cancel		Help	[OK] をクリックして、
メイン・	ページの [App	ly] をクリ	ックします。	同等の CLI	設定	
9. VPN ク	フィアントに	ネットワー	- ク内から戻る	<b>トフノイ</b> ツ	ックのNA	AI

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>CLI を使用した ASA 7.2(2) の設定</u>

#### Cisco ASA 7.2(2)

```
ciscoasa#show running-config
: Saved
:
ASA Version 7.2(2)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
nameif inside
security-level 100
ip address 10.77.241.142 255.255.255.192
!
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
interface Management0/0
shutdown
no nameif
no security-level
no ip address
1
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
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 mtu inside 1500 mtu outside 1500 ip local
pool vpnpool 192.168.10.1-192.168.10.254
!--- The address pool for the SSL VPN Clients no
failover icmp unreachable rate-limit 1 burst-size 1 asdm
image disk0:/asdm-522.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
access-group 100 in interface outside
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 0:05:0
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:
timeout uauth 0:05:00 absolute
group-policy clientgroup internal
!--- Create an internal group policy "clientgroup".
group-policy clientgroup attributes
vpn-tunnel-protocol webvpn
!--- Enable webvpn as tunneling protocol. split-tunnel-
policy tunnelspecified
```

split-tunnel-network-list value split-tunnel

--- Encrypt the traffic specified in the split tunnel ACL only. webvpn svc required !--- Activate the SVC under webvpn mode. svc keepinstaller installed !--- When the security appliance and the SVC perform a rekey, !--- they renegotiate the crypto keys and initialization vectors, !--- and increase 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. username ssluser1 password ZRhW85jZqEaVd5P. encrypted !--- Create an user account "ssluser1". aaa local authentication attempts max-fail 16 !--- Enable the AAA local authentication. 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 tunnelgroup sslgroup type webvpn !--- Create a tunnel group "sslgroup" with type as WebVPN. tunnel-group sslgroup general-attributes address-pool vpnpool !--- Associate the address pool vpnpool created. default-group-policy clientgroup !--- Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-attributes group-alias sslgroup\_users enable !--- Configure the group alias as sslgroup-users. telnet timeout 5 ssh timeout 5 console timeout 0 ! class-map inspection\_default match default-inspection-traffic ! ! 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-policy global\_policy global webvpn enable outside !--- Enable WebVPN on the outside interface. svc image disk0:/sslclient-win-1.1.4.179.pkg 1

!--- Assign an order to the SVC image. **svc enable** 

!--- Enable the security appliance to download !--- SVC images to remote computers. tunnel-group-list enable



### <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。

1. Web ブラウザで ASA の WebVPN インターフェイスの URL または IP アドレスを次に示す 形式で入力します。

1/+webvpn+/index.html
1/+webypn+/index.html
PN Service
VFN Service
Login
Please enter your username and password.
USERNAME:
PASSWORD:
GROUP: sslaroup users

	1	Login	
	Please enter you	r username and p	assword.
	USERNAME:	ssluser1	
	PASSWORD:	•••••	
	GROUP	sslaroup users	~
	enteen .		Clear
ループを選択します。			
3.SVC をダウンロードす く 必要があります。	る前に ActiveX ソフト	ウェアをコンピュータ	にインストールしてお
File Edit View Fa	vorites Tools Help		
General Back   ▼     Address   Image: Back	2.16.1.1/CACHE/stc/1/inc	Search 👷 Favori	tes 🚱 🧯
CISCO SYSTEMS SSL	VPN CLIENT for W	ebvpn	
	e installer is down ease wait	loading the Active	×.
		Use	ful Tips

4. SSL VPN 接続が確立される前に次のウィンドウが表示されます。



5. 接続が確立されると、次のウィンドウが表示されます。



6. コンピュータのタスクバーに表示される黄色いキーをクリックします。SSL 接続についての 情報を提供するウィンドウが表示されます。たとえば、192.168.10.1 はクライアントの IP に割り当てられ、サーバ IP アドレスは 172.16.1.1 で、スプリット トンネリングは有効、な

Statistics Route D	etails About		
Address Informa	tion	SSL Information	
Server:	172.16.1.1	Cipher:	3DES SHA
Client:	192.168.10.1	Version:	TLSV
Bytes		Transport Informat	ion
Sent	2887	Local LAN:	Disable
Received:	940	Split Tunneling:	Enable
Frames		Connection Inform	ation
Sent	35	Time:	00:00:2
Received:	12		

どです。

た、SSL で暗号化されたセキュアなネットワークを確認でき、ネットワークリストは ASA で設定されたスプリットトンネル アクセス リストからダウンロードされます。この例では 、SSL VPN クライアントは 10.77.241.128/24 へのアクセスを保護しますが、一方で、他の すべてのトラフィックは暗号化されず、トンネルを経由しては送信されません。

Cisco Systems SSL VPN Clie	ent 🕑
ISCO SYSTEMS SSL VPN CLIEN	T for WEBVPN
Statistics Boute Details About	
Local LAN Routes	Secure Routes
Network Subnet Mask	Network         Subnet Mask           10.77.241.128         255.255.255
Close Cisco Systems SSL VPN Clie	Disconnect
SSLVPN CLIEN	T for WEBVPN
Statistics   Route Details (About)	
CISCO SYSTEMS SSL VP for WEB	N CLIENT VPN Version 1.1.4.179
Create anywhe	a fully secure connection ere anytime
Copyright 2004-2008 Cisco System and the Cisco Systems Logo are reg its affiliates in the United States and	ms, Inc. All rights reserved. Cisco, Cisco Systems istered trademarks of Cisco Systems, Inc. and/or certain other countries.
Close	Disconnect



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。

- 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:/sslclient-win-1.1.4.179.pkg 1
    CISCO STC win2k+ 1.0.0
    1,1,4,179
    Fri 01/18/2008 15:19:49.43
  - 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			
Index	:	1			
Assigned IP	:	192.168.10.1	Public IP	:	192.168.1.1
Protocol	:	SVC	Encryption	:	3DES
Hashing	:	SHA1			
Bytes Tx	:	131813	Bytes Rx	:	5082
Client Type	:	Mozilla/4.0 (compatible	; MSIE 6.0;	Wir	ndows NT 5.1; SV1)
Client Ver	:	Cisco Systems SSL VPN C	lient 1, 1,	4,	179
Group Policy	:	clientgroup			
Tunnel Group	:	sslgroup			
Login Time	:	12:38:47 UTC Mon Mar 17	2008		
Duration	:	0h:00m:53s			
Filter Name	:				

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。

W Doos Turnels	Sessions						
Sessions	Remote Access	LAN-to-LAN	WebVPN	SSL VPN Client	E-mail Proxy	Total	Total Cumulative
VPN Statistics — Crypto Statistics	0	0	,i	0	0	1 1	2
Compression Statistics Encryption Statistics Global IKE/PSec Stat	Filter By: Veb	VPN 💌 🗖	AI Sessions			Fiter	
NAC Session Summa     Protocol Statistics	Usernam IR Addres	e Gr Re Tu	oup Policy nnel Group	Protocol Encryption		Login Time Duration	Deta
The contraction of the second se							

## <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
Called vpn_remove_uauIth: success!
webvpn_svc_np_tear_down: no ACL
NFO: Number of sessions with name "ssluser1" logged off : 1
```

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, etc) Called vpn\_remove\_uauth: success! webvpn\_svc\_np\_tear\_down: no 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

```
ATTR_CISCO_AV_PAIR: got SVC ACL: -1
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 Systems SSL VPN Client 1, 1, 4, 179'
Processing CSTP header line: 'User-Agent: Cisco Systems SSL VPN Client 1, 1, 4,
179'
Setting user-agent to: 'Cisco Systems SSL VPN Client 1, 1, 4, 179'
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: 'Cookie: webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486
D5BC554D2'
Processing CSTP header line: 'Cookie: webvpn=16885952@10@1205757506@D4886D33FBF1
CF236DB5E8BE70B1486D5BC554D2'
Found WebVPN cookie: 'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1
486D5BC554D2'
WebVPN Cookie: 'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486D5B
C554D2'
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
```

webvpn\_svc\_np\_setup SVC ACL Name: NULL SVC ACL ID: -1 SVC ACL ID: -1 vpn\_put\_uauth success! SVC: adding to sessmgmt SVC: Sending response CSTP state = CONNECTED

4. ASDM で、[Monitoring] > [Logging] > [Real-time Log Viewer] > [View] を選択してリアルタイ ムイベントを表示します。次に、ASA 172.16.1.5 経由のインターネットにおける、SVC 192 168 10 1 と Webserver 10 2 2 2 の間のセッション情報の例を示します。

-	ov.l		in the second that
D	Source IP	Destination P	Description
	192.168.10.255		No translation group found for udp are outside:192.168.10.1/138 dst inside:192.168.10.255/138
	10.77.244,193		Nothranslation group found for upp and outside:192,168,18.1// 027 dat inside:19.77 244.193/53
_	10.77.244,193		No translation group found for udp are outside:192.168.10.17.028 dat inside:10.77.244.19363
	192.168.10.1	10.2.2.2	Bult inbound TCP connection 1902 for outside:192.168.10.1/1100 (172.16.1.5/1025) to outside:10.2.2.2/80 (10.2.2.2/80) (soluser1)
	192.168.10.1	172,16.1.5	Built dynamic TCP translation from outside: 192.168.10.1/1100 to outside: 172.16.1.5/1025
_	192.168.10.255		No transistion group found for udp pro.outside;192.168.10.1/138 dst inside:192.168.10.255//38
	10.77.244.198		No translation group found for udp are outside 192/168.10.1/1927 dat inside:10.77.244.193/53
	10:77.244.193		No transiblion group found for udp are outside 192.168.10.1/1028 dst.inside:10.77.244.193/53
as	10:77 244 193		No transietion group found for uplaiers outside 192.168.10.1/1027 det inside:10.77.244.193/53
lea	ase select a sys	log entry to see	the explanation

## <u>関連情報</u>

- <u>Cisco 5500 シリーズ適応型セキュリティ アプライアンス製品に関するサポート</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</u> 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</u> 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>