SDMを使用したCisco IOSでのクライアントレス SSL VPN(WebVPN)の設定

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 設定前の作業 Cisco IOS での WebVPN の設定 <u>ステップ 1. WebVPN ゲー</u>トウェイの設定 ステップ 2. ポリシー グループに対して許可されるリソースの設定 <u>ステップ 3. WebVPN ポリシー グル</u>ープの設定とリソースの選択 ステップ 4. WebVPN コンテキストの設定 ステップ 5. ユーザ データベースと認証方法の設定 成果 確認 手順 コマンド トラブルシュート <u>手順</u> コマンド

関連情報

<u>概要</u>

クライアントレス SSL VPN (WebVPN)では、SSL 対応ブラウザがあれば、ユーザはどんな場 所からでも安全に企業 LAN のリソースへアクセスできます。ユーザはまず WebVPN ゲートウェ イで認証を受けますが、WebVPN ゲートウェイでは、あらかじめ設定されたネットワーク リソ ースへのユーザ アクセスが許可されます。WebVPN ゲートウェイは、Cisco IOS® ルータ、 Cisco Adaptive Security Appliances (ASA; 適応型セキュリティ アプライアンス)、Cisco VPN 3000 コンセントレータ、Catalyst 6500 および 7600 ルータ対応 Cisco WebVPN サービス モジュ ールに設定できます。

Secure Socket Layer (SSL) Virtual Private Network (VPN; 仮想プライベート ネットワーク)テ クノロジーは、3 つの主要モードで Cisco デバイス上に設定できます。3 つのモードとは、クラ イアントレス SSL VPN (WebVPN)、シンクライアント SSL VPN (ポート転送)、および SSL VPN クライアント (SVC)モードです。このドキュメントでは、Cisco IOS ルータでの WebVPN の設定方法を紹介します。 注:ルータのIPドメイン名またはホスト名を変更しないでください。変更すると、自己署名証明 書が再生成され、設定済みのトラストポイントが上書きされます。ルータが WebVPN 用に設定 されている場合、自己署名証明書が再生成されると、接続の問題が発生します。WebVPN は、 SSL トラストポイント名を WebVPN ゲートウェイ設定に結びつけます。このため、新しい自己 署名証明書が発行されると、新しいトラストポイント名が WebVPN の設定と一致せず、ユーザ が接続できません。

注:永続的自己署名証明書を使用するWebVPNルータでip https-secure serverコマンドを実行す ると、新しいRSAキーが生成され、証明書が無効になります。新しいトラストポイントが作成さ れて、このトラストポイントが SSL WebVPN を中断します。ip https-secure server コマンドを 実行した後に、永続的な自己署名証明書を使用するルータが再起動すると、同じ問題が発生しま す。

シンクライアント SSL VPN の詳細については、「<u>SDM によるシンクライアント SSL</u> VPN(WebVPN)の IOS 設定例」を参照してください。

SSL VPN Client の詳細は、『<u>SDM を使用した IOS での SSL VPN Client(SVC)の設定例</u>』を参 照してください。

SSL VPN は次の Cisco ルータ プラットフォームで動作します。

- Cisco 870、1811、1841、2801、2811、2821 および 2851 シリーズ ルータ
- Cisco 3725、3745、3825、3845、7200、および 7301 シリーズ ルータ

<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。

- Cisco IOS ソフトウェア リリース 12.4(6)T 以降の拡張イメージ
- 「概要」に記載されている Cisco ルータ プラットフォームのいずれか

<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 3825 ルータ

• 拡張 Enterprise ソフトウェア イメージ: Cisco IOS ソフトウェア リリース 12.4(9)T

• Cisco Router and Security Device Manager (SDM) - バージョン 2.3.1

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。次の例で使用する IP アドレスは、RFC 1918 から引用したプライベート アドレスで、インターネットでの使用には適格ではありません 。

<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。



<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。

設定前の作業

開始する前に、次の作業を実行してください。

- 1. ホスト名とドメイン名を設定します。
- 2. ルータを SDM 対応に設定します。一部のシスコ ルータには、SDM がプリインストールさ れています。Cisco SDM がまだルータにロードされていない場合は、ソフトウェアのダウ ンロードのページ(登録ユーザ専用)からソフトウェアを無料で取得できます。 サービス 契約を結んでいる CCO アカウントが必要です。SDM のインストールと設定の詳細につい ては、Cisco Router and Security Device Manager のページを参照してください。
 3. ルータで正しい日付、時刻、および時間帯を設定します。

<u>Cisco IOS での WebVPN の設定</u>

1 つのデバイスに、複数の WebVPN ゲートウェイを関連付けることができます。各 WebVPN ゲ ートウェイは、ルータ上の 1 つの IP アドレスにのみリンクされます。特定の WebVPN ゲートウ ェイに複数の WebVPN コンテキストを作成できます。各コンテキストを識別するため、コンテ キストに一意の名前を付けます。1 つのポリシー グループは、1 つの WebVPN コンテキストに のみ関連付けられます。ポリシー グループは、特定の WebVPN コンテキストでどのリソースが 利用可能かを説明します。

Cisco IOS に WebVPN を設定するには、次の手順を実行します。

- 1. <u>WebVPN ゲートウェイの設定</u>
- 2. ポリシー グループに対して許可されるリソースを設定する
- 3. WebVPN ポリシー グループの設定とリソースの選択
- 4. <u>WebVPN コンテキストの設定</u>

5. ユーザ データベースと認証方法の設定

<u>ステップ 1. WebVPN ゲートウェイの設定</u>

WebVPN ゲートウェイを設定するには、次の手順を実行します。

- 1. SDM アプリケーションで、[Configure] 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 Gateways] を選択します。

🚰 Cisco Router and Security Device Manager (SDM): 10.89.129.170										
File Edit View	Tools Help									
🔥 Home	କ୍ଷି Configure	Monitor	(C) Refresh	Gave	Q Search	? Help			CISCO SYSTE	M S
Tasks	🕺 VPN									
÷	Site-to-Sit	te VPN	WebVPN Gate	ways				an Equation	t 🏦 Delete 🥑 Ens	ble
Interfaces and	Easy VPN	Remote Server	Name		IP Address		No. of Contexts	Status	Administrative Statu	18
connections	Dynamic	Multipoint VPN								
Firmul and BCL	WebVPN	N Gateways								
	E- VPN Com	ges iponents								
	1									
Security Audit										
~ ² ~										
Routing										
2			Details of Web	VPN Gatewa	ayr.					
NRT			Item Name				Item Value			
(
Intrusion Prevention										
) 🕲 #										
Quality of Service										
200										
NRC										
5										
Additional Tasks										
VPN							1	5:28:57 UT	C Wed Jul 26 2006	Ó

3. [Add] をクリックします。[Add WebVPN Gateway] ダイアログ ボックスが表示されます。

Add WebVPN Gate	eway	
Gateway Name:	WidgetSSLVPNGW1	_
Enable Gateway	, I	
IP Address		
WebVPN clients v to the WebVPN ga	vill use this IP address and ateway.	port number to connect
IP Address:	192.168.0.37	Port: 443
Hostname:	ausnml-3825-01	(Optional)
Enable secure	SDM access through 192.	168.0.37
Digital Certifica	ite	
Digital Certificate client for SSL aut	configured under this trust; nentication.	point will be sent to the
Trustpoint:	ausnml-3825-01_Certifica	te 💌
Configure HTTP (using HTTP will k service that Web)	TP Traffic (Optional) redirect so that clients acce be automatically redirected t /PN uses.	ssing the portal page to the secure HTTPS
HTTP Port:	80	
	OK Cancel	Help

- 4. [Gateway Name] および [IP Address] フィールドに値を入力し、[Enable Gateway] チェック ボックスをオンにします。
- 5. [Redirect HTTP Traffic] チェック ボックスをオンにして、[OK] 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>ステップ 2. ポリシー グループに対して許可されるリソースの設定</u>

ポリシー グループを作成する前にリソースを設定すれば、ポリシー グループへ簡単にリソースを 追加できます。

ポリシー グループに対して許可されるリソースを設定するには、次の手順を実行します。

1. [Configure]をクリックし、次に [VPN] をクリックします。



2. [WebVPN]を選択し、[Edit WebVPN]タブをクリックします。注:WebVPNでは、HTTP、 HTTPS、Common Internet File System(CIFS)プロトコルによるWindowsファイルブラウジ ング、およびCitrixのアクセスを設定できます。



3. [Add] をクリックします。[Add WebVPN Context] ダイアログ ボックスが表示されます。

🛃 Cisco Router a	and Security Device	Manager (SDM): 10.89.129.170			
File Edit View	Tools Help				
🔥 Home	ଞ୍ଚି Configure	Monitor Refresh Sar	ne Search Help		CISCO SYSTEMS
Tasks	🝠 VPN				
Interfaces and Interfaces and Freewal and RCL Interfaces and VPN Security Rudt Security Rudt NRT NRT NRT Dusting Custing of Service NRC Security Rudt	B-WVPN Easy VPN Easy VPN Dynamic WebVPN Packag B-WVPN Com	Add WebVPN Context Add WebVPN Context Group Policies HTML Display Settings NetBIOS Name Server Li Port Forward Lists URL Lists Cisco Secure Desktop	Edit WebVFN Name: Associated Gateway: Domain: Authentication List: Authentication Domain: F Enable Context Maximum Number of users: VRF Name: Default Group Policy: OK Cancel	None International of the second se	
Configuration delive	ered to router.			15:50:11 UTC We	ed Jul 26 2006 👩
L					

4. [WebVPN Context] を展開し、[URL Lists] を選択します。

Í	Add WebVPN Context		×
	WebVPN Context Group Policies HTML Display Settings NetBIOS Name Server List Port Forward Lists URL Lists Cisco Secure Desktop	Group policies use URL Lists to expose corporate URLs to the WebVPN users through the portal page. URL List Add Edit Delete URL List Name	
		Item Name Item Value	
	4	OK Cancel Help	

5. [<u>Add] をクリックします。[Add URL List] ダイアログ ボックスが表示されます。</u>

Add URL List			
URL List Nam	e: InternalWebServers	_	
Heading:	WidgetWebServers	(This will appear	on Portal page)
List of URLs:			
Label (URL Link	Outlook Web Acces	Add ⊽
			Website
			E-mail
·		•	
	OK Cancel	Help	

- 6. [URL List Name] および [Heading] フィールドに値を入力します。
- 7. **[Add]** をクリックし、**[Website]** を選択します。

Add URL Lis	t				
URL List Na	ame:	InternalWebServers	_		
Heading:		WidgetWebServers	_	(This will appear	on Portal page)
List of URLs	3 :				
Label	UR	L Link	0	utlook Web Acces	Add $ abla$
WidgetWeb	http:	//172.22.1.30			
OWA	http:	//172.22.1.50/exchang	Er	nabled	Edit
					Delete
•				•	
		OK Cancel		Help	

トには、この WebVPN 接続で利用可能にする、すべての HTTP および HTTPS Web サーバ が含まれています。

- 8. Outlook Web Access (OWA) へのアクセスを追加するには、[Add] をクリックし、[E-mail] を選択して、必要なすべてのフィールドへ入力してから [OK] をクリックします。
- 9. NetBIOS Name Service (NBNS) サーバを指定し、Windows ドメイン内の共有を順序通りに 設定すれば、CIFS による Windows ファイル ブラウジングが可能になります。[WebVPN Context] リストから、[NetBIOS Name Server Lists] を選択します。

Add WebVPN Context			×
WebVPN Context Group Policies HTML Display Settings NetBIOS Name Server Lis Port Forward Lists URL Lists Cisco Secure Desktop	The Common Internet File the corporate Microsoft Win NetBIOS Name Server List Server Name	System feature uses NetBl dows File System to WebV	OS name servers to expose PN users.
	IP Address	Retry	Timeout
<	OK Cancel	Help	

[Add] をクリックします。[Add NBNS Server List] ダイアログ ボックスが表示されます。リ ストの名前を入力し、[Add] をクリックします。[NBNS Server] ダイアログ ボックスが表示 されます。

File Edit View Tools Help	wice manager (50m): 10.69.129.170	
Home 🖓 Configu	re 😥 Monitor 🔮 🗔 🔍 🦻 Refresh Save Search Help	CISCO SYSTEMS
Task Add WebVPN Contex	t	
Task Add WebVPN Contex Interface Preval of Security Route Contex Port Forward Cisco Security Cisco Security	t t t t t t t t t t t t t	Edi Edi Discole Administrative Status
NRT NRT Intrusion Pre Cuusify of NRC	IP Address of NBNS Server 172.22.1.30 If the Server does not respond, the router tries to contact it again after the specified timeout period. Timeout 2 Number of Retries: 2 V Make this the Master Server. OK Cancel Help	
Additional Tasks		

該当する場合、[Make This the Master Server] チェック ボックスをオンにします。[OK]をクリックし、次に、[OK] をクリックします。

<u>ステップ 3. WebVPN ポリシー グループの設定とリソースの選択</u>

WebVPN ポリシー グループを設定し、リソースを選択するには、次の手順を実行します。

- 1. [Configure]をクリックし、次に [VPN] をクリックします。
- 2. [WebVPN] を展開し、[WebVPN Context] を選択します。



3. [Group Policies] を選択し、[Add] をクリックします。[Add Group Policy] ダイアログ ボック スが表示されます。

Add Group Policy
General Clientless Thin Client SSL VPN Client (Full Tunnel)
Name: policy_1
Make this the default group policy for context.
Client's WebVPN session will be disconnected if the client is connected longer than the session timeout or if the client is idle longer than the idle timeout.
Idle Timeout: 2100 (sec) Session Timeout: 43200 (sec)
OK Cancel Help

- 4. 新しいポリシーの名前を入力し、**[Make this the default group policy for context]** チェック ボックスにチェックマークを入れます。
- 5. ダイアログ ボックスの上にある [Clientless] タブをクリックします。

Clientless Thin Client SSL VPN Client (Full Tunnel) Clientless Web Browsing Ect a list of URLs from the global list of URLs configured in this WebVPN contex ect a list of URLs from the global list of URLs configured in this WebVPN contex is list appear to the WebVPN client in the WebVPN portal page. Action URL List Select InternalWebServers	xt. The URLs View Add ⊽
Clientless Web Browsing ect a list of URLs from the global list of URLs configured in this WebVPN contex his list appear to the WebVPN client in the WebVPN portal page. Action URL List Select InternalWebServers	xt. The URLs View Add ⊽
Clientless Web Browsing ect a list of URLs from the global list of URLs configured in this WebVPN content his list appear to the WebVPN client in the WebVPN portal page. Action URL List Select InternalWebServers	xt. The URLs View Add ⊽
ect a list of URLs from the global list of URLs configured in this WebVPN contex his list appear to the WebVPN client in the WebVPN portal page. Action URL List Select InternalWebServers	xt. The URLs View Add ⊽
Action URL List	View Add ⊽
Action URL List	View Add ⊽
Select InternalWebServers	Add ⊽
Hide LIRL har in the nortal name	
Enable CIFS	
mmon Internet File System(CIFS) allows users to view, create, or edit files on se	ervers
ning Microsoft Windows operating systems using a web browser. Use this feat	ture to
ess shared files in the corporate network from any public network using WebVF	PN. Specify
WINS server list.	
Read	
Write	
NS Server List NBNSServers View	
OK Cancel Help	

- 6. 選択する URL リストの [Select] チェック ボックスにチェックマークを付けます。
- 7. お客様が Citrix クライアントを使用するため、Citrix サーバへのアクセスが必要な場合は、 [Enable Citrix] チェック ボックスをオンにします。
- 8. [Enable CIFS]、[Read]、および [Write] チェック ボックスをオンにします。
- 9. [NBNS Server List] ドロップダウンの矢印をクリックして、<u>ステップ 2</u> で Windows ファイ ル ブラウジング用に作成した NBNS サーバ リストを選択します。
- 10. [OK] をクリックします。

<u>ステップ 4. WebVPN コンテキストの設定</u>

WebVPN ゲートウェイ、グループ ポリシー、およびリソースをリンクさせるには、WebVPN コ ンテキストを設定する必要があります。WebVPN コンテキストを設定するには、次の手順を実行 します。

1. [WebVPN Context] を選択し、コンテキストの名前を入力します。

Add WebVPN Context			 \mathbf{x}
WebVPN Context Group Policies HTML Display Settings NetBIOS Name Server Lis Port Forward Lists URL Lists Cisco Secure Desktop	Name: Associated Gateway: Domain: Authentication List: Authentication Domain: I♥ Enable Context Maximum Number of users: VRF Name: Default Group Policy:	SalesContext WidgetSSLVPNGW1 None 2 < <pre> None Policy_1 </pre>	
	OK Cancel	Help	

- 2. [Associated Gateway] ドロップダウンの矢印をクリックして、関連付けられているゲートウェイを選択します。
- 複数のコンテキストを作成する場合は、このコンテキストを識別する一意の名前を [Domain] フィールドに入力します。[Domain] フィールドを空欄にすると、ユーザは https://IPAddress で WebVPN にアクセスすることになります。ドメイン名(たとえば、 Sales)を入力すると、ユーザは https://IPAddress/Sales で接続することになります。
- 4. [Enable Context] チェック ボックスをオンにします。
- 5. [Maximum Number of Users] フィールドで、デバイスのライセンスで許可されている最大の ユーザ数を入力します。
- 6. [Default Group policy] ドロップダウンの矢印をクリックし、グループ ポリシーを選択してこのコンテキストに関連付けます。
- 7. [OK]をクリックし、次に、[OK] をクリックします。

<u>ステップ 5. ユーザ データベースと認証方法の設定</u>

Radius、Cisco AAA サーバ、またはローカル データベースで認証を行うように、クライアントレ ス SSL VPN(WebVPN)セッションを設定できます。次の例では、ローカル データベースを使 用します。

ユーザ データベースと認証方法を設定するには、次の手順を実行します。

- 1. [Configuration] をクリックし、[Additional Tasks] をクリックします。
- 2. [Router Access] を展開し、[User Accounts/View] を選択します。

🖾 Cisco Router and Security Device Manager (SDM): 10.89.129.170					
File Edit View	Tools Help				
🔥 Home	Configure 🔯 Monito	Refresh Sav	e Search Help		CISCO SYSTEMS
Tasks	Additional Tasks				
Tasks	Additional Tasks Additional Tasks Router Properties Router Access VIY Management Access SSH Secure Device Provisioning DHCP DNS Dynamic DNS Methods ACL Editor Port to Application Mapping: ACL Editor Port to Application Mapping: AAA Local Pools Router Provisioning Configuration Management	User Accounts/View Username admin austin austin fallback	Password	Privilege Level 15 15 15 15	Add Edit Delete View Name <none> <none> <none></none></none></none>
Intrusion Prevention				17:1	2-15 LTC West Jul 26 2008
Additional Tasks 17:12:15 UTC Wed Jul 26 2006					

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

Add an Account		
Enter the username and password		
Username:	sales_user1	
Password		
Password	<none></none>	
New Password:	****	
Confirm New Password:	****	
Encrypt password using MD5 hash algorithm		
Privilege Level:		
Associate a View with the user		
View Name : SDM_Administrator(root) View Details		
OK Cance	I Help	

- 4. ユーザ アカウントとパスワードを入力します。
- 5. [OK]をクリックし、次に、[OK] 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>成果</u>

ASDM は次のコマンドライン設定を作成します。

ausiiiii-3023-01
Building configuration
Current configuration : 4190 bytes ! ! Last configuration change at 17:22:23 UTC Wed Jul 26 2006 by auspml

```
NVRAM config last updated at 17:22:31 UTC Wed Jul 26
2006 by ausnml
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname ausnml-3825-01
boot-start-marker
boot system flash c3825-adventerprisek9-mz.124-9.T.bin
boot-end-marker
no logging buffered
enable secret 5 $1$KbIu$508qKYAVpWvyv9rYbrJLi/
aaa new-model
1
aaa authentication login default local
aaa authentication login sdm_vpn_xauth_ml_1 local
aaa authorization exec default local
1
aaa session-id common
resource policy
1
ip cef
ip domain name cisco.com
voice-card 0
no dspfarm
1
!--- Self-Signed Certificate Information crypto pki
trustpoint ausnml-3825-01_Certificate enrollment
selfsigned serial-number none ip-address none
revocation-check crl rsakeypair ausnml-3825-
01_Certificate_RSAKey 1024 ! crypto pki certificate
chain ausnml-3825-01_Certificate certificate self-signed
02 30820240 308201A9 A0030201 02020102 300D0609 2A864886
F70D0101 04050030 29312730 2506092A 864886F7 0D010902
16186175 736E6D6C 2D333832 352D3031 2E636973 636F2E63
6F6D301E 170D3036 30373133 32333230 34375A17 0D323030
31303130 30303030 305A3029 31273025 06092A86 4886F70D
01090216 18617573 6E6D6C2D 33383235 2D30312E 63697363
6F2E636F 6D30819F 300D0609 2A864886 F70D0101 01050003
818D0030 81890281 8100C97D 3D259BB7 3A48F877 2C83222A
A1E9E42C 5A71452F 9107900B 911C0479 4D31F42A 13E0F63B
E44753E4 0BEFDA42 FE6ED321 8EE7E811 4DEEC4E4 319C0093
C1026C0F 38D91236 6D92D931 AC3A84D4 185D220F D45A411B
09BED541 27F38EF5 1CC01D25 76D559AE D9284A74 8B52856D
BCBBF677 0F444401 D0AD542C 67BA06AC A9030203 010001A3
78307630 0F060355 1D130101 FF040530 030101FF 30230603
551D1104 1C301A82 18617573 6E6D6C2D 33383235 2D30312E
63697363 6F2E636F 6D301F06 03551D23 04183016 801403E1
5EAABA47 79F6C70C FBC61B08 90B26C2E 3D4E301D 0603551D
0E041604 1403E15E AABA4779 F6C70CFB C61B0890 B26C2E3D
4E300D06 092A8648 86F70D01 01040500 03818100 6938CEA4
2E56CDFF CF4F2A01 BCD585C7 D6B01665 595C3413 6B7A7B6C
F0A14383 4DA09C30 FB621F29 8A098FA4 F3A7F046 595F51E6
7C038112 0934A369 D44C0CF4 718A8972 2DA33C43 46E35DC6
5DCAE7E0 B0D85987 A0D116A4 600C0C60 71BB1136 486952FC
55DE6A96 1135C9D6 8C5855ED 4CD3AE55 BDA966D4 BE183920
```

88A8A55E quit username admin privilege 15 secret 5 \$1\$jm6N\$2xNfhupbAinq3BQZMRzrW0 username ausnml privilege 15 password 7 15071F5A5D292421 username fallback privilege 15 password 7 08345818501A0A12 username austin privilege 15 secret 5 \$1\$3xFv\$W0YUsKDx1adDc.cVQF2Ei0 username sales_user1 privilege 5 secret 5 \$1\$2/SX\$ep4fsCpodeyKaRji2mJkX/ ! interface GigabitEthernet0/0 ip address 192.168.0.37 255.255.255.0 duplex auto speed auto media-type rj45 ! interface GigabitEthernet0/1 ip address 172.22.1.151 255.255.255.0 duplex auto speed auto media-type rj45 ! ip route 0.0.0.0 0.0.0.0 172.22.1.1 ! ip http server ip http authentication local ip http timeout-policy idle 600 life 86400 requests 100 ! control-plane ! line con 0 stopbits 1 line aux 0 stopbits 1 line vty 0 4 exectimeout 40 0 privilege level 15 password 7 071A351A170A1600 transport input telnet ssh line vty 5 15 exec-timeout 40 0 password 7 001107505D580403 transport input telnet ssh ! scheduler allocate 20000 1000 ! !--- WebVPN Gateway webvpn gateway WidgetSSLVPNGW1 hostname ausnml-3825-01 ip address 192.168.0.37 port 443 http-redirect port 80 ssl trustpoint ausnml-3825-01_Certificate inservice ! webvpn context SalesContext ssl authenticate verify all ! !---Identify resources for the SSL VPN session url-list "InternalWebServers" heading "WidgetWebServers" url-text "WidgetWeb" url-value "http://172.22.1.30" url-text "OWA" url-value "http://172.22.1.50/exchange" ! nbnslist NBNSServers nbns-server 172.22.1.30 ! !--- Identify the policy which controls the resources available policy group policy_1 url-list "InternalWebServers" nbns-list "NBNSServers" functions file-access functions filebrowse functions file-entry hide-url-bar citrix enabled default-group-policy policy_1 gateway WidgetSSLVPNGW1 max-users 2 inservice ! end

<u>確認</u>

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>手順</u>

設定が正常に動作していることを確認するには、次の手順を実行します。

 ユーザを使用して設定をテストします。SSL対応のWebブラウザに https://WebVPN_Gateway_IP_Addressと入力します。この場合、 WebVPN_Gateway_IP_Address は WebVPN サービスの IP アドレスです。証明書を承認して ユーザ名とパスワードを入力すると、次のイメージのようなイメージが表示されます。

Cince Systems WebV	PN Service	2:0×	
	If the Floating Toolbar does not open, click here to open it.		
Care Web Sites			
Tacacs	Enter Web Address (URL) Go		
https://192.168.0.37	- WebVPN Service Toolbar COX Browse Network		
Websites			
Enter Web Address	(URL)		
	Go		
2	🔒 💿 Internet		

- SSL VPN セッションをチェックします。SDM アプリケーションで、[Monitor] ボタンをクリ ックし、次に [VPN Status] をクリックします。[WebVPN (All Contexts)] を展開し、適切なコ ンテキストを展開して、[Users] を選択します。
- エラー メッセージを確認します。SDM アプリケーションで、[Monitor] ボタンをクリックし、[Logging] をクリックして、次に [Syslog] タブをクリックします。
- デバイスの実行コンフィギュレーションを表示します。SDM アプリケーションで [Configure] ボタンをクリックし、[Additional Tasks] をクリックします。[Configuration Management] を 展開し、[Config Editor] を選択します。

<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。

注:コピーの実行中は、[Copy File to Server]コマンドを中断したり、別のウィンドウに移動した りしないでください。操作を中断すると、不完全なファイルがサーバに保存される可能性があり ます。

注:ユーザはWebVPNクライアントを使用して新しいファイルをアップロードおよびダウンロー ドできますが、WebVPN上のCommon Internet File System(CIFS)のファイルをCopy File to Serverコマンドを使用して上書きすることは許可されませんんす。ユーザがサーバ上のファイル を置き換えようとすると、次のメッセージが表示されます。



設定をトラブルシューティングするには、次の手順を実行します。

- 1. クライアントでポップアップ ブロッカーが無効になっていることを確認します。
- 2. クライアントで cookie が有効になっていることを確認します。
- 3. クライアントで Netscape、Internet Explorer、Firefox、または Mozilla ブラウザが使用され ていることを確認します。

<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。

<u>関連情報</u>

- <u>Cisco IOS SSLVPN</u>
- <u>Cisco IOS SSLVPN Q&A</u>
- <u>SDM によるシンクライアント SSL VPN (WebVPN) の IOS 設定例</u>
- <u>SDM を使用した IOS での SSL VPN Client (SVC)の設定例</u>
- ・<u>テクニカル サポートとドキュメント Cisco Systems</u>