# ASA 8.X:トンネリングされたデフォルト ゲー トウェイを使用した SSL VPN トラフィック ル ーティングの設定例

### 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 6.1(5) を使用した ASA 設定</u> <u>確認</u> トラブルシュート <u>関連情報</u>

### <u>概要</u>

このドキュメントでは、適応型セキュリティ アプライアンス(ASA)を設定して、トンネリング されたデフォルト ゲートウェイ(TDG)を経由するように SSL VPN トラフィックをルーティン グする方法について説明します。 tunneled オプションを使用してデフォルト ルートを作成する と、ASA で終端しているトンネルからのトラフィックで、学習されたルートまたはスタティック ルートのいずれを使用してもルーティングできないトラフィックは、すべてこのルートに送信さ れます。トンネルから出るトラフィックの場合、このルートは、その他の設定または学習された デフォルト ルートをすべて上書きします。

# <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。

- バージョン 8.x が稼働する ASA
- Cisco SSL VPN Client (SVC) 1.x注: SSL VPN Clientパッケージ(sslclient-win\*.pkg)を<u>Cisco</u> Software Download (登録ユーザ専用)から ダウンロードしてください。 SVC を ASA のフ ラッシュ メモリにコピーします。ASA との SSL VPN 接続を確立するには、リモート ユーザ のコンピュータに SVC をダウンロードする必要があります。

### <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。

- ・ソフトウェア バージョン 8.x が稼働している Cisco 5500 シリーズ ASA
- Windows 1.1.4.179 用のバージョンの Cisco SSL VPN Client
- Windows 2000 Professional または Windows XP が稼働している PC
- Cisco Adaptive Security Device Manager (ASDM)  $\mathcal{N} \mathcal{V} = \mathcal{V} 6.1(5)$

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。

現在のシナリオでは、SSL VPN トンネルを経由して ASA の背後にある内部リソースに接続する SSL VPN クライアントが存在します。スプリットトンネルはイネーブルではありません。SSL VPN クライアントが ASA に接続しているときは、すべてのデータがトンネリングされます。主 な基準は、内部リソースへのアクセスに加えて、このトンネリングされたトラフィックを Default Tunneled Gateway (DTG)を経由してルーティングすることです。

標準のデフォルト ルートに加えて、トンネル トラフィック用に別のデフォルト ルートを定義で きます。ASA が受信した暗号化されていないトラフィック(スタティック ルートも学習されたル ートも存在しないもの)は、標準のデフォルト ルートを経由してルーティングされます。ASA が 受信した暗号化されているトラフィック(スタティック ルートも学習されたルートも存在しない もの)は、トンネリングされたデフォルト ルートを使用して定義された DTG に渡されます。

トンネリングされたデフォルト ルートを定義するには、次のコマンドを使用します。

route <if\_name> 0.0.0.0 0.0.0.0 <gateway\_ip> tunneled

### <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。

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。



この例では、SSL VPN クライアントはトンネル経由で ASA の内部ネットワークにアクセスしま す。スプリットトンネルは設定されていないため、内部ネットワーク以外に送信されるトラフィ ックもトンネリングされ、TDG(192.168.100.20)経由でルーティングされます。

パケットが TDG (この例ではルータ2)にルーティングされた後は、これらのパケットをインタ ーネットにルーティングするためのアドレス変換が実行されます。インターネット ゲートウェイ としてのルータ設定の詳細については、「Cisco 製ではないケーブル モデムに接続された Cisco ルータの設定方法」を参照してください。

### ASDM 6.1(5) を使用した ASA 設定

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:ASDMで**ASAを設定する方法については、『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 <u>WebVPN」を参照してください。</u>

SSL VPN ウィザードを使用して SSL VPN を設定するには、次の手順を実行します。

View	Tools Wiz	ards Window Help	
Home	Cor	Startup Wizard IPsec VPN Wizard SSL VPN Wizard	h Back Forward ? Help
Devic	e Info	High Availability and Scalability Wizard Packet Capture Wizard	

1 [Wizardel V - 7 \_から [SSI\_\/DNI\//jaard] を選択します 2. [Cisco SSL VPN Client] チェックボックスをクリックし、[Next] をクリックします。



3. [Connection Name] フィールドに接続の名前を入力して、ユーザが SSL VPN へのアクセス に使用しているインターフェイスを [SSL VPN Interface] ドロップダウン リストから選択し ます。

🚳 SSL VPN Wizard	
SSL VPN Wizard	SSL VPN Interface (Step 2 of 6)
	Provide a connection name and the interface that SSL VPN users connect to. Connection Name: Test The interface users access for SSL VPN connections. SSL VPN Interface: Outside Digital Certificate
	When users connect, the security appliance sends this digital certificate to the remote web browser to authenticate the ASA. Certificate:
Catho Ve	Connection Group Settings
1 the	Display Group Alias list at the login page
	Information URL to access SSL VPN Service: https://209.165.201.2 URL to access ASDM: https://209.165.201.2/admin
£	≤Back Next > Filsh Gancel Help

- 4. [next] をクリックします。
- 5. 認証モードを選択し、[Next] をクリックします。(この例では、ローカル認証を使用しています。

)

SSI VPN Wizard	User Authentication (Step 3 of 6)	
	The security appliance supports authentication of users by an external AAA server or local user accounts. Specify how the security appliance authenticates users when they login. AAA Server Group Name: AAA Server Group Name: New Authenticate using the local user database User to be Added Username: clsco Password: Delete Confirm Password: eeeeeee	
<u> </u>	<u>≤Back</u> (Next >)Enish Cancel Help	]
既存のデフォルト グル	レープ ポリシー以外の新しいグループ ポリシーを作成します。	
🖆 SSL VPN Wizard		×
SSL VPN Wizard	Group Policy (Step 4 of 6)	
12 II	A group policy is a collection of user-oriented attribute/value pairs. Unless assigned to a specific group policy, all users are members of the default group policy (Dfl:GrpPolicy). Therefore, configuring the default group policy lets users inherit attributes that you have not configured at the individual group policy or username level.	P
6.6	Greate new group policy     grppolicy	
	Modify existing group policy     DRtGrpPolicy	

SSL VPN Wizard	Group Policy (Step 4 of 6)		
12 A	A group policy is a collection of user- policy, all users are members of the default group policy lets users inherit policy or username level.	oriented attribute/value p default group policy (DfkG t attributes that you have	airs. Unless assigned to a specific group rpPolicy). Therefore, configuring the not configured at the individual group
610	Create new group policy	grppolicy	$\triangleright$
	O Modify existing group policy	DhkGepPolicy	
		S Back	ext > Brish Cancel Help

7. SSL VPN クライアント PC の接続が確立したときにこれらの PC に割り当てられるアドレ

#### スのプールを新規作成します。

🚳 SSL VPN Wizard				
SSL VPN Wizard	IP Address Pools	and Client Image - Any	Connect VPN Client Conn	ections Only (Step 5 of 6)
	The security applia client self-installs, to resources on a IP Address Pool – Create a new a	ance downloads the AnyCo uses SSL or DTLS encrypti corporate network. The re ddress pool or select an ex	nnect VPN Client to remote u on for the duration of the cor mote PC becomes part of the isting address pool. Remote I	sers when they connect. The mection, and allows full access corporate network. PCs are assigned addresses
0.0	from the pool wi	hen they connect.		
	IP Address Pool	:	New	
100 m	Address Pool Ra	inge:		
	AnyConnect VPN (	Client Image Location		
Service .	Identify a file in the file and load	flash memory as an AnyC Is it into cache memory for	onnect VPN Client image. The downloading to remote users	security appliance expands i.
THE TAKE	Location:		Browse	
	Download lates	t AnyConnect VPN Client f	rom Osco.com	
			<u>≤Back</u> <u>N</u> ext > E	inish Cancel Help
192.168.10.40 ~ 192	2.168.10.50 の筆	範囲のプールが、	「newpool」という	る前で作成されま
🖆 Add IP P	ool			
Name:	3	newpool		
Startin	a IP Address:	192,168,10,40		

Starting Ir Haarossi	
Ending IP Address:	192.168.10.50
Subnet Mask:	255.255.255.0
ОК	Cancel Help

した。

8. [Browse] をクリックし、SSL VPN クライアント イメージを選択して ASA のフラッシュ メ モリにアップロードします。

🖆 SSL VPN Wizard				×		
SSL VPN Wizard	IP Address Pools and	l Client Image - AnyConne	ct VPN Client Connections Only (Step 5 of	6)		
18 M	The security appliano client self-installs, use to resources on a cor IP Address Pool	e downloads the AnyConnect V is SSL or DTLS encryption for th porate network. The remote PC	/PN Client to remote users when they connect. Th he duration of the connection, and allows full acc C becomes part of the corporate network.	ne ess		
66	Create a new address pool or select an existing address pool. Remote PCs are assigned address from the pool when they connect.					
and the second	IP Address Pool:	newpool	New			
	Address Pool Rang	e: 192.168.10.40 - 192.168	3.10.50			
	AnyConnect VPN Clie	nt Image Location				
Section 14	Identify a file in fla the file and loads it	sh memory as an AnyConnect V Into cache memory for downloa	VPN Client image. The security appliance expands ading to remete users.	ŝ		
J. J.	Location:		Browse			
	Download latest A	nyConnect VPN Client from Cisc	co.com			
I HUIMAN						
AND THE REAL PROPERTY AND INC.	1					
- D						
		51	Back Next > Enish Cancel Help	1		

9. [Upload] をクリックして、マシンのローカル ディレクトリのファイルのパスを設定します

💰 Add SSL VPN C	lient Image	
AnyConnect Image:	Browse	Flash
	OK Cancel Help	

10. [Browse Local Files] をクリックして、sslclient.pkg ファイルが存在するディレクトリを選択します。

🖆 Upload Image	
Upload a file from local c few minutes. Please wai	omputer to flash file system on the device. The upload process might take a t for the operation to finish.
Local File Path:	Browse Local Files
Flash File System Path:	Browse Flash
	Upload File Close Help

11. [Upload File] をクリックして、選択したファイルを ASA のフラッシュにアップロードします。

🖆 Upload In	nage
Upload a file fr few minutes. F	rom local computer to flash file system on the device. The upload process might take a Please wait for the operation to finish.
Local File Path	C:\Documents and Settings\jtammera\My Documents Browse Local Files
Flash File Syst	em Path: disk0:/sslclient-win-1.1.4.179.pkg Browse Flash
12	Upload File Close Help
🔂 Status	S S S S S S S S S S S S S S S S S S S
Pl Pr Ca	ease wait while ASDM is uploading the file. The upload rocess may take a few minutes.
📧 Informat	ion 🛛 🔀
<b>(i)</b>	File has been uploaded to flash successfully.
	OK
ー ファイルが AS	A のフラッシュにアップロードされたら、[OK] をクリックしてタスクを

了します。 <mark>値</mark> Add SSL VPN C	lient Image	E
AnyConnect Image:	disk0:/sslclient-win-1.1.4.179.pkg	Browse Flash
		Upload
	OK Cancel Help	]

13. ASA のフラッシュにアップロードされた最新の anyconnect pkg ファイルが表示されます

#### 。[next] をクリックします。

🖆 SSL VPN Wizard					
SSL VPN Wizard	<b>IP Address Pools and</b>	d Client Image - AnyCo	nnect VPN C	ient Connectio	ns Only (Step 5 of 6)
	The security appliance client self-installs, use to resources on a corr IP Address Pool Create a new addre from the pool when	e downloads the AnyConn as SSL or DTLS encryption porate network. The remo ess pool or select an exist they connect.	ect VPN Client for the duratio te PC becomes ing address poo	to remote users n of the connect s part of the corp ol. Remote PCs a	when they connect. The ion, and allows full access iorate network. re assigned addresses
Section Section	IP Address Pool:	newpool	× (	New	
	Address Pool Rang	e: 192.168.10.40 - 192	.168.10.50		
a.	AnyConnect VPN Clie	nt Image Location			
	Identify a file in fla the file and loads it	sh memory as an AnyConr Into cache memory for do	ect VPN Client whileading to m	image. The secu emote users.	rity appliance expands
-Itt	Location:	disk0:/sslclient-win-1.1	.4.179.pkg	Browse	
	Download latest A	nvConnect VPN Clent from	n <u>Cisco.com</u>		
			≤ Back (	lexit > ) Einish	Gancel Help

14. SSL VPN クライアントの設定の要約が表示されます。[Finish] をクリックしてウィザード を完了します。

	Europeanu (Etop E of	E)
SSL VPN Wizard	Summary (Step 6 of You have created a SS Selected Features: Connection Name: SSL VPN Interface: User Authentication: Group Policy: JP Address Pool: SSL VPN Client Locatio	5) SL VPN connection with following attributes: SSL VPN Client Test outside LOCAL grppolicy newpool m:disk0:/sslclient-win-1.1.4.179.pkg
		< Back Next > (Finish) Cancel Help

ASDM に表示された設定は、主に SSL VPN クライアントのウィザード設定に関係があります。

CLI では、追加の設定の一部を確認できます。次に CLI の設定のすべてを示します。重要なコマンドは強調表示されています。

CiscoASA
ciscoasa# <b>show running-config</b>
: Saved
:
ASA Version 8.0(4)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
nameif outside
security-level 0
ip address 209.165.201.2 255.255.255.224
!
interface Ethernet0/1
nameif inside
security-level 100
ip address 192.168.100.2 255.255.255.0
interface Ethernet0/2
nameif manage
security-level U
1p address 10.1.1.1 255.255.255.0
interface Ethernet0/3

```
shutdown
no nameif
no security-level
no ip address
I
interface Ethernet0/4
shutdown
no nameif
no security-level
no ip address
1
interface Ethernet0/5
shutdown
no nameif
no security-level
no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
access-list nonat extended permit ip 192.168.100.0
255.255.255.0 192.168.10.0 255.255.255.0
access-list nonat extended permit ip 192.168.10.0
255.255.255.0 192.168.100.0 255.255.255.0
!--- ACL to define the traffic to be exempted from NAT.
no pager logging enable logging asdm informational mtu
outside 1500 mtu inside 1500 mtu manage 1500 !---
Creating IP address block to be assigned for the VPN
clients ip local pool newpool 192.168.10.40-
192.168.10.50 mask 255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-615.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list nonat
!--- The traffic permitted in "nonat" ACL is exempted
from NAT. nat (inside) 1 192.168.100.0 255.255.255.0
route outside 0.0.0.0 0.0.0.0 209.165.201.1 1
!--- Default route is configured through "inside"
interface for normal traffic. route inside 0.0.0.0
0.0.0.0 192.168.100.20 tunneled
!--- Tunneled Default route is configured through
"inside" interface for encrypted traffic ! 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
!--- Configuring the ASA as HTTP server. http 10.1.1.0
255.255.255.0 manage
!--- Configuring the network to be allowed for ASDM
access. ! !--- Output is suppressed ! telnet timeout 5
ssh timeout 5 console timeout 0 threat-detection basic-
threat threat-detection statistics access-list ! 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 ! servicepolicy global\_policy global ! !--- Output suppressed ! webvpn enable outside !--- Enable WebVPN on the outside interface svc image disk0:/sslclient-win-1.1.4.179.pkg 1 !--- Assign the AnyConnect SSL VPN Client image to be used svc enable !--- Enable the ASA to download SVC images to remote computers group-policy grppolicy internal !--- Create an internal group policy "grppolicy" grouppolicy grppolicy attributes VPN-tunnel-protocol svc !--- Specify SSL as a permitted VPN tunneling protocol ! username cisco password ffIRPGpDSOJh9YLq encrypted privilege 15 !--- Create a user account "cisco" tunnel-group Test type remote-access !--- Create a tunnel group "Test" with type as remote access tunnel-group Test general-attributes address-pool newpool !--- Associate the address pool vpnpool created defaultgroup-policy grppolicy !--- Associate the group policy "clientgroup" created prompt hostname context Cryptochecksum:1b247197c8ff70ee4432c13fb037854e : end ciscoasa#

## <u>確認</u>

このセクションで説明するコマンドは、設定の確認に使用できます。

<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。
- show VPN-sessiondb svc :現在の SSL 接続についての情報を表示します。

# <u>トラブルシュート</u>

現在、この設定に関する特定のトラブルシューティング情報はありません。

## 関連情報

- <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</u>
- <u>公衆インターネット VPN on a Stick のための PIX/ASA および VPN Client の設定例</u>
- 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>