# Beispiel einer Thin-Client SSL VPN (WebVPN)-Konfiguration für ASA mit ASDM

## Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Netzwerkdiagramm Konventionen Hintergrundinformationen SSL-VPN-Konfiguration mit Thin-Client unter Verwendung von ASDM Schritt 1: Aktivierung von WebVPN auf der ASA Schritt 2: Konfigurieren von Port Forwarding-Eigenschaften Schritt 3: Erstellen einer Gruppenrichtlinie und Verknüpfen Sie diese mit der Port Forwarding List Schritt 4: Erstellen einer Tunnelgruppe und Verknüpfen Sie diese mit der Gruppenrichtlinie Schritt 5: Erstellen eines Benutzers und Hinzufügen dieses Benutzers zur Gruppenrichtlinie SSL-VPN-Konfiguration mit Thin-Client über CLI Überprüfen Vorgehensweise **Befehle** Fehlerbehebung Ist der SSL-Handshake-Prozess abgeschlossen? Ist der SSL VPN Thin-Client funktionsfähig? Befehle Zugehörige Informationen

## **Einführung**

Die Thin-Client SSL VPN-Technologie ermöglicht den sicheren Zugriff für einige Anwendungen mit statischen Ports, z. B. Telnet(23), SSH(22), POP3(110), IMAP4(143) und SMTP(25). Sie können das Thin-Client SSL VPN als benutzergesteuerte Anwendung, richtliniengesteuerte Anwendung oder beides verwenden. Das heißt, Sie können den Zugriff auf Benutzerbasis konfigurieren oder Gruppenrichtlinien erstellen, in denen Sie einen oder mehrere Benutzer hinzufügen.

 Clientless SSL VPN (WebVPN) - Stellt einen Remote-Client bereit, der einen SSL-f\u00e4higen Webbrowser f\u00fcr den Zugriff auf HTTP- oder HTTPS-Webserver in einem lokalen Unternehmensnetzwerk (LAN) ben\u00fötigt. Dar\u00fcber hinaus bietet Clientless-SSL-VPN Zugriff f\u00fcr das Durchsuchen von Windows-Dateien \u00fcber das Common Internet File System (CIFS)-Protokoll. Outlook Web Access (OWA) ist ein Beispiel f\u00fcr den HTTP-Zugriff.Weitere Informationen zum <u>Clientless-SSL-VPN (WebVPN) finden Sie</u> im <u>Konfigurationsbeispiel</u> der

#### <u>ASA</u>.

- Thin-Client SSL VPN (Port Forwarding) Bietet einen Remote-Client, der ein kleines, Javabasiertes Applet herunterlädt und sicheren Zugriff für TCP-Anwendungen (Transmission Control Protocol) ermöglicht, die statische Portnummern verwenden. Beispiele für sicheren Zugriff sind das Post Office Protocol (POP3), Simple Mail Transfer Protocol (SMTP), Internet Message Access Protocol (IMAP), Secure Shell (SSH) und Telnet. Da sich Dateien auf dem lokalen Computer ändern, müssen Benutzer über lokale Administratorberechtigungen verfügen, um diese Methode verwenden zu können. Diese SSL VPN-Methode funktioniert nicht mit Anwendungen, die dynamische Portzuweisungen verwenden, wie z. B. einige FTP-Anwendungen (File Transfer Protocol).**Hinweis:** User Datagram Protocol (UDP) wird nicht unterstützt.
- SSL VPN Client (Tunnel-Modus): Lädt einen kleinen Client zur Remote-Workstation herunter und ermöglicht einen vollständigen sicheren Zugriff auf Ressourcen in einem internen Unternehmensnetzwerk. Sie können den SSL VPN Client (SVC) dauerhaft auf eine Remote-Workstation herunterladen oder den Client entfernen, wenn die sichere Sitzung beendet ist.Weitere Informationen zum SSL VPN-Client finden Sie unter <u>SSL VPN Client (SVC) auf ASA mit ASDM Configuration Example</u>.

Dieses Dokument zeigt eine einfache Konfiguration für das Thin-Client SSL VPN auf der Adaptive Security Appliance (ASA). Die Konfiguration ermöglicht es Benutzern, sicher Telnet zu einem Router in der ASA zu übertragen. Die Konfiguration in diesem Dokument wird für ASA 7.x und höher unterstützt.

## **Voraussetzungen**

### **Anforderungen**

Bevor Sie diese Konfiguration versuchen, stellen Sie sicher, dass Sie die folgenden Anforderungen für die Remote-Client-Stationen erfüllen:

- SSL-fähiger Webbrowser
- SUN Java JRE Version 1.4 oder höher
- Cookies aktiviert
- Popup-Blocker deaktiviert
- Lokale Administratorrechte (nicht erforderlich, aber dringend empfohlen)

**Hinweis:** Die neueste Version der SUN Java JRE steht als kostenloser Download von der <u>Java-</u> <u>Website</u> zur Verfügung.

#### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Adaptive Security Appliance der Serie 5510
- Cisco Adaptive Security Device Manager (ASDM) 5.2(1)Hinweis: Informationen zur Konfiguration der ASA durch den ASDM finden Sie unter <u>Zulassen von HTTPS-Zugriff für</u> <u>ASDM</u>.
- Cisco Adaptive Security Appliance Software Version 7.2(1)
- Remote-Client Microsoft Windows XP Professional (SP 2)

Die Informationen in diesem Dokument wurden in einer Laborumgebung entwickelt. Alle in diesem Dokument verwendeten Geräte wurden auf ihre Standardkonfiguration zurückgesetzt. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen. Alle in dieser Konfiguration verwendeten IP-Adressen wurden in einer Laborumgebung aus RFC 1918-Adressen ausgewählt. Diese IP-Adressen sind nicht im Internet routbar und dienen nur zu Testzwecken.

#### **Netzwerkdiagramm**

In diesem Dokument wird die in diesem Abschnitt beschriebene Netzwerkkonfiguration verwendet.

Wenn ein Remote-Client eine Sitzung mit der ASA initiiert, lädt der Client ein kleines Java-Applet auf die Workstation. Dem Client wird eine Liste vorkonfigurierter Ressourcen angezeigt.



#### Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den <u>Cisco Technical Tips</u> <u>Conventions</u>.

## Hintergrundinformationen

Um eine Sitzung zu starten, öffnet der Remote-Client einen SSL-Browser zur externen Schnittstelle der ASA. Nach Einrichtung der Sitzung kann der Benutzer die auf der ASA konfigurierten Parameter verwenden, um Telnet- oder Anwendungszugriff aufzurufen. Die ASA stellt die sichere Verbindung her und ermöglicht dem Benutzer den Zugriff auf das Gerät.

**Hinweis:** Eingehende Zugriffslisten sind für diese Verbindungen nicht erforderlich, da die ASA bereits weiß, was eine rechtliche Sitzung darstellt.

## SSL-VPN-Konfiguration mit Thin-Client unter Verwendung von

## <u>ASDM</u>

Gehen Sie wie folgt vor, um Thin-Client SSL VPN auf der ASA zu konfigurieren:

- 1. Aktivierung von WebVPN auf der ASA
- 2. Konfigurieren von Port Forwarding-Eigenschaften
- 3. <u>Erstellen einer Gruppenrichtlinie und Verknüpfen Sie diese mit der Portweiterleitungsliste</u> (erstellt in Schritt 2)
- 4. <u>Erstellen einer Tunnelgruppe und Verknüpfen Sie diese mit der Gruppenrichtlinie</u> (erstellt in Schritt 3)
- 5. <u>Erstellen eines Benutzers und Hinzufügen dieses Benutzers zur Gruppenrichtlinie</u> (erstellt in Schritt 3)

#### Schritt 1: Aktivierung von WebVPN auf der ASA

Gehen Sie wie folgt vor, um WebVPN auf der ASA zu aktivieren:

- 1. Klicken Sie in der ASDM-Anwendung auf Konfiguration und dann auf VPN.
- 2. Erweitern Sie WebVPN, und wählen Sie WebVPN Access aus.



- 3. Markieren Sie die Schnittstelle, und klicken Sie auf Aktivieren.
- 4. Klicken Sie auf **Übernehmen**, klicken Sie auf **Speichern** und dann auf **Ja**, um die Änderungen zu übernehmen.

### Schritt 2: Konfigurieren von Port Forwarding-Eigenschaften

Gehen Sie wie folgt vor, um die Eigenschaften der Port-Weiterleitung zu konfigurieren:

1. Erweitern Sie **WebVPN**, und wählen Sie **Port Forwarding aus**.



2. Klicken Sie auf die Schaltfläche Hinzufügen.

Timzulug	<b>J</b> OI 1.										
File Options	Tools Wizards	Help							Search		Find •
Shome	Configuration	Monitoring	Back	Forward	Packet Tracer	Refresh	- Save	? Help			Cisco Systems
Interfaces		on - VPN - We eral VPN System Opti Client Update Tunnel Group Group Policy Jaers Default Tunnel G- Zone Labs Integr C ddress Managem Assignment P Pools	ateway ty Server	Port Forwa	Configure port for This parameter List Name rding List	warding lists fo	r application a n either a VP lort Remot	Incress over	WebVPN. aroup policy con Remote TCP	figuration. Description	Add
PS CSD Manager CSD Manager Routing Global Objects Properties	(1)     (2)     (	VPN WebVPN Access Proxies APCF Content Rewrite Java Trustpoint Proxy Bypass Servers and URL Servers and URL Soft Serversure ACLs Encoding SSL VPN Client SSO Servers al Proxy		ocal TCP Port	Remote Ser	ver Remot	e TCP Port	Description	Help		Add Edit Delete
	1					ciso	0 11	5			18/06 12:40:29 PM UT

3. Geben Sie im Dialogfeld "Portweiterleitungsliste hinzufügen" einen Listennamen ein, und klicken Sie auf **Hinzufügen**.Das Dialogfeld Port Forwarding Entry (Port-Weiterleitungseintrag

hinzufügen) wird angezeigt.

General States and Sta	
😼 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

- 4. Geben Sie im Dialogfeld Add Port Forwarding Entry (Port-Weiterleitungseintrag hinzufügen) die folgenden Optionen ein:Geben Sie im Feld Local TCP Port (Lokaler TCP-Port) eine Portnummer ein, oder akzeptieren Sie den Standardwert.Beim eingegebenen Wert kann es sich um eine beliebige Zahl zwischen 1024 und 65535 handeln.Geben Sie im Feld Remote Server (Remote-Server) eine IP-Adresse ein.In diesem Beispiel wird die Adresse des Routers verwendet.Geben Sie im Feld Remote TCP Port (Remote-TCP-Port) eine Portnummer ein.In diesem Beispiel wird Port 23 verwendet.Geben Sie im Feld Beschreibung eine Beschreibung ein, und klicken Sie auf OK.
- 5. Klicken Sie auf OK und dann auf Übernehmen.
- 6. Klicken Sie auf **Speichern** und dann auf **Ja**, um die Änderungen zu übernehmen.

#### Schritt 3: Erstellen einer Gruppenrichtlinie und Verknüpfen Sie diese mit der Port Forwarding List

Gehen Sie wie folgt vor, um eine Gruppenrichtlinie zu erstellen und mit der Port Forwarding-Liste zu verknüpfen:

1. Erweitern Sie Allgemein, und wählen Sie Gruppenrichtlinie aus.

File Options To	ola Vilizanda Help						Search	Find +
Canal Home	Configuration Monitoring Back	Porward	Recket Tracer	(C+ Refresh	Save	? Help		Cisco Systems
interfaces Security Policy	Contouration > PS VPN Vizard General Client Update Client Update	:	Group Policy Manage 1 may be a reference	VPN group pol tored internalit ed by VPN turn	icies: A VPN g y an the device nel groups and Turce	oup policy is a collection or externally on a RADIL luser accounts.	of user-oriented attribute/value p IS server. The group policy inform AAA Server Group	ers that istion is
NAT	Tone Labs Integrity Server		DritGrysPolicy	(System Det	a Internal	L2TP-PSec PSec	N/A	Internal Group Policy.
SK VPH	R P Address Management							External Group Policy
IS IS CSD Manager Routing Global Objects Properties	Pools     NAC     VebVPN     VebVPN							
	AAA Authentication					Apply	Reset	
						cisco 2		8/28/06 2:14:19 PM UTC

2. Klicken Sie auf **Hinzufügen**, und wählen Sie **Interne Gruppenrichtlinie aus**.Das Dialogfeld Interne Gruppenrichtlinie hinzufügen wird angezeigt.

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. Geben Sie einen Namen ein, oder akzeptieren Sie den Standardnamen der Gruppenrichtlinie.
- 4. Deaktivieren Sie das Kontrollkästchen **Tunneling Protocols Inherit** (Tunneling-Protokolle erben), und aktivieren Sie das **WebVPN-**Kontrollkästchen.
- 5. Klicken Sie auf die Registerkarte **WebVPN** oben im Dialogfeld, und klicken Sie dann auf die Registerkarte **Funktionen**.
- 6. Deaktivieren Sie das Kontrollkästchen Erben, und aktivieren Sie die Kontrollkästchen Auto Applet Download und Enable Port Forwarding aktivieren, wie in diesem Bild gezeigt:

Add Internal Group Policy	
Name: NetAdmins	
Consul DCos Clast Configuration Clast Engund Manhard Clast Mich VPN	
General IPSec Client Configuration Client Firewall Hardware Client NAC Web Priv	
Configure WebVPN attributes using the following tabs .	
Check an Inherit checkbox to let the corresponding setting take its value from the default group policy.	
Functions Content Filtering Homepage Port Forwarding Other SSL VPN Client Auto Signon	
nherit	
Enable URL entry	
Enable file server access Enable Outlook/Exchange proxy	
Enable file server entry     Apply Web-type ACL     Enable file server browsing     Enable file server browsing	
Enable auto applet download     Enable Citrix MetaFrame	
	_
OK Cancel Help	

7. Klicken Sie auch auf der Registerkarte WebVPN auf die Registerkarte **Port Forwarding** (**Portweiterleitung**), und deaktivieren Sie das Kontrollkästchen Port Forwarding List **Inherit** (**Portweiterleitungsliste vererben**).

🚰 Add Internal Group Policy
Name: NetAdmins
General IPSec Client Configuration Client Firewall Hardware Client NAC WebVPN
Configure WebVPN attributes using the following tabs .
Check an Inherit checkbox to let the corresponding setting take its value from the default group policy.
Functions Content Filtering Homepage Port Forwarding Other SSL VPN Client Auto Signon
Port Forwarding List: Inherit Routers New
Applet Name: Inherit Secure Router Access

- 8. Klicken Sie auf den Pfeil des Dropdown-Menüs **Portweiterleitungsliste**, und wählen Sie die in <u>Schritt 2</u> erstellte Liste für die Portweiterleitung aus.
- 9. Deaktivieren Sie das Kontrollkästchen **Erben von** Applet-Name, und ändern Sie den Namen im Textfeld.Der Client zeigt den Applet-Namen bei der Verbindung an.
- 10. Klicken Sie auf OK und dann auf Übernehmen.
- 11. Klicken Sie auf **Speichern** und dann auf **Ja**, um die Änderungen zu übernehmen.

# Schritt 4: Erstellen einer Tunnelgruppe und Verknüpfen Sie diese mit der Gruppenrichtlinie

Sie können die Standard-*DefaultWebVPNGroup*-Tunnelgruppe bearbeiten oder eine neue Tunnelgruppe erstellen.

Gehen Sie wie folgt vor, um eine neue Tunnelgruppe zu erstellen:

1. Erweitern Sie General, und wählen Sie Tunnel Group

#### (Tunnelgruppe).



 Klicken Sie auf Hinzufügen, und wählen Sie WebVPN Access aus.Das Dialogfeld "Tunnel-Gruppe hinzufügen" wird angezeigt.

Name:       NetGroup       Type:       webvpn         General       WebVPN         Configure general access attributes from the following sub-tabs.         Basic       Authentication       Authorization       Accounting       Client Address Assignment       Advanced         Group Policy:       NetAdmins       Image: Client Address Assignment       Advanced         Group Policy:       NetAdmins       Image: Client Address Assignment       Advanced         Strip the realm from username before passing it on to the AAA server       Image: Coverride account-disabled indication from AAA server       Image: Coverride account-disabled indication from AAA server         Image: Coverride account-disabled indication from AAA server       Image: Coverride account-disabled indication from AAA server       Image: Coverride account-disabled indication from AAA server         Image: Coverride account-disabled indication from AAA server       Image: Coverride account-disabled indication from AAA server       Image: Coverride account-disabled indication from AAA server         Imable notification upon password expiration to allow user to change password       Image: Coverride account-disabled indication from from from from from from from from	dd Tunr	el Group						
General       WebVPN         Configure general access attributes from the following sub-tabs.         Basic       Authentication         Authentication       Authorization         Coroup 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         Override account-disabled indication from AAA server         Enable notification upon password expiration to allow user to change password         Enable notification prior to expiration	Name:	NetGroup	)		Туре:	webypn		
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 Strip the group from username before passing it on to the AAA server Coverride account-disabled indication from AAA server Coverride account-disabled indication from AAA server Coverride account-disabled indication to allow user to change password Coverride account of expiration Coverride account	General	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  Readed adverse passing it on to the AAA server  Control of the expiration of the expi		100111						
Basic       Authentication       Authorization       Accounting       Client Address Assignment       Advanced         Group Policy:       NetAdmins       Image: Client Address Assignment       Advanced         Group Policy:       NetAdmins       Image: Client Address Assignment       Advanced         Group Policy:       NetAdmins       Image: Client Address Assignment       Advanced         Strip the realm from username before passing it on to the AAA server       Image: Client Address Asserver       Image: Client Address Asserver         Password Management       Image: Client Address Asserver       Image: Client Address Asserver       Image: Client Address Asserver         Image: Client Address Asserver       Image: Client Address Asserver       Image: Client Address Asserver       Image: Client Address Asserver         Image: Client Address Asserver       Image: Client Address Asserver       Image: Client Address Asserver       Image: Client Address Asserver         Image: Client Address Asserver       Image: Client Address Asserver       Image: Client Address Asserver       Image: Client Address Asserver         Image: Client Address Asserver       Image: Client Address Asserver       Image: Client Address Asserver       Image: Client Address Asserver         Image: Client Address Asserver       Image: Client Address Asserver       Image: Client Address Asserver       Image: Client Address Asserver <tr< th=""><th>Config</th><th>ure general acce</th><th>ess attributes fro</th><th>om the followi</th><th>ng sub-t</th><th>tabs.</th><th></th><th></th></tr<>	Config	ure general acce	ess attributes fro	om the followi	ng sub-t	tabs.		
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         Inable notification prior to expiration         Notify       days prior to expiration	Basic	Authentication	Authorization	Accounting	Client /	Address Assignmen	Advanced	
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	Gro	up 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 Mays prior to expiration								
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 Management Notify		Strip the realm f	rom username b	efore passing	g 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		Strip the group	from username t	pefore passin	g it on ta	o 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								
Override account-disabled indication from AAA server  Finable notification upon password expiration to allow user to change password  Finable notification prior to expiration  Notify  days prior to expiration	Pa	ssword Manage	ment					
Enable notification prior to expiration Notify days prior to expiration		Epable potific	count-disabled in	idication from	AAA st	erver	neceword	
		Enable	notification prior	to expiration		Notify	days prior to expiration	
			-					
			OK		Cano		leip	

- 3. Geben Sie im Feld Name einen Namen ein.
- 4. Klicken Sie auf den Pfeil des Dropdown-Menüs **Gruppenrichtlinie**, und wählen Sie die Gruppenrichtlinie aus, die Sie in <u>Schritt 3</u> erstellt haben.
- 5. Klicken Sie auf **OK** und dann auf **Übernehmen**.
- 6. Klicken Sie auf **Speichern** und dann auf **Ja**, um die Änderungen zu übernehmen.Die Eigenschaften von Tunnelgruppe, Gruppenrichtlinie und Port Forwarding sind nun miteinander verknüpft.

#### <u>Schritt 5: Erstellen eines Benutzers und Hinzufügen dieses Benutzers zur</u> <u>Gruppenrichtlinie</u>

Gehen Sie wie folgt vor, um einen Benutzer zu erstellen und der Gruppenrichtlinie diesen hinzuzufügen:

1. Erweitern Sie **Allgemein**, und wählen Sie **Benutzer aus**.

File Options Too	ols Wizerds	Help							Search		Find •
Home C	ogg Configuration	Monitoring	O Back	Forward	C Packet Tracer	Q Refresh	Save 1	?			Cisco Systems
Interfaces Interfaces Security Policy NAT Security Policy NAT Security Policy PS CSD Manager CSD Manager Routing Sciobal Objects Properties		Noncoring IN System Option Jent Update Unnel Group Kroup Policy Broze Sone Labs Integrity See Rules Iransform Sets tre-Fragmentation diress Management Assignment Prools VPN NebVPN Access travies VPN NebVPN Access travies VPN NebVPN Access travies VPN Secret Content Rewrite lava Trustpoint travy Bypass Servers and URLs forcoding SL VPN Clent	at	Create entries be user accou User Name nable_15 isco usermi aliest	In the ASA local Int privileges to b Privilege 15 15 15 4	user datab e enforced	save r ase. Command . To enable com VPN Group Polic MA DitGrpPolicy DitGrpPolicy SalesGroupPolicy	authorization mand author cy VPN C N/A Inher y Inher	must be enabl ization, go to st iroup Lock # Group Polic # Group Polic # Group Polic	ed in order for chorecolor.	
	:::::::::::::::::::::::::::::::::::::	SO Servers I Proxy					Apply	Reset			

2. Klicken Sie auf die Schaltfläche **Hinzufügen**. Das Dialogfeld Benutzerkonto hinzufügen wird angezeigt.

🖆 Add User Account	
Identity VPN Policy WebVPN	
Thereacy Victoria	
Username:	user1
Password:	****
Confirm Password:	A#A#A#A
	Ed Using MSCHAP
Privilege level is used with	h command authorization.
Privilege Level:	2
OK	Cancel Help

3. Geben Sie Werte für den Benutzernamen, das Kennwort und die Berechtigungsinformationen ein, und klicken Sie dann auf die Registerkarte VPN Policy.

Charle on Inherit sheekhow to let the se	wreenending ant	ing take its using from the sur	
Tunneling Protocols:	Inherit	PSec WebVPN	L2TP over IPSec
Filter:	🗹 Inherit		Manage
Tunnel Group Lock:	🗹 Inherit		~
Store Password on Client System:	🗹 Inherit	O Yes O No	
Connection Settings			
Access Hours:	🗹 Inherit		V New
Simultaneous Logins:	🗹 Inherit		
Maximum Connect Time:	🔽 Inherit	Unlimited	minutes
Idle Timeout:	🔽 Inherit	Unlimited	minutes
Dedicated IP Address (Optional)	Subr	et Mask:	<b>×</b>

- 4. Klicken Sie auf den Pfeil des Dropdown-Menüs **Gruppenrichtlinie**, und wählen Sie die Gruppenrichtlinie aus, die Sie in <u>Schritt 3</u> erstellt haben.Dieser Benutzer erbt die WebVPN-Eigenschaften und -Richtlinien der ausgewählten Gruppenrichtlinie.
- 5. Klicken Sie auf OK und dann auf Übernehmen.
- 6. Klicken Sie auf **Speichern** und dann auf **Ja**, um die Änderungen zu übernehmen.

## **SSL-VPN-Konfiguration mit Thin-Client über CLI**

```
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
!--- Create a new group policy for enabling WebVPN
access group-policy NetAdmins attributes
vpn-tunnel-protocol IPSec 12tp-ipsec webvpn
!--- Configure group policy attributes webvpn
 functions port-forward auto-download
!--- Configure group policies for WebVPN
                                           port-forward
value portforward
!--- Configure port-forward to enable WebVPN
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
!--- Create a new tunnel group and link it to the group
policy 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>Überprüfen</u>

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

#### **Vorgehensweise**

In diesem Verfahren wird beschrieben, wie Sie die Gültigkeit der Konfiguration bestimmen und die Konfiguration testen.

 Geben Sie auf einer Client-Workstation https://outside\_ASA\_IP address ein; wobei outside\_ASA\_IPAddress die SSL-URL der ASA ist.Sobald das digitale Zertifikat akzeptiert und der Benutzer authentifiziert wurde, wird die Webseite f
ür den WebVPN-Dienst angezeigt.

File Edit View Favorites Tools Help		nnnnnn sy Mil		
🚱 Back 🔹 🕥 - 💌 😰 🏠 🔎 Sear	ch 🤺 Favorites	🚱 🔗 🌺	w •	, »
Address Address Address Address Address	1	~	🔁 Go	Links »
Google - G Search	• 🥥 💰 🛃	Popups okay >>	SnagIt	: 🛃
CISCO SYSTEMS WebVPN Service				_
		?		$\mathbf{X}$
SECORE ROUTER ACCESS Start Application Client Go thttps://172.22.1.160 - Secure Router A Close this window when you finish us Please wait for the table to be displa If you shut down your computer with later have problems running the applied details.	Access - Microsoft ing Application yed before start out closing this y lications listed b	t Internet Ex Access. ing applications. window, you migh elow. <u>Click here t</u>	t for	
Name         Local         R           Telnet to R1         127.0.0.1:3044         10.2.2           CSUME R1         127.0.0.1:3044         10.2.2	emote Bytes (	Out Bytes in Soc	kets 0	
Image: Solution ref         Image: Solution ref	.2.22	S S Internet		
E Done	2	🔒 🥩 Inter	met	

Die für den Zugriff auf die Anwendung erforderlichen Adress- und Port-Informationen werden in der lokalen Spalte angezeigt. Die Spalten Bytes Out und Bytes In zeigen keine Aktivität an, da die Anwendung zu diesem Zeitpunkt nicht aufgerufen wurde.

- 2. Verwenden Sie die DOS-Eingabeaufforderung oder eine andere Telnet-Anwendung, um eine Telnet-Sitzung zu starten.
- 3. Geben Sie an der Eingabeaufforderung telnet 127.0.0.1 3044 ein. Hinweis: Mit diesem Befehl wird ein Beispiel für den Zugriff auf den lokalen Port angezeigt, der im WebVPN Service-Webseiten-Bild in diesem Dokument angezeigt wird. Der Befehl enthält keinen Doppelpunkt (:). Geben Sie den Befehl wie in diesem Dokument beschrieben ein. Die ASA erhält den Befehl über die sichere Sitzung. Da sie eine Übersicht der Informationen speichert, weiß die ASA sofort, die sichere Telnet-Sitzung mit dem zugeordneten Gerät zu öffnen.



Sobald Sie Ihren Benutzernamen und Ihr Kennwort eingegeben haben, ist der Zugriff auf das Gerät abgeschlossen.

4. Um den Zugriff auf das Gerät zu überprüfen, überprüfen Sie die Spalten Bytes Out und Bytes In, wie in diesem Bild

gezeigt:

街 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</u> <u>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 🤢												

## **Befehle**

Mehrere **show**-Befehle sind WebVPN zugeordnet. Sie können diese Befehle in der Befehlszeilenschnittstelle (CLI) ausführen, um Statistiken und andere Informationen anzuzeigen. Detaillierte Informationen zu **show**-Befehlen finden Sie unter <u>Verifying WebVPN Configuration</u>.

Hinweis: Das <u>Output Interpreter Tool</u> (nur registrierte Kunden) (OIT) unterstützt bestimmte show-Befehle. Verwenden Sie das OIT, um eine Analyse der Ausgabe des Befehls show anzuzeigen.

## **Fehlerbehebung**

In diesem Abschnitt finden Sie eine Fehlerbehebung für Ihre Konfiguration.

#### Ist der SSL-Handshake-Prozess abgeschlossen?

Wenn Sie eine Verbindung zur ASA herstellen, überprüfen Sie, ob das Echtzeitprotokoll den Abschluss des SSL-Handshake anzeigt.

🎼 Real-time Log Viewer										
0 Pause	в 🗈 Сору 🔓	JSave 🛐	Clear 👩	Color Settings	🔁 Create Rule 🥈	Show Rule 🔞 Show Details 🤌 Help				
Filler By		~	- Elter	Show All Fig	dt.					
riter by. agrine and showing riter										
Severity	Date	Time	Syslog	Source IP	Destination IP	Description				
<b>2</b>	Jun 27 2006	11:40:42	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172.22.1.203/3102 to 216.239.53.				
<b>@</b> 2	Jun 27 2006	11:40:34	106006	172.22.1.203	171.70.157.215	Deny inbound UDP from 172.22.1.203/3101 to 171.70.157.215/1029 on				
<b>@</b> 2	Jun 27 2006	11:40:34	106006	172.22.1.203	64.101.176.170	Deny inbound UDP from 172:22.1.203/3101 to 64.101.176.170/1029 on				
<b>@</b> 2	Jun 27 2006	11:40:34	106006	172.22.1.203	171.68.222.149	Deny inbound UDP from 172.22.1.203/3101 to 171.68.222.149/1029 on				
<b>@</b> 2	Jun 27 2006	11:40:32	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172.22.1.203/3100 to 216.239.53.				
2	Jun 27 2006	11:40:24	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172.22.1.203/3098 to 216.239.53.				
2	Jun 27 2006	11:40:22	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172.22.1.203/3098 to 216.239.53.				
4.6	Jun 27 2006	11:40:18	725002	172.22.1.203		Device completed SSL handshake with client outside:172.22.1.203/309				
A 6	Jun 27 2006	11:40:18	725003	172.22.1.203		SSL client outside:172.22.1.203/3097 request to resume previous sess				
<b>A</b> 6	Jun 27 2006	11:40:18	725001	172.22.1.203		Starting SSL handshake with client 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 TCP connection 3711 for outside:172.22.1.203/3097 (172.				
<b>A</b> 6	Jun 27 2006	11:40:18	725007	172.22.1.203		SSL session with client outside:172.22.1.203/3096 terminated.				
A 6	Jun 27 2006	11:40:17	302014	172.22.1.203	172.22.1.160	Teardown TCP connection 3710 for outside:172.22.1.203/3096 to NP Id				
A 6	Jun 27 2006	11:40:17	725002	172.22.1.203		Device completed SSL handshake with client outside:172.22.1.203/309				
A 6	Jun 27 2006	11:40:17	725001	172.22.1.203		Starting SSL handshake with client 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 TCP connection 3710 for outside:172.22.1.203/3096 (172.				
<b>G</b> 3	Jun 27 2006	11:40:16	305005	64.101.176.170		No translation group found for udp src inside:10.2.2.4/1830 dst outside				
🔂 3	Jun 27 2006	11:40:16	305005	171.70.157.215		No translation group found for udp src inside:10.2.2.4/1830 dst outside				
<b>6</b> 3	Jun 27 2006	11:40:16	305005	171.68.222.149		No translation group found for udp 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 connection denied from 172.22.1.203/3095 to 216.239.53.				
<b>0</b> 2	Jun 27 2006	11:40:12	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172.22.1.203/3095 to 216.239.53.				
<			10			>				
Please select a syslog entry to see the explanation ×										
Explanation Recommended Action Details										
	🔾 Emergencies 🔇 Alerts 🥝 Critical 🤒 Errors 🔥 Warnings 🌲 Notifications 🗼 Informational 🛞 Debugging									

#### Ist der SSL VPN Thin-Client funktionsfähig?

Gehen Sie wie folgt vor, um zu überprüfen, ob der SSL VPN Thin-Client funktioniert:

- 1. Klicken Sie auf Monitoring und dann auf VPN.
- Erweitern Sie VPN Statistics, und klicken Sie auf Sitzungen. Ihre SSL VPN Thin-Client-Sitzung sollte in der Sitzungsliste angezeigt werden. Filtern Sie nach WebVPN, wie in diesem Bild gezeigt:



#### **Befehle**

Dem WebVPN sind mehrere **Debugbefehle** zugeordnet. Ausführliche Informationen zu diesen Befehlen finden Sie unter <u>Verwenden von WebVPN-Debug-Befehlen</u>.

**Hinweis:** Die Verwendung von **Debug-**Befehlen kann sich negativ auf Ihr Cisco Gerät auswirken. Bevor Sie **Debug-**Befehle verwenden, lesen Sie <u>die Informationen unter Wichtige Informationen</u> <u>über Debug-Befehle</u>.

## Zugehörige Informationen

- <u>Clientless-SSL-VPN (WebVPN) auf ASA-Konfigurationsbeispiel</u>
- <u>SSL VPN Client (SVC) auf ASA mit ASDM Konfigurationsbeispiel</u>
- <u>Cisco Adaptive Security Appliances der Serie ASA 5500</u>
- ASA mit WebVPN und Single Sign-On mit ASDM und NTLMv1 Konfigurationsbeispiel
- <u>Technischer Support und Dokumentation Cisco Systems</u>