

ASA 7.2(2) : 公衆インターネット VPN on a Stick のための SSL VPN Client (SVC) の設定例

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[ASDM 5.2\(2\) を使用した ASA 7.2\(2\) の設定](#)

[ASA 7.2\(2\) CLI の設定](#)

[SVC との SSL VPN 接続の確立](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、SSL VPN on a Stick を実行するために、適応型セキュリティ アプライアンス (ASA) 7.2.2 をセットアップする方法について説明します。この設定は、ASA でスプリット トンネリングが許可されない特定のケースに対して適用されます。ユーザはインターネットへの接続が許可される前に直接 ASA に接続されます。

注: ASA バージョン 7.2.2 では、**same-security-traffic permit** 設定モード コマンドの **intra-interface** キーワードにより、すべてのトラフィックが同じインターフェイス (IPSec トラフィックだけでなく) を出入りすることができます。

前提条件

要件

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。

- ハブ ASA セキュリティ アプライアンスはバージョン 7.2.2 を稼働する必要があります。
- Cisco SSL VPN Client (SVC) 1.x注: シスコの「[ソフトウェアダウンロード](#)」([登録ユーザ専用](#)) から、SSL VPN Client パッケージ (sslclient-win*.pkg) をダウンロードします。SVC

を ASA のフラッシュ メモリにコピーします。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。詳細は、『Cisco セキュリティ アプライアンス コマンドライン コンフィギュレーション ガイド、バージョン 7.2』の「[SVC ソフトウェアのインストール](#)」セクションを参照してください。

[使用するコンポーネント](#)

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ソフトウェア バージョン 7.2(2) を実行する Cisco 5500 シリーズ 適応型セキュリティ アプライアンス (ASA)
- Windows 1.1.4.179 用のバージョンの Cisco SSL VPN Client
- Windows 2000 Professional または Windows XP が稼働している PC
- Cisco Adaptive Security Device Manager (ASDM) バージョン 5.2(2)

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。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。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。

[表記法](#)

ドキュメント表記の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

[背景説明](#)

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

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

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

[設定](#)

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

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](#)) を使用してください。

[ネットワーク図](#)

このドキュメントでは、次のネットワーク構成を使用しています。

注: この設定で使用している IP アドレス スキームは、インターネット上で正式にルーティング可能なものではありません。これらは、ラボ環境で使用された [RFC 1918](#) のアドレスです。

[ASDM 5.2\(2\) を使用した ASA 7.2\(2\) の設定](#)

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: ASA を ASDM で設定できるようにするには、『[ASDM 用の HTTPS アクセスの許可](#)』を参照してください。

注: WebVPN と ASDM は、ポート番号を変更しない限り、同じ ASA インターフェイス上では有効にできません。詳細については、『[ASA の同じインターフェイスで有効になる ASDM および WebVPN](#)』を参照してください。

ASA 上で SSL VPN on a stick を設定するには、次の手順を実行します。

1. [Configuration] > [Interfaces] を選択し、[Enable traffic between two or more hosts connected to the same interface] チェックボックスをオンにして、SSL VPN トラフィックを同じインターフェイスで発着信できるようにします。
2. [Apply] をクリックします。注: 同等の CLI コンフィギュレーション コマンドを次に挙げます。
3. [Configuration] > [VPN] > [IP Address Management] > [IP Pools] > [Add] を選択し、IP アドレス プール *vpnpool* を作成します。
4. [Apply] をクリックします。注: 同等の CLI コンフィギュレーション コマンドを次に挙げます。
5. WebVPN をイネーブルにします。[Configuration] > [VPN] > [WebVPN] > [WebVPN Access] を選択し、外部インターフェイスを選択します。[Enable] をクリックします。[Enable Tunnel Group Drop-down List on WebVPN Login Page] チェックボックスをオンにして、ユーザがログイン ページからそれぞれのグループを選択できるようにします。[Apply] をクリックします。[Configuration] > [VPN] > [WebVPN] > [SSL VPN Client] > [Add] を選択し、SSL VPN のクライアント イメージを ASA のフラッシュ メモリから追加します。[OK] をクリックします。[OK] をクリックします。[SSL VPN Client] チェック ボックスをクリックします。注: 同等の CLI コンフィギュレーション コマンドを次に挙げます。
6. グループ ポリシーを設定します。[Configuration] > [VPN] > [General] > [Group Policy] > [Add (Internal Group Policy)] の順に選択し、内部グループ ポリシー *clientgroup* を作成します。[General] タブをクリックし、[WebVPN] チェックボックスをオンにし、トンネリング プロトコルとして WebVPN を有効にします。[Client Configuration] タブをクリックし、[General Client Parameters] タブをクリックします。[Split Tunnel Policy] ドロップ ダウン リストから [Tunnel All Networks] を選択し、リモート PC からのすべてのパケットが、セキュア トンネルを通過できるようにします。[WebVPN] > [SSLVPN Client] タブの順番にクリックして、次のオプションを選択します。[Use SSL VPN Client] オプションで、[Inherit] チェック ボックスをオフにし、[Optional] オプション ボタンをクリックします。このオプシ

ンを選択すると、リモートクライアントが SVC をダウンロードするかどうかを選択できるようになります。Always を選択すると、SSL VPN 接続のたびにリモートワークステーションに SVC がダウンロードされるようになります。[Keep Installer on Client System] オプションで、[Inherit] チェックボックスをオフにし、[Yes] オプション ボタンをクリックします。このオプションによって、SVC ソフトウェアはクライアントマシン上に留まります。これにより、ASA は接続が確立するたびに SVC ソフトウェアをクライアントにダウンロードする必要がなくなります。このオプションは、社内ネットワークに頻繁にアクセスするリモートユーザが選択するのに適しています。[Renegotiation Interval] オプションで、[Inherit] チェックボックスをオフにし、[Unlimited] チェックボックスをオフにし、キーの再生成が行われるまでの時間 (分) を入力します。注: セキュリティは、キーが有効である時間に制限を設けることで強化されます。[Renegotiation Method] オプションで、[Inherit] チェックボックスをオフにして、[SSL] オプション ボタンをクリックします。注: 再ネゴシエーションは、現在の SSL トンネルまたは再ネゴシエーション用に特に作成された新しいトンネルを使用できます。SSL VPN クライアントの属性は次の図で示すように設定することになります。[OK] をクリックして、[Apply] をクリックします。注: 同等の CLI コンフィギュレーション コマンドを次に挙げます。

7. [Configuration] > [VPN] > [General] > [Users] > [Add] を選択し、新しいユーザアカウント *ssluser1* を作成します。
8. [OK] をクリックして、[Apply] をクリックします。注: 同等の CLI コマンドは次のようになります。
9. [Configuration] > [Properties] > [AAA Setup] > [AAA Servers Groups] > [Edit] を選択します。
10. デフォルト サーバグループ *LOCAL* を選択し、[Edit] をクリックします。
11. [Edit LOCAL Server Group] ダイアログボックスで、[Enable Local User Lockout] チェックボックスをクリックし、[Maximum Attempts] テキスト ボックスに 16 と入力します。
12. [OK] をクリックします。注: 同等の CLI コマンドは次のようになります。
13. トンネルグループを設定します。[Configuration] > [VPN] > [General] > [Tunnel Group] > [Add (WebVPN アクセス)] の順に選択し、新しいトンネルグループ *sslgroup* を作成します。[General] タブをクリックし、[Basic] タブをクリックします。[Group Policy] ドロップダウン リストから *clientgroup* を選択します。[Client Address Assignment] タブをクリックし、次に [Add] をクリックして利用可能なアドレスプール *vpnpool* を割り当てます。[WebVPN] タブをクリックし、次に [Group Aliases and URLs] タブをクリックします。パラメータ ボックスにエイリアス名を入力し、[Add] をクリックして [Login] ページのグループ名のリストにエイリアス名を追加します。[OK] をクリックして、[Apply] をクリックします。注: 同等の CLI コンフィギュレーション コマンドを次に挙げます。
14. NAT の設定 : [Configuration] > [NAT] > [Add] > [Add Dynamic NAT Rule] を選択し、Inside ネットワークからのトラフィックが Outside IP アドレス 172.16.1.5 を使用して変換できるようにします。[OK] をクリックします。[Configuration] > [NAT] > [Add] > [Add Dynamic NAT Rule] を選択し、Outside ネットワーク 192.168.10.0 からのトラフィックが Outside IP アドレス 172.16.1.5 を使用して変換できるようにします。[OK] をクリックします。[Apply] をクリックします。注: 同等の CLI コンフィギュレーション コマンドを次に挙げます。

ASA 7.2(2) CLI の設定

Cisco ASA 7.2(2)

```
ciscoasa#show running-config
: Saved
```

```
:
ASA Version 7.2(2)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 10.77.241.142 255.255.255.192
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter
!--- and exit the same interface. access-list 100
extended permit icmp any any pager lines 24 mtu inside
1500 mtu outside 1500 ip local pool vpnpool
192.168.10.1-192.168.10.254

!--- The address pool for the SSL VPN Clients. no
failover icmp unreachable rate-limit 1 burst-size 1 asdm
image disk0:/asdm-522.bin no asdm history enable arp
timeout 14400 global (outside) 1 172.16.1.5

!--- The global address for Internet access used by VPN
Clients. !--- Note: Uses an RFC 1918 range for lab
setup. !--- Apply an address from your public range
provided by your ISP. nat (inside) 1 0.0.0.0 0.0.0.0

!--- The NAT statement to define what to encrypt !---
(the addresses from vpn-pool). nat (outside) 1
192.168.10.0 255.255.255.0

access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
```

```
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:0
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:
timeout uauth 0:05:00 absolute
group-policy clientgroup internal

!--- Create an internal group policy "clientgroup."
group-policy clientgroup attributes
  vpn-tunnel-protocol webvpn

!--- Enable webvpn as tunneling protocol. split-tunnel-
policy tunnelall

!--- Encrypt all the traffic coming from the SSL VPN
Clients. webvpn
  svc required

!--- Activate the SVC under webvpn mode svc keep-
installer installed

!--- When the security appliance and the SVC perform a
rekey, they renegotiate !--- the crypto keys and
initialization vectors, increasing the security of !---
the connection. svc rekey time 30

--- Command that specifies the number of minutes from
the start of the !--- session until the rekey takes
place, from 1 to 10080 (1 week). svc rekey method ssl

!--- Command that specifies that SSL renegotiation takes
place during SVC rekey. username ssluser1 password
ZRhW85jZqEaVd5P. encrypted

!--- Create an user account "ssluser1." aaa local
authentication attempts max-fail 16

!--- Enable the AAA local authentication. http server
enable http 0.0.0.0 0.0.0.0 inside no snmp-server
location no snmp-server contact snmp-server enable traps
snmp authentication linkup linkdown coldstart tunnel-
group sslgroup type webvpn

!--- Create a tunnel group "sslgroup" with type as
WebVPN. tunnel-group sslgroup general-attributes
  address-pool vpnpool

!--- Associate the address pool vpnpool created.
default-group-policy clientgroup

!--- Associate the group policy "clientgroup" created.
tunnel-group sslgroup webvpn-attributes

group-alias sslgroup_users enable

!--- Configure the group alias as sslgroup-users. telnet
timeout 5 ssh timeout 5 console timeout 0 ! class-map
inspection_default match default-inspection-traffic ! !
policy-map type inspect dns preset_dns_map parameters
message-length maximum 512 policy-map global_policy
class inspection_default inspect dns preset_dns_map
inspect ftp inspect h323 h225 inspect h323 ras inspect
netbios inspect rsh inspect rtsp inspect skinny inspect
esmtip inspect sqlnet inspect sunrpc inspect tftp inspect
```

```
sip inspect xdmcp ! service-policy global_policy global
webvpn
  enable outside

!--- Enable WebVPN on the outside interface. svc image
disk0:/sslclient-win-1.1.4.179.pkg 1

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

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

!--- Enable the display of the tunnel-group list on the
WebVPN Login page. prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
ciscoasa#
```

SVC との SSL VPN 接続の確立

次の手順を実行して、ASA との SSL VPN 接続を確立します。

1. Web ブラウザのアドレス フィールドに、ASA の WebVPN インターフェイスの URL または IP アドレスを入力します。次に、例を示します。

```
ciscoasa#show running-config
: Saved
:
ASA Version 7.2(2)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
  nameif inside
  security-level 100
  ip address 10.77.241.142 255.255.255.192
!
interface Ethernet0/1
  nameif outside
  security-level 0
  ip address 172.16.1.1 255.255.255.0
!
interface Ethernet0/2
  shutdown
  no nameif
  no security-level
  no ip address
!
interface Ethernet0/3
  shutdown
  no nameif
  no security-level
  no ip address
!
interface Management0/0
  shutdown
  no nameif
  no security-level
  no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
```

```

ftp mode passive
same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter !--- and exit the same interface.
access-list 100 extended permit icmp any any pager lines 24 mtu inside 1500 mtu outside
1500 ip local pool vpnpool 192.168.10.1-192.168.10.254

!--- The address pool for the SSL VPN Clients. no failover icmp unreachable rate-limit 1
burst-size 1 asdm image disk0:/asdm-522.bin no asdm history enable arp timeout 14400 global
(outside) 1 172.16.1.5

!--- The global address for Internet access used by VPN Clients. !--- Note: Uses an RFC
1918 range for lab setup. !--- Apply an address from your public range provided by your
ISP. nat (inside) 1 0.0.0.0 0.0.0.0

!--- The NAT statement to define what to encrypt !--- (the addresses from vpn-pool). nat
(outside) 1 192.168.10.0 255.255.255.0

access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:0
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:
timeout uauth 0:05:00 absolute
group-policy clientgroup internal

!--- Create an internal group policy "clientgroup." group-policy clientgroup attributes
vpn-tunnel-protocol webvpn

!--- Enable webvpn as tunneling protocol. split-tunnel-policy tunnelall

!--- Encrypt all the traffic coming from the SSL VPN Clients. webvpn
svc required

!--- Activate the SVC under webvpn mode svc keep-installer installed

!--- When the security appliance and the SVC perform a rekey, they renegotiate !--- the
crypto keys and initialization vectors, increasing the security of !--- the connection. svc
rekey time 30

--- Command that specifies the number of minutes from the start of the !--- session until
the rekey takes place, from 1 to 10080 (1 week). svc rekey method ssl

!--- Command that specifies that SSL renegotiation takes place during SVC rekey. username
ssluser1 password ZRhW85jZqEaVd5P. encrypted

!--- Create an user account "ssluser1." aaa local authentication attempts max-fail 16

!--- Enable the AAA local authentication. http server enable http 0.0.0.0 0.0.0.0 inside no
snmp-server location no snmp-server contact snmp-server enable traps snmp authentication
linkup linkdown coldstart tunnel-group sslgroup type webvpn

!--- Create a tunnel group "sslgroup" with type as WebVPN. tunnel-group sslgroup general-
attributes
address-pool vpnpool

!--- Associate the address pool vpnpool created. default-group-policy clientgroup

!--- Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-
attributes

group-alias sslgroup_users enable

```



```
!--- Configure the group alias as sslgroup-users. telnet timeout 5 ssh timeout 5 console
timeout 0 ! class-map inspection_default match default-inspection-traffic !! policy-map
type inspect dns preset_dns_map parameters message-length maximum 512 policy-map
global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323
h225 inspect h323 ras inspect netbios inspect rsh inspect rtsp inspect skinny inspect esmtp
inspect sqlnet inspect sunrpc inspect tftp inspect sip inspect xdmcp ! service-policy
global_policy global webvpn
enable outside
```

```
!--- Enable WebVPN on the outside interface. svc image disk0:/sslclient-win-1.1.4.179.pkg 1
```

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

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

```
!--- Enable the display of the tunnel-group list on the WebVPN Login page. prompt hostname
context Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end ciscoasa#
```

2. ユーザ名とパスワードを入力し、[Group] ドロップダウン リストからそれぞれのグループを選択します。注: SSL VPN クライアントをダウンロードする前に ActiveX ソフトウェアをコンピュータにインストールしておく必要があります。接続が確立されると、このダイアログボックスが表示されます。接続が確立されると、このメッセージが表示されます。
3. 接続が確立されたら、コンピュータのタスクバーに表示される黄色い鍵アイコンをダブルクリックします。[Cisco Systems SSL VPN Client] ダイアログボックスに、SSL 接続についての情報が表示されます。

確認

このセクションでは、設定が正常に機能していることを確認します。

[Output Interpreter Tool](#) (OIT) ([登録ユーザ専用](#)) では、特定の **show** コマンドがサポートされています。OIT を使用して、**show** コマンド出力の解析を表示できます。

- **show webvpn svc** : ASA フラッシュ メモリに格納された SVC イメージを表示します。

```
ciscoasa#show webvpn svc
1. disk0:/sslclient-win-1.1.4.179.pkg 1
   CISCO STC win2k+ 1.0.0
   1,1,4,179
   Fri 01/18/2008 15:19:49.43

1 SSL VPN Client(s) installed
```

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

```
ciscoasa#show vpn-sessiondb svc

Session Type: SVC

Username      : ssluser1
Index         : 1
Assigned IP   : 192.168.10.1      Public IP    : 192.168.1.1
Protocol      : SVC              Encryption   : 3DES
Hashing       : SHA1
Bytes Tx      : 131813         Bytes Rx     : 5082
Client Type   : Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Client Ver    : Cisco Systems SSL VPN Client 1, 1, 4, 179
Group Policy  : clientgroup
Tunnel Group  : sslgroup
```

```
Login Time   : 12:38:47 UTC Mon Mar 17 2008
Duration    : 0h:00m:53s
Filter Name :
```

- **show webvpn group-alias** : さまざまなグループに対する設定済みのエイリアスを表示します

```
o
ciscoasa#show webvpn group-alias
Tunnel Group: sslgroup   Group Alias: sslgroup_users enabled
```

- ASDM で、[Monitoring] > [VPN] > [VPN Statistics] > [Sessions] を選択すると、ASA の現在の WebVPN セッションに関する情報が表示されます。

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

- **vpn-sessiondb logoff name <username>** : 特定のユーザ名の SSL VPN セッションをログオフします。

```
ciscoasa#vpn-sessiondb logoff name ssluser1
Called vpn_remove_uauth: success!
webvpn_svc_np_tear_down: no ACL
INFO: Number of sessions with name "ssluser1" logged off : 1
```

同様に、**vpn-sessiondb logoff svc** コマンドを使用すると、すべての SVC セッションを終了できます。注: PC がスタンバイ モードまたは休止状態モードになった場合、SSL VPN 接続を終了することができます。

```
webvpn_rx_data_cstp
webvpn_rx_data_cstp: got message
SVC message: t/s=5/16: Client PC is going into suspend mode (Sleep, Hibernate, etc)
Called vpn_remove_uauth: success!
webvpn_svc_np_tear_down: no ACL
```

```
ciscoasa#show vpn-sessiondb svc
INFO: There are presently no active sessions
```

- **Debug webvpn svc <1-255>** : セッションを確立するために、リアルタイムの WebVPN イベントを提供します。

```
Ciscoasa#debug webvpn svc 7

ATTR_CISCO_AV_PAIR: got SVC ACL: -1
webvpn_rx_data_tunnel_connect
CSTP state = HEADER_PROCESSING
http_parse_cstp_method()
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field()
...input: 'Host: 172.16.1.1'
Processing CSTP header line: 'Host: 172.16.1.1'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: Cisco Systems SSL VPN Client 1, 1, 4, 179'
Processing CSTP header line: 'User-Agent: Cisco Systems SSL VPN Client 1, 1, 4, 179'
Setting user-agent to: 'Cisco Systems SSL VPN Client 1, 1, 4, 179'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Version: 1'
Processing CSTP header line: 'X-CSTP-Version: 1'
```

```
Setting version to '1'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Hostname: tacweb'
Processing CSTP header line: 'X-CSTP-Hostname: tacweb'
Setting hostname to: 'tacweb'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Accept-Encoding: deflate;q=1.0'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: deflate;q=1.0'
webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486
D5BC554D2'
Processing CSTP header line: 'Cookie: webvpn=16885952@10@1205757506@D4886D33FBF1
CF236DB5E8BE70B1486D5BC554D2'
Found WebVPN cookie: 'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1
486D5BC554D2'
WebVPN Cookie: 'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486D5B
C554D2'
Validating address: 0.0.0.0
CSTP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 192.168.10.1/0.0.0.0
CSTP state = HAVE_ADDRESS
No subnetmask... must calculate it
SVC: NP setup
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
SVC ACL ID: -1
vpn_put_uauth success!
SVC: adding to sessmgmt
SVC: Sending response
CSTP state = CONNECTED
```

- ASDM で、[Monitoring] > [Logging] > [Real-time Log Viewer] > [View] を選択してリアルタイム イベントを表示します。次に、ASA 172.16.1.5 経由のインターネットにおける、SVC 192.168.10.1 と Webserver 10.2.2.2 の間のセッション情報の例を示します。

[関連情報](#)

- [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 ページ](#)
- [公衆インターネット VPN on a Stick のための PIX/ASA 7.x および VPN クライアント間の設定例](#)
- [ASDM を使用した ASA での SSL VPN Client \(SVC \) の設定例](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)