ASDM を使った ASA でのシンクライアント SSL VPN(WebVPN)の設定例

内容

概要 前提条件 要件 <u>使用するコンポーネント</u> ネットワーク図 表記法 背景説明 ASDM を使用したシンクライアント SSL VPN 設定 手順1: ASA で WebVPN を有効にする 手順2:ポートフォワーディング特性を設定する 手順3:グループポリシーを作成して、ポートフォワーディングリストにリンクする <u>手順4:トンネルグループを作成して、グ</u>ループポリシーにリンクする 手順5:ユーザを作成して、そのユーザをグループポリシーに追加する CLI を使用したシンクライアント SSL VPN 設定 確認 手順 コマンド トラブルシュート SSL ハンドシェイク プロセスは完了しているか SSL VPN シンクライアントは機能しているか <u>コマンド</u> 関連情報

<u>概要</u>

シンクライアント SSL VPN テクノロジーは、Telnet (23)、SSH (22)、POP3 (110)、 IMAP4 (143) および SMTP (25) などのスタティック ポートを持つ一部のアプリケーションで 安全なアクセスを可能にします。 シンクライアント SSL VPN をユーザ主導アプリケーション、 ポリシー主導アプリケーション、またはその両方として使用できます。つまり、ユーザ単位でア クセス権を設定するか、1 人以上のユーザを追加するグループ ポリシーを作成できます。

クライアントレス SSL VPN (WebVPN): 企業のローカル エリア ネットワーク (LAN)上の HTTP サーバまたは HTTPS Web サーバへアクセスする際に SSL 対応の Web ブラウザが必要となるリモート クライアントです。
 また、クライアントレス SSL VPN は、Common Internet File System (CIFS)プロトコルによる Windows ファイル ブラウジングへのアクセスも提供します。Outlook Web Access (OWA)は、HTTP アクセスの一例です。
 クライアントレス SSL VPN の詳細は、『ASA でのクライアントレス SSL VPN (WebVPN)の設定例』

を参照してください。

- シンクライアント SSL VPN (ポート転送):小規模な Java ベースのアプレットをダウンロ ードし、スタティックなポート番号を使用する Transmission Control Protocol (TCP; 伝送制 御プロトコル)のアプリケーションでのセキュアなアクセスを可能にするリモート クライア ントを提供します。Post Office Protocol (POP3)、Simple Mail Transfer Protocol (SMTP)、Internet Message Access Protocol (IMAP)、Secure Shell (ssh; セキ ュア シェル)、および Telnet は、セキュアなアクセスの例です。ローカル マシン上のファ イルが変更されるため、この方法を使用するには、ユーザにローカル管理者特権が必要です 。SSL VPN のこの方法は、一部の File Transfer Protocol (FTP; ファイル転送プロトコル
-)アプリケーションなど、ダイナミックなポート割り当てを使用するアプリケーションでは 使用できません。**注:ユー**ザーデータグラムプロトコル(UDP)はサポートされていません。
- SSL VPN Client(トンネルモード): リモート ワークステーションに小規模なクライアント をダウンロードし、社内ネットワーク上のリソースへの完全なセキュア アクセスを可能にし ます。SSL VPN Client(SVC)をリモート ワークステーションに永続的にダウンロードする ことも、セキュアなセッションが閉じられた後にクライアントを削除することもできます。 SSL VPN Clientの詳細は、『ASDM を使用した ASA での SSL VPN Client(SVC)の設定例 』を参照してください。

このドキュメントでは、Adaptive Security Appliance(ASA)でのシンクライアント SSL VPN の 簡単な設定を示します。 この設定により、ASA 内にあるルータに安全に telnet 接続できます。こ のドキュメントの設定は ASA バージョン 7.x 以降でサポートされています。

前提条件

<u>要件</u>

この設定を試す前に、リモート クライアント ステーションで以下の要件が満たされていることを 確認してください。

- SSL 対応の Web ブラウザ
- SUN Java JRE バージョン 1.4 以降
- Cookie の有効化
- ポップアップの許可
- ローカルの管理者特権(必須ではないが強く推奨)

注:最新バージョンのSUN Java JREは、Java Webサイトから無料でダウンロード<u>できます</u>。

<u>使用するコンポーネント</u>

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

- Cisco 適応型セキュリティ アプライアンス 5510 シリーズ
- Cisco Adaptive Security Device Manager(ASDM)5.2(1)**注:ASAを**ASDMで設定<u>するには、</u> <u>『</u>ASDMでのHTTPSアクセスの許可』を参照してください。
- 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 7.2(1)
- Microsoft Windows XP Professional (SP 2) リモート クライアント

このドキュメントに記載されている情報は、ラボ環境で作成されたものです。このドキュメント で使用されるデバイスはすべてデフォルト設定にリセットされました。稼働中のネットワークで 作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。この設定で 使用される IP アドレスはすべてラボ環境の RFC 1918 アドレスから選択されました。これらの IP アドレスはインターネット上でルーティングできず、テスト専用です。

<u>ネットワーク図</u>

このドキュメントでは、このセクションで示すネットワーク設定を使用しています。

リモート クライアントが ASA でセッションを開始すると、このクライアントは小さな Java アプ レットをワークステーションにダウンロードします。クライアントには、事前設定されたリソー スのリストが表示されます。



<u>表記法</u>

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。

<u>背景説明</u>

セッションを開始するために、リモート クライアントで ASA の外部インターフェイスへの SSL ブラウザを開きます。セッションを確立した後、ユーザは ASA で設定されたパラメータを使用し て、Telnet またはアプリケーション アクセスを呼び出すことができます。ASA は安全な接続を プロキシし、ユーザがデバイスにアクセスできるようにします。

注: ASA ですでに正規セッションの構成内容が認識されているため、これらの接続に着信アク セス リストは不要です。

ASDM を使用したシンクライアント SSL VPN 設定

ASA でシンクライアント SSL VPN を設定するには、以下の手順に従います。

1. <u>ASA で WebVPN を有効にする</u>

- 2. ポートフォワーディング特性を設定する
- 3. <u>グループ ポリシーを作成して、ポート フォワーディング リスト(手順 2 で作成)にリンク</u> <u>する</u>
- 4. <u>トンネル グループを作成して、グループ ポリシー(手順 3 で作成)にリンクする</u>
- 5. <u>ユーザを作成して、そのユーザをグループ ポリシー(手順3で作成)に追加する</u>

<u>手順1:ASA で WebVPN を有効にする</u>

ASA で WebVPN を有効にするには、以下の手順に従います。

- 1. ASDM アプリケーション内で [Configuration]をクリックし、次に [VPN] をクリックします。 2. [WebVPN]を展開して、[WebVPN Access] を選択します。
 - Cisco ASDM 5.2 for ASA 10.2.2.1 File Options Tools Wizards Help Find . Search Cisco Systems ? Help 0 2 2 2 O Q Home Configuration Monitoring Packet Tracer Back Forward Refresh Save General KE WebVPN Access . Interfaces Configure access parameters for WebVPN B-IB PSec 12 P Address Management NAC ÷ Security Policy 🐨 WebVPN WebVPN Enabled Interface Enable 品 WebVPN Acce Proxies inside No NAT Disable A Auto Signon Cache Content Rewrite Java Trustpoint ١, Proxy Bypass **IPS** Servers and URLs 443 Port Number: Port Forwarding A Webpage Customizat 1800 CSD Manager ACL: Default Idle Timeout seconds Encoding 120 SSL VPN Client Max. Sessions Limit 2 SSO Servers Routing E-mail Proxy 50 % of total physical memory WebVPN Memory Size: v 8 Enable Tunnel Group Drop-down List on WebVPN Login Page **Global Objects** E Properties Reset > 6/27/06 7:01:44 AM UTC 15 cisco
- 3. インターフェイスを選択し、[Enable] をクリックします。
- 4. [Apply] をクリックし、[Save] をクリックし、[Yes] をクリックして変更を確定します。

<u>手順2:ポートフォワーディング特性を設定する</u>

ポート フォワーディング特性を設定するには、以下の手順に従います。

1. [WebVPN] を展開して、[Port Forwarding] を選択します。



2. [Add] ボタンをクリックします。

File Options T	ools Wizards	Help							Search:		Find •
S Home	oggi Configuration	Monitoring	Back	O Forward	्यू Packet Tracer	Refresh	Save	?		CI	sco Systems
Interfaces Security Policy MAT Security Policy MAT Security Policy MAT Security Policy Security Policy Manager Security Policy PS Security Policy Security Pol		VPN - Weard real APN System Option Sector Update funnel Group Proup Policy Jaers Netault Tunnel Gate Cone Labs Integrity Assignment P Pools VPN NebVPN Access YPN NebVPN Access Yowies VPN NebVPN Access Yowies VPN NebVPN Access Sector Content Rewrite Iava Trustpoint Yowy Bypass Servers and URL: Sol Forwarding SSL VPN Client SSO Servers I Proxy	PN = Port I Server Server List N Loc	ionwarding Port Co T Co T Co T Co T Co T Co T Co T Co	Forwarding onfigure port forv his parameter List Name List Name Memote Serv	verding lists fo	te TCP Port	access over PN user or g ote Server Description	WebVPN. sroup policy con Remote TCP	Iguration. Description Ad Ed Dele	Add E to to to to to to to to to to
						cisc	• 1	15		- 	2:40:29 PM UT

3. [Add Port Forwarding List] ダイアログ ボックスで、リスト名を入力して [Add] をクリックし ます。[Add Port Forwarding Entry] ダイアログ ボックスが表示されます。

🚰 Add Port Forwarding	Entry	×
Local TCP Port:	3044	
Remote Server:	10.2.2.2	
Remote TCP Port:	23	
Description:	Telnet to R1	
ок	Cancel Help	

- [Add Port Forwarding Entry] ダイアログ ボックスで、以下のオプションを入力します。
 [Local TCP Port] フィールドにポート番号を入力するか、デフォルト値をそのまま使用します。1024 ~ 65535 の範囲の任意の数値を入力できます。[Remote Server] フィールドに IP アドレスを入力します。この例では、ルータのアドレスが使用されています。[Remote TCP Port] フィールドにポート番号を入力します。この例では、ポート 23 が使用されています。
 [Description] フィールドに説明を入力し、[OK] をクリックします。
- 5. [OK] をクリックして、[Apply] をクリックします。
- 6. [Save]をクリックし、次に [Yes] をクリックして変更を確定します。

<u>手順 3 : グループ ポリシーを作成して、ポート フォワーディング リストにリンク</u> <u>する</u>

グループ ポリシーを作成して、ポート フォワーディング リストにリンクするには、以下の手順 に従います。

1. [General]を展開して、[Group Policy]を選択します。



2. [Add] をクリックして、[Internal Group Policy] を選択します。[Add Internal Group Policy] ダ イアログボックスが表示されます。

Tunneling Protocols:	🔲 inherit	♥ IPSec ♥ WebVPN ♥ L2TP over IPSec
Filter:	🗹 Inherit	Manage
Connection Settings		
Access Hours:	🗹 Inherit	Manage
Simultaneous Logins:	🗹 Inherit	
Maximum Connect Time:	🗹 Inherit	Unlimited minutes
Idle Timeout:	🗹 Inherit	Unlimited minutes
Servers		
DNS Servers:	🗹 Inherit	Primary: Secondary:
WINS Servers:	🗹 Inherit	Primary: Secondary:
DHCP Scope:	🗹 Inherit	

- 3. 名前を入力するか、デフォルトのグループ ポリシー名をそのまま使用します。
- 4. [Tunneling Protocols] の [Inherit] チェック ボックスをオフにし、[WebVPN] チェック ボック スをオンにします。
- 5. ダイアログ ボックスの上部にある [WebVPN] タブをクリックして、次に [Functions] タブを クリックします。
- 6. [Inherit] チェック ボックスをオフにし、[Enable auto applet download] および [Enable port forwarding] チェック ボックスをオンにします(下図参照)。

dd Internal	Group Policy						×
Name:	NetAdmins		7				
			J				
General IPS	ec Client Configu	ration Clien	t Firewall Hardw	are Clier	t NAC WebVF	PN	
Configure W	∕eb∀PN attributes u	ising the follo	wing tabs .				
Check an Ini	nerit checkbox to le	t the corresp	onding setting tak	e its valu	e from the defaul	t group policy.	
Functions	Content Filtering	Homepage	Port Forwarding	Other	SSL VPN Client	Auto Signon	
[
🗌 Inhe	rit						
E	nable URL entry		🗹 Er	able por	t forwarding		
E	hable file server ac	cess	Er	able Out	look/Exchange pr	юху	
	hable file server en hable file server br	try owsina		oply Web able http	p-type ACL		
E	nable auto applet d	ownload	Er	able Citr	ix MetaFrame		
L							
		ок	Canc	el	Help		

7. また、[WebVPN] タブ内の [Port Forwarding] タブをクリックして、[Port Forwarding List] の [Inherit] チェック ボックスもオフにします。

	id Internal	Group Policy						×
	Name:	NetAdmins		1				
	Concerned Inc		- Free Office		05	A MAG MARNYON		
ſ	General	sec Client Contigu	ration Clien	t Firewall Hardy	vare Cliei	TT NAC WEDVPN		٦
	Configure W	√eb∀PN attributes u herit checkbox to k	using the follo	wing tabs . conding setting ta	ke its valı	e from the default or	roup policy	
	Functions	Content Filtering	Homepage	Port Forwarding	Other	SSL VPN Client A	uto Signon	
				-				
	Port F	onwarding List	Diphe	wit Rout	PYS	~	New	
	Apple	t Name:		enit Sec	ure Route	r Access		
	, defere							
			01		a al	tata		
			UK	Can	cel	Неір		

- 8. [Port Forwarding List] のドロップダウンの矢印をクリックして、<u>手順 2</u> で作成したポート フ ォワーディング リストを選択します。
- 9. [Applet Name] の [Inherit] チェック ボックスをオフにして、テキスト フィールド内の名前を 変更します。クライアントに接続時のアプレット名が表示されます。
- 10. [OK] をクリックして、[Apply] をクリックします。
- 11. [Save]をクリックし、次に [Yes] をクリックして変更を確定します。

<u>手順 4:トンネル グループを作成して、グループ ポリシーにリンクする</u>

デフォルトの DefaultWebVPNGroup トンネル グループを編集するか、新しいトンネル グループ を作成します。

新しいトンネル グループを作成するには、以下の手順に従います。

1. [General]を展開して、[Tunnel Group] を選択します。



2. **[Add]** をクリックし、**[WebVPN Access]** を選択します。[Add Tunnel Group] ダイアログ ボ ックスが表示されます。

🖆 Add Tunnel Group	×
Name: NetGroup Type: webvpn	
Configure general access attributes from the following sub-tabs.	
Basic Authentication Authorization Accounting Client Address Assignment Advanced	_
Group Policy: NetAdmins	
Strip the realm from username before passing it on to the AAA server	
Strip the group from username before passing it on to the AAA server	
Password Management Override account-disabled indication from AAA server Enable notification upon password expiration to allow user to change password	
Enable notification prior to expiration Notify days prior to expiration	
OK Cancel Help	

- 3. [Name] フィールドに名前を入力します。
- 4. [Group Policy] のドロップダウンの矢印をクリックして、<u>手順 3</u> で作成したグループ ポリシ ーを選択します。
- 5. [OK] をクリックして、[Apply] をクリックします。
- 6. [Save]をクリックし、次に [Yes] をクリックして変更を確定します。これで、トンネル グル ープ、グループ ポリシー、およびポート フォワーディング特性がリンクされました。

<u>手順 5:ユーザを作成して、そのユーザをグループ ポリシーに追加する</u>

ユーザを作成して、そのユーザをグループ ポリシーに追加するには、以下の手順に従います。

1. [General]を展開して、[Users] を選択します。

File Options To	ols Wizards Help					Search	Find •
Shome a	Configuration Monitoring	Back Forward	Packet Tracer	Refresh Save	? Неір		Cisco Systems
Interfaces Security Policy NAT	Configuration -> VPN >> Ge VPN Witzard General VPN System Opt Client Update Tunnel Group Group Poicy Croup Poicy Croup Poicy Croup Poicy Croup Defaut Tunnel 3	erable 15	ies in the ASA local count privileges to Privilege 15	user database. Comm be enforced. To enable Level (Role) VPN Group MA	and authorization mi command authorization p Policy VPN Grou N/A	ust be enabled in order fo tion, go to <mark>sufraction</mark> # Lock Add	2
VPN	RE PSec Transform Sets Pre-Fragmentation	ausnml sales1	15	Dittorphic SalesGroup	y Inherit G Policy Inherit G	roup Polic Toup Polic Delete	
PS CSD Manager & Routing	P Address Manager Assignment P Pools P Pools P Address Manager Pools Pools	*					
Global Objects Properties	Content Rewrite Java Trustpoint Proxy Bypass Servers and UR Port Forwarding Webpage Custo ACLs Encoding SSL VPN Client SSO Servers E-mail Proxy	Ls		Apply	Reset	٦	
	SSL VPN Clent SSO Servers E-mail Proxy	>		Apply	Reset		

2. [Add] ボタンをクリックします。[Add User Account] ダイアログボックスが表示されます。

🖆 Add User Account	
Identity VPN Policy WebVPN	
Thready Vicevin	1
Username:	user1
Password:	******
Confirm Password:	*****
User authenticate	ed using MSCHAP
Privilege level is used with	h command authorization.
Privilege Level:	2
ОК	Cancel Help

3. ユーザ名、パスワード、および特権情報の値を入力し、次に [VPN Policy] **タブをクリックし** ます。

Check an Inherit checkbox to let the cr	arresponding sett	ing take its value from the group policy
Tunneling Protocols:	🗹 Inherit	IPSec WebVPN L2TP over IPSec
Filter:	🗹 Inherit	Manage
Funnel Group Lock:	🗹 Inherit	~
Store Password on Client System:	🗹 Inherit	O Yes O No
Connection Settings		
Access Hours:	🗹 Inherit	New
Simultaneous Logins:	🗹 Inherit	
Maximum Connect Time:	🗹 Inherit	Unlimited minutes
Idle Timeout:	🔽 Inherit	Unlimited minutes
Dedicated IP Address (Optional)	Subr	net Mask:

- 4. [Group Policy] のドロップダウンの矢印をクリックして、<u>手順 3</u> で作成したグループ ポリシ ーを選択します。このユーザは、選択したグループ ポリシーの WebVPN 特性およびポリシ ーを継承します。
- 5. [OK] をクリックして、[Apply] をクリックします。
- 6. [Save] をクリックし、[Yes] をクリックして変更を確定します。

<u>CLI を使用したシンクライアント SSL VPN 設定</u>

ASA
ASA Version 7.2(1)
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
nameif inside

security-level 100
ip address 10.1.1.1 255.255.255.0
! Output truncated port-forward portforward 3044
10.2.2.2 telnet Telnet to R1
! Configure the set of applications that WebVPN
users ! can access over forwarded TCP ports group-
policy NetAdmins internal
<pre>! Create a new group policy for enabling WebVPN</pre>
access group-policy NetAdmins attributes
vpn-tunnel-protocol IPSec 12tp-ipsec webvpn
! Configure group policy attributes webvpn
functions port-forward auto-download
<pre>! Configure group policies for WebVPN port-forward</pre>
value portforward
<pre>! Configure port-forward to enable WebVPN</pre>
application access ! for the new group policy port-
forward-name value Secure Router Access
! Configure the display name that identifies TCP
port ! forwarding to end users username user1
password tJsDL6po9m1UFs.h encrypted
username user1 attributes
vpn-group-policy NetAdmins
! Create and add User(s) to the new group policy
http server enable http 0.0.0.0 0.0.0.0 DMZ no snmp-
server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart tunnel-group NetGroup type webvpn
tunnel-group NetGroup general-attributes
default-group-policy NetAdmins
<pre>! Create a new tunnel group and link it to the group</pre>
<i>policy</i> 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 Web VPN on Outside interface port-forward
portforward 3044 10.2.2.2 telnet Telnet to R1 prompt
hostname context

<u>確認</u>

このセクションでは、設定が正常に動作していることを確認します。

<u>手順</u>

この手順では、設定の有効性を調べる方法と設定をテストする方法を示します。

 クライアント ワークステーションで、https://outside_ASA_IP Address と入力します。ここで outside_ASA_IPAddress は、ASA の SSL URL です。デジタル証明書が受け入れられ、 ユーザが認証されると、WebVPN Service Web ページが表示されます。

File Edit View Fav	orites Tools Help	c exprorer				
🚱 Back 🔹 🕥 🗸	🖹 🗟 🏠 🍃	🔎 Search 👷 Fa	avorites 🔗	Ø• 🎍	w •	, »
Address Address //172.3	22.1.160/+webvpn+/p	ortal.html		~	Go	Links »
Google -	✓ G	Search 🝷 🧭	🌮 🔁 Popup	s okay »	SnagI	t 🛃
Cisco Systems	ebVPN Servi	ce				^
				?	۵	\times
SECURE ROU ACCESS Start Application C	TER lient Go					
https://172.22	2.1.160 - Secure F	Router Access - A	Aicrosoft Inte	rnet Ex	. 🗆 🗙	i 📗
Close this win Please wait fo If you shut do later have pro	dow when you fi or the table to be wn your compute oblems running th	nish using Appl displayed befor er without closin he applications	ication Acce re starting a 1g this windo listed below	ess. pplications. ow, you migl . <u>Click here</u>	ıt <u>for</u>	18
details.						
Name Teinet to R1	Local 127.0.0.1:3044	Remote 10.2.2.2:23	Bytes Out 0	Bytes In Sou	ckets 0	
SSH to R1	127.0.0.1:3255	10.2.2.2:22	0	0	0	
Done				Internet		
				_		~
🕘 Done			2	🔒 🌒 Inte	ernet	

アプリケーションにアクセスするために必要なアドレスとポート情報が Local 列に表示され ます。この時点ではアプリケーションが起動していないため、Bytes Out 列および Bytes In 列に動作は表示されません。

- 2. DOS プロンプトまたはその他の Telnet アプリケーションを使用して、Telnet セッションを 開始します。
- コマンド プロンプトで telnet 127.0.0.1 3044 と入力します。注:このコマンドでは、このドキュメントのWebVPN Service Webページのイメージに表示されるローカルポートにアクセスする方法の例を示します。このコマンドには、コロン(:)が含まれていません。このドキュメントで説明されているとおりに、コマンドを入力します。ASA は安全なセッション経由でコマンドを受け取ります。さらに、ASA は情報のマップを格納しているため、マップされたデバイスへの安全な Telnet セッションをすぐに開くことができます。

Command Prompt	×
C:\>telnet 127.0.0.1 3044	-
	-

ユーザ名とパスワードを入力したら、デバイスへのアクセスは完了です。

4. デバイスへのアクセスを確認するには、Bytes Out 列および Bytes In 列を確認します(下図 参照)。

🐔 https://172.22.1.160 - Secure Router Access - Microsoft Internet Ex... 😑 🗖 🔀

Close this window when you finish using Application Access. Please wait for the table to be displayed before starting applications.

If you shut down your computer without closing this window, you might later have problems running the applications listed below. <u>Click here for details.</u>

	Name	Local	Remote	Bytes Out	Bytes In	Sockets			
	Telnet to R1	127.0.0.1:3044	10.2.2.2:23	56	127	1			
	SSH to R1	127.0.0.1:3255	10.2.2.2:22	0	0	0			
🖹 https://172.22.1.160/+webvpn+/help/warning.ht 🔒 🥑 Internet 😕									

<u>コマンド</u>

いくつかの show コマンドは WebVPN に関連しています。これらのコマンドをコマンドライン インターフェイス(CLI)で実行して、統計情報や他の情報を表示できます。show コマンドの詳 細については、「WebVPN 設定の検証」を参照してください。

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

<u>トラブルシュート</u>

このセクションは、設定のトラブルシューティングを行う際に参照してください。

<u>SSL ハンドシェイク プロセスは完了しているか</u>

ASA に接続したら、リアルタイム ログに SSL ハンドシェイクの完了が表示されているか確認し ます。

📽 Real-time Log Viewer									
II Paus	е 🗈 Сору 🕻	🚽 Save 🔓	Clear 👩	Color Settings	🔁 Create Rule 置	Show Rule	Show Details	? Help	
Filter By:			Filter	Show All Fin	vet:	0.			
Seventy	Date	Time	Syslog	Source IP	Destination IP	Description			
2	Jun 27 2006	11:40:42	106001	172.22.1.203	216.239.53.147	Inbound TCP co	onnection denied t	from 172.22.1.203	/3102 to 216.239.53.1
0 2	Jun 27 2006	11:40:34	106006	172.22.1.203	171.70.157.215	Deny inbound L	UDP from 172.22.1	.203/3101 to 171	70.157.215/1029 on i
@ 2	Jun 27 2006	11:40:34	106006	172.22.1.203	64.101.176.170	Deny inbound U	UDP from 172.22.1	.203/3101 to 64.1	01.176.170/1029 on i
@ 2	Jun 27 2006	11:40:34	106006	172.22.1.203	171.68.222.149	Deny inbound L	UDP from 172.22.1	.203/3101 to 171	68.222.149/1029 on i
@ 2	Jun 27 2006	11:40:32	106001	172.22.1.203	216.239.53.147	Inbound TCP co	onnection denied i	from 172.22.1.203	/3100 to 216.239.53.1
@ 2	Jun 27 2006	11:40:24	106001	172.22.1.203	216.239.53.147	Inbound TCP co	onnection denied t	rom 172.22.1.203	/3098 to 216.239.53.1
2	Jun 27 2006	11:40:22	106001	172.22.1.203	216.239.53.147	Inbound TCP co	onnection denied (rom 172.22.1.203	/3098 to 216.239.53.1
4.6	Jun 27 2006	11:40:18	725002	172.22.1.203		Device complet	ted SSL handshal	e with client outsi	de:172.22.1.203/3097
A 6	Jun 27 2006	11:40:18	725003	172.22.1.203		SSL client outs	ide:172.22.1.203/	3097 request to re	sume previous sessi
A 6	Jun 27 2006	11:40:18	725001	172.22.1.203		Starting SSL ha	andshake with clie	ent outside:172.22	.1.203/3097 for TLSv
A 6	Jun 27 2006	11:40:18	302013	172.22.1.203	172.22.1.160	Built inbound To	CP connection 37	1 for outside:172	22.1.203/3097 (172.1
A 6	Jun 27 2006	11:40:18	725007	172.22.1.203		SSL session w	with client outside:"	72.22.1.203/3098	sterminated.
A 6	Jun 27 2006	11:40:17	302014	172.22.1.203	172.22.1.160	Teardown TCP	connection 3710	for outside:172.2	2.1.203/3096 to NP lde
A 6	Jun 27 2006	11:40:17	725002	172.22.1.203		Device complet	ted SSL handshal	e with client outsi	de:172.22.1.203/3096
A 6	Jun 27 2006	11:40:17	725001	172.22.1.203		Starting SSL ha	andshake with clie	ent outside:172.22	.1.203/3096 for TLSv
A 6	Jun 27 2006	11:40:17	302013	172.22.1.203	172.22.1.160	Built inbound To	CP connection 37"	0 for outside:172	.22.1.203/3096 (172.2
G 3	Jun 27 2006	11:40:16	305005	64.101.176.170		No translation g	group found for u	tp src inside:10.2	2.4/1830 dst outside:
6 3	Jun 27 2006	11:40:16	305005	171.70.157.215		No translation g	group found for u	tip src inside:10.2	2.4/1830 dst outside:
63	Jun 27 2006	11:40:16	305005	171,68.222,149		No translation g	group found for u	tp src inside:10.2	2.4/1830 dst outside:
@ 2	Jun 27 2006	11:40:15	106001	172.22.1.203	216.239.53.147	Inbound TCP co	onnection denied t	rom 172.22.1.203	/3095 to 216.239.53.1
0 2	Jun 27 2006	11:40:12	106001	172.22.1.203	216.239.53.147	Inbound TCP co	onnection denied t	from 172.22.1.203	/3095 to 216.239.53.1
٢.									>
Please select a syslog entry to see the explanation									
Explanation Recommended Action Details									
🗿 Emergencies 🔇 Alerts 🙆 Critical 🔒 Errors 🙏 Warnings 🗼 Notifications 🗼 Informational 🛞 Debugging									

<u>SSL VPN シンクライアントは機能しているか</u>

SSL VPN シンクライアントが機能していることを確認するには、以下の手順に従います。

- 1. [Monitoring] をクリックし、次に [VPN] をクリックします。
- 2. [VPN Statistics] を展開して、[Sessions] をクリックします。SSL VPN シンクライアント セッションがセッション リストに表示されます。下図に示すように、必ず WebVPN でフィルタを適用してください。



<u>コマンド</u>

いくつかの debug コマンドは、WebVPN に関連しています。これらのコマンドの詳細について は、「<u>WebVPN の Debug コマンドの使用</u>」を参照してください。

注:debugコマンドを使用すると、シスコデバイスに悪影響が及ぶ可能性があります。debug コマンドを使用する前に、「debug コマンドの重要な情報」を参照してください。

関連情報

- ASA でのクライアントレス SSL VPN (WebVPN)の設定例
- ASDM を使用した ASA での SSL VPN Client (SVC)の設定例
- <u>Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス</u>
- <u>ASDM および NTLMv1 を使用した WebVPN およびシングル サインオン機能付き ASA の設</u> <u>定例</u>
- <u>テクニカル サポートとドキュメント Cisco Systems</u>