## ASA 9.XでのAnyConnect VPNクライアントUタ ーンのトラフィックの設定

## 内容

概要 前提条件 要件 使用するコンポーネント 背景説明 Uターン型リモートアクセストラフィックの設定 公衆インターネット VPN on a Stick のための AnyConnect VPN Client の設定例 ネットワーク図 ASDM リリース 7.1(6) での ASA リリース 9.1(2) の設定 CLIの ASA リリース 9.1(2) の設定 TunnelAll 設定の実施による AnyConnect VPN Client 間の通信の許可 ネットワーク図 ASDM リリース 7.1(6) での ASA リリース 9.1(2) の設定 CLIの ASA リリース 9.1(2) の設定 スプリットトンネルを使用した AnyConnect VPN Client 間の通信 ネットワーク図 ASDM リリース 7.1(6) での ASA リリース 9.1(2) の設定 CLIのASA リリース 9.1(2)の設定 確認 トラブルシュート 関連情報

### 概要

このドキュメントでは、Cisco適応型セキュリティアプライアンス(ASA)リリース9.Xをセットア ップして、VPNトラフィックをUターンできるようにする方法について説明します。次の設定シ ナリオについて説明します。リモートアクセスクライアントからのUターンのトラフィック。

注: ネットワークでの IP アドレスのオーバーラップを避けるために、IP アドレスの完全に 異なるプールを VPN Client に割り当ててください(たとえば、10.x.x.x、172.16.x.x および 192.168.x.x)。 このIPアドレス方式は、ネットワークのトラブルシューティングに役立ち ます。

### ヘアピンまたはUターン

この機能は、あるインターフェイスに着信した後に同じインターフェイスからルーティングされ る VPN トラフィックに対して便利な機能です。たとえば、ハブ アンド スポークの VPN ネット ワークを構築していて、セキュリティ アプライアンスがハブであり、リモート VPN ネットワー クがスポークであるとします。あるスポークが他のスポークと通信するためには、トラフィック がセキュリティ アプライアンスに着信した後、他のスポーク宛てに再び発信される必要がありま す。

次を入力します。 same-security-traffic コマンドを発行して、トラフィックが同じインターフェイス で発着信できるようにします。

ciscoasa(config)#same-security-traffic permit intra-interface

## 前提条件

### 要件

この設定を行う前に、以下の要件を満たしていることを確認してください。

- ハブ ASA セキュリティ アプライアンスはリリース 9.x を稼働する必要があります。
- Cisco AnyConnect VPN Client 3.x注: AnyConnect VPN Clientパッケージ(anyconnect-win\*.pkg)か らダウンロードできます(登録ユーザ専用)。 AnyConnect VPNクライアントをCisco ASAフラ ッシュメモリにコピーします。このフラッシュメモリは、ASAとのSSL VPN接続を確立する ためにリモートユーザコンピュータにダウンロードされます。詳細については、ASAコンフ ィギュレーションガイドの「AnyConnect VPNクライアント接続」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いています。

- ソフトウェア バージョン 9.1(2) が稼働している Cisco 5500 シリーズ ASA
- Windows 3.1.05152 用のバージョンの Cisco AnyConnect SSL VPN Client
- ・「<u>サポートされているVPNプラットフォーム、Cisco ASAシリーズ</u>」に従ってサポートされ ているOSが稼働するPC。
- Cisco Adaptive Security Device Manager (ASDM) バージョン 7.1(6)

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 。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく ださい。

## 背景説明

Cisco AnyConnect VPN Client は、リモート ユーザのためにセキュリティ アプライアンスへのセキュアな SSL 接続を提供しています。以前にインストールしたクライアントがない場合、リモート ユーザは SSL VPN 接続を受け入れるように設定したインターフェイスのブラウザに IP アドレスを入力します。セキュリティアプライアンスがリダイレクトするように設定されていない場合 http:// 要求 https://ユーザは次の形式でURLを入力する必要があります。 https://

.URL が入力されると、ブラウザはそのインターフェイスに接続し、ログイン画面が表示されます 。ユーザがログインと認証を満たし、セキュリティアプライアンスがそのユーザをクライアント が必要であると識別した場合、セキュリティアプライアンスはリモートコンピュータのオペレー ティングシステムに一致するクライアントをダウンロードします。ダウンロード後、クライアン トは自身をインストールして設定し、セキュアな SSL 接続を確立して、接続が終了したときに自 身を残すか、アンインストールします(これは、セキュリティ アプライアンスの設定に従います )。以前にインストールされているクライアントの場合、ユーザが認証を行うと、セキュリティ アプライアンスはクライアントのリビジョンを調査して、必要に応じてクライアントをアップグ レードします。クライアントがセキュリティ アプライアンスとの SSL VPN 接続をネゴシエート する場合は、Transport Layer Security (TLS) や Datagram Transport Layer Security (DTLS)を 使用して接続します。DTLS により、一部の SSL 接続で発生する遅延および帯域幅の問題が回避 され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上 します。AnyConnect クライアントは、セキュリティ アプライアンスからダウンロードすること も、システム管理者がリモートの PC に手動でインストールすることもできます。クライアント を手動でインストールする方法の詳細については、『Cisco AnyConnectセキュアモビリティクラ イアント管理者ガイド』を参照してください。セキュリティ アプライアンスは、接続を確立する ユーザのグループポリシーまたはユーザ名属性に基づいてクライアントをダウンロードします。 セキュリティ アプライアンスは、クライアントを自動的にダウンロードするように設定すること も、クライアントをダウンロードするかどうかをユーザにプロンプトで表示してから設定するこ ともできます。後者の場合、ユーザが応答しないときには、タイムアウト期間が経過した後にク ライアントをダウンロードするか、ログイン ページを表示するか、いずれかを実行するようにセ キュリティアプライアンスを設定できます。注:このドキュメントで使用されている例では、 IPv4を使用しています。IPv6 Uターンのトラフィックの場合、手順は同じですが、IPv4の代わり

にIPv6アドレスを使用します。**Uターン型リモートアクセストラフィックの** 設定このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提 供しています。注:このセクションで使用されているコマンドの詳細を調べるには、<u>コマンドリ</u> <u>ファレンス</u>ガイドを使用してください。公衆インターネット VPN on a Stick のための AnyConnect VPN Client の設定例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 セットアップを使用します。



ASDM リリース 7.1(6) での ASA リリース 9.1(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完了し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、『<u>管理アクセスの設定</u>』を参照してください。注 : リリース 8.0(2) 以降、ASA はクライアントレス SSL VPN (WebVPN) セッションと ASDM 管 理セッションを外部インターフェイスのポート 443 で同時にサポートします。8.0(2) 以前のバー ジョンでは、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 上で有効にはできません。詳細は、『<u>ASAの同じインターフェイスでイネーブルになるASDMと</u> 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. 選択 Configuration > Device Setup > Interfaces および Enable traffic between two or more hosts connected to the same interface SSL VPNトラフィックが同じインターフェイスで発着信できるようにするに

Interface	Name	State	Security	IP Address	Subnet Mask Prefix Length	Group	Туре	Add 👻
inabitEthemet0/0	outside	Enabled		172 16 1 1	255,255,255,0		Hardware	Edit
igabitEthernet0/1	inside	Enabled	100	10.77.241.142	255,255,255,192		Hardware	100-00
igabitEthernet0/2		Disabled					Hardware	Delete
igabitEthernet0/3		Disabled					Hardware	
anagement0/0	mgmt	Disabled	D				Hardware/Ma	
	m						Þ	
Enable traffic between	nt n two or more inte	efaces which a	are configure	d with same security	levels		Þ	

### 同等の CLI 設定

ciscoasa(config)#**same-security-traffic permit intra-interface** 

2. 選択 Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools > Add IPアドレスプールを作成するため vpnpool.

Name:	vpnpool	
Starting IP Address:	192.168.10.1	
Ending IP Address:	192.168.10.254	
Subnet Mask:	255.255.255.0	

3. クリック Apply. **同等の CLI 設定** 

ciscoasa(config)#ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0

4. WebVPN をイネーブルにします。 選択 Configuration > Remote Access VPN > Network (Client) Access >

SSL VPN Connection Profiles 以下 Access Interfaces チェックボックスをクリックします Allow Access と Enable DTLS 設定します。また、 Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below 外部インターフェイスでSSL VPNを有効にするには、このチェックボックス をオンにします。

The security ap administrative r options. Cess Interfaces Denable Osc SSL access mus	plance automatically dep ights. The Cisco AnyCon o AnyConnect VPN Client t be enabled if you allow	loys the Claco AnyCon nect VPN Client support t access on the interfac AnyConnect client to b	nect VPN Client to remot is IPsec (IKEv2) tunnel a es selected in the table t e launched from a brows	e users upon connection. The initia s well as SSL tunnel with Datagram pelow per (Web Launch) .	l dient deployment requires end-user Transport Layer Security (DTLS) tunnelin
access mas					
	SSL Access		IPsec (IKEv2) Acco	355	
Interface	SSL Access Allow Access	Enable DTLS	IPsec (IKEv2) Acco Allow Access	Enable Client Services	Device Certificate
Interface outside	SSL Access Allow Access	Enable DTLS	IPsec (IKEv2) Acco Allow Access	Enable Client Services	Device Certificate

クリック Apply.選択 Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Client Software > Add Cisco AnyConnect VPNクライアントイメージをASAのフラッシュメモリから 次のように追加します。

ocal File Path:	C:\Users\josemed\Desktop\anyconnect-win-3.1.05152-k9.pkg	Browse Local Files
lash File System Path:	disk0:/anyconnect-win-3.1.05152-k9.pkg	Browse Flash
	epieda i lie eleve	
Add AnyConne	ct Client Image	×
Add AnyConne AnyConnect Image	ct Client Image : anyconnect-win-3.1.05152-k9.pkg	Browse Flash
Add AnyConne	ct Client Image : anyconnect-win-3.1.05152-k9.pkg	Browse Flash Upload

### 同等の CLI 設定

ciscoasa(config)#**webvpn** 

ciscoasa(config-webvpn)#**enable outside** 

ciscoasa(config-webvpn)#anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1
ciscoasa(config-webvpn)#tunnel-group-list enable
ciscoasa(config-webvpn)#anyconnect enable

5. グループ ポリシーを設定します。 選択 Configuration > Remote Access VPN > Network (Client) Access > Group Policies 内部グループポリシーを作成するため clientgroup. 下 General タブで、 SSL VPN Client トンネルプロトコルとしてWebVPNを有効にするには、このチェックボックスをオンにします。

stera	fare:	ntgroup	
dvanced	Barner:	Intext	
	SCEP forwarding URL	Ines:	
	Activess Pools	Intest	Ereck
	3Pv6 Address Pools	Intex	 Seet

内 Advanced > Split Tunneling タブ、選択 Tunnel All Networks 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するように、ポリシーの[Policy]ドロップダウンリストから設定し ます。

Add Internal Group Policy	a las Mais Mais Ma	
General Servers Edit Tennetis Broken Youty Hi AnyConnect Clarit Hi Paue/2021/1 Clarit	The VEN diest makes split humaing decisions on the basis of a network list that can be specified below by providing the proper parameters to Policy' and Wetwork list fields. UNS Names: Inf Infent. Policy: Infent. Network list: Infent.	 ngk

### 同等の CLI 設定

ciscoasa(config)#group-policy clientgroup internal ciscoasa(config)#group-policyclientgroup attributes ciscoasa(config-group-policy)#vpn-tunnel-protocol ssl-client ciscoasa(config-group-policy)#split-tunnel-policy tunnelall

6. 選択 Configuration > Remote Access VPN > AAA/Local Users > Local Users > Add 新しいユーザアカウント を作成するため ssluser1.クリック OK それから Apply.

Add User Account	and a second
(B-VEN Policy	Usermane:       external         Descenard:       ************************************

### 同等の CLI 設定

ciscoasa(config)#username ssluser1 password asdmASA@

7. トンネル グループを設定します。 選択 Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Connection Profiles > Add 新しいトンネルグループを作成するため sslgroup.内 Basic タ ブをクリックすると、次に示すように設定のリストを実行できます。 トンネルグループに 次の名前を付けます。 sslgroup.通常の Client Address Assignment アドレスプールを選択します。 vpnpool Client Address Pools 選択します。通常の Default Group Policyグループポリシーを選択しま す clientgroup Group Policy 選択します。

Basic	Name: s	slgroup	
Advanced	Aliases:		
	Authentication		
	Method:	🛛 🗛 💮 Certificate 💮 Both	
	AAA Server Group:	ocal 🔹	Manage
	E	Use LOCAL if Server Group fails	
	Client Address Assignment		
	DHCP Servers:		
		None 💿 DHCP Link 💿 DHCP Subnet	
	Client Address Pools:	pnpool	Select
	Client IPv6 Address Pools:		Select
	IP	v6 address pool is only supported for SSL.	
	Default Group Policy		8
	Group Policy:	lientgroup	Manage
	(Following field is an attribute	of the group policy selected above.)	

# 下 Advanced > Group Alias/Group URL タブをクリックし、グループエイリアス名を sslgroup\_users をクリックし、 OK. **同等の CLI 設定**

ciscoasa(config)#tunnel-group sslgroup type remote-access ciscoasa(config)#tunnel-group sslgroup general-attributes ciscoasa(config-tunnel-general)#address-pool vpnpool ciscoasa(config-tunnel-general)#default-group-policy clientgroup ciscoasa(config-tunnel-general)#exit ciscoasa(config)#tunnel-general)#exit ciscoasa(config)#tunnel-group sslgroup webvpn-attributes ciscoasa(config-tunnel-webvpn)#group-alias sslgroup\_users enable

8. NAT の設定 選択 Configuration > Firewall > NAT Rules > Add "Network Object" NAT Rule そのため、内部 ネットワークからのトラフィックは外部IPアドレス172.16.1.1で変換できます。

	🗣 Add - 🖉 Edit 👔 Delete 🛧 🖨 👗 - Q. Fr	🗣 Add 🗸 📝 Edit 👔 Delete 🗇 🗲 👗 📴 🏬 - 🔍 Find 🖽 Diagram 🥂 Paduet Trace					
172.31.245.74:8443	Add NAT Rule Before "Network Object" NAT Rules		Action: Transle	sted Packet			
localhost:55000	Add "Network Object" NAT Rule	Service	Source	Destination	Service		
	Add half Rule After Meoron Object half Rules	sany 🔅	Original (5)	Original	Original		
al 0.0	insert After	🌍 any	Original (5)	Original	Original		
' AAA Rules ' Filter Rules   Public Servers ' URU Filtering Servers							
Threat Detection Botnet Traffic Filter Objects							
Threat Detection Dotnet Traffic Filter Objects Unified Communications Advanced							

ame.	obj-inside	
уре:	Network	•
Address:	10.77.241.128	
etmask:	255.255.255.192	-
escription:		
NAT		۲
NAT Add Auto Type:	matic Address Translation Rules	۲
NAT Add Auto Type: Translated	matic Address Translation Rules Dynamic + Addr: outside	*

Firewall > NAT Rules > Add "Network Object" NAT Rule そのため、外部ネットワークからのVPNトラフィックに対するトラフィックは、外部IPアドレス172.16.1.1で変換できます。

🛓 Edit Networ	k Object
Name:	obj-AnyconnectPool
Туре:	Network
IP Address:	192.168.10.0
Netmask:	255.255.255.0
Description:	
NAT Add Autor	matic Address Translation Rules
Туре:	Dynamic PAT (Hide) 👻
Translated	Addr: outside
	Advanced
	OK Cancel Help
coasa (config) # coasa (config-ne coasa (config-ne coasa (config) # coasa (config-ne coasa (config-ne coasa (config-ne <b>NSA UU—X 9</b> (config) #show 1	object network obj-inside etwork-object)# subnet 10.77.241.128 255.255.255.192 etwork-object)# nat (inside,outside) dynamic interface object network obj-AnyconnectPool etwork-object)# subnet 192.168.10.0 255.255.255.0 etwork-object)# nat (outside,outside) dynamic interface 0.1(2) の設定 running-config
ion 9.1(2)	
tion 9.1(2) ciscoasa	nain invalid
tion 9.1(2) ciscoasa ame default.dom assword 8Ry2Yj1	nain.invalid Tyt7RRXU24 encrypted
rion 9.1(2) • ciscoasa • ame default.dom • assword 8Ry2Yj1 • GigabitEtherr	nain.invalid Tyt7RRXU24 encrypted

!

- interface GigabitEthernet0/1 nameif inside
- security-level 100

ip address 10.77.241.142 255.255.255.192
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address

!

passwd 2KFQnbNIdI.2KYOU encrypted boot system disk0:/asa802-k8.bin ftp mode passive clock timezone IST 5 30 dns server-group DefaultDNS domain-name default.domain.invalid same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter and exit the same interface.

object network obj-AnyconnectPool subnet 192.168.10.0 255.255.255.0 object network obj-inside subnet 10.77.241.128 255.255.255.192

!--- Commands that define the network objects we will use later on the NAT section.

pager lines 24 logging enable logging asdm informational mtu inside 1500 mtu outside 1500 ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0

!--- The address pool for the Cisco AnyConnect SSL VPN Clients

no failover icmp unreachable rate-limit 1 burst-size 1 asdm image disk0:/asdm-602.bin no asdm history enable arp timeout 14400

*nat (inside,outside) source static obj-inside obj-inside destination static obj-AnyconnectPool obj-AnyconnectPool* 

*!--- The Manual NAT that prevents the inside network from getting translated when going to the Anyconnect Pool.* 

object network obj-AnyconnectPool nat (outside,outside) dynamic interface object network obj-inside nat (inside,outside) dynamic interface

!--- The Object NAT statements for Internet access used by inside users and Anyconnect Clients. !--- Note: Uses an RFC 1918 range for lab setup.

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 0:05:00 timeout sip 0:30:00 sip\_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute

dynamic-access-policy-record DfltAccessPolicy http server enable 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 no crypto isakmp nat-traversal telnet timeout 5 ssh timeout 5 console timeout 0 threat-detection basic-threat threat-detection statistics access-list 1 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

anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1

!--- Assign an order to the AnyConnect SSL VPN Client image

#### anyconnect 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

!--- Create an internal group policy "clientgroup"

group-policy clientgroup attributes
vpn-tunnel-protocol ssl-client

!--- Specify SSL as a permitted VPN tunneling protocol

split-tunnel-policy tunnelall

!--- Encrypt all the traffic from the SSL VPN Clients.

username ssluser1 password ZRhW85jZqEaVd5P. encrypted

!--- Create a user account "ssluser1"

tunnel-group sslgroup type remote-access

!--- Create a tunnel group "sslgroup" with type as remote access

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

prompt hostname context Cryptochecksum:af3c4bfc4ffc07414c4dfbd29c5262a9 : end ciscoasa(config)# TunnelAll 設定の実施による AnyConnect VPN Client 間の通信の許可ネットワーク図



AnyConnect Client 間の通信が必要で、公衆インターネット on a Stick 用の NAT が実施されてい る場合は、双方向通信を可能にするために手動 NAT も必要になります。これは、Anyconnectク ライアントが電話サービスを使用し、相互にコールできる必要がある場合の一般的なシナリオで す。ASDM リリース 7.1(6) での ASA リリース 9.1(2) の設定選択 Configuration > Firewall > NAT Rules > Add NAT Rule Before "Network Object" NAT Rules そのため、外部ネットワーク(Anyconnectプール)から送 信され、同じプールから別のAnyconnectクライアントに送信されるトラフィックは、外部IPアド レス172.16.1.1で変換されません。

File View Tools Wizards Wind	ow Help				
Home 🔏 Configuration 👩 Ma	nitoring 🔚 Save 🔇 Refresh 🔇 Back 🚫 Forward 🦻 He	P			
Device List 📅 🔍 🗡	Configuration > Firewall > NAT Rules				0
🌩 Add 📋 Delete 🚿 Connect	🗣 Acid 🗸 🗹 Edit 🗻 Delete 🎓 🗲 🗼 🛼 📖 - 🔍 Find	📴 Disgram 🕰	Packet Trace		
Find: Go	Add NAT Rule Before "Network Object" NAT Rules		Action: Transla	ted Packet	
	Add "Network Object" NAT Rule	Service	Source	Destination	Service
	Add NAT Rule After "Network Object" NAT Rules	any any	Original (S)	Original	Original
	👷 Insert	🏟 any	Original (S)	Original	Original
Firewall	🐺 Insert After	. 🏟 any	Original (S)	- Original	Original

Source Interface:	outside	Destination Interface:	outside	•
iource Address:	obj-AnyconnectPool		obj-AnyconnectPool	[
		Service:	any	
action: Translated	Packet			
iource NAT Type:	Static	•		
iource Address:	obj-AnyconnectPool [		obj-AnyconnectPool	
Fall through to	interface PAT	Service:	Original	
ptions				
🚺 Enable rule				
Translate DNS	replies that match this rule			
Direction: Both	•			
)accrimition (				

### 同等の CLI 設定

nat (outside, outside) source static obj-AnyconnectPool obj-AnyconnectPool destination static obj-AnyconnectPool obj-AnyconnectPool CLIのASA リリース 9.1(2)の設定 ciscoasa(config)#show running-config : Saved : ASA Version 9.1(2)

```
ASA Version 9.1(2)
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
1
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.77.241.142 255.255.255.192
!
interface Management0/0
shutdown
no nameif
no security-level
```

no ip address

passwd 2KFQnbNIdI.2KYOU encrypted boot system disk0:/asa802-k8.bin ftp mode passive clock timezone IST 5 30 dns server-group DefaultDNS domain-name default.domain.invalid same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter and exit the same interface.

object network obj-AnyconnectPool subnet 192.168.10.0 255.255.255.0 object network obj-inside subnet 10.77.241.128 255.255.255.192

!--- Commands that define the network objects we will use later on the NAT section.

pager lines 24 logging enable logging asdm informational mtu inside 1500 mtu outside 1500 ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0

!--- The address pool for the Cisco AnyConnect SSL VPN Clients

no failover icmp unreachable rate-limit 1 burst-size 1 asdm image disk0:/asdm-602.bin no asdm history enable arp timeout 14400

nat (inside,outside) source static obj-inside obj-inside destination static obj-AnyconnectPool obj-AnyconnectPool nat (outside,outside) source static obj-AnyconnectPool obj-AnyconnectPool destination static obj-AnyconnectPool obj-AnyconnectPool

!--- The Manual NAT statements used so that traffic from the inside network destined to the Anyconnect Pool and traffic from the Anyconnect Pool destined to another Client within the same pool does not get translated.

object network obj-AnyconnectPool nat (outside,outside) dynamic interface object network obj-inside nat (inside,outside) dynamic interface

!--- The Object NAT statements for Internet access used by inside users and Anyconnect Clients. !--- Note: Uses an RFC 1918 range for lab setup.

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 0:05:00
timeout sip 0:30:00 sip\_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
http server enable
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
no crypto isakmp nat-traversal
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
1
class-map inspection_default
match default-inspection-traffic
1
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
1
service-policy global_policy global
webvpn
enable outside
```

```
!--- Enable WebVPN on the outside interface
```

anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1

!--- Assign an order to the AnyConnect SSL VPN Client image

anyconnect 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

```
group-policy clientgroup internal
```

!--- Create an internal group policy "clientgroup"

group-policy clientgroup attributes
vpn-tunnel-protocol ssl-client

!--- Specify SSL as a permitted VPN tunneling protocol

split-tunnel-policy tunnelall

!--- Encrypt all the traffic from the SSL VPN Clients. username ssluser1 password ZRhW85jZqEaVd5P. encrypted

!--- Create a user account "ssluser1"

tunnel-group sslgroup type remote-access

!--- Create a tunnel group "sslgroup" with type as remote access

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

prompt hostname context Cryptochecksum:af3c4bfc4ffc07414c4dfbd29c5262a9 : end ciscoasa(config)# スプリットトンネルを使用した AnyConnect VPN Client 間の通信ネットワーク図



Anyconnectクライアント間の通信が必要で、スプリットトンネルが使用される場合。このトラフィックの設定に影響を与える NAT ルールがない限り、双方向通信を可能にするために手動 NAT を使用する必要はありません。ただし AnyConnect VPN Pool はスプリットトンネル ACL に含む 必要があります。これは、Anyconnectクライアントが電話サービスを使用し、相互にコールでき る必要がある場合の一般的なシナリオです。ASDM リリース 7.1(6) での ASA リリース 9.1(2) の 設定

1. 選択 Configuration > Remote Access VPN > Network (Client) Access > Address Assignment> Address Pools > Add IPアドレスプールを作成するため vpnpool.

Name:	vpnpool	
Starting IP Address:	192.168.10.1	
Ending IP Address:	192.168.10.254	
Subnet Mask:	255.255.255.0	•

- 2. クリック Apply. 同等の CLI 設定
- ciscoasa (config) #ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0 3. WebVPN をイネーブルにします。 選択 Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles 以下 Access Interfaces チェックボックスをクリックします Allow Access と Enable DTLS 設定します。また、 Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below 外部インターフェイスでSSL VPNを有効にするには、このチェックボックス をオンにします。

The security ap administrative r options. Cess Interfaces CEnable Osc SSL access mus	plance automatically dep ights. The Cisco AnyCon : o AnyConnect VPN Clien t be enabled if you allow	oloys the Cisco AnyCon nect VPN Client support t access on the interfac	es selected in the table t e launched from a brows	e users upon connection. The initial s well as SSL tunnel with Datagram below ser (Web Launch) .	l dient deployment requires end-user Transport Layer Security (DTLS) tunnelin
	SSI Arress		IPsec (IKEv2) Acco	855	
	2261100000				and the second se
Interface	Allow Access	Enable DTLS	Allow Access	Enable Client Services	Device Certificate
Interface outside	Allow Access	Enable DTLS	Allow Access	Enable Client Services	Device Certificate

クリック Apply.選択 Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Client Software > Add *Cisco AnyConnect VPNクライアントイメージをASAのフラッシュメモリから* 次のように追加します。

Jpload a file from local ( Please wait for the oper	computer to flash file system on the device. The upload process min ation to finish.	ght take a few minutes.
Local File Path:	C:\Users\josemed\Desktop\anyconnect-win-3.1.05152-k9.pkg	Browse Local Files
Flash File System Path:	disk0:/anyconnect-win-3.1.05152-k9.pkg	Browse Flash

AnyConnect Image:	anyconnect-win	Browse Flash		
				Upload
Regular expressi	ion to match u	ser-agent		*

### 同等の CLI 設定

ciscoasa(config)#webvpn ciscoasa(config-webvpn)#enable outside ciscoasa(config-webvpn)#anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1 ciscoasa(config-webvpn)#tunnel-group-list enable ciscoasa(config-webvpn)#anyconnect enable

4. グループ ポリシーを設定します。 選択 Configuration > Remote Access VPN > Network (Client) Access > Group Policies 内部グループポリシーを作成するため clientgroup. 下 General タブで、 SSL VPN Client チェックボックスをオンにして、WebVPNを許可されたトンネルプロトコルとして有効にします。

General	farm:	ntarsap	I	
Servera # Advanced	Barner:	inter:		
	SCEP forwarding URL)	Intex:		
	Activess Pools	Intest:	]	Stat.
	3PV6 Address Pools	ine:		Seet

内 Advanced > Split Tunneling タブ、選択 Tunnel Network List Below [Policy]ドロップダウンリストか ら選択して、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するようにし ます。

eral Social	The WW cleanting lesi sole training decisions	on the basis of a network list that, can be specified basis by a constructing the proper data ratios to Yoke's a tributeric test india.			
Browser Pronf Browser Pronf -> Ty Connect Client -Pseo(XEV1) Client	Ellovi Timme Nesacris List Below 🔄 🔹 👻				
	Network List: 🔄 Innert: 🔤 SPLID-ACL		- Manage		
	Pressing Unstance to set up split of using	n All Manager	.22		
	Set up Oplit Curley on by: Web Centerly	biordard Ac. Texteented as 1			
	Intercept DHCP Configuration Mes	P Add + ≝tolt ∰ twin + 4 & 8 % m -			
		No Address Action Securitytian			
		Image: State State         Image: State         Image: State<			

### 同等の CLI 設定

ciscoasa(config)#access-list SPLIt-ACL standard permit 10.77.241.0 255.255.255.0 ciscoasa(config)#access-list SPLIt-ACL standard permit 192.168.10.0 255.255.255.0

ciscoasa(config)#group-policy clientgroup internal ciscoasa(config)#group-policy clientgroup attributes ciscoasa(config-group-policy)#vpn-tunnel-protocol ssl-client ciscoasa(config-group-policy)#split-tunnel-policy tunnelspecified ciscoasa(config-group-policy)#split-tunnel-network-list SPLIt-ACL

5. 選択 Configuration > Remote Access VPN > AAA/Local Users > Local Users > Add 新しいユーザアカウント を作成するため ssluser1 クリック OK それから Apply

Add User Account		-
G - UPN Policy	Binstmane:       externel         Preservent       ************************************	

#### 同等の CLI 設定

ciscoasa(config)#username ssluser1 password asdmASA@

6. トンネル グループを設定します。 選択 Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Connection Profiles > Add 新しいトンネルグループを作成するため sslgroup.内 Basic タ ブをクリックすると、次に示すように設定のリストを実行できます。 トンネルグループに 次の名前を付けます。 sslgroup.通常の Client Address Assignment アドレスプールを選択します。 vpnpool Client Address Pools 選択します。通常の Default Group Policy グループポリシーを選択しま す clientgroup Group Policy 選択します。

Basic	Name:	ssigroup	
Advanced	Aliases:		
	Authentication		
	Method:	💿 AAA 💿 Certificate 💿 Both	
	AAA Server Group:	LOCAL 👻	Manage
		Use LOCAL if Server Group fails	
	Client Address Assignment -		2
	DHCP Servers:		
		None OHCP Link OHCP Subnet	
	Client Address Pools:	vpnpool	Select
	Client IPv6 Address Pools:		Select
		IPv6 address pool is only supported for SSL.	
	Default Group Policy		
	Group Policy:	clientgroup 🗸	Manage
	/Enlleyuing field is an attuin	the of the many college collected should V	

下 Advanced > Group Alias/Group URL タブをクリックし、グループエイリアス名を sslgroup\_users をクリックし、 OK. **同等の CLI 設定** 

ciscoasa(config)#tunnel-group sslgroup type remote-access ciscoasa(config)#tunnel-group sslgroup general-attributes ciscoasa(config-tunnel-general)#address-pool vpnpool ciscoasa(config-tunnel-general)#default-group-policy clientgroup ciscoasa(config-tunnel-general)#exit ciscoasa(config)#tunnel-group sslgroup webvpn-attributes ciscoasa(config-tunnel-webvpn)#group-alias sslgroup\_users enable

#### CLIのASA リリース 9.1(2)の設定 ciscoasa (config)#show running-config

```
: Saved
ASA Version 9.1(2)
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.77.241.142 255.255.255.192
interface Management0/0
shutdown
no nameif
no security-level
no ip address
```

boot system disk0:/asa802-k8.bin ftp mode passive clock timezone IST 5 30 dns server-group DefaultDNS domain-name default.domain.invalid same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter and exit the same interface.

object network obj-inside subnet 10.77.241.128 255.255.255.192

!--- Commands that define the network objects we will use later on the NAT section.

access-list SPLIt-ACL standard permit 10.77.241.0 255.255.255.0 access-list SPLIt-ACL standard permit 192.168.10.0 255.255.255.0

*!--- Standard Split-Tunnel ACL that determines the networks that should travel the Anyconnect tunnel.* 

pager lines 24 logging enable logging asdm informational mtu inside 1500 mtu outside 1500 ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0

!--- The address pool for the Cisco AnyConnect SSL VPN Clients

no failover icmp unreachable rate-limit 1 burst-size 1 asdm image disk0:/asdm-602.bin no asdm history enable arp timeout 14400

*nat (inside, outside) source static obj-inside obj-inside destination static obj-AnyconnectPool obj-AnyconnectPool* 

!--- The Manual NAT that prevents the inside network from getting translated when going to the Anyconnect Pool

object network obj-inside nat (inside,outside) dynamic interface

!--- The Object NAT statements for Internet access used by inside users.
!--- Note: Uses an RFC 1918 range for lab setup.

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 0:05:00 timeout sip 0:30:00 sip\_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute dynamic-access-policy-record DfltAccessPolicy http server enable 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 no crypto isakmp nat-traversal telnet timeout 5 ssh timeout 5 console timeout 0 threat-detection basic-threat

threat-detection statistics access-list 1 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

anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1

!--- Assign an order to the AnyConnect SSL VPN Client image

anyconnect 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

group-policy clientgroup internal

!--- Create an internal group policy "clientgroup"

group-policy clientgroup attributes
vpn-tunnel-protocol ssl-client

!--- Specify SSL as a permitted VPN tunneling protocol

!--- Encrypt only traffic specified on the split-tunnel ACL coming from the SSL VPN Clients.

split-tunnel-network-list value SPLIt-ACL

!--- Defines the previosly configured ACL to the split-tunnel policy.

username ssluser1 password ZRhW85jZqEaVd5P. encrypted

!--- Create a user account "ssluser1"

tunnel-group sslgroup type remote-access

!--- Create a tunnel group "sslgroup" with type as remote access

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

prompt hostname context
Cryptochecksum:af3c4bfc4ffc07414c4dfbd29c5262a9
: end
ciscoasa(config)#

### **確認**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。

• show vpn-sessiondb svc – 現在のSSL接続に関する情報を表示します。 ciscoasa#show vpn-sessiondb anyconnect

Session Type: SVC

Username : ssluser1 Index : 12 Assigned IP : 192.168.10.1 Public IP : 192.168.1.1 Protocol : Clientless SSL-Tunnel DTLS-Tunnel Encryption : RC4 AES128 Hashing : SHA1 Bytes Tx : 194118 Bytes Rx : 197448 Group Policy : clientgroup Tunnel Group : sslgroup Login Time : 17:12:23 IST Mon Mar 24 2008 Duration : 0h:12m:00s NAC Result : Unknown VLAN Mapping : N/A VLAN : none

- show webvpn group-alias さまざまなグループの設定済みエイリアスを表示します。 ciscoasa#show webvpn group-alias
  - Tunnel Group: **sslgroup** Group Alias: **sslgroup\_users enabled**
- ASDMで、 Monitoring > VPN > VPN Statistics > Sessions ASAの現在のセッションを確認します。

Device List 🕈 Add   îî Dele	급 무 × te 🚿 Connect	Monitoring > VPN >	VPN Statistics > Session
ind: 	Go 5.74:8443 55000	Туре	Active
VPN	ся s Ister Loads	Filter By: AnyConr	nect Client
Crypto Compre Encrypt Global I NAC Se Protoco VLAN M Clientless S VPN Conner	scatistics ession Statistics tion Statistics KE/IPsec Statistics ession Summary I Statistics lapping Sessions SL VPN ction Graphs	Username ssluser1 192.168.10.1	Connection Profile clientgroup sslgroup

## **ト ラブルシュート**ここでは、設定のトラブルシューティングに使用できる情報を示しま す。

 vpn-sessiondb logoff name - 特定のユーザ名のSSL VPNセッションをログオフするコマンド。 ciscoasa#vpn-sessiondb logoff name ssluser1
 Do you want to logoff the VPN session(s)? [confirm] Y
 INFO: Number of sessions with name "ssluser1" logged off : 1

ciscoasa#Called vpn\_remove\_uauth: success! webvpn\_svc\_np\_tear\_down: no ACL webvpn\_svc\_np\_tear\_down: no IPv6 ACL 同様に、 vpn-sessiondb logoff anyconnect すべてのAnyConnectセッションを終了します。

# • debug webvpn anyconnect <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 anyconnect 7

```
CSTP state = HEADER_PROCESSING
http_parse_cstp_method()
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field()
...input: 'Host: 10.198.16.132'
Processing CSTP header line: 'Host: 10.198.16.132'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: Cisco AnyConnect VPN Agent for Windows 3.1.05152'
Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Agent for Windows
3.1.05152'
Setting user-agent to: 'Cisco AnyConnect VPN Agent for Windows 3.1.05152'
webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60'
Processing CSTP header line: 'Cookie: webvpn=
146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60'
Found WebVPN cookie: 'webvpn=146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60'
WebVPN Cookie: 'webvpn=146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60'
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: WCRSJOW7Pnbc038'
Processing CSTP header line: 'X-CSTP-Hostname: WCRSJOW7Pnbc038'
Setting hostname to: 'WCRSJOW7Pnbc038'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-MTU: 1280'
Processing CSTP header line: 'X-CSTP-MTU: 1280'
webvpn_cstp_parse_request_field()
... input: 'X-CSTP-Address-Type: IPv6, IPv4'
Processing CSTP header line: 'X-CSTP-Address-Type: IPv6, IPv4'
webvpn_cstp_parse_request_field()
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Base-MTU: 1300'
Processing CSTP header line: 'X-CSTP-Base-MTU: 1300'
webvpn_cstp_parse_request_field()
webvpn_cstp_parse_request_field()
... input: 'X-CSTP-Full-IPv6-Capability: true'
Processing CSTP header line: 'X-CSTP-Full-IPv6-Capability: true'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Master-Secret: F1810A764A0646376F7D254202A0A602CF075972F91EAD1
9BB6BE387BB8C6F893BFB49886D47F9A4BE2EA2A030BF620D'
Processing CSTP header line: 'X-DTLS-Master-Secret: F1810A764A0646376F7D254202A0
A602CF075972F91EAD19BB6BE387BB8C6F893BFB49886D47F9A4BE2EA2A030BF620D'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA'
Processing CSTP header line: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3
-SHA:DES-CBC-SHA'
webvpn_cstp_parse_request_field()
... input: 'X-DTLS-Accept-Encoding: lzs'
Processing CSTL header line: 'X-DTLS-Accept-Encoding: lzs'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Header-Pad-Length: 0'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Accept-Encoding: lzs,deflate'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: lzs,deflate'
webvpn_cstp_parse_request_field()
```

...input: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.' Processing CSTP header line: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.' Validating address: 0.0.0.0 CSTP state = WAIT\_FOR\_ADDRESS webvpn\_cstp\_accept\_address: 192.168.10.1/255.255.255.0 webvpn\_cstp\_accept\_ipv6\_address: No IPv6 Address CSTP state = HAVE ADDRESS SVC: Sent gratuitous ARP for 192.168.10.1. SVC: NP setup np\_svc\_create\_session(0x5000, 0xa930a180, TRUE) webvpn\_svc\_np\_setup SVC ACL Name: NULL SVC ACL ID: -1 vpn\_put\_uauth success for ip 192.168.10.1! No SVC ACL Iphdr=20 base-mtu=1300 def-mtu=1500 conf-mtu=1406 tcp-mss = 1260path-mtu = 1260 (mss)mtu = 1260(path-mtu) - 0(opts) - 5(ssl) - 8(cstp) = 1247tls-mtu = 1247(mtu) - 20(mac) = 1227 DTLS Block size = 16 mtu = 1300(base-mtu) - 20(ip) - 8(udp) - 13(dtlshdr) - 16(dtlsiv) = 1243 mod-mtu = 1243(mtu) & 0xfff0(complement) = 1232 dtls-mtu = 1232(mod-mtu) - 1(cdtp) - 20(mac) - 1(pad) = 1210 computed tls-mtu=1227 dtls-mtu=1210 conf-mtu=1406 DTLS enabled for intf=2 (outside) tls-mtu=1227 dtls-mtu=1210 SVC: adding to sessmgmt Unable to initiate NAC, NAC might not be enabled or invalid policy CSTP state = CONNECTED webvpn\_rx\_data\_cstp webvpn\_rx\_data\_cstp: got internal message Unable to initiate NAC, NAC might not be enabled or invalid policy

• ASDMで、 Monitoring > Logging > Real-time Log Viewer > View リアルタイムのイベントを表示します 。次に、ASA 172.16.1.1 経由のインターネットにおける、AnyConnect 192.168.10.1 と Telnet Server 10.2.2.2 の間のセッション情報の例を示します。

Life lo	nic LUQ view	a Lielo					
þ. Ræun	· Rh Copy	Same Og ti	wer   😰 Celor S	erange i 🏥 Cons	w Rule 🎆 Show Ri	🖛 🖗 Show Details	bio
Hillan Bys	600 - 12 F			- Spritz	👯 suld nitor 📲 :	show All And:	0.
Tre	Syring ID	Source IP	Source Part	Destination IP	Destination Port	Description	
22:03:02	302013	292.368.31.1	6/050	30.2.2.2	60	Built rissond TCP come	ater 109 for outside 292, 568, 10, 1/8-1960 (172, 16, 1, 1/8-1960)(1/0/2-C)adaser () to conside 10, 2, 2, 2/80 (10, 2, 2, 2/80) (adaser ()
22/03/02	305011	:92.363.30.3	64059	\$72.35.1.1	64059	Built dynamic TCP trans	after from outsists: (52, 168, 10, 1/64039), OCAL (soluser () to outside: (72, 16, 1, 1/64039

## 関連情報

- <u>Cisco ASA 5500-Xシリーズファイアウォール</u>
- <u>公衆インターネット VPN on a Stick のための PIX/ASA および VPN Client の設定例</u>
- ASDM を使用した ASA での SSL VPN Client (SVC)の設定例
- ・ <u>テクニカル サポートとドキュメント Cisco Systems</u>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。